

ESP-DIRETORIA TEC. INFORMACAO E COMUNICACAO

Edital 70/2025

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
70/2025	180183-ESP-DIRETORIA TEC. INFORMACAO E COMUNICACAO	SERGIO FIRMINO DA SILVA NETO	25/05/2026 15:42 (v 0.16)
Status	ASSINADO		

Outras informações

Categoria	Número da Contratação	Processo Administrativo
V - prestação de serviços, inclusive os técnico-profissionais especializados/Serviço continuado com dedicação exclusiva de mão de obra		057.00495038/2025-41

1. Minuta de Edital

PREGÃO ELETRÔNICO

90041/2025

CONTRATANTE (UASG)

180183 - Diretoria de Tecnologia da Informação e Comunicação

OBJETO

Serviços de Gerenciamento de Cibersegurança e Infraestrutura de Tecnologia da Informação e Comunicação (TIC) presencial com Setor Operacional, NOC e SOC.

VALOR TOTAL DA CONTRATAÇÃO

Sigiloso

DATA DA SESSÃO PÚBLICA

Dia 11/06/2026 às 09h30 (horário de Brasília)

CRITÉRIO DE JULGAMENTO:

Menor preço

MODO DE DISPUTA:

Aberto

PREFERÊNCIA ME/EPP/EQUIPARADAS

NÃO

Sumário

1.	DO OBJETO	3
2.	DO REGISTRO DE PREÇOS	3
3.	DA PARTICIPAÇÃO NA LICITAÇÃO	4
4.	DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO	6
5.	DO PREENCHIMENTO DA PROPOSTA	7
6.	DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES	9
7.	DA FASE DE JULGAMENTO	13
8.	DA FASE DE HABILITAÇÃO	17
9.	DA ATA DE REGISTRO DE PREÇOS	19
10.	DA FORMAÇÃO DO CADASTRO DE RESERVA	20
11.	DOS RECURSOS	21
12.	DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES	21
13.	DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO	25
14.	DAS DISPOSIÇÕES GERAIS	25

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - DTIC

PREGÃO ELETRÔNICO Nº 90041/2025

Processo Administrativo nº 057.00495038/2025-41

Torna-se público que a Polícia Militar do Estado de São Paulo, por meio da Diretoria de Tecnologia da Informação e Comunicação - DTIC, sediada na Avenida Cruzeiro do Sul, 260 – 6º Andar – Canindé – São Paulo /SP – CEP: 03033-020, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 1º de abril de 2021, do Decreto estadual nº 67.608, de 27 de março de 2023, da Instrução Normativa SEGES/ME nº 73, de 30 de setembro de 2022, e demais normas da legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital e em seus Anexos, observando-se as subdivisões subsequentes na forma de itens que compõem este instrumento.

1.	DO OBJETO	
----	-----------	--

1.1. O objeto da presente licitação é Serviços de Gerenciamento de Cibersegurança e Infraestrutura de Tecnologia da Informação e Comunicação (TIC) presencial com Setor Operacional, NOC e SOC, conforme condições, quantidades e exigências estabelecidas neste Edital e seus Anexos.

1.2. A licitação será realizada em único item.

2. DO REGISTRO DE PREÇOS

2.1. A disciplina deste item 2 não se aplica no presente procedimento, por não se tratar de licitação para registro de preços.

3. DA PARTICIPAÇÃO NA LICITAÇÃO

3.1. Poderão participar deste Pregão os interessados que atuarem em atividade compatível com o objeto da licitação e que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - Sicaf e no Sistema de Compras do Governo Federal (www.gov.br/compras).

3.1.1. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o 3º (terceiro) dia útil anterior à data prevista para recebimento das propostas.

3.1.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluindo a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

3.2. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados na subdivisão anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

3.3. A não observância do disposto na subdivisão anterior poderá ensejar desclassificação no momento da habilitação.

3.4. Nos limites previstos no art. 4º da Lei nº 14.133, de 2021, e na Lei Complementar nº 123, de 14 de dezembro de 2006, serão observadas, caso aplicáveis, as regras de tratamento favorecido para as microempresas e empresas de pequeno porte, bem como para as cooperativas que atendam ao disposto no art. 34 da Lei nº 11.488, de 15 de junho de 2007, e no art. 16 da Lei nº 14.133, de 2021, para o agricultor familiar, para o produtor rural pessoa física e para o microempreendedor individual – MEI.

3.5. Em relação às regras aplicáveis à presente licitação concernentes a tratamento favorecido para as microempresas, empresas de pequeno porte e equiparadas, observa-se que:

3.5.1. Considerando o valor estimado do item objeto desta licitação, não se aplicam a ele as regras de tratamento favorecido constantes dos arts. 42 a 49 da Lei Complementar nº 123, de 2006, nos termos dos §§ 1º e 3º do art. 4º da Lei nº 14.133, de 2021.

3.6. Não poderão disputar esta licitação:

3.6.1. aquele que não atenda às condições deste Edital e seu(s) Anexo(s);

3.6.2. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados, observado o disposto nos §§ 2º e 4º do art. 14 da Lei nº 14.133, de 2021;

3.6.3. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários, observado o disposto nos §§ 2º e 4º do art. 14 da Lei nº 14.133, de 2021;

3.6.4. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

3.6.5. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

3.6.6. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

3.6.7. pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

3.6.8. agente público do órgão ou entidade licitante;

3.6.9. aquele que não tenha representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente.

3.7. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade licitante ou contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei nº 14.133, de 2021.

3.7.1. A vedação de participação de agente público do órgão ou entidade licitante ou contratante de que trata a subdivisão acima estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

3.8. O impedimento decorrente de imposição de sanção de que trata o item 3.6.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

3.9. No que concerne aos itens 3.6.2 e 3.6.3, equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

3.10. Não poderão disputar esta licitação sociedades cooperativas, tendo em vista o disposto no art. 16 da Lei nº 14.133, de 2021, e no art. 5º da Lei nº 12.690, de 2012.

3.11. Será admitida a participação de pessoas jurídicas em consórcio, nos termos do art. 15 da Lei nº 14.133, de 2021.

3.11.1. Será vedada a participação de empresa consorciada, na mesma licitação, de mais de um consórcio ou de forma isolada, nos termos do art. 15, inc. IV, da Lei nº 14.133, de 2021.

4. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

4.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

4.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço, até a data e o horário estabelecidos para abertura da sessão pública.

4.3. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

4.3.1. está ciente e concorda com as condições contidas no Edital e seus Anexos, bem como que a proposta apresentada compreenderá a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

4.3.2. não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesesseis) anos, salvo menor, a partir de 14 (quatorze) anos, na condição de aprendiz, nos termos do artigo 7º, XXXIII, da Constituição Federal;

4.3.3. não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

4.3.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

4.4. O fornecedor enquadrado como microempresa, empresa de pequeno porte deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3º da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º da Lei nº 14.133, de 2021, excetuada a hipótese de se verificar uma das exceções dos §§ 1º ao 3º do art. 4º supracitado, conforme especificado nos itens 4.4.1 e 4.4.2 subsequentes.

4.4.1. Não se aplica o tratamento favorecido estabelecido nos arts. 42 a 49 da Lei Complementar nº 123, de 2006, na hipótese em que o objeto tenha valor estimado superior ao limite estabelecido nos §§ 1º e 3º do art. 4º da Lei nº 14.133, de 2021, conforme seja especificado, quando houver, em subdivisão do item 3.5.

4.4.2. Não têm direito ao tratamento favorecido estabelecido nos arts. 42 a 49 da Lei Complementar nº 123, de 2006, as microempresas, as empresas de pequeno porte que, no ano-calendário de realização da licitação, tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, nos termos do § 2º do art. 4º da Lei nº 14.133, de 2021.

4.4.3. Na hipótese de se verificar uma das exceções especificadas no item 4.4.1 ou no item 4.4.2, ou de não cumprimento de outro requisito legal para tratamento favorecido, o licitante deverá assinalar o campo “não”, por não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006.

4.4.4. Na hipótese de item para participação exclusiva de microempresas, empresas de pequeno porte e equiparadas, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item.

4.4.5. Na hipótese de itens em que a participação não seja exclusiva para microempresas, empresas de pequeno porte e equiparadas, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte.

4.5. A falsidade da declaração de que tratam os itens 4.3 e 4.4 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

4.6. Os licitantes poderão retirar ou substituir a proposta anteriormente inserida no sistema, até a abertura da sessão pública.

4.7. Não haverá ordem de classificação na etapa de apresentação da proposta pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

4.8. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

4.9. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

4.10. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

5. DO PREENCHIMENTO DA PROPOSTA

5.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

5.1.1. Valor mensal e total estimado do item;

5.1.2. Marca;

5.1.3. Fabricante;

5.1.4. Quantidade cotada, devendo respeitar o mínimo especificado na documentação que constitui Anexo deste Edital.

5.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.

5.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

5.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

5.5. Independentemente do percentual de tributo inserido na planilha, quando houver determinação legal de retenção de tributo, no pagamento serão retidos na fonte os percentuais que sejam estabelecidos na legislação vigente.

5.6. As microempresas e empresas de pequeno porte impedidas de optar pelo Simples Nacional, ante as vedações previstas na Lei Complementar nº 123, de 2006, não poderão aplicar os benefícios decorrentes desse regime tributário diferenciado em sua proposta, devendo elaborá-la de acordo com as normas aplicáveis às demais pessoas jurídicas.

5.6.1. Quando for o caso, e se vier a ser contratado, o licitante na situação descrita na subdivisão acima deverá requerer ao órgão fazendário competente a sua exclusão do Simples Nacional até o último dia útil do mês subsequente àquele em que ocorrida a situação de vedação, nos termos do art. 30, caput, inc. II, e § 1º, inc. II, da Lei Complementar nº 123, de 2006, apresentando à Administração a comprovação da exclusão ou o seu respectivo protocolo.

5.6.2. Se o Contratado não realizar espontaneamente o requerimento de que trata a subdivisão acima, caberá ao ente público contratante comunicar o fato ao órgão fazendário competente, solicitando que o Contratado seja excluído de ofício do Simples Nacional, nos termos do art. 29, inc. I, da Lei Complementar nº 123, de 2006.

5.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe a documentação que integra este Edital, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de utilizar os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

5.8. O prazo de validade da proposta não será inferior a 60 (sessenta) dias, a contar da data de sua apresentação.

5.9. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas, quando participarem de licitações públicas.

5.10. O descumprimento das regras supramencionadas por parte do Contratado pode ensejar a responsabilização pelo Tribunal de Contas competente e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inc. IX, da Constituição Federal, e do art. 33, inc. X, da Constituição do Estado de São Paulo; ou condenação dos agentes públicos responsáveis e do Contratado ao pagamento de indenização pelos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

6. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

6.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

6.2. Os licitantes poderão retirar ou substituir a proposta anteriormente inserida no sistema, até a abertura da sessão pública.

6.3. O sistema disponibilizará campo próprio para troca de mensagens entre o pregoeiro e os licitantes.

6.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

6.5. O lance deverá ser ofertado pelo valor unitário do item.

6.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas neste Edital.

6.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

6.8. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta, deverá ser de R\$ 12.000,00 (doze mil).

6.9. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de 15 (quinze) segundos após o registro no sistema, na hipótese de lance inconsistente ou inexecutável.

6.10. O procedimento seguirá de acordo com o modo de disputa adotado, definido no início deste Edital.

6.11. Será adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto”, segundo o qual os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

6.11.1. A etapa de lances da sessão pública terá duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 2 (dois) minutos do período de duração da sessão pública.

6.11.2. A prorrogação automática da etapa de lances, de que trata a subdivisão acima, será de 2 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

6.11.3. Não havendo novos lances na forma estabelecida nas subdivisões anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem de classificação.

6.11.4. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

6.11.5. Após o reinício previsto na subdivisão acima, os licitantes serão convocados para apresentar lances intermediários.

- 6.12. Após o término dos prazos estabelecidos nas subdivisões anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.
- 6.13. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.
- 6.14. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.
- 6.15. No caso de desconexão com o pregoeiro, no decorrer da etapa competitiva do pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.
- 6.16. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão pública será suspensa e reiniciada somente após decorridas 24 (vinte e quatro) horas da comunicação do fato pelo pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.
- 6.17. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.
- 6.17.1. Não se aplica o tratamento favorecido estabelecido nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, na hipótese em que o objeto tenha valor estimado superior ao limite estabelecido nos §§ 1º e 3º do art. 4º da Lei nº 14.133, de 2021, conforme seja especificado, quando houver, em subdivisão do item 3.5.
- 6.18. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado (se adotado esse modo de disputa no início deste Edital e no item 6.11).
- 6.18.1. Havendo eventual empate entre propostas ou lances, os critérios de desempate serão aqueles previstos no caput do art. 60 da Lei nº 14.133, de 2021, nesta ordem:
- 6.18.1.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;
- 6.18.1.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos na Lei nº 14.133, de 2021, conforme regulamento;
- 6.18.1.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;
- 6.18.1.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.
- 6.18.2. Persistindo o empate, será assegurada preferência, nos termos do § 1º do art. 60 da Lei nº 14.133, de 2021, sucessivamente, aos bens e serviços produzidos ou prestados por:
- 6.18.2.1. empresas estabelecidas no território do Estado de São Paulo;
- 6.18.2.2. empresas brasileiras;
- 6.18.2.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;
- 6.18.2.4. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.
- 6.18.3. Caso persista o empate após obedecido o disposto no caput e no § 1º do art. 60 da Lei nº 14.133, de 2021, o desempate ocorrerá por sorteio, a ser realizado em local, data e horário que serão divulgados por meio de mensagem no sistema, sendo facultada a presença a todos os interessados, incluindo os demais licitantes.

6.18.4. Será observado o disposto no § 2º do art. 60 da Lei nº 14.133, de 2021, e no inciso III do art. 41 c/c o inciso I do art. 58 da Lei Complementar nº 225, de 2026, quando for o caso.

6.19. Encerrada a etapa de envio de lances da sessão pública, na hipótese de a proposta do primeiro colocado permanecer acima do preço máximo definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

6.19.1. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do orçamento estimado definido pela Administração.

6.19.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

6.19.3. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

6.19.4. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, de documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

6.19.5. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante antes de findo o prazo, ou de ofício, a critério do pregoeiro, quando constatado que o prazo estabelecido não é suficiente para o envio da documentação exigida.

6.20. Após a negociação do preço, o pregoeiro iniciará a fase de aceitação e julgamento da proposta.

7. DA FASE DE JULGAMENTO

7.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133, de 2021, na legislação correlata, e no item 3.6 deste Edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

7.1.1. Sicaf;

7.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - Ceis, mantido pela Controladoria-Geral da União (<https://portaldatransparencia.gov.br/sancoes/consulta>);

7.1.3. Cadastro Nacional de Empresas Punidas – Cnep, mantido pela Controladoria-Geral da União (<https://portaldatransparencia.gov.br/sancoes/consulta>);

7.1.4. Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade – CNCIAI, do Conselho Nacional de Justiça (http://www.cnj.jus.br/improbidade_adm/consultar_requerido.php);

7.1.5. Sistema Eletrônico de Aplicação e Registro de Sanções Administrativas – e-Sanções (<http://www.esancoes.sp.gov.br>);

7.1.6. Relação de apenados publicada pelo Tribunal de Contas do Estado de São Paulo (<https://www.tce.sp.gov.br/apenados>); e

7.1.7. Cadastro Informativo de créditos não quitados do setor público federal – Cadin, de que trata a Lei nº 10.522, de 2002, no que concerne à medida prevista no inciso I, alíneas “b” e “c”, do art. 13 da Lei Complementar nº 225, de 2026.

7.2. Em relação a pessoa jurídica licitante, a consulta ao cadastro CNCIAI será realizada também quanto a seu sócio majoritário, por força do art. 12 da Lei nº 8.429, de 1992.

- 7.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 29, caput, c/c Decreto estadual nº 67.608, de 2023).
- 7.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 29, § 1º, c/c Decreto estadual nº 67.608, de 2023).
- 7.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 29, § 2º, c/c Decreto estadual nº 67.608, de 2023).
- 7.3.3. Constatada a existência de sanção, o licitante será considerado inabilitado, por falta de condição de participação.
- 7.4. Caso atendidas as condições de participação, prosseguirá a análise da fase de julgamento da proposta classificada em primeiro lugar.
- 7.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido a microempresas e empresas de pequeno porte, o pregoeiro verificará se faz jus ao benefício, em conformidade com os itens 3.5 e 4.4 deste Edital.
- 7.6. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus Anexos.
- 7.6.1. Se a proposta vencedora for desclassificada, o pregoeiro examinará a proposta subsequente, e, assim sucessivamente, na ordem de classificação.
- 7.6.2. Encerrada a fase de julgamento, caso se verifique a conformidade da proposta de que trata o item 7.6, o pregoeiro passará à verificação da documentação de habilitação do licitante conforme disposições do item 8.
- 7.7. Será desclassificada a proposta vencedora que:
- 7.7.1. contiver vícios insanáveis;
- 7.7.2. não obedecer às especificações técnicas pormenorizadas neste Edital ou em seus Anexos;
- 7.7.3. apresentar preços inexequíveis ou permanecer acima do orçamento estimado definido para a contratação;
- 7.7.4. não tiver sua exequibilidade demonstrada, quando exigido pela Administração;
- 7.7.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus Anexos, desde que insanável.
- 7.8. Serão considerados indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.
- 7.8.1. A inexequibilidade, na hipótese de que trata a subdivisão acima, só será considerada após diligência do pregoeiro, que comprove:
- 7.8.1.1. que o custo do licitante ultrapassa o valor da proposta; e
- 7.8.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.
- 7.9. Em acréscimo às disposições acima, deverão ser observados os seguintes preceitos:

7.9.1. A análise da exequibilidade da proposta de preços deverá ser realizada com o auxílio de planilha de custos e formação de preços, a ser preenchida pelo licitante em relação à sua proposta final, conforme modelo constante de Anexo deste Edital.

7.9.2. A apresentação de valores abaixo dos respectivos custos referentes a itens isolados da planilha de custos e formação de preços não caracteriza motivo suficiente para a desclassificação da proposta, desde que não contrariem exigências legais.

7.9.3. A fim de assegurar o tratamento isonômico entre os licitantes, informa-se que foi(ram) utilizado(s) o(s) seguinte(s) acordo(s), dissídio(s) ou convenção(ões) coletiva(s) de trabalho no cálculo do valor estimado pela Administração:

a) O acordo coletivo que será utilizado como cálculo é aquele a que pertencer ao trabalhador, conforme Assembleia realizada e homologada vigente.

7.9.3.1. O(s) sindicato(s) e instrumento(s) coletivo(s) indicado(s) na subdivisão acima não são de utilização obrigatória pelos fornecedores, tendo em vista que a definição do(s) sindicato(s) e instrumento(s) coletivo(s) adequado(s) a cada fornecedor depende do enquadramento sindical a ele aplicável nos termos da legislação vigente. Ao longo da execução contratual, sempre se exigirá o cumprimento dos acordos, dissídios ou convenções coletivas aos quais o Contratado estiver vinculado nos termos da legislação vigente.

7.9.4. É vedado ao licitante incluir na planilha de custos e formação de preços:

a) item relativo a despesas decorrentes de disposições contidas em acordos, convenções ou dissídios coletivos de trabalho que tratem de matéria não trabalhista, de pagamento de participação dos trabalhadores nos lucros ou resultados do Contratado, ou que estabeleçam direitos não previstos em lei, tais como valores ou índices obrigatórios de encargos sociais ou previdenciários, bem como de preços para os insumos relacionados ao exercício da atividade (art. 135, § 1º, da Lei nº 14.133, de 2021);

b) item relativo a despesas decorrentes de disposições contidas em acordos, convenções ou dissídios coletivos de trabalho que tratem de obrigações e direitos que somente se aplicam aos contratos com a Administração Pública (art. 135, § 2º, da Lei nº 14.133, de 2021).

7.9.5. A inclusão na proposta de item de custo vedado não acarretará a desclassificação do licitante, devendo o pregoeiro determinar que o respectivo custo seja excluído da planilha, observando-se o disposto no inciso III do art. 12 da Lei nº 14.133, de 2021.

7.9.6. Na hipótese de contratação com a previsão de itens de custos vedados, tais valores serão glosados e os itens serão excluídos da planilha, garantidos ampla defesa e contraditório.

7.9.7. Em todo caso, deverá ser garantido o pagamento do salário normativo previsto no instrumento coletivo aplicável ou do salário-mínimo vigente, o que for maior.

7.9.8. Será solicitado que o licitante mais bem classificado envie, junto com sua proposta adequada ao último lance ofertado, declaração informando o enquadramento sindical do licitante, a atividade econômica preponderante e a justificativa para adoção do(s) instrumento(s) coletivo(s) do trabalho em que se baseia sua proposta.

7.9.8.1. O licitante mais bem classificado deverá indicar os sindicatos, acordo(s) coletivo(s), convenção(ões) coletiva(s) ou sentença(s) normativa(s) que regem a(s) categoria(s) profissional(is) que executará(ão) o serviço e a(s) respectiva(s) data(s)-base(s) e vigência(s), com base na Classificação Brasileira de Ocupações – CBO.

7.9.9. Anteriormente à celebração da contratação, o licitante vencedor deverá apresentar:

7.9.9.1. cópia da carta ou registro sindical do sindicato no qual ele declara ser enquadrado, em razão do regramento do enquadramento sindical previsto na Consolidação das Leis do Trabalho (CLT) ou por força de decisão judicial;

7.9.9.2. comprovação de capital social integralizado compatível com o número de empregados, na forma do art. 4º-B da Lei nº 6.019, de 1974.

7.9.10. O licitante se responsabiliza pelas situações de ocorrência de erro no enquadramento sindical, ou fraude pela utilização de instrumento coletivo incompatível com o enquadramento sindical declarado ou no qual o licitante não tenha sido representado por órgão de classe de sua categoria, que daí tenha resultado vantagem indevida na fase de julgamento das propostas, sujeitando o Contratado às sanções previstas no art. 156, caput, incisos III e IV, da Lei nº 14.133, de 2021.

7.9.11. O Contratado possui responsabilidade exclusiva pelo cometimento de erro ou fraude no enquadramento sindical e pelo eventual ônus financeiro decorrente, por repactuação ou por força de decisão judicial, em razão da necessidade de se proceder ao pagamento de diferenças salariais e de outras vantagens, ou ainda por intercorrências na execução dos serviços contratados, resultante da adoção de instrumento coletivo do trabalho inadequado.

7.9.12. Deverá ser observada a aderência ao instrumento coletivo do trabalho ao qual a proposta do licitante esteja vinculada para fins de atendimento à eventual necessidade de repactuação dos valores decorrentes da mão de obra, consignados na planilha de custos e formação de preços do contrato, em observância ao disposto no inc. II do art. 135 da Lei nº 14.133, de 2021.

7.9.13. Considerando que o objeto da licitação consiste em prestação de serviços contínuos com regime de dedicação exclusiva de mão de obra, cuja produtividade é mensurável e indicada na documentação que integra este Edital, o licitante deverá indicar a produtividade adotada e a quantidade de pessoal que será alocado na execução contratual.

7.9.13.1. Caso a produtividade seja diferente daquela utilizada pela Administração como referência, ou não esteja contida na faixa referencial de produtividade, mas seja admitida pelo Edital, o licitante deverá apresentar a respectiva comprovação de exequibilidade.

7.9.13.2. Os licitantes poderão apresentar produtividades diferenciadas daquela estabelecida pela Administração como referência, desde que não alterem o objeto da contratação, não contrariem dispositivos legais vigentes e, caso não estejam contidas nas faixas referenciais de produtividade, comprovem a exequibilidade da proposta.

7.9.13.3. Para efeito da subdivisão anterior, admite-se a adequação técnica da metodologia empregada pelo licitante, visando assegurar a execução do objeto, desde que mantidas as condições para a justa remuneração do serviço.

7.10. Se houver indícios de inexecuibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que o licitante comprove a exequibilidade da proposta.

7.11. Considerando que o custo global estimado do objeto licitado é decomposto em seus respectivos custos unitários por meio de planilha elaborada pela Administração conforme documentação anexada a este Edital, o licitante classificado em primeiro lugar será convocado para apresentar planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

7.12. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação.

7.12.1. O ajuste de que trata a subdivisão acima se limita ao saneamento de erros ou falhas que não alterem a substância das propostas.

7.12.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

7.13. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante ou da área especializada no objeto.

8. DA FASE DE HABILITAÇÃO

8.1. Os documentos que serão exigidos para fins de habilitação estão especificados no Anexo I deste Edital, consistindo na documentação necessária e suficiente para demonstrar a capacidade do licitante de realizar o objeto da licitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

8.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira poderá ser substituída pelo registro cadastral no Sicafe.

8.1.2. Considerando que na presente licitação a avaliação prévia do local de execução é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, o licitante deve atestar, sob pena de inabilitação, que conhece o local e as condições de realização do objeto da licitação, assegurado a ele o direito de realização de vistoria prévia, ou de apresentar declaração de conhecimento pleno das condições e peculiaridades da contratação, observando-se o disposto na documentação que integra este Edital como Anexo.

8.1.3. Se for permitida a participação de pessoas jurídicas em consórcio em subdivisão do item 3, para efeito de habilitação técnica, caso exigida na documentação que integra este Edital como Anexo, será admitido o somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, caso exigida na documentação que integra este Edital como Anexo, será admitido o somatório dos valores de cada consorciado.

8.1.3.1. Na hipótese de admissão da participação de pessoas jurídicas em consórcio e exigência de requisito(s) de habilitação econômico-financeira de que trata a subdivisão acima, se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte, haverá um acréscimo de 20% (vinte por cento) para o consórcio em relação ao valor exigido dos licitantes individuais para habilitação econômico-financeira.

8.1.4. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, caso exigidos, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

8.2. Os documentos exigidos para fins de habilitação poderão ser apresentados em original ou por cópia.

8.3. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133, de 2021.

8.4. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133, de 2021).

8.5. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

8.6. O licitante deverá apresentar, sob pena de desclassificação, declaração de que sua proposta econômica compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

8.7. A habilitação será verificada por meio do Sicafe, quanto aos documentos por ele abrangidos.

8.7.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 4º, § 1º, e art. 6º, § 4º, c/c Decreto estadual nº 67.608, de 2023).

8.8. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 7º, caput, c/c Decreto estadual nº 67.608, de 2023).

8.8.1. A não observância do disposto na subdivisão acima poderá ensejar desclassificação no momento da habilitação (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 7º, parágrafo único, c/c Decreto estadual nº 67.608, de 2023).

8.9. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

8.9.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de 2 (duas) horas, prorrogável por igual período, contado da solicitação do pregoeiro.

8.10. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

8.10.1. Os documentos relativos à regularidade fiscal especificados na documentação que integra este Edital como Anexo somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

8.11. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei nº 14.133, de 2021, art. 64):

8.11.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

8.11.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas.

8.12. Na análise dos documentos de habilitação, o pregoeiro poderá sanar erros ou falhas que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

8.13. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente Edital, observado o prazo definido no item 8.9.1.

8.14. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao Edital de licitação, após concluídos os procedimentos de que trata a subdivisão anterior.

8.15. Não se aplica nesta licitação o tratamento favorecido estabelecido nos arts. 42 e 43 da Lei Complementar nº 123, de 2006, conforme definido em subdivisão do item 3.5.

8.16. A disciplina da adjudicação e da homologação encontra-se no item 14 deste Edital.

9. DA ATA DE REGISTRO DE PREÇOS

9.1. A disciplina deste item 9 não se aplica no presente procedimento, por não se tratar de licitação para registro de preços.

10. DA FORMAÇÃO DO CADASTRO DE RESERVA

10.1. A disciplina deste item 10 não se aplica no presente procedimento, por não se tratar de licitação para registro de preços.

11. DOS RECURSOS

11.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

11.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

11.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

11.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

11.3.2. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos;

11.3.3. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação.

11.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

11.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar o recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

11.6. Os recursos interpostos fora do prazo não serão conhecidos.

11.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

11.8. O recurso terá efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

11.9. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

11.10. Os autos do processo permanecerão com vista franqueada aos interessados pelo meio eletrônico dticslic@policiamilitar.sp.gov.br ou vistas em cartório, Av. Cruzeiro do Sul, 260, 6º andar, Canindé, cidade de São Paulo-SP.

12. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

12.1. Comete infração administrativa, nos termos da lei, o licitante ou Contratado que, com dolo ou culpa:

12.1.1. der causa à inexecução parcial do contrato;

12.1.2. der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

12.1.3. der causa à inexecução total do contrato;

12.1.4. deixar de entregar a documentação exigida para o certame, inclusive não entregar qualquer documento que tenha sido solicitado pelo pregoeiro durante o certame;

12.1.5. salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta, em especial quando:

12.1.5.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

- 12.1.5.2. recusar-se a enviar o detalhamento da proposta quando exigível;
- 12.1.5.3. pedir para ser desclassificado quando encerrada a etapa competitiva;
- 12.1.6. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
- 12.1.6.1. recusar-se, sem justificativa, a formalizar a contratação no prazo e condições estabelecidos pela Administração;
- 12.1.7. ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- 12.1.8. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;
- 12.1.9. fraudar a licitação ou praticar ato fraudulento na execução do contrato;
- 12.1.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:
 - 12.1.10.1. agir em conluio ou em desconformidade com a lei;
 - 12.1.10.2. induzir deliberadamente a erro no julgamento;
 - 12.1.11. praticar atos ilícitos com vistas a frustrar os objetivos da licitação;
 - 12.1.12. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 2013.
- 12.2. Com fundamento na Lei nº 14.133, de 2021, a Administração poderá, após regular processo administrativo, garantida a prévia defesa, aplicar aos licitantes, adjudicatários e/ou Contratado as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:
 - 12.2.1. advertência;
 - 12.2.2. multa;
 - 12.2.3. impedimento de licitar e contratar; e
 - 12.2.4. declaração de inidoneidade para licitar ou contratar.
- 12.3. Na aplicação das sanções serão considerados:
 - 12.3.1. a natureza e a gravidade da infração cometida;
 - 12.3.2. as peculiaridades do caso concreto;
 - 12.3.3. as circunstâncias agravantes ou atenuantes;
 - 12.3.4. os danos que dela provierem para a Administração Pública;
 - 12.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.
- 12.4. As sanções serão aplicadas em conformidade com a Resolução nº SSP-05/2026, publicada no diário oficial do Estado de São Paulo em 02MAR26, que integra este instrumento (Anexo III), após regular processo administrativo.**
 - 12.4.1. A sanção de multa prevista no inciso II do caput do art. 156 da Lei nº 14.133, de 2021, calculada na forma deste Edital, não poderá ser inferior a 0,5% (cinco décimos por cento) nem superior a 30% (trinta por cento) do valor do contrato (§ 3º do art. 156 da Lei nº 14.133, de 2021).

12.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas cumulativamente com a penalidade de multa, garantido o exercício de prévia e ampla defesa.

12.6. Antes da aplicação da sanção de multa, será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

12.7. A sanção de advertência será aplicada, após regular processo administrativo, ao responsável em decorrência da infração administrativa relacionada no item 12.1.1, quando não se justificar a imposição de penalidade mais grave.

12.8. A sanção de impedimento de licitar e contratar será aplicada, após regular processo administrativo, ao responsável em decorrência das infrações administrativas relacionadas nos itens 12.1.2, 12.1.3, 12.1.4, 12.1.5, 12.1.6 e 12.1.7, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta do Estado de São Paulo, pelo prazo máximo de 3 (três) anos.

12.9. A sanção de declaração de inidoneidade para licitar ou contratar será aplicada, após regular processo administrativo, ao responsável em decorrência das infrações administrativas relacionadas nos itens 12.1.8, 12.1.9, 12.1.10, 12.1.11 e 12.1.12, bem como das infrações administrativas previstas nos itens 12.1.2, 12.1.3, 12.1.4, 12.1.5, 12.1.6 e 12.1.7 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja extensão e duração observará o disposto no art. 156, § 5º, da Lei nº 14.133, de 2021.

12.10. A recusa injustificada do adjudicatário em formalizar a contratação no prazo e condições estabelecidos pela Administração, descrita no item 12.1.6.1, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades legalmente estabelecidas (art. 90, § 5º, da Lei nº 14.133, de 2021).

12.11. A apuração de responsabilidade relacionada às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta nos termos do art. 158 da Lei nº 14.133, de 2021, que avaliará fatos e circunstâncias conhecidos e intimará o licitante, o adjudicatário ou o Contratado para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

12.12. As sanções são autônomas e a aplicação de uma não exclui a de outra.

12.13. Da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, caberá recurso no prazo de 15 (quinze) dias úteis, contado da data da intimação, observando-se o disposto no art. 166 da Lei nº 14.133, de 2021.

12.14. Da aplicação da sanção de declaração de inidoneidade para licitar ou contratar, caberá pedido de reconsideração no prazo de 15 (quinze) dias úteis, contado da data da intimação, observando-se o disposto no art. 167 da Lei nº 14.133, de 2021.

12.15. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

12.16. A aplicação das sanções previstas neste Edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados à Administração Pública.

12.17. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada, caso exigida na documentação que integra o Edital, ou, quando for o caso, será cobrada judicialmente (art. 156, § 8º, da Lei nº 14.133, de 2021).

12.18. Os atos previstos como infrações administrativas na lei de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na referida Lei.

12.19. A personalidade jurídica poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos na Lei nº 14.133, de 2021, ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, a pessoa jurídica sucessora ou a empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o sancionado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia, nos termos do art. 160 do referido diploma legal.

12.20. O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ele aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo federal (art. 161 da Lei nº 14.133, de 2021).

13. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

13.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, ou para solicitar esclarecimento sobre os seus termos, devendo protocolar a impugnação ou o pedido de esclarecimento até 3 (três) dias úteis antes da data da abertura do certame.

13.2. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, pelos seguintes meios: e-mail dticslic@policiamilitar.sp.gov.br – ou por petição protocolada no seguinte endereço, Avenida Cruzeiro do Sul, 260 – 6º andar – CEP: 03033-901 – DTIC – Canindé, São Paulo-SP.

13.3. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

13.3.1. A concessão de efeito suspensivo à impugnação é medida excepcional, e, caso ocorra, será motivada nos autos do processo de licitação.

13.4. A decisão da impugnação ou a resposta ao pedido de esclarecimento serão divulgadas em sítio eletrônico oficial conforme especificado na subdivisão subsequente, no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

13.4.1. As decisões das impugnações e as respostas aos pedidos de esclarecimento serão juntadas aos autos do processo licitatório, ficarão disponíveis para consulta por qualquer interessado, e serão publicadas no sistema e no(s) sítio(s) eletrônico(s) na Internet www.compras.gov.br, sem informar a identidade do responsável pela impugnação ou pelo pedido de esclarecimento.

13.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame, exceto quando a alteração não comprometer a formulação das propostas.

13.6. A ausência de impugnação implicará na aceitação tácita, pelo licitante, das condições previstas neste Edital e em seus Anexos.

13.7. A ausência de pedido de esclarecimento implicará na presunção de que os interessados não tiveram dúvidas a respeito da presente licitação, razão pela qual não serão admitidos questionamentos extemporâneos.

14. DAS DISPOSIÇÕES GERAIS

14.1. Exaurida a fase recursal, será observado o disposto no art. 71 da Lei nº 14.133, de 2021.

14.1.1. Constatada a regularidade dos atos praticados, a autoridade superior adjudicará o objeto da licitação ao licitante vencedor e homologará o procedimento licitatório.

14.2. A disciplina da formalização da contratação observará o disposto nas subdivisões deste item 14.2.

14.2.1. Após a homologação da licitação, em sendo realizada a contratação, sua formalização ocorrerá mediante a assinatura de Termo de Contrato, cuja minuta integra este Edital como Anexo.

14.2.1.1. Se, por ocasião da formalização da contratação, algum dos documentos apresentados pelo adjudicatário para fins de comprovação das condições de habilitação estiver com o prazo de validade expirado, a Administração verificará a situação por meio eletrônico hábil de informações e certificará a regularidade nos autos do processo, anexando a ele os documentos comprobatórios, salvo impossibilidade devidamente justificada.

14.2.1.2. Se não for possível atualizar os documentos referidos na subdivisão acima por meio eletrônico hábil de informações, o adjudicatário será notificado para, no prazo de 02 (dois) dias úteis, comprovar a sua situação de regularidade mediante a apresentação das certidões respectivas com prazos de validade em plena vigência, sob pena de a contratação não se realizar.

14.2.1.3. Constitui condição para a celebração da contratação, bem como para a realização dos pagamentos dela decorrentes, a inexistência de registros em nome do adjudicatário no “Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais – Cadin estadual”, de que trata a Lei estadual nº 12.799, de 2008. Esta condição será considerada cumprida se o devedor comprovar que os respectivos registros se encontram suspensos, nos termos do art. 8º, §§ 1º e 2º, da Lei estadual nº 12.799, de 2008.

14.2.1.4. Com a finalidade de verificar se o licitante mantém as condições de participação no certame, serão novamente consultados, previamente à celebração da contratação, os cadastros especificados no item 7.1 deste Edital.

14.2.1.5. Constitui(em), igualmente, condição(ões) para a celebração da contratação:

14.2.1.5.1. a apresentação do(s) documento(s) que deva(m) ser exibido(s) pelo adjudicatário anteriormente ou por ocasião da celebração da contratação, caso exigida em disposição(ões) ou declaração(ões) específica(s) que esteja(m) prevista(s) neste instrumento ou na documentação que o integra como Anexo;

14.2.2. O adjudicatário terá o prazo de 05 (cinco) dias, contados a partir da data de sua convocação, para assinar o Termo de Contrato, sob pena de decadência do direito, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

14.2.2.1. O contrato será assinado com a utilização de meio eletrônico, nos termos da legislação aplicável.

14.2.2.2. O prazo para assinatura previsto na subdivisão anterior poderá ser prorrogado por igual período, por solicitação justificada do interessado e aceita pela Administração.

14.2.2.3. Será considerado celebrado o contrato, em caso de assinaturas por meio eletrônico em datas diferentes, na data da última assinatura eletrônica das partes do termo contratual.

14.2.3. Na hipótese de o vencedor da licitação não comprovar manter as condições de habilitação e preencher as condições de contratação consignadas neste Edital, ou não assinar o contrato, ou recusar a contratação, a Administração, sem prejuízo da apuração do cabimento de aplicação de sanções e das demais cominações legais cabíveis a esse licitante, poderá convocar os licitantes remanescentes, respeitada a ordem de classificação, para a celebração do contrato em conformidade com o procedimento e as condições estabelecidas no art. 90 da Lei nº 14.133, de 2021.

14.2.4. Será facultada à Administração a convocação dos demais licitantes classificados para a contratação de remanescente em consequência de rescisão de contrato celebrado com fundamento nesta licitação, observados os critérios estabelecidos no § 7º do art. 90 da Lei nº 14.133, de 2021.

14.3. Será divulgada ata da sessão pública no sistema eletrônico.

14.4. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o 1º (primeiro) dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo pregoeiro.

14.5. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

14.6. A homologação do resultado desta licitação não implicará direito à contratação.

14.7. As normas disciplinadoras da licitação serão interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse público, o princípio da isonomia, a finalidade e a segurança da contratação.

14.8. Os casos omissos serão solucionados pelo pregoeiro.

14.9. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

14.10. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

14.11. No julgamento das propostas e da habilitação, o pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

14.11.1. As falhas passíveis de saneamento na documentação apresentada pelo licitante são aquelas cujo conteúdo retrate situação fática ou jurídica já existente na data da abertura da sessão pública deste Pregão.

14.11.2. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público, nos termos do inc. III do art. 12 da Lei nº 14.133, de 2021.

14.12. Caso seja vencedor da licitação, o licitante a ser contratado estará sujeito à assinatura de Termo de Ciência e de Notificação, quando prevista a sua apresentação em ato normativo editado pelo Tribunal de Contas do Estado de São Paulo, conforme a disciplina aplicável.

14.13. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e no sítio eletrônico www.imprensaoficial.com.br.

14.14. Para dirimir quaisquer questões decorrentes da licitação, não resolvidas na esfera administrativa, será competente o foro da Comarca da Capital do Estado de São Paulo.

14.15. Integram este Edital, para todos os fins e efeitos, os seguintes Anexos:

14.15.1. ANEXO I - Termo de Referência;

14.15.1.1 ANEXO I.1 – Estudo Técnico Preliminar;

14.15.2. ANEXO II – Minuta de Termo de Contrato;

14.15.3. ANEXO III – Resolução SSP-05-2026 Sanções;

14.15.4. ANEXO IV – Modelo referente a planilha de proposta;

14.15.5. ANEXO V – Modelo de Declaração;

14.15.6. ANEXO VI – Modelo referente à vistoria prévia.

São Paulo, na data da assinatura digital

BEATRIZ DE ASSIS BASTOS MORASSI

Coronel PM Subscritor de edital

2. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

BEATRIZ DE ASSIS BASTOS MORASSI

Subscritor do Edital



Assinou eletronicamente em 25/05/2026 às 15:42:55.

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - 1. Anexo I TR 107 25 e ETP 121 25.pdf (4.28 MB)
- Anexo II - 2. Anexo II Minuta de contrato 9 25.pdf (184.02 KB)
- Anexo III - 3. Anexo III Resolucao SSP n 05 Sancoes.pdf (1.2 MB)
- Anexo IV - 4. Anexo IV Planilha de proposta.pdf (233.62 KB)
- Anexo V - 5. Anexo V Modelo de declaracao.pdf (170.08 KB)
- Anexo VI - 6. Anexo VI Modelo referente a vistoria previa.pdf (175.25 KB)

ESP-DIRETORIA TEC. INFORMACAO E COMUNICACAO

Termo de Referência 107/2025

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
107/2025	180183-ESP-DIRETORIA TEC. INFORMACAO E COMUNICACAO	MARCELO FUMIO TAMASHIRO	09/04/2026 17:06 (v 0.29)
Status			
DISPONIBILIZADO			

Outras informações

Categoria	Número da Contratação	Processo Administrativo
V - prestação de serviços, inclusive os técnico-profissionais especializados/Serviço continuado com dedicação exclusiva de mão de obra	141/2025	057.00495038/2025-41

1. Condições gerais da contratação

1.1. Contratação de serviços especializados de suporte técnico de cibersegurança, data center e redes, bem como de governança, gerenciamento e monitoramento, das demandas e mudanças de tecnologia da informação e comunicação e infraestrutura de data center e redes para ambiente computacional e de telecomunicações, de forma a garantir a continuidade dos serviços de TIC., nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste Termo de Referência, de acordo com as subdivisões na forma de itens que compõem este instrumento.

Item	CATMAT Contabiliza	CATMAT Compras.gov.br	Descrição – Categoria de Serviço	Qtd	HTS	Custo Mensal (R\$)	Custo 30 Meses (R\$)
			Gerente de infraestrutura de tecnologia da informação	1	176	Sigiloso	Sigiloso
			Gerente de suporte técnico de tecnologia da informação	1	176	Sigiloso	Sigiloso
			Analista de sistemas de automação - Júnior	8	180	Sigiloso	Sigiloso
			Técnico de suporte ao usuário de tecnologia da informação Júnior	2	176	Sigiloso	Sigiloso
			Técnico de Rede (Telecomunicações) - Júnior	1	176	Sigiloso	Sigiloso
			Gerente de suporte técnico de tecnologia da informação	1	176	Sigiloso	Sigiloso
			Analista de suporte computacional Pleno	4	176	Sigiloso	Sigiloso

1	91693	27090	Administrador de sistemas operacionais Sênior	4	176	Sigiloso	Sigiloso
			Administrador de sistemas operacionais Sênior	3	176	Sigiloso	Sigiloso
			Administrador de banco de dados - Sênior	1	176	Sigiloso	Sigiloso
			Administrador de banco de dados - Pleno	2	176	Sigiloso	Sigiloso
			Especialista em Cloud Sênior	1	176	Sigiloso	Sigiloso
			Gerente de segurança da informação	1	176	Sigiloso	Sigiloso
			Gerente de segurança da informação	1	176	Sigiloso	Sigiloso
			Analista de redes e de comunicação de dados Sênior	4	176	Sigiloso	Sigiloso
			Analista de redes e de comunicação de dados Pleno	7	176	Sigiloso	Sigiloso
			Administrador em segurança da informação - Sênior	1	176	Sigiloso	Sigiloso
			Analista de sistemas de automação - Pleno	1	176	Sigiloso	Sigiloso
			Desenvolvedor de sistemas de tecnologia da informação Sênior	1	176	Sigiloso	Sigiloso
				45		Sigiloso	Sigiloso

1.1.1. Em caso de eventual divergência entre a descrição do item do catálogo do sistema Compras.gov.br e as disposições deste Termo de Referência, prevalecem as disposições deste Termo de Referência.

1.1.2. Este Termo de Referência foi elaborado em conformidade com o Decreto estadual nº 68.185, de 11 de dezembro de 2023.

1.1.3. O objeto desta contratação não se enquadra como serviços de luxo, observando o disposto no Decreto estadual nº 67.985, de 27 de setembro de 2023.

1.2. Os serviços objeto desta contratação são caracterizados como Serviços Comuns, conforme justificativa constante do Estudo Técnico Preliminar, elaborado nos termos do Decreto estadual nº 68.017, de 11 de outubro de 2023.

1.3. O prazo de vigência da contratação é de 30 (trinta) meses, contados da assinatura do contrato, prorrogável por até 10 (dez) anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

1.3.1. O serviço é enquadrado como serviço contínuo, tendo em vista que se trata de contratação de serviços especializados de suporte técnico de cibersegurança, data center e redes, bem como de governança, gerenciamento e monitoramento, das demandas e mudanças de tecnologia da informação e comunicação e infraestrutura de data center e redes para ambiente computacional e de telecomunicações, de forma a garantir a continuidade dos serviços de TIC, sendo a vigência plurianual mais vantajosa considerando o Estudo Técnico Preliminar.

1.4. O contrato estabelece a disciplina que será aplicada em relação à vigência da contratação.

Subcontratação

1.4. É admitida a subcontratação parcial do objeto, conforme as regras estabelecidas no contrato.

2. Fundamentação e descrição da necessidade

2.1. A fundamentação da contratação e de seus quantitativos encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

2.2. O objeto da contratação está previsto no Plano de Contratações Anual 2, nos termos do Decreto estadual nº 67.689, de 3 de maio de 2023, conforme detalhamento a seguir:

I) ID PCA no PNCP: 46377800000127-0-000019/2025;

II) Data de publicação no PNCP: 28/05/2024;

III) Id do item no PCA: 525 - SERVICOS PARA A INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC), NAO CLASSIFICADOS EM OUTROS TÓPICOS;

IV) Classe/Grupo: 165;

V) Identificador da Futura Contratação: 180183-141/2025.

3. Descrição da solução como um todo

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

4. Requisitos da contratação

Sustentabilidade

4.1. A Polícia Militar do Estado de São Paulo – PMESP, está comprometida com a sustentabilidade e com a redução dos impactos ambientais de suas atividades.

4.1.1. A Contratada deverá aplicar em todo o contrato, práticas que priorizem materiais recicláveis, demonstrando o comprometimento com a sustentabilidade.

4.1.2. A Contratada deverá implementar um sistema de logística reversa, garantindo o descarte responsável de materiais e equipamentos inservíveis. Este sistema deve incluir um plano detalhado que demonstre o compromisso com o descarte adequado de resíduos, incluindo os eletrônicos, em conformidade com as normas ambientais locais.

Da exigência de carta de solidariedade

4.2. Será exigida carta de solidariedade emitida pelo fabricante do software, a qual assegure a execução do contrato em conjunto com o fornecedor.

4.2.1. A carta deverá garantir expressamente:

I – a disponibilização das licenças necessárias à execução dos serviços;

II – a manutenção de atualizações, correções de segurança e evoluções tecnológicas durante toda a vigência do contrato;

III – o fornecimento de suporte técnico de segundo nível, quando demandado, em complementaridade ao prestado pelo fornecedor;

IV – o compromisso do fabricante em cooperar para a continuidade dos serviços em caso de falha, indisponibilidade ou descontinuidade do distribuidor/revendedor.

4.2.2. Esta exigência excepcional justifica-se pela criticidade dos serviços contratados, que envolvem operação de ambientes de Cibersegurança (SOC), Data Center (SO) e Redes (NOC), considerados essenciais à continuidade da infraestrutura de TIC e à segurança da informação da Administração, de modo que eventual descontinuidade de suporte de empresa especializada em TIC representaria risco grave à execução contratual.

Garantia da contratação

4.3. Não haverá exigência da garantia da contratação dos arts. 96 e seguintes da Lei nº 14.133, de 2021, pelas razões constantes do Estudo Técnico Preliminar.

Vistoria

4.4. A avaliação prévia nos locais de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, bem como retirada dos documentos classificados com restrito, mediante assinatura de Termo de Sigilo e Confidencialidade, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 09h00 horas às 17h00 horas.

4.5. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia que deverão ser agendadas via e-mail dassidc@policiamilitar.sp.gov.br e cópia para dassodc@policiamilitar.sp.gov.br e/ou telefones (11) 3327-7418/ (11) 3327-7423.

4.6. Para a vistoria técnica, o representante legal do fornecedor ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pelo fornecedor comprovando sua habilitação para a realização da vistoria.

4.7. O interessado não poderá pleitear modificações nos preços, nos prazos ou nas condições contratuais, tampouco alegar quaisquer prejuízos ou reivindicar quaisquer benefícios sob a invocação de insuficiência de dados ou de informações sobre os locais em que será realizado o objeto da contratação.

4.8. Caso o licitante opte por não realizar a vistoria, deverá prestar declaração formal de seu representante legal de que conhece o local e as condições da realização do objeto, ou declaração formal assinada por seu responsável técnico acerca do conhecimento pleno das condições e peculiaridades da contratação.

5. Modelo de execução do objeto

Condições de execução

5.1. A execução do objeto seguirá a seguinte dinâmica:

5.1.1. Início da execução do objeto: em até 30 (trinta) dias a contar da assinatura do contrato, constituindo o Período de Transição Operacional (PTO).

5.1.2. Descrição detalhada dos métodos, rotinas, etapas, tecnologias, procedimentos, frequência e periodicidade de execução do trabalho, conforme pormenorizado em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

Local e horário da prestação dos serviços

5.2. As atividades previstas da solução como um todo encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência

Rotinas a serem cumpridas

5.3. A execução contratual encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

Materiais a serem disponibilizados

5.4. Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, para realizar os serviços dentro dos padrões exigidos nos Apêndices anexos a este instrumento, promovendo sua substituição quando necessário.

5.5. Além da mão de obra especializada, todos os materiais de consumo e equipamentos serão fornecidos obrigatoriamente pela Contratada, de forma a oferecer um bom desempenho dos trabalhos, tais como: monitores, estações de trabalho, mesas, cadeiras, entre outros;

5.5.1. O rol acima descrito é meramente exemplificativo, não exaurindo a Contratada da possibilidade de fornecimento de materiais e equipamentos eventualmente não mencionados.

Especificação da garantia do serviço (art. 40, §1º, inciso III, da Lei nº 14.133, de 2021)

5.6. O prazo de garantia contratual dos serviços é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

5.7. Os procedimentos de transição e finalização do contrato encontram-se pormenorizados em tópico específico do Estudo Preliminar, apêndice deste Termo de Referência.

6. Modelo de gestão do contrato

6.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

6.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

6.3. As comunicações entre o Contratante e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

6.4. O Contratante poderá convocar representante do Contratado para adoção de providências que devam ser cumpridas de imediato.

6.5. Após a celebração da contratação, o Contratante poderá convocar o representante do Contratado para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução do Contratado, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

Preposto

6.6. O Contratado designará formalmente o seu preposto, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

6.7. O Contratado não precisa manter preposto no local da execução do objeto durante o período.

6.8. O Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto do Contratado, hipótese em que o Contratado designará outro para o exercício da atividade.

Fiscalização

6.9. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelo(s) respectivo(s) substituto(s) (Lei nº 14.133, de 2021, art. 117, caput).

Fiscalização Técnica

6.10. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração (Decreto estadual nº 68.220, de 2023, art. 17).

6.11. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto estadual nº 68.220, de 2023, art. 17, II).

6.12. O fiscal técnico realizará, em conformidade com cronograma físico-financeiro, as medições dos serviços executados e aprovará a planilha de medição emitida pelo Contratado (Decreto estadual nº 68.220, de 2023, art. 17, III).

6.13. O fiscal técnico adotará medidas preventivas de controle de contratos, manifestando-se quanto à necessidade de suspensão da execução do objeto (Decreto estadual nº 68.220, de 2023, art. 17, IV).

6.14. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso (Lei nº 14.133, de 2021, art. 117, § 2º).

6.15. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato (Decreto estadual nº 68.220, de 2023, art. 17, II).

6.16. A fiscalização técnica do contrato deve avaliar constantemente a execução dos serviços através do Instrumento de Medição de Resultado (IMR), conforme previsto no Anexo A, para aferição da qualidade da prestação dos serviços, que poderá acarretar o redimensionamento no pagamento com base nos indicadores estabelecidos.

6.17. Durante a execução do objeto, fase do recebimento provisório, o fiscal técnico designado deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer ao Contratado a correção das faltas, falhas e irregularidades constatadas.

6.18. O fiscal técnico do contrato deverá apresentar ao preposto do Contratado a avaliação da execução do objeto ou, se for o caso, a avaliação de desempenho e qualidade da prestação dos serviços realizada.

6.19. O preposto deverá apor assinatura no documento, tomando ciência da avaliação realizada.

6.20. O Contratado poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pelo fiscal técnico, desde que comprovada a excepcionalidade da ocorrência, resultante exclusivamente de fatores imprevisíveis e alheios ao controle do prestador.

6.21. Na hipótese de comportamento contínuo de desconformidade da prestação do serviço em relação à qualidade exigida, bem como quando esta ultrapassar os níveis mínimos toleráveis previstos nos indicadores, além dos fatores redutores que sejam previstos na documentação que compõe a contratação, devem ser aplicadas as sanções ao Contratado de acordo com as regras previstas no ato convocatório.

6.22. É vedada a atribuição ao Contratado da avaliação de desempenho e qualidade da prestação dos serviços por ele realizada.

6.23. O fiscal técnico poderá realizar a avaliação diária, semanal ou mensal, desde que o período escolhido seja suficiente para avaliar ou, se for o caso, aferir o desempenho e qualidade da prestação dos serviços.

6.24. A fiscalização do contrato, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na

execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação contratual à produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos na Lei nº 14.133, de 2021 (Decreto estadual nº 68.220, de 2023, art. 17, parágrafo único, 6).

6.25. A conformidade do material/técnica/equipamento a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento do Contratado que contenha a relação detalhada destes, de acordo com o estabelecido neste Termo de Referência e na proposta, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso (art. 47, §2º, Instrução Normativa SEGES/MPDG nº 05, de 2017, c/c a Instrução Normativa SEGES/ME nº 98, de 2022, e o art. 1º, VII, do Decreto estadual nº 67.608, de 2023).

6.26. A fiscalização da execução dos serviços abrange, ainda, as seguintes rotinas constantes no Anexo E.

6.27. A fiscalização de que trata este item 6 não exclui nem reduz a responsabilidade do Contratado, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade do Contratante.

6.28. As disposições previstas neste Termo de Referência quanto à fiscalização técnica não excluem a incidência de outras regras da legislação que disciplina a fiscalização contratual.

6.29. Para efeito de recebimento provisório, ao final de cada período mensal, o fiscal técnico do contrato deverá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos no ato convocatório, que poderá resultar no redimensionamento de valores a serem pagos ao Contratado, registrando em relatório a ser encaminhado ao gestor do contrato.

Fiscalização Administrativa

6.30. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação do Contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Decreto estadual nº 68.220, de 2023, art. 18, II e III).

6.31. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência (Decreto estadual nº 68.220, de 2023, art. 18, IV).

6.32. A fiscalização administrativa poderá ser efetivada com base em critérios estatísticos, levando-se em consideração falhas que impactem o contrato como um todo e não apenas erros e falhas eventuais no pagamento de alguma vantagem a um determinado empregado.

6.33. Na fiscalização do cumprimento das obrigações trabalhistas e sociais exigir-se-á, dentre outras, as seguintes comprovações em relação aos empregados diretamente envolvidos na execução da contratação (os documentos poderão ser originais ou cópias autenticadas por cartório competente ou por servidor da Administração), no caso de Contratado que mantém vínculos regidos pela Consolidação das Leis do Trabalho (CLT):

6.33.1 no 1º (primeiro) mês da prestação dos serviços, o Contratado deverá apresentar a seguinte documentação:

6.33.1.1. relação dos empregados, contendo nome completo, cargo ou função, horário do posto de trabalho, número da inscrição no Cadastro de Pessoas Físicas (CPF), com indicação dos responsáveis técnicos pela execução dos serviços, quando for o caso;

6.33.1.2. Carteira de Trabalho e Previdência Social (CTPS) dos empregados admitidos e dos responsáveis técnicos pela execução dos serviços, quando for o caso, devidamente assinada pelo Contratado;

6.33.1.3. exames médicos admissionais dos empregados do Contratado que prestarão os serviços;

6.33.1.4. cópia de Acordo Coletivo, Convenção Coletiva de Trabalho ou Sentença Normativa vigentes, e, ao longo da vigência da contratação, do(s) instrumento(s) que o suceda(m); e

6.33.1.5. comprovação de capital social integralizado compatível com o número de empregados, na forma do art. 4º-B da Lei nº 6.019, de 1974;

6.33.2 até o dia 30 (trinta) do mês seguinte ao da prestação dos serviços (ou último dia do mês seguinte ao da prestação dos serviços, se não houver equivalente), o Contratado deverá entregar ao setor responsável pela fiscalização do contrato dos seguintes documentos, quando não for possível a verificação da regularidade destes no Sistema de Cadastramento Unificado de Fornecedores (Sicaf) ou em outros meios eletrônicos hábeis de informações:

6.33.2.1. Certidão Negativa, ou positiva com efeitos de negativa, de Débitos relativos a Créditos Tributários Federais e à Dívida Ativa da União;

6.33.2.2. Certidões que comprovem regularidade fiscal perante as Fazendas Estadual/Distrital e/ou Municipal/Distrital do domicílio ou sede do Contratado que tenham sido exigidas para fins de habilitação neste instrumento;

6.33.2.3. Certidão de Regularidade do Fundo de Garantia do Tempo de Serviço (CRF - FGTS); e

6.33.2.4. Certidão Negativa, ou positiva com efeitos de negativa, de Débitos Trabalhistas;

6.33.3 quando solicitado pelo Contratante e no prazo fixado, o Contratado deverá entregar ao setor responsável pela fiscalização da contratação os documentos comprobatórios do cumprimento das obrigações trabalhistas e com o Fundo de Garantia do Tempo de Serviço (FGTS) em relação a qualquer dos empregados diretamente envolvidos na execução da contratação, em especial quanto aos seguintes documentos, relativos a qualquer mês da prestação dos serviços (artigo 50 da Lei nº 14.133, de 2021):

6.33.3.1. extrato da conta do INSS e do FGTS do empregado;

6.33.3.2. cópia da folha de pagamento analítica, em que conste como tomador o Contratante;

6.33.3.3. cópia dos contracheques dos empregados ou, ainda, quando necessário, cópia de recibos de depósitos bancários;

6.33.3.4. comprovantes de entrega de benefícios suplementares (vale-transporte, vale-alimentação, entre outros) e de cumprimento de outras exigências a que estiver obrigado por força de lei, acordo, convenção ou dissídio coletivo de trabalho; e

6.33.3.5. comprovantes de realização de eventuais cursos de treinamento e reciclagem que forem exigidos por lei ou pelo contrato;

6.33.4 O Contratado deverá entregar ao setor responsável pela fiscalização da contratação cópia da documentação abaixo relacionada, quando da extinção do contrato, até 10 (dez) dias após o último mês de prestação dos serviços:

6.33.4.1. termos de rescisão dos contratos de trabalho dos empregados que realizaram o serviço, nos termos da legislação em vigor, ou documentação que comprove que os empregados serão realocados em outra atividade do Contratado sem extinção de seus contratos de

- trabalho;
- 6.33.4.2. documentação relativa à concessão de Aviso Prévio Trabalhado ou Indenizado, e ao pagamento de verbas rescisórias que forem devidas, referentes às rescisões contratuais, de forma a comprovar a quitação de obrigações trabalhistas e previdenciárias dos empregados dispensados;
- 6.33.4.3. guias de recolhimento da contribuição previdenciária e do FGTS, referentes às rescisões contratuais;
- 6.33.4.4. extratos dos depósitos efetuados nas contas vinculadas individuais do FGTS de cada empregado dispensado; e
- 6.33.4.5. exames médicos demissionais dos empregados dispensados.
- 6.34. Nas hipóteses de exigência de comprovações de que tratam as subdivisões anteriores, a não apresentação dos documentos solicitados pela fiscalização contratual no prazo por ela fixado acarretará a aplicação de multa ao Contratado, conforme previsto no instrumento da contratação (art. 50 da Lei nº 14.133, de 2021).
- 6.35. Sempre que houver admissão de novo empregado pelo Contratado, os documentos correspondentes aos exigidos no 1º (primeiro) mês da prestação dos serviços conforme esta seção deverão ser apresentados em relação a cada novo empregado. O desligamento de empregados no curso do contrato administrativo deve ser devidamente comunicado ao Contratante, com a apresentação pelo Contratado de toda a documentação pertinente ao empregado dispensado, à semelhança do que se exige quando do encerramento do contrato administrativo.
- 6.36. O Contratante deverá analisar a documentação exigida por ocasião da extinção da contratação conforme esta seção no prazo de 30 (trinta) dias após o recebimento dos documentos, prorrogáveis por mais 30 (trinta) dias, justificadamente.
- 6.37. A cada período de 12 (doze) meses de vigência do contrato de trabalho, o Contratado deverá encaminhar termo de quitação anual das obrigações trabalhistas, na forma do art. 507-B da CLT, ou comprovar a tentativa de sua obtenção, relativamente aos empregados alocados em dedicação exclusiva, na prestação de serviços contratados, observando-se as seguintes disposições:
- 6.37.1 O termo de quitação anual efetivado deverá ser firmado junto ao respectivo Sindicato dos Empregados e obedecerá ao disposto no art. 507-B, parágrafo único, da CLT;
- 6.37.2 Para fins de comprovação da tentativa a que se refere a subdivisão anterior, será aceito qualquer meio de prova, tais como: recibo de convocação, declaração de negativa de negociação, ata de negociação, dentre outros;
- 6.37.3 Não haverá pagamento adicional pelo Contratante ao Contratado em razão do cumprimento das obrigações previstas na subdivisão anterior.
- 6.38. No caso de entidades diversas, será exigida a comprovação de atendimento a eventuais obrigações decorrentes da legislação que rege as respectivas organizações.
- 6.39. Os documentos necessários à comprovação do cumprimento das obrigações sociais e trabalhistas poderão ser apresentados em original ou por qualquer processo de cópia autenticada por cartório competente ou por servidor da Administração.
- 6.40. Em caso de indício de irregularidade no recolhimento das contribuições previdenciárias, o Contratante oficiará à Receita Federal do Brasil (RFB).
- 6.41. Em caso de indício de irregularidade no recolhimento da contribuição para o FGTS, o Contratante oficiará ao Ministério do Trabalho e Emprego.
- 6.42. O descumprimento total ou parcial das obrigações e responsabilidades assumidas pelo Contratado, incluindo o descumprimento das obrigações trabalhistas, não recolhimento das contribuições sociais, previdenciárias ou para com o FGTS, ou a não manutenção das condições de habilitação pelo Contratado, ensejará a aplicação de sanções administrativas, previstas no instrumento da contratação e na legislação vigente, podendo culminar em extinção contratual, por ato unilateral e escrito do Contratante, com base nos arts. 50 e 121 da Lei nº 14.133, de 2021.
- 6.42.1 O Contratante adotará as medidas cabíveis para assegurar o cumprimento das obrigações trabalhistas e demais obrigações contratuais pelo Contratado sempre que identificar descumprimento, inclusive quando for cientificado dessa circunstância por meio do recebimento de notificação formal enviada por trabalhador, sindicato, Ministério do Trabalho, Ministério Público, Defensoria Pública ou outro meio idôneo.
- 6.43. Caso não seja apresentada a documentação comprobatória do cumprimento das obrigações trabalhistas, previdenciárias e para com o FGTS, o Contratante comunicará o fato ao Contratado e reterá o pagamento da fatura mensal, até que a situação seja regularizada (art. 121, § 3º, inciso II, da Lei nº 14.133, de 2021).
- 6.43.1 Não havendo quitação das verbas trabalhistas por parte do Contratado no prazo de 15 (quinze) dias, o Contratante poderá efetuar o pagamento das verbas trabalhistas diretamente aos empregados do Contratado que tenham participado da execução dos serviços objeto do contrato, que serão deduzidas do pagamento devido ao Contratado.
- 6.43.1.1. O sindicato representante da categoria do trabalhador deverá ser notificado pelo Contratante para acompanhar o pagamento das verbas mencionadas na subdivisão acima.
- 6.43.1.2. Os pagamentos das verbas trabalhistas diretamente aos empregados do Contratado não configuram vínculo empregatício, tampouco implicam a assunção de responsabilidade pelo Contratante em relação aos empregados do Contratado por quaisquer obrigações dele decorrentes.
- 6.44. O contrato só será considerado integralmente cumprido após a comprovação, pelo Contratado, do pagamento de todas as obrigações trabalhistas, sociais, previdenciárias e para com o FGTS referentes à mão de obra alocada em sua execução, inclusive quanto às verbas rescisórias.
- 6.45. O Contratado é responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato.
- 6.46. A inadimplência do Contratado quanto aos encargos trabalhistas, fiscais e comerciais não transfere à Administração Pública a responsabilidade por seu pagamento.
- 6.47. Sempre que solicitado pelo Contratante, o Contratado deverá comprovar o cumprimento da reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas em outras normas específicas, com a indicação dos empregados que preencherem as referidas vagas, nos termos do parágrafo único do art. 116 da Lei nº 14.133, de 2021.
- 6.48. As disposições previstas neste Termo de Referência quanto à fiscalização administrativa não excluem a incidência de outras regras da legislação que disciplina a fiscalização contratual.

6.49. Para efeito de recebimento provisório, ao final de cada período mensal, o fiscal administrativo deverá verificar a efetiva realização dos dispêndios concernentes aos salários e às obrigações trabalhistas, previdenciárias e com o FGTS do mês anterior, dentre outros, emitindo relatório que será encaminhado ao gestor do contrato.

Gestor do Contrato

6.50. O gestor do contrato exercerá a atividade de coordenação dos atos de fiscalização técnica, administrativa e setorial e dos atos preparatórios à instrução processual visando, entre outros, à prorrogação, à alteração, ao reequilíbrio, ao pagamento, à eventual aplicação de sanções e extinção do contrato (Decreto estadual nº 68.220, de 2023, inciso III do art. 2º).

6.51. O gestor do contrato acompanhará a manutenção das condições de habilitação do Contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais (Decreto estadual nº 68.220, de 2023, art. 16, inciso IX).

6.52. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações (Decreto estadual nº 68.220, de 2023, art. 16, inciso VI).

6.53. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso (Decreto estadual nº 68.220, de 2023, art. 16, inciso VIII).

6.54. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração (Decreto estadual nº 68.220, de 2023, art. 16, inciso VII e parágrafo único).

6.55. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

7. Critérios de medição e pagamento

7.1. A avaliação da execução do objeto se dará por avaliação dos relatórios de serviço mensais que deverão ser encaminhados pela contratada, o qual observará o disposto nesta seção.

7.1.1. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratado:

7.1.1.1. não produzir os resultados acordados,

7.1.1.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

7.1.1.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

7.2. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

7.3. A aferição da execução contratual para fins de pagamento considerará os seguintes critérios:

7.3.1. Cronograma de visitas programadas e visitas corretivas (Relatório mensal de Manutenções Preventivas e Corretivas);

7.3.2. Relatório englobando todas as ordens de serviços corretivas e visitas programadas para cada manutenção executada;

Do recebimento

7.4. Os serviços serão recebidos provisoriamente, no prazo de 05 (cinco) dias, pelo(s) fiscal(is) técnico e administrativo, mediante termo (s) detalhado(s), quando verificado o cumprimento das exigências de caráter técnico e administrativo (Art. 140, I, 'a', da Lei nº 14.133, de 2021, e arts. 17, X, e 18, VI, do Decreto estadual nº 68.220, de 2023).

7.5. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do Contratado com a comprovação da prestação dos serviços a que se refere a parcela a ser paga.

7.6. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico (Art. 17, X, Decreto estadual nº 68.220, de 2023).

7.7. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo (Art. 18, VI, Decreto estadual nº 68.220, de 2023).

7.8. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

7.9. Para efeito de recebimento provisório, ao final de cada período de faturamento, que observará a periodicidade mensal:

7.9.1 o fiscal técnico do contrato deverá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos no ato convocatório, que poderá resultar no redimensionamento de valores a serem pagos ao Contratado, registrando em relatório a ser encaminhado ao gestor do contrato;

7.9.2 o fiscal administrativo deverá verificar a efetiva realização dos dispêndios concernentes aos salários e às obrigações trabalhistas, previdenciárias e com o FGTS do mês anterior, dentre outros, emitindo relatório que será encaminhado ao gestor do contrato.

7.10. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último.

7.11. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

- 7.12. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório (Art. 119 c/c art. 140 da Lei nº 14133, de 2021).
- 7.13. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.
- 7.14. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades cabíveis.
- 7.15. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.
- 7.16. Os serviços serão recebidos definitivamente no prazo de 03 (três) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:
- 7.16.1 Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (Decreto estadual nº 68.220, de 2023, art. 16, inciso VI);
- 7.16.2 Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando ao Contratado, por escrito, as respectivas correções;
- 7.16.3 Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas;
- 7.16.4 Comunicar ao Contratado para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização; e
- 7.16.5 Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.
- 7.17. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, se houver parcela incontroversa, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, com a comunicação ao Contratado para emissão de Nota Fiscal no que pertine à parcela incontroversa, para efeito de liquidação e pagamento.
- 7.18. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo Contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.
- 7.19. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

Liquidação

- 7.20. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 10 (dez) dias úteis para fins de liquidação, a contar de seu recebimento pela Administração, na forma desta seção, prorrogáveis por igual período, justificadamente, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais (art. 7º, I, e §§ 2º e 3º, da Instrução Normativa SEGES/ME nº 77, de 4 de novembro de 2022, c/c o Decreto estadual nº 67.608, de 2023).
- 7.20.1 O prazo de que trata a subdivisão acima será reduzido à metade, mantendo-se a possibilidade de prorrogação nele especificada, no caso de contratação decorrente de despesa cujo valor não ultrapasse o limite de que trata o inciso II do caput do art. 75 da Lei nº 14.133, de 2021.
- 7.21. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como, caso aplicáveis:
- a) o prazo de validade;
 - b) a data da emissão;
 - c) os dados do contrato e do órgão contratante;
 - d) o período respectivo de execução do contrato;
 - e) o valor a pagar; e
 - f) eventual destaque do valor de retenções tributárias cabíveis.
- 7.22. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante.
- 7.23. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao Sicaf ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.
- 7.24. A Administração deverá realizar consulta ao Sicaf para: a) verificar a manutenção das condições de habilitação exigidas; b) identificar possível razão que impeça a contratação, no âmbito do órgão ou entidade, tais como a proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (Instrução Normativa SEGES/MPDG nº 3, de 26 de abril de 2018 c/c Decreto estadual nº 67.608, de 2023).
- 7.25. Constatando-se, junto ao Sicaf, a situação de irregularidade do Contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do Contratante.
- 7.26. Não havendo regularização ou sendo a defesa considerada improcedente, o Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do Contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.
- 7.27. Persistindo a irregularidade, o Contratante deverá adotar as medidas necessárias à extinção contratual nos autos do processo administrativo correspondente, assegurada ao Contratado a ampla defesa.
- 7.28. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela extinção do

contrato, caso o Contratado não regularize sua situação junto ao Sicaf.

Prazo de pagamento

7.29. O pagamento será efetuado no prazo de 30 (trinta) dias, contados da apresentação da nota fiscal ou documento de cobrança equivalente, desde que tenha sido finalizada a liquidação da despesa, conforme seção anterior, nos termos do art. 2º, II, do Decreto estadual nº 67.608, de 2023.

7.30. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente na forma da legislação aplicável (art. 2º, inciso III, do Decreto estadual nº 67.608, de 2023, c/c o art. 1º do Decreto estadual nº 32.117, de 1990), bem como incidirão juros moratórios, a razão de 0,5% (meio por cento) ao mês, calculados pro rata temporis, em relação ao atraso verificado.

Forma de pagamento

7.31. O pagamento será realizado por meio de ordem bancária, para depósito em conta corrente bancária em nome do Contratado no Banco do Brasil S/A.

7.31.1 Constitui condição para a realização dos pagamentos a inexistência de registros em nome do Contratado no “Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais– Cadin estadual”, de que trata a Lei estadual nº 12.799, de 2008, o qual deverá ser consultado por ocasião da realização de cada pagamento. O cumprimento desta condição poderá se dar pela comprovação, pelo Contratado, de que os registros estão suspensos, nos termos do art. 8º da Lei estadual nº 12.799, de 2008.

7.32. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

7.33. O Contratante poderá, por ocasião do pagamento, efetuar a retenção de tributos determinada por lei, ainda que não haja indicação de retenção na nota fiscal apresentada ou que se refira a retenções não realizadas em meses anteriores.

7.33.1 Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

7.34. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

8. Forma e critérios de seleção e regime

Forma de seleção e critério de julgamento da proposta

8.1. O fornecedor será selecionado por meio da realização de procedimento de licitação, na forma eletrônica, com fundamento na hipótese do art. 28, caput, inciso I da Lei nº 14.133, de 2021, que culminará com a seleção da proposta de MENOR PREÇO POR ITEM.

Regime de execução

8.2. O regime de execução do contrato será de empreitada por preço unitário.

Exigências de habilitação

8.3. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos das seções subsequentes deste item 8, que serão exigidos conforme sua natureza jurídica:

Habilitação jurídica

8.4. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

8.5. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

8.6. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

8.7. Sociedade empresária: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

8.8. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME nº 77, de 18 de março de 2020;

8.9. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

8.10. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

8.11. Ato de autorização para o exercício da atividade, expedido pelo órgão competente, quando a atividade assim o exigir.

8.12. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

8.13. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

8.14. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela

Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente aos créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

8.15. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

8.16. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

8.17. Prova de inscrição no cadastro de contribuintes Estadual/Distrital e/ou Municipal/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

8.18. Prova de regularidade com a Fazenda Estadual/Distrital [quanto ao Imposto sobre operações relativas à Circulação de Mercadorias e sobre prestações de Serviços de transporte interestadual e intermunicipal e de comunicação - ICMS, e,] nos termos da Lei Complementar nº 214, de 2025, quanto ao Imposto sobre Bens e Serviços – IBS, e/ou de regularidade com a Fazenda Municipal/Distrital quanto ao Imposto sobre Serviços de Qualquer Natureza - ISSQN, do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

8.19. Caso o fornecedor se considere isento ou imune de tributos relacionados ao objeto contratual, em relação aos quais seja exigida regularidade fiscal neste instrumento, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

8.20. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar nº 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

8.21. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021 c/c Decreto estadual nº 67.608, de 2023), ou de sociedade simples;

8.22. Certidão negativa de falência, expedida pelo distribuidor da sede do fornecedor, caso se trate de empresário individual ou sociedade empresária;

8.23. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

a) Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

b) Capital Circulante Líquido ou Capital de Giro (Ativo Circulante - Passivo Circulante) de, no mínimo, 16,66% (dezesesseis inteiros e sessenta e seis centésimos por cento) do valor estimado da contratação;

c) Patrimônio líquido mínimo de 10% (dez por cento) do valor estimado da contratação.

8.23.1 As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

8.23.2 Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

8.23.3 Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped, quando for o caso, ou outro limite estabelecido pela legislação aplicável.

8.24. Declaração do licitante, acompanhada da relação de compromissos assumidos, conforme modelo constante em anexo, de que um doze avos dos contratos firmados com a Administração Pública e/ou com a iniciativa privada vigentes na data da apresentação da proposta não é superior ao patrimônio líquido do licitante, observados os seguintes requisitos:

a) A declaração deve ser acompanhada da Demonstração do Resultado do Exercício (DRE), relativa ao último exercício social; e

b) Caso a diferença entre a declaração e a receita bruta discriminada na Demonstração do Resultado do Exercício (DRE) apresentada seja superior a 10% (dez por cento), para mais ou para menos, o licitante deverá apresentar justificativas.

8.24.1 As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura (Lei nº 14.133, de 2021, art. 65, §1º).

8.25. O atendimento dos índices econômicos previstos nesta seção deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

Qualificação Técnica

8.26. Declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação, assegurado a ele o direito de realização de vistoria prévia;

8.26.1 A declaração acima poderá ser substituída por declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação;

8.27. Registro ou inscrição do licitante na entidade profissional, em plena validade;

8.27.1 Sociedades empresárias estrangeiras atenderão à exigência prevista na subdivisão acima por meio da apresentação, no momento da celebração da contratação, da solicitação de registro perante a entidade profissional competente no Brasil;

8.28. Prova de atendimento aos requisitos abaixo, previstos na Lei.

Qualificação Técnico-Operacional

8.28. Comprovação de capacidade operacional para execução de serviço similar de complexidade tecnológica e operacional equivalente ou superior ao objeto desta contratação, ou ao item pertinente, por meio da apresentação de certidão(ões) ou atestado(s), fornecido(s) por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

8.28.1 Para fins da comprovação de que trata a subdivisão acima, o(s) atestado(s) ou certidão(ões) deverá(ão) dizer respeito a contrato(s) executado(s) com a(s) seguinte(s) característica(s) mínima(s):

- 8.28.1.1. Deverá haver a comprovação da experiência mínima de 12 (doze) meses na prestação de serviços similares, sendo aceito o somatório de atestados ou certidões de períodos diferentes, não havendo obrigatoriedade de os meses serem ininterruptos;
- 8.28.1.2. Comprovação de que já executou contrato(s) similar envolvendo operação contínua, prestação de serviços dedicados e atendimento a níveis de serviço (SLA), com remuneração mensal baseada em entrega de serviços, e demonstrada a capacidade técnica compatível com o escopo a ser contratado.
- 8.28.1.3. Deverá ainda comprovar a prestação de fornecimento dos seguintes itens previstos no Estudo Técnico Preliminar:
- a) 25% dos ativos de EDR/XDR;
 - b) 50% de infraestrutura para o módulo de APM;
 - c) 50% do módulo de NPM;
 - d) 50% do módulo de NPB;
 - e) 25% para o módulo de gerência e monitoramento (Zabbix/Grafana);
 - f) 20% do módulo de Sistemas de Log (Syslog);
 - g) 30% do módulo de Gestão e Correlação de Eventos (SIEM);
 - h) módulo de Threat Intelligence (Osint).
- 8.28.1.4. Será admitida, para fins de comprovação de quantitativo mínimo de serviço similar, a apresentação de diferentes atestados de comprovem serviços executados.
- 8.28.1.5. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.
- 8.29 O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade do(s) atestado(s), apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.
- 8.30. O SOC deverá, obrigatoriamente, estar fisicamente localizado em território nacional brasileiro;
- 8.31. Não será admitido que a solução de nuvem/cloud/SaaS adotada, que esteja hospeda fora do território nacional brasileiro.

Qualificação Técnico-Profissional

8.32. Apresentação da declaração formal da licitante que possui o(s) profissional(is) abaixo, com as respectivas certificações e experiências previstas no Estudo Técnico Preliminar, detentor(es) de atestado de responsabilidade técnica por execução de serviço(s) de características abaixo:

8.32.1. 01 (um) Especialista em Cloud - Arquiteto de solução;

8.32.2. 01 (um) Analista de sistemas operacionais Windows (Sênior);

8.32.3. 01 (um) Analista de sistemas operacionais Linux (Sênior);

8.32.4. 01 (um) Administrador de Banco de Dados (DBA);

8.32.5. 01 (um) Administrador Notes (Sênior);

8.32.6. 01 (um) Analista de redes (N3);

8.32.7. 01 (um) Administrador em Segurança da Informação (Threat Hunting).

8.32.8. As certificações mencionadas no Estudo Técnico Preliminar são obrigatórias, ou seja, somente serão aceitos profissionais que as possuam, não sendo aceitos aqueles que possuem apenas comprovação da experiência nos conhecimentos e atividades que elas comportam.

8.32.9. Deverá ser apresentada a comprovação de experiência exigidas conforme a função, bem como certificações em até 30 (trinta) dias após a assinatura do contrato.

8.33.1 O(s) profissional(is) indicado(s) na forma da subdivisão acima deverá(ão) participar do serviço objeto do contrato, e será admitida a sua substituição por profissional(is) de experiência equivalente ou superior, desde que aprovada pela Administração (§ 6º do art. 67 da Lei nº 14.133, de 2021).

8.33.2 Por ocasião do início da execução da contratação, a comprovação do vínculo do(s) profissional(is) a que se refere a subdivisão anterior poderá se dar mediante a apresentação de contrato de trabalho, de anotações da CTPS – Carteira de Trabalho e Previdência Social, ou, no caso de prestador de serviços autônomo, do respectivo contrato de prestação de serviços, ou, no caso de sócio(s), de cópia do contrato social atualizado.

8.33.3 Deve o fornecedor apresentar relação dos compromissos assumidos que importem em diminuição da disponibilidade do pessoal técnico indicado na subdivisão anterior.

8.33.4 Não serão admitidos atestados de responsabilidade técnica de profissionais que, na forma de regulamento, tenham dado causa à aplicação das sanções previstas nos incisos III e IV do caput do art. 156 da Lei nº 14.133, de 2021, em decorrência de orientação proposta, de prescrição técnica ou de qualquer ato profissional de sua responsabilidade.

Outras comprovações

8.34. Declaração subscrita por representante legal do licitante, atestando que:

- a) cumpre as normas relativas à saúde e segurança no trabalho, nos termos do art. 117, parágrafo único, da Constituição Estadual;
- b) atenderá, na data da contratação, ao disposto no art. 5º-C e se compromete a não disponibilizar empregado que incorra na vedação

prevista no art. 5º-D, ambos da Lei nº 6.019, de 1974, com redação dada pela Lei nº 13.467, de 2017, quando o caso;

8.35. Tratando-se de consórcio:

8.35.1 Apresentação do compromisso público ou particular de constituição do consórcio, subscrito pelos consorciados, o qual deverá incluir, pelo menos, os seguintes elementos:

- a) Designação do consórcio e sua composição;
- b) Finalidade do consórcio;
- c) Prazo de duração do consórcio, que deve coincidir, no mínimo, com o prazo de vigência contratual;
- d) Endereço do consórcio e o foro competente para dirimir eventuais demandas entre os consorciados;
- e) Definição das obrigações e responsabilidades de cada consorciado e das prestações específicas;
- f) Previsão de responsabilidade solidária de todos os consorciados pelos atos praticados pelo consórcio, tanto na fase de licitação quanto na de execução do contrato, abrangendo também os encargos fiscais, trabalhistas e administrativos referentes ao objeto da contratação;
- g) Indicação da empresa líder do consórcio e seu respectivo representante legal, que deverá ter poderes para receber citação, interpor e desistir de recursos, firmar a contratação e praticar todos os demais atos necessários à participação na licitação e execução do objeto contratado, sendo responsável pela representação do consórcio perante a Administração;
- h) Compromisso subscrito pelas consorciadas de que o consórcio não terá a sua composição modificada sem a prévia e expressa anuência do Contratante até o integral cumprimento do objeto da contratação, observado o prazo de duração do consórcio, definido na alínea "c" desta subdivisão.

8.35.2 O fornecedor vencedor é obrigado a promover, antes da celebração da contratação, a constituição e o registro do consórcio, nos termos de seu compromisso de constituição.

8.35.3 Cada consorciado, individualmente, deverá atender as exigências relativas a habilitação jurídica e habilitação fiscal, social e trabalhista, e a certidão negativa de falência/insolvência. Para efeito de habilitação econômico-financeira e de habilitação técnica, quando exigida, será observado o disposto no inciso III do caput do art. 15 da Lei nº 14.133, de 2021.

8.35.4 A inabilitação de qualquer consorciado acarretará a automática inabilitação do consórcio.

8.48. Deverá ser apresentada autodeclaração de aderência e adequação a LGPD (Lei Geral de Proteção de Dados Pessoais) e ESG (Environmental, Social and Governance).

9. Estimativas do valor da contratação

[Conteúdo Sigiloso | Justificativa: A justificativa para manter o sigilo da estimativa de custo total da contratação no TR está prevista no art. 24 da Lei nº 14.133/2021, que permite o sigilo do orçamento estimado quando houver fundamentação técnica. O objetivo é preservar a competitividade e evitar que os licitantes ajustem suas propostas ao valor previamente divulgado, o que poderia comprometer a obtenção da proposta mais vantajosa para a PMESP.]

10. Adequação orçamentária

10.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento do Estado.

10.2. No presente exercício, a contratação será atendida pela seguinte dotação:

I) Gestão/Unidade: DTIC – Diretoria de Tecnologia da Informação e Comunicação;

II) Fonte de Recursos: 10010001;

III) Programa de Trabalho: 180433;

IV) Elemento de Despesa: 339039;

V) Plano Interno: Plano de Comando 2024 - 2031 Versão nº 1 e Decreto nº 68.828 de 04Set24.

10.3. Quando a execução do contrato ultrapassar o presente exercício, a dotação relativa ao(s) exercício(s) financeiro(s) subsequente(s) será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

11. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

MARCELO FUMIO TAMASHIRO

Equipe de apoio



Assinou eletronicamente em 09/04/2026 às 17:06:14.

ESP-DIRETORIA TEC. INFORMACAO E COMUNICACAO

Estudo Técnico Preliminar 121/2025**1. Informações Básicas**

Número do processo: 057.00495038/2025-41

2. Descrição da necessidade

- 2.1. O Estudo Técnico Preliminar – ETP é o documento constitutivo da primeira etapa do planejamento de uma contratação, que caracteriza o interesse público envolvido e a sua melhor solução. Ele serve de base para elaboração do Termo de Referência, caso se conclua pela viabilidade da contratação. Além da definição das seguintes tarefas:
- 2.1.1. definição e especificação das necessidades de negócio e tecnológicas, e dos requisitos necessários e suficientes à escolha da solução de TIC, contendo de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo, o quantitativo de bens e serviços necessários para a sua composição;
- 2.1.2. análise comparativa de soluções, que deve considerar, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.
- 2.2. O objetivo do Estudo Técnico Preliminar é mapear e avaliar os cenários possíveis para o atender à demanda apresentada no Documento de Oficialização da Demanda, além de comprovar a viabilidade técnica e econômica das soluções propostas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.
- 2.3. A Polícia Militar do Estado de São Paulo - PMESP, integrante da administração direta da Secretaria da Segurança Pública necessita da contratação de serviços especializados técnicos de suporte de cibersegurança, data center e redes, bem como de governança, gerenciamento e monitoramento, das demandas e mudanças de tecnologia da informação e comunicação e infraestrutura de data center e redes para ambiente computacional e de telecomunicações, de forma a garantir a continuidade dos serviços de TIC.
- 2.4. Este estudo técnico preliminar tem como objetivo definir os requisitos e especificações para a contratação de serviços especializados em cibersegurança, data center e redes, com monitoramentopor meio de SOC – Security Operation Center, do NOC – Network Operations Center e SO - Setor Operacional. Recomenda-se que os serviços sejam planejados com integração operacional entre SOC e NOC, promovendo sinergia entre segurança e desempenho da rede e ambiente computacional, para melhorar os tempos de detecção e resposta, preservando a integridade, disponibilidade e confiabilidade. O acompanhamento das operações será realizado pela Diretoria de Tecnologia da Informação e Comunicação - DTIC.
- 2.5. Os serviços de SOC e NOC serão prestados remotamente de forma ininterrupta, garantindo a observabilidade contínua e a capacidade de resposta imediata a potenciais ameaças, ataques cibernéticos e tentativas de invasão. Para isso, a contratada deverá adotar soluções amplamente reconhecidas e estáveis para ambientes de missão crítica, como ferramentas essenciais para operações de SOC e NOC modernas, permitindo a implementação de um ecossistema SIEM / Syslog com visibilidade, automação de resposta e análise forense integrada.
- 2.6. Para ampliar a eficácia do SOC e NOC e reduzir o tempo de resposta a incidentes, é essencial a adoção de tecnologias de orquestração e reposta automatizada. Complementarmente, a adoção escalonada de acordo com o nível de maturidade e capacidade da contratante, de uma arquitetura baseada de Data Center Baseada em XDR (Extended Detection and Response) que fornece visibilidade unificada sobre múltiplos domínios (endpoing, rede, e-mail, identidade), permitindo uma análise contextualizada e proativa das ameaças, com alta eficiência na detecção de ataques avançados, como APTs.
- 2.7. Os Serviços de Gerenciamento, Detecção e Resposta reforçam a capacidade de prevenção e exploração de ataques em conjunto com o uso de tecnologias de EDR e XDR atuando de forma adjacente as atividades do SOC, e trará mais eficiência para a proteção continuada do ambiente tecnológico da PMESP.
- 2.8. A principal vantagem do XDR está na correlação temporal automatizada de eventos em diferentes domínios (endpoint, rede, identidade, e-mail, aplicação). Essa funcionalidade permite montar uma linha do tempo unificada do ataque, desde a intrusão inicial até a movimentação lateral, facilitando a investigação, resposta e documentação forense de incidentes. Trata-se de uma capacidade indispensável para ambientes de missão crítica, como o da PMESP, principalmente com foco no 190/193, cabe a Contratante em conjunto, maturação do tempo de implantação e ampliação devida a característica computacional existente.
- 2.9. A sinergia entre SIEM/Syslog e XDR/EDR promove uma operação cibernética mais eficiente, com alto grau de automação, rastreabilidade e capacidade de resposta, alinhando-se ao modelo Zero Trust.
- 2.10. A integração entre SIEM (correlação e centralização de logs), EDR (detecção em endpoints) e XDR (correlação multidomínio) é o alicerce da segurança moderna. A arquitetura proposta deve permitir:
- 2.10.1. Envio automatizado de alertas do EDR para o SIEM;
- 2.10.2. Execução de playbooks como isolamento de máquina, revogação de token, abertura de ticket no ITSM;
- 2.10.3. Visualização centralizada de todo o ataque com detalhamento técnico, evidência e tempo de execução.
- 2.11. Os serviços de SOC, deve com auxílio da ferramenta OSINT, realizar a análise, coleta automatizada, correlação e visualização dos dados, visando o propósito de apoiar as investigações de ameaça cibernéticas, testes de penetração, monitoramento de exposição digital e defesa proativa de ativos, observando os princípios legais e éticos aplicáveis.
- 2.12. Os serviços solução WebSec no ambiente de produção DevOps é fundamental para mitigar os riscos decorrentes da entrega acelerada de software

em ciclos ágeis, onde a segurança muitas vezes é sacrificada em prol da velocidade e prazo. No contexto DevSecOps, a integração da WebSec aos pipelines CI/CD possibilita a identificação precoce de vulnerabilidades, minimizando a exposição de aplicações críticas a ataques cibernéticos, como injeções de código ou exploração de APIs, alinhados com a fábrica de software que realiza testes nas aplicações. Já no âmbito do SOC, a solução proporciona visibilidade contínua e resposta automatizada a ameaças em tempo real, atendendo à necessidade de proteção proativa contra superfícies de ataque ampliadas por tecnologias modernas, e reforça a resiliência organizacional diante do crescente volume de incidentes cibernéticos.

2.13. Sem o emprego de uma ferramenta WebSec, vulnerabilidades podem permanecer ocultas em ambientes de produção, comprometendo dados sensíveis, a continuidade dos serviços e a reputação institucional. A combinação de análise dinâmica, alertas em tempo real e integração com sistemas SIEM torna-se indispensável para que o SOC opere com eficácia, reduzindo significativamente o tempo de resposta a incidentes e os custos associados à remediação tardia.

2.14. Já os serviços de NOC são essenciais para garantir a disponibilidade, o desempenho e a continuidade dos ambientes tecnológicos, atuando como a central de operação responsável pelo monitoramento, detecção e gestão proativa de incidentes de infraestrutura e rede. Com o apoio integrado de ferramentas de APM (Application Performance Monitoring), NPM (Network Performance Monitoring), NPB (Network Packet Broker) e ITSM (IT Service Management), o NOC passa a contar com recursos avançados para coleta automatizada, análise contínua e correlação inteligente de indicadores de desempenho, permitindo uma gestão holística dos ativos críticos. Essa combinação possibilita visibilidade abrangente da saúde dos serviços, aplicações e redes, garantindo respostas mais rápidas e eficazes aos eventos que possam impactar os usuários e as operações corporativas, sempre observando as melhores práticas operacionais e de governança.

2.15. A implementação de soluções de APM, NPM e NPB no ambiente de produção permite que o NOC identifique, em tempo real, gargalos, falhas de conectividade, degradação de serviços e anomalias que possam comprometer a experiência do usuário ou o funcionamento de sistemas essenciais. O APM assegura o monitoramento profundo de aplicações, rastreando transações, dependências e desempenho; o NPM monitora a estabilidade, latência e capacidade da rede; e o NPB organiza, filtra e distribui tráfego para ferramentas de análise, garantindo precisão e eficiência no tratamento dos dados. Em conjunto, essas tecnologias criam uma camada essencial de observabilidade, fortalecendo a operação contínua de TI em ambientes modernos e distribuídos.

2.16. A integração do NOC com uma plataforma ITSM, no caso da PMESP atualmente implantado a solução da Cherwel que torna os processos mais estruturados, possibilitando que incidentes, problemas, mudanças e solicitações sejam tratados de forma padronizada, auditável e com rastreabilidade completa. Essa sinergia permite que o NOC opere com maior maturidade operacional, reduzindo o tempo médio de detecção (MTTD) e o tempo médio de resolução (MTTR), além de promover uma comunicação mais eficiente entre equipes multidisciplinares. No contexto organizacional, tal integração garante alinhamento com práticas de governança, continuidade de negócios e conformidade exigidas por auditorias e marcos regulatórios.

2.17. Sem o emprego adequado dessas ferramentas, falhas críticas podem permanecer ocultas na infraestrutura ou nos serviços, gerando indisponibilidade, prejuízos à imagem institucional e interrupções prolongadas das operações, principalmente do 190 e 193. A combinação de monitoramento contínuo, análise contextualizada de desempenho e automatização de processos torna-se indispensável para que o NOC opere com eficácia, reduzindo significativamente o risco de interrupções e assegurando que os serviços tecnológicos da organização mantenham os níveis de confiabilidade e desempenho esperados.

2.18. A implementação de um SOC e NOC para órgãos públicos como a PMESP envolve desafios estruturais como escopo mal definido, excesso de ruído em logs e dificuldade na integração entre sistemas legados e modernos. Para mitigar esses problemas, recomenda-se a definição clara dos objetivos do SOC e NOC, o mapeamento de ativos críticos e o uso de modelos de arquitetura de cibersegurança, que orientam desde a identificação de riscos até a recuperação de eventos adversos. Esses elementos são cruciais para garantir a efetividade, sustentabilidade e escalabilidade da operação.

2.19. A prestação dos serviços deve contar a expertise em utilizar a ferramenta DAST (Dynamic Application Security Testing), que emprega análise dinâmica de código para identificar problemas em tempo de execução, incluindo vulnerabilidades que permanecem invisíveis quando o programa não está ativo, representando uma de suas principais vantagens. Além disso, o DAST avalia o comportamento real de um aplicativo diante de um ataque, oferecendo insights valiosos sobre a probabilidade de exploração de uma vulnerabilidade.

2.20. Complementarmente, a Contratada deverá também ter know how em solução de SAST (Static Application Security Testing) integrada ao modelo DevSecOps, garantindo que o pipeline da fábrica de software incorpore inspeções de segurança desde as primeiras etapas do desenvolvimento, na qual ocorre em contrato distinto no Departamento de Aplicações e Sistemas. A saber, a solução SAST deverá executar análises estáticas de código-fonte de forma automatizada nos pipelines de CI/CD, identificando vulnerabilidades estruturais, más práticas de programação e falhas de segurança antes da execução do software. Além disso, o serviço deverá integrar-se ao contrato vigente da outra Fábrica de Software, permitindo que os pipelines, repositórios, controles de qualidade e fluxos de desenvolvimento já estabelecidos sejam estendidos para incluir verificações de segurança contínuas. Essa integração deverá possibilitar gatilhos automáticos, geração de relatórios unificados, bloqueio de builds vulneráveis e visibilidade centralizada para equipes de desenvolvimento, segurança e operações, sem a necessidade de rupturas de processo ou duplicidade de ferramentas.

2.21. A Contratada deverá conhecer a solução de segurança dinâmica para aplicações web (WebSec) que combine funcionalidades de Dynamic Application Security Testing – DAST com capacidades avançadas de monitoramento contínuo, detecção automatizada de vulnerabilidades e integração com o ecossistema de um Centro de Operações de Segurança (SOC) e pipelines DevOps, visando proteger aplicações críticas, APIs e superfícies de exposição web em tempo real.

2.22. A prestação dos serviços seguirá um modelo de serviço continuado, com possibilidade de escalabilidade sob demanda e com dedicação exclusiva, que além dos serviços remotos de SOC e NOC, contará com uma equipe alocada no Departamento de Aplicações e Sistemas - DAS, e no SO, que deverá estar integrada com o SOC e NOC, com possibilidade de unificação.

2.23. A contratação será realizada por meio de licitação, respeitando os princípios da economicidade, eficiência e escalabilidade, conforme a Lei 14.133/2021, direcionadas e instruídas por normas, como a 94 de 23 de dezembro de 2022 da SGD/ME. Recomendam-se exigências técnicas mínimas como: experiência prévia em ambientes militares ou órgãos de segurança pública, comprovação de operação de SOC/NOC em regime 24x7, e uso de ferramentas compatíveis com padrões internacionais como ISO/IEC 27.001, ISO/IEC 20.000, NIST, MITRE ATT&CK e CIS Controls, e a empresa especializada será responsável por fornecer suporte técnico e operacional, garantindo a continuidade dos serviços de Tecnologia da Informação e Comunicação (TIC) e a segurança do ambiente computacional e de telecomunicações da PMESP.

2.24. A DTIC mantém soluções tecnológicas que suportam toda a administração e operação nos ambientes de internet, intranet e redes corporativas da PMESP, bem como cibersegurança.

2.25. Diante da rápida evolução da tecnologia e a necessidade de inovação e transformação digital na administração pública, é imprescindível realizar uma nova licitação para selecionar uma empresa especializada capaz de atender essa demanda promovendo a melhoria dos processos da PMESP em consonância com os objetivos estratégicos do Plano de Comando – 2024/2031.

- 2.26. A tecnologia, quando sustentada por boas práticas de gestão de serviços (ISO/IEC 20.000 e ITSM), governança (COBIT, ISO/IEC 38.500) e segurança cibernética (ISO/IEC 27.001, NIST CSF), torna-se um pilar estratégico para que a PMESP seja reconhecida como referência nacional e internacional. Para tanto, é essencial garantir resiliência digital, integridade dos dados, soberania tecnológica e resposta rápida a incidentes, elevando a maturidade digital da corporação.
- 2.27. Visando o aprimoramento dos serviços da PMESP, a contratação terá aderência ao Decreto nº 68.828, de 4 de setembro de 2024, que institui o Programa Muralha Paulista. O programa segue o princípio de oferecer suporte informacional e tecnológico à formulação e implementação de políticas de segurança pública voltadas ao controle de crimes, com ênfase especial em crimes contra a vida e o patrimônio.
- 2.28. Como parte do Programa Muralha Paulista, as bases de dados armazenadas nos datacenters da Secretaria da Segurança Pública e dos demais órgãos policiais e conveniados são essenciais para a operação integrada de inteligência e monitoramento.
- 2.29. O programa conta com um conjunto integrado de soluções tecnológicas, incluindo infraestrutura física e operações em nuvem, com destaque para a adoção de modelos híbridos e serviços em IaaS (Infrastructure as a Service), alinhados com práticas de Cloud Security Posture Management (CSPM) e Zero Trust Architecture, além de inteligência artificial aplicada à segurança pública, redes dedicadas e centros de dados.
- 2.30. Nesse contexto, a DTIC desempenha um papel fundamental ao realizar estudos técnicos preliminares alinhados aos normativos vigentes, que possuem características no combate a ameaças e apoiar a construção de arquiteturas de defesa proativas no ambiente de TIC da PMESP, garantindo a segurança e a continuidade dos serviços de TIC.
- 2.31. A DTIC, por meio do DAS, realizou um levantamento detalhado do ambiente de TIC, analisando dados históricos e projeções futuras para fundamentar a estimativa das necessidades desta contratação.
- 2.32. Este estudo se refere à contratação de serviços técnicos especializados de suporte de cibersegurança, data center e redes, bem como de governança, gerenciamento e monitoramento, das demandas e mudanças de tecnologia da informação e comunicação e infraestrutura de data center e redes para ambiente computacional e de telecomunicações, de forma a garantir a continuidade dos serviços de TIC, seguindo padrões estabelecidos por normas técnicas, como ISO/IEC 20.000 e ISO/IEC 27.001, e práticas ágeis DevSecOps.
- 2.33. Como extensão das práticas de segurança integradas no ciclo de vida do desenvolvimento (DevSecOps), é recomendada a adoção de metodologias e ferramentas que complementem a proteção de aplicações e ativos críticos, como:
- 2.33.1. DAST (Dynamic Application Security Testing): Execução de testes dinâmicos em aplicações em tempo de execução, simulando ataques reais para detectar falhas que não são visíveis em análise estática.
- 2.33.2. WebSec (Segurança de Aplicações Web): Estratégia de proteção voltada para aplicações baseadas na web, com ênfase em controles como WAF, validação de entrada e autenticação multifator.
- 2.33.3. OSINT (Open Source Intelligence): Coleta de inteligência em fontes abertas para identificação de vazamentos, exposição de credenciais, domínios associados à corporação e menções suspeitas que possam representar vetores de ataque ou risco reputacional. Além da aplicação tradicional de OSINT, recomenda-se o fortalecimento da área de Cyber Threat Intelligence (CTI), promovendo a integração de dados de fontes abertas (OSINT), fechadas (Threat Feeds), indicadores internos (IOCs) e plataformas de inteligência (MISP, OpenCTI). A prática de CTI permite à PMESP construir uma inteligência acionável com foco na antecipação de ameaças, construção de perfis de atacantes (TTPs) e apoio à tomada de decisão estratégica. Essa camada agrega alto valor à operação do SOC, permitindo uma resposta proativa e contextualizada a ameaças emergentes.
- 2.34. A integração dessas abordagens à esteira DevSecOps reforça o modelo de defesa em profundidade da PMESP, garantindo que desde o desenvolvimento até a operação os sistemas estejam protegidos e monitorados continuamente.
- 2.35. De mesmo modo, convém registrar as diretrizes do Governo do Estado de São Paulo, estabelecidas no Decreto nº 68.538/2024, que instituiu o Plano São Paulo na Direção Certa, impondo aos órgãos públicos a adoção de mecanismos voltados à redução de despesas correntes, em razão da escassez de recursos e da multiplicidade de demandas administrativas. Não obstante as necessidades específicas deste órgão, observa-se que o objeto pretendido encontra-se plenamente alinhado às determinações da referida norma, especialmente ao disposto em seu artigo 10, que trata da racionalização e da unificação da prestação de serviços técnico-especializados. Nessa perspectiva, o novo contrato proposto possibilitará o encerramento de contratos atualmente vigentes que apresentam similaridade de objetos, como, por exemplo, aqueles relacionados ao suporte de redes e data center da PMESP, permitindo a substituição por uma solução mais ampla, integrada e segura, em consonância com as diretrizes governamentais de eficiência, economicidade e otimização dos recursos públicos.
- 2.36. Por fim, por se tratar de um serviço continuado com mão de obra dedicada, é claro que ocorrerá avaliação da execução será realizada mensalmente por meio do Instrumento de Medição de Resultado (IMR), com indicadores de maturidade cibernética e níveis de conformidade com ISO 27.001, conforme preconiza a Lei 14.133/2021, que servirá como incentivo para a contratada promover eficiência na entrega dos serviços qualitativamente. O Termo de Referência e este Estudo Técnico Preliminar contém todas as informações e detalhes necessários para a execução deste objeto.

3. Área requisitante

Área Requisitante	Responsável
Seção de Processamento de Dados	Cap PM Basileu
Seção de Engenharia de Redes	Cap PM Fernet
Divisão de Cibersegurança	Maj PM Tamashiro
Seção de Cibersegurança	Cap PM Lucena
Departamento de Aplicações e Sistemas	Ten Cel PM Panzarini
Diretoria de Tecnologia da Informação e Comunicação	Cel PM Beatriz

4. Necessidades de Negócio

4.1. A Polícia Militar do Estado de São Paulo – PMESP busca contratação de serviços técnicos especializados de suporte de cibersegurança, data center e redes, bem como de governança, gerenciamento e monitoramento, das demandas e mudanças de tecnologia da informação e comunicação e infraestrutura de data center e redes para ambiente computacional e de telecomunicações, de forma a garantir a continuidade dos serviços de TIC. O objetivo é assegurar a continuidade dos serviços de TIC, buscando a excelência no serviço prestado pela DTIC tanto ao seu público interno quanto externo.

4.2. Detalhamento dos serviços:

4.2.1. Os serviços descritos neste projeto envolvem a operação de infraestrutura de TIC. Entende-se por operação de infraestrutura de TIC a prestação de serviços técnicos relacionados à segurança da informação, telecomunicação, rede de dados, banco de dados, servidores, sistemas operacionais e backup. Esses serviços devem contemplar mecanismos de continuidade de negócios (BCP/DRP), automação de monitoramento, segmentação de rede baseada em Zero Trust e integração com plataformas SIEM, garantindo resiliência, escalabilidade e governança em tempo real.

4.2.2. A operação de infraestrutura de TIC é um serviço fundamental para a garantia da disponibilidade, integridade, resiliência e segurança de recursos tecnológicos necessários para a sustentação de quaisquer serviços baseados em TIC da PMESP, independentemente de sua natureza.

4.2.3. Os serviços descritos nesta contratação podem ser executados de forma indireta, conforme permitido pela legislação vigente, e possuem elevada relevância por apoiar tanto os processos finalísticos quanto as atividades administrativas e operacionais da Polícia Militar, pertencente à Secretaria da Segurança Pública do Estado de São Paulo, órgão da administração direta.

4.2.4. A prestação dos serviços ocorrerá sob um modelo de serviço continuado, garantindo a continuidade operacional por meio de:

4.2.5. Monitoramento ininterrupto do Security Operation Center (SOC) e do Network Operation Center (NOC).

4.2.6. A prestação de serviços da equipe na Diretoria de Tecnologia da Informação e Comunicação, conforme detalhado nos itens especificados neste documento.

4.2.7. Atendimento aos Acordos de Nível de Serviço (SLAs) estabelecidos, incluindo um serviço de dispatcher, baseado em práticas de ITIL v4, com base de conhecimento integrada, suporte por múltiplos canais (telefone, e-mail, portal web e app) e classificação automática de incidentes baseada em criticidade e severidade, visando acelerar a resolução e escalonamento e acionamento de especialistas quando necessário.

4.2.8. Estes serviços são considerados comuns, com padrões objetivos definidos por SLAs e KPIs, conforme orientações da ITIL4. No entanto, para órgãos de segurança pública, recomenda-se que os indicadores de qualidade sejam calibrados para ambientes de alta criticidade, com penalizações por não conformidade e auditorias baseadas em métricas de disponibilidade, tempo de resposta e taxa de resolução no primeiro nível (FCR), sendo prestados preferencialmente por empresas especializadas em serviços técnicos de TIC.

4.2.9. A operação de infraestrutura de TIC representa uma solução estratégica, guiada pelos princípios de segurança, escalabilidade e conformidade com normativas vigentes, contribuindo para o fortalecimento da capacidade tecnológica da PMESP.

4.3. Termos e definições:

4.3.1. Para os efeitos deste documento e não se esgotam, aplicam-se os seguintes termos e definições:

4.3.1.1. Termos:

4.3.1.1.1. AD – Active Directory;

4.3.1.1.2. APM – Application Performance Monitoring;

4.3.1.1.3. AV – Antivírus;

4.3.1.1.4. CD – Continuous Deployment (entrega/implementação continua);

4.3.1.1.5. CI – Continuous Integration (integração continua);

4.3.1.1.6. DAST - Dynamic Application Security Testing;

4.3.1.1.7. DLP – Data Loss Prevention (Prevenção contra Perda de Dados);

4.3.1.1.8. DNS – Domain Name System;

4.3.1.1.9. DP – Deployment Pipeline;

4.3.1.1.10. DRP – Disaster Recovery Plan (Plano de Recuperação de Desastres);

4.3.1.1.11. EDR – Endpoint Detection and Response (Detecção e Resposta de Endpoint);

4.3.1.1.12. Fator-K – Índice para estimar custo de serviços com base na remuneração dos profissionais;

4.3.1.1.13. IAM – Identity and Access Management (Gerenciamento de Identidade e Acesso);

4.3.1.1.14. IaaS – Infrastructure as a Service (Infraestrutura como Serviço);

4.3.1.1.15. IDS/IPS – Intrusion Detection System/Intrusion Prevention System (Sistema de Detecção e Prevenção de Intrusões);

4.3.1.1.16. ISO/IEC 20000 – Gestão de Serviços de TI;

4.3.1.1.17. ISO/IEC 27001 – Segurança da Informação;

4.3.1.1.18. ITIL v4 – Information Technology Infrastructure Library (Melhores práticas para Gestão de TI);

4.3.1.1.19. ITIM – IT Infrastructure Monitoring (Monitoramento de Infraestrutura de TI);

4.3.1.1.20. ITSM – Information Technology Service Management (Gerenciamento de Serviços de TI);

4.3.1.1.21. KPI – Key Performance Indicator (Indicador de Desempenho);

4.3.1.1.22. LGPD – Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018);

4.3.1.1.23. NGFW – Next-Generation Firewall;

4.3.1.1.24. NIST – National Institute of Standards and Technology (Padrões de Segurança Cibernética);

4.3.1.1.25. NMS – Níveis Mínimos de Serviço;

4.3.1.1.26. NOC – Network Operations Center;

4.3.1.1.27. NPM – Network Performance Monitoring;

4.3.1.1.28. OSINT – Open Source Intelligence;

4.3.1.1.29. PaaS – Platform as a Service (Plataforma como Serviço);

4.3.1.1.30. PDCA – Plan Do Check Action

4.3.1.1.31. PMESP – Polícia Militar do Estado de São Paulo;

4.3.1.1.32. RPA – Robotic Process Automation (Automação Robótica de Processos);

- 4.3.1.1.33. SAST - Static Application Security Testing
- 4.3.1.1.34. SGBD – Sistema de Gerenciamento de Banco de Dados;
- 4.3.1.1.35. SIEM – Security Information and Event Management (Gestão de Informações e Eventos de Segurança);
- 4.3.1.1.36. SISP – Sistema de Administração dos Recursos de Tecnologia da Informação;

- 4.3.1.1.37. SLA – Service Level Agreement (Acordo de Nível de Serviço);
- 4.3.1.1.38. SLM – Service Level Management (Gerenciamento de Nível de Serviço);
- 4.3.1.1.39. SO – Setor Operacional;
- 4.3.1.1.40. SOC – Security Operation Center;
- 4.3.1.1.41. SSL/TLS – Secure Sockets Layer / Transport Layer Security;
- 4.3.1.1.42. TCO – Total Cost of Ownership (Custo Total de Propriedade);
- 4.3.1.1.43. TIC – Tecnologia da Informação e Comunicação;
- 4.3.1.1.44. UEBA – User and Entity Behavior Analytics
- 4.3.1.1.45. VPN – Virtual Private Network (Rede Privada Virtual);
- 4.3.1.1.46. WAF – Web Application Firewall;
- 4.3.1.1.47. WEBSEC - Web Security;
- 4.3.1.1.48. XDR – Extended Detection and Response (Detecção e Resposta Estendida);
- 4.3.2. Definições:
- 4.3.2.1. Administração: órgão, entidade ou unidade administrativa da Administração Pública contratante de serviços terceirizados;
- 4.3.2.2. Área de TIC: unidade setorial, seção, departamento ou diretoria, responsável por gerir a tecnologia da informação e comunicação e pelo planejamento, coordenação e acompanhamento das ações relacionadas às soluções de TIC da DTIC/PMESP;
- 4.3.2.3. Base de Conhecimento: repositório digital estruturado que armazena artefatos técnicos, scripts de atendimento, resoluções documentadas, e procedimentos padronizados. A manutenção e atualização constante da base é essencial para a eficiência da Central de Atendimento, bem como para permitir a automação de respostas em sistemas de ticketing como Jira Service Management e Confluence, ferramentas utilizadas amplamente por governos em ambientes de missão crítica.;
- 4.3.2.4. Catálogo de Serviços: informação documentada sobre os serviços que uma organização fornece aos seus usuários;
- 4.3.2.5. Categoria de Serviço: consiste no agrupamento de atividades com características e perfis profissionais similares, considerados necessários à manutenção e gestão da infraestrutura de TIC do órgão ou entidade;
- 4.3.2.6. Central de Serviços: refere-se a um ponto único de atendimento, cujo objetivo é permitir maior controle e proporcionar um atendimento mais adequado;
- 4.3.2.7. DevSecOps: refere-se a uma extensão do conceito de DevOps que combina dois grupos de recursos: desenvolvimento e operações. O DevSecOps integra a dimensão de segurança como terceiro grupo de recursos. Assim, usando práticas, ferramentas e uma nova abordagem cultural, as equipes podem construir e entregar serviços em maior velocidade e em escala. A esteira DevSecOps adotada deverá contemplar processos automatizados de verificação contínua, incluindo testes de segurança (SAST/DAST), verificação de infraestrutura como código (IaC) e análise de composição de software (SCA). Deve-se garantir que os commits em repositórios versionados (Git) disparem automaticamente os testes de conformidade antes da publicação em ambiente produtivo, evitando vulnerabilidades conhecidas ou más práticas de codificação.
- 4.3.2.8. Disponibilidade: condição de um serviço ou recurso estar acessível e apto para desempenhar plenamente suas funções, em determinado momento ou durante um período acordado;
- 4.3.2.9. Equipe de Planejamento da Contratação: equipe responsável pelo planejamento da contratação;
- 4.3.2.10. Equipe de Fiscalização do Contrato: equipe responsável pela fiscalização do contrato;
- 4.3.2.11. Evento: qualquer requisição feita de maneira automática para a área de TI;
- 4.3.2.12. Ferramentas de automação robótica de processos - RPA: tecnologia capaz de automatizar tarefas humanas que são repetitivas, reproduzindo os mesmos passos de uma transação humana, utilizando principalmente interações orquestradas de Interface do Usuário;
- 4.3.2.13. Ferramentas de monitoramento de infraestrutura de TI - ITIM: tecnologia capaz de monitorar em tempo real saúde de componentes de infraestrutura de TI que residem em um data center, na infraestrutura como serviço - IaaS ou na plataforma como serviço - PaaS na nuvem;
- 4.3.2.14. Incidente: qualquer acontecimento não planejado que cause redução na qualidade do serviço ou interrupção do serviço em parte ou como um todo, ou ainda evento que ainda não impactou o serviço do usuário;
- 4.3.2.15. Incidente de Segurança da Informação: qualquer evento de segurança da informação indesejável e inesperado, seja único ou em série, que pode comprometer as operações de negócio e ameaçar a segurança da informação;
- 4.3.2.16. Critérios de Aceitação: parâmetros objetivos e mensuráveis utilizados para verificar se um bem ou serviço recebido está em conformidade com os requisitos especificados;
- 4.3.2.17. Gerenciamento de Incidentes: processo que estabelece procedimentos de registro, classificação, priorização e resolução de incidentes;
- 4.3.2.18. Gerenciamento de Mudanças: processo que estabelece procedimentos e controles a serem utilizados no caso de necessidade de modificação, adição ou exclusão de componentes de infraestrutura de TIC;
- 4.3.2.19. Gerenciamento de Requisição: processo que estabelece procedimentos de registro, controle e monitoramento de requisições relacionadas à infraestrutura de TIC;
- 4.3.2.20. Gerenciamento de Serviços de TIC: conjunto de capacidades e processos para dirigir e controlar atividades e recursos de tecnologia da Administração no planejamento, desenho, transição, entrega e melhoria de serviços de TIC para entrega de valor;
- 4.3.2.21. Infraestrutura de TIC: abrange todos os componentes técnicos, hardwares, softwares, bancos de dados implantados, procedimentos técnicos e documentação técnica usados para disponibilizar as informações;
- 4.3.2.22. Listas de Verificação: documentos ou ferramentas estruturadas contendo um conjunto de elementos que devem ser acompanhados pela equipe de fiscalização do contrato durante a execução contratual, permitindo à Administração o registro e a obtenção de informações padronizadas e de forma objetiva;
- 4.3.2.23. Melhoria Contínua: processo que possibilita entregar resultados mais eficientes, no mesmo intervalo de tempo, identificando a possibilidade de aumentar a eficácia ou a efetividade de serviços e produtos, sem perda de qualidade, utilizando os mesmos recursos de custeio, como insumos, infraestrutura, tecnologias e pessoas;

- 4.3.2.24. Operação de infraestrutura de TIC: conjunto de tarefas e atividades destinadas à sustentação da infraestrutura de TIC, que inclui o gerenciamento, monitoramento, manutenção e aprimoramento contínuo de seus componentes;
- 4.3.2.25. Ordem de Serviço - OS: é a formalização do trabalho que será prestado pelo contratado ao contratante. É o documento que contém as definições e informações necessárias para planejar e executar um serviço, bem como a autorização formal para sua realização;
- 4.3.2.26. Problema: causa de um ou mais incidentes reais ou potenciais;
- 4.3.2.27. Profissional Júnior: adequado para exercer atividades de menor complexidade e que exigem menor experiência ou qualificação profissional. Geralmente, não apresenta autonomia para tomadas de decisão operacional;
- 4.3.2.28. Profissional Pleno: adequado para exercer atividades com um maior grau de complexidade, que requerem uma capacidade maior de análise crítica e resolução de problemas, além de exigir maior experiência ou qualificação profissional;
- 4.3.2.29. Profissional Sênior: adequado para exercer atividades com grau elevado de complexidade e criticidade, e que requer experiência e qualificação profissional diferenciada;
- 4.3.2.30. Requisição de Mudança: pedido por alteração a ser feita em um serviço, componente de serviço ou no sistema de gerenciamento de serviços;
- 4.3.2.31. Requisição de Serviço: pedido por informações ou recomendações, ou por uma alteração de um padrão (uma mudança pré-aprovada que tem baixo risco, é relativamente comum e dá continuidade a um procedimento), ou para obter acesso a um serviço de TIC; e
- 4.3.2.32. Serviço: meio de entregar valor aos usuários internos ou externos à organização ao facilitar o alcance de resultados almejados.
- 4.4. Local e horário de execução dos serviços
- 4.5. Os serviços serão prestados, em sua maioria, nas instalações do Departamento de Aplicações e Sistemas (DAS), sito na Rua Ribeiro de Lima, nº 140, Luz, São Paulo/SP e na Divisão de Cibersegurança, sito na Rua Alfredo Maia, 218, 7º andar, Luz, São Paulo/SP, na seguinte conformidade:
- 4.5.1. O Coordenador deverá desempenhar suas funções de segunda à sexta-feira, em dias úteis, no horário de expediente;
- 4.5.2. O SOC e NOC/SO deverão desempenhar suas funções de segunda-feira a domingo, vinte e quatro horas (24 h) por dia, sete (7) dias por semana (24x7), conforme descritos nos itens que tratam de SOC e NOC/SO;
- 4.5.3. O Ciber, SPD e SER deverão desempenhar suas funções de segunda-feira a sexta-feira, no horário definido nos perfis de cada descrito nos seus itens, sendo que as mudanças e eventuais acionamentos que tiverem que ocorrer em horário diferente desse deverão ser acionados pelo Dispatcher/NOC, não podendo incorrer em custos adicionais para a PMESP;
- 4.5.4. Os serviços prestados por N2/3, Windows/Linux, Notes e DBA de TIC deverão desempenhar suas funções de segunda-feira a sexta-feira, no horário de expediente e nos demais horários em regime de sobreaviso, não incorrendo em custos adicionais para a PMESP eventuais acionamentos e atendimentos presenciais por parte dos profissionais deste serviço;
- 4.5.5. O serviço de Projetos/ Processos, N1/Dispatcher, Cabista, Líder, Arquiteto de Soluções e IA, Threat Hunting e Threat Intelligence de TIC deverá ser desempenhado de segunda-feira a sexta-feira, no horário de expediente;
- 4.5.6. Os profissionais disponibilizados terão dedicação exclusiva ao objeto licitado e permanecerão sob a coordenação técnica direta do respectivo Coordenador, bem como dos Líderes de Serviços;
- 4.5.7. Havendo necessidade de acionamento de recursos, a CONTRATADA deverá providenciar meios e formas seguras e eficientes para que os mesmos possam oferecer pronta resposta ao ambiente da Polícia Militar, conforme as necessidades apresentadas pelo Gestor do Contrato ao Líder de Serviços.
- 4.6. Escopo do projeto
- 4.6.1. O escopo deste projeto abrange a serviços técnicos especializados de suporte de cibersegurança, data center e redes, bem como de governança, gerenciamento e monitoramento, das demandas e mudanças de tecnologia da informação e comunicação e infraestrutura de data center e redes para ambiente computacional e de telecomunicações, de forma a garantir a continuidade dos serviços de TIC na PMESP.
- 4.6.2. Os serviços serão prestados sob o modelo de regime de dedicação de mão de obra e pagamento mensal fixo, para atendimento contínuo das demandas operacionais e de suporte das unidades do órgão e utilização do IMR para eficiência do Contrato. Busca-se garantir a disponibilidade, a estabilidade e o adequado funcionamento dos sistemas, equipamentos, infraestrutura e demais serviços essenciais de TIC que sustentam as atividades institucionais, indicados no Anexo A – Instrumento de Medição de Resultado – IMR.
- 4.6.3. A contratação pela natureza contínua e ininterrupta das atividades de TIC desempenhadas diariamente, que exigem profissionais dedicados integralmente ao órgão, conforme previsto no art. 6º, XVI, da Lei nº 14.133/2021. Essas atividades requerem acompanhamento permanente, pronta resposta a incidentes, atendimento tempestivo aos usuários e interação com ambientes operacionais críticos. Embora determinadas tarefas possam ser executadas em regime híbrido ou remoto, a complexidade e a criticidade do serviço demandam uma equipe dedicada, com alocação e disponibilidade compatíveis com as necessidades da Administração, assegurando a continuidade, o controle e a qualidade da execução contratada, bem como seja é tecnicamente viável e economicamente vantajoso, através destes seguintes serviços:
- 4.6.3.1. Monitoramento ininterrupto do SOC e do NOC pela contratada;
- 4.6.3.2. Equipe na Diretoria de Tecnologia da Informação e Comunicação, conforme detalhado nos itens específicos deste estudo técnico preliminar;
- 4.6.3.3. Disponibilidade de um dispatcher para suporte técnico e possibilitar o acionamento de especialistas de acordo com os níveis de serviço estabelecidos nos SLAs e KPIs.
- 4.6.4. Dessa forma, o escopo foi delineado para atender a missão crítica da PMESP, focando nos serviços técnicos especializados de suporte de cibersegurança, data center e redes, bem como de governança, gerenciamento e monitoramento, das demandas e mudanças de tecnologia da informação e comunicação e infraestrutura de data center e redes para ambiente computacional e de telecomunicações, de forma a garantir a continuidade dos serviços de TIC da PMESP. Isso agrega valor às atividades finalísticas e administrativas da instituição, ao mesmo tempo em que exclui atividades que extrapolam os objetivos desta contratação, ora já contratados ou que serão licitados em outros processos.
- 4.7. Balizadores Do Projeto
- 4.7.1. No intuito de simplificar o projeto para aplicação tanto pela PMESP quanto pela empresa contratada, foram estabelecidas as seguintes diretrizes fundamentais:
- 4.7.1.1. Definição de critérios de governança no gerenciamento de serviços de operações de TIC, promovendo uma estrutura clara e organizada;
- 4.7.1.2. Diretrizes para definição de processos relacionados ao gerenciamento de serviços de TIC e delimitação do escopo da solução de TIC relacionada ao objeto do modelo.
- 4.7.1.3. Padronização da forma de mensuração dos serviços e pagamento fixo mensal com mão de obra dedicada e aplicação de SLA de serviços, a serem aferidos e controle de eficiência.
- 4.7.2. A definição do valor fixo mensal está associada ao cumprimento de níveis de serviços e critérios de qualidade executados pela mão de obra

alocada no projeto, buscando gerar incentivos para que os contratados prestem serviços associados ao uso de recursos tecnológicos que forneçam a agilidade e qualidade adequada às condições exigidas.

4.7.3. Ainda neste documento, parte integrante do IMR é descrito para compreensão clara, de forma que o contratante seja capaz se adaptar e consequentemente atendê-los, de forma que a prestação do serviço seja eficiente, no Anexo A – Instrumento de Medição de Resultado – IMR.

4.8. Processo de Operação de Infraestrutura de TIC

4.8.1. Diretrizes sobre gerenciamento de serviços de TIC

4.8.2. A formalização de processos de gerenciamento de serviços de TIC é fundamental para assegurar a adoção adequada do Modelo de Referência, bem como garantir condições adequadas de governança e gestão dos serviços de suporte e operação da TIC.

4.8.3. Como prática recomendada, e a capacidade de gerenciamento de serviços de TIC por parte da instituição - incluindo processos e ferramentas - não deve depender exclusivamente de contratos derivados deste estudo. Isso visa assegurar maior autonomia e estabilidade nos processos de gestão de serviços bem como reforçar a governança na execução e supervisão das atividades da área de TIC.

4.8.4. A observância aos padrões constantes da série ABNT NBR ISO/IEC 20.000 provê estabilidade e previsibilidade aos processos de gerenciamento de serviços de TIC, ao passo que a observância às práticas ágeis constantes do modelo de DevSecOps provê agilidade na prestação dos serviços.

4.8.5. Para assegurar a governança adequada em relação ao modo de atuação da área de TIC na entrega de serviços a PMESP, considera a formalização e implementação das seguintes práticas:

4.8.5.1. Gerenciamento de requisição de serviços;

4.8.5.2. Gerenciamento de mudanças;

4.8.5.3. Gerenciamento de problemas; e

4.8.5.4. Gerenciamento de incidentes.

4.8.6. Um ambiente DevSecOps possui um ou mais recursos que asseguram condições para se alcançar um elevado grau de automação da infraestrutura. Em geral, são empregadas ferramentas de:

4.8.6.1. Controle de versão;

4.8.6.2. Integração contínua;

4.8.6.3. Testes contínuos;

4.8.6.4. Gerenciamento de configuração e deployment;

4.8.6.5. Monitoramento contínuo;

4.8.6.6. Containerização;

4.8.6.7. Orquestração;

4.8.6.8. Elasticidade;

4.8.6.9. Segurança integrada; e

4.8.6.10. Gerenciamento integrado de demandas.

4.8.7. Dessa forma, é importante que a contratada apoie na revisão, defição e evolução dos processos de gerenciamento de serviços de TIC da PMESP, de forma gradativa.

4.8.8. A evolução desses processos é um passo estratégico para assegurar que a infraestrutura de TIC da PMESP esteja preparada para atender às demandas atuais e futuras, mantendo a instituição alinhada às melhores práticas de tecnologia e governança;

4.9. Catálogo de Serviços de TIC

4.9.1. A adoção de catálogos de serviços para descrição dos serviços prestados pela área de TIC, resultados esperados e níveis mínimos de qualidade exigidos são fundamentais para assegurar a estabilidade e previsibilidade do processo de gerenciamento dos serviços de TIC.

4.9.2. A utilização de catálogo de serviços de TIC não se confunde com a mensuração dos serviços para fins de pagamento, descritos em detalhes nesse modelo, mas trata-se de uma prática constante da ABNT NBR ISO/IEC 20.000-1:2020.

4.9.3. Nesse sentido, a adoção de um Catálogo de Serviços abrangente, que contemple todos os serviços prestados e executados em suas operações de TIC. Para facilitar sua gestão os serviços são organizados em duas categorias principais:

4.9.3.1. Divisão do Catálogo de Serviços:

4.9.3.1.1. Catálogo de Serviços Negocial: contém todos os serviços de TIC em operação e disponíveis para os clientes ou sendo preparados para serem entregues aos clientes.

4.9.3.1.2. Catálogo de Serviços Técnicos: contém todas as requisições de serviço disponíveis para os clientes e usuários de serviços de TI.

4.9.4. Tipos de Serviços: os serviços constantes no Catálogo de Serviços devem ser organizados por tipos. Os tipos de serviço mais comuns são:

4.9.4.1. Serviços de negócio: todo serviço que é entregue a clientes de negócio pelas unidades de negócio. São serviços que impactam diretamente nos resultados de negócios e são suportados pelos serviços de TI.

4.9.4.2. Serviços de TIC: são todos os serviços fornecidos por um provedor de serviço de TIC que suportam diretamente processos e serviços de negócio de um ou mais clientes. Um serviço de TIC é composto de uma combinação de hardware, software, processos e pessoas; e

4.9.4.3. Serviços de Apoio: são os serviços necessários para suportar os serviços de TIC e entregar um serviço de negócio. Não são diretamente usados pelo negócio, porém são exigidos pelo provedor de serviço de TIC para entregar serviços voltados ao cliente.

4.9.5. Assim, é fundamental que exista um Catálogo de Serviços da DTIC claro, organizado, preciso e disponível aos usuários da unidade de TI e que atenda às necessidades de negócio da PMESP, ele deve ser projetado para:

4.9.5.1. Permitir a configuração adequada das ferramentas de controle de demanda;

4.9.5.2. Garantir a padronização e o monitoramento de todos os serviços prestados, promovendo consistência e qualidade nas entregas há diversas maneiras de identificar os serviços de TIC existentes em uma organização, tais como: a decomposição dos processos de negócio, a análise da infraestrutura de TIC, a análise de aplicativos disponibilizados, a análise de metas de departamentos e a análise de patrimônio.

4.9.6. Para facilitar a identificação dos serviços de TIC foram classificá-los em grupos, tornando a busca mais eficiente. Seguem, abaixo, os grupos comuns utilizados para classificar os serviços de TIC:

4.9.6.1. Serviços a usuários de TIC:

4.9.6.1.1. Serviços de Aplicação Padrão: os serviços de TIC mais utilizados nas estações de trabalho, como pacotes de aplicativos de escritório, aplicativos de leitura de e-mails, etc;

4.9.6.1.2. Serviços de Aplicação Específicos: os serviços de TIC específicos da organização ou de determinados departamentos, como por exemplo, Software ERP e aplicativos de design gráfico;

- 4.9.6.1.3. Serviços de Estação de Trabalho: as configurações dos computadores dos usuários relativas à organização, como por exemplo, configuração de rede e criação de contas de acesso;
- 4.9.6.1.4. Serviços de Internet: as configurações e restrições de uso de Internet para determinados usuários ou departamentos;
- 4.9.6.1.5. Serviços de Intranet: configurações, permissões e restrições de uso quanto aos serviços internos da organização;
- 4.9.6.1.6. Serviços de Base de Conhecimento: acessos ao repositório de conhecimento dos serviços e recursos disponíveis;
- 4.9.6.1.7. Serviços de Compartilhamento de Arquivos: acesso aos repositórios públicos e específicos de arquivos da organização;
- 4.9.6.1.8. Serviços de Impressão: acessos e permissões referentes às impressoras da organização;
- 4.9.6.1.9. Serviços de Gerenciamento de Chamados de TIC: também conhecido como Service Desk, responsável por registrar as requisições de suporte dos usuários;
- 4.9.6.1.10. Serviços de Dispositivos Especiais: responsável pelo provimento de dispositivos específicos como, por exemplo, copiadoras e projetores multimídia;
- 4.9.6.1.11. Serviços de Backup: cópias de segurança dos dados e sistemas e suas respectivas configurações.
- 4.9.6.1.12. Serviços de operação de infraestrutura de TIC:
- 4.9.6.1.13. Serviço de Contas e Perfis de Acesso: criação, modificação, inativação e exclusão de perfis e atributos de contas;
- 4.9.6.1.14. Ativos de Rede: instalação, configuração, manutenção preventiva e corretiva de equipamentos de infraestrutura de redes;
- 4.9.6.1.15. Servidores: instalação, configuração, manutenção preventiva e corretiva de servidores;
- 4.9.6.1.16. Aplicações: deploy, atualização, configuração, manutenções e otimizações de desempenho das aplicações;
- 4.9.6.1.17. Banco de Dados: criação, remoção, migração, execução de scripts, manutenção, otimização de desempenho, alteração de privilégios de acesso de banco de dados;
- 4.9.6.1.18. Backup: execução de rotinas, restauração, checagem dos backups;
- 4.9.6.1.19. Armazenamento e Storage: instalação, configuração, otimização de storage, criação, realocação e restauração de sistemas de arquivos de storage;
- 4.9.6.1.20. Documentação: atualização, inclusão, alteração, exclusão de itens de configuração de TIC e itens de conhecimento;
- 4.9.6.1.21. Segurança da Informação: inclusão, alteração, exclusão de regras de firewall, execução de procedimentos para busca de vulnerabilidades e falhas de segurança no ambiente de TIC, configuração de antivírus;
- 4.9.6.2. A estruturação detalhada do catálogo fortalece a capacidade da PMESP de gerenciar seus serviços de TIC, alinhando-os às necessidades operacionais e estratégicas, além de proporcionar uma base sólida para a interação com os usuários e a contratada;
- 4.9.7. O catálogo de serviços pode conter os seguintes atributos:
 - 4.9.7.1. Nome do serviço: declaração do nome do serviço;
 - 4.9.7.2. Objetivos do Serviço: exposição resumida do que o serviço faz e como ele é útil para seus usuários e clientes;
 - 4.9.7.3. Grupos de serviços: definição do grupo de serviço;
 - 4.9.7.4. Partes interessadas: pessoas ou entidades que têm interesse em uma organização, um projeto, um serviço de TI, etc. Podem estar interessadas nas atividades, metas, recursos ou entregáveis. As partes interessadas podem incluir clientes, parceiros, usuários, etc;
 - 4.9.7.5. Meios de solicitação: indicação do telefone, endereço de Internet/Intranet, e-mail ou qualquer outra forma oficial onde cliente ou usuário pode solicitar o serviço;
 - 4.9.7.6. Período definido para atendimento: indicação dos meses, dias das semanas e horários que o serviço será atendido pela parte executora do serviço;
 - 4.9.7.7. Processo: indicação do processo que o serviço deverá seguir, considerando suas peculiaridades (tal como se consiste em uma solicitação ou incidente);
 - 4.9.7.8. Aprovadores: indicação dos aprovadores do serviço, caso existam. Um grupo de pessoas ou uma pessoa específica;
 - 4.9.7.9. Tempo de atendimento: descrever qual o tempo de atendimento que está definido para o atendimento do serviço;
 - 4.9.7.10. Template do formulário: indicação das informações que serão necessárias para efetuar o atendimento do serviço e compor as informações;
 - 4.9.7.11. Riscos Associados: eventos possíveis que podem causar perdas ou danos, ou afetar a habilidade de atingir objetivos, durante a execução do serviço;
 - 4.9.7.12. Fluxo de Atividades: indicar o fluxo de trabalho mapeado do respectivo serviço, caso ele exista;
 - 4.9.7.13. Link da Base de Conhecimento: indicar o link da Base de Conhecimento que dá acesso ao histórico de evolução do item de serviço.
- 4.9.8. Recomenda-se que o Catálogo de Serviços deva ser amplamente divulgado e estar acessível e disponível, principalmente atualizado na ferramenta de ITSM.
- 4.9.9. Toda a mudança aplicada no catálogo, incluindo os novos serviços de TIC que irão compô-lo, as atualizações em serviços de TIC que o integram, ou ainda a desativação de serviços, devem obrigatoriamente ser autorizados por um responsável ou comitê competente da DTIC/PMESP.
- 4.9.10. Os catálogos de serviços definidos pela PMESP nortearão a definição dos requisitos temporais e de qualidade de cada tipo de serviço a constar do instrumento convocatório. Portanto, deve-se considerar a inclusão desses requisitos por tipo de serviço balizado pelos catálogos de serviços ou, na ausência destes catálogos, por diretrizes mínimas relacionadas a qualidade e prazos definidos pelo Comitê de Governança Digital.
- 4.9.11. Observações relevantes:
 - 4.9.11.1. Os catálogos de serviço estão diretamente associados à configuração dos níveis mínimos de serviços previstos no Estudo Técnico Preliminar e Termo de Referência.
 - 4.9.11.2. Portanto, observa-se ao menos os níveis de serviço por grupo de serviços constante do catálogo, parte integrante deste projeto, com vistas a promover maior estabilidade durante a execução do contrato.
 - 4.9.11.3. Quando alterações no catálogo implicarem em aumento dos volumes de serviços que propicie desequilíbrio econômico-financeiro, devem ser tomadas tempestivamente as devidas providências para que as condições originais da prestação sejam restabelecidas.
- 4.10. Base de Conhecimento
 - 4.10.1. A PMESP manterá com a contratada, atualizada a Base de Conhecimentos técnicos com vistas a assegurar a padronização do atendimento, retenção do conhecimento e agilidade na execução dos serviços.
 - 4.10.2. Uma Base de Conhecimento é um repositório de bases de dados ou conhecimentos que armazenam orientações, scripts e soluções para os principais problemas que chegam à Central de Suporte e Atendimento.
 - 4.10.3. Essas informações podem ser utilizadas na solução dos problemas apresentados pelos usuários, por meio de ferramentas especializadas. O

- conhecimento construído e inserido na Base de Conhecimento ao longo da execução dos diversos atendimentos minimiza o custo de suporte para os problemas. Sem a Base de Conhecimento, diferentes técnicos poderiam se defrontar com um mesmo tipo de incidente diversas vezes e resolvê-lo com métodos e resultados diferentes. São vários os benefícios que estimulam a utilização desse repositório de conhecimento, tais como:
- 4.10.3.1. Compartilhamento do conhecimento: através de um mecanismo organizado democratiza o conhecimento dos técnicos;
 - 4.10.3.2. Redução de tempo de resposta: a redução de tempo de resposta para uma solicitação aumenta a capacidade da Central de Atendimento em atender mais demandas;
 - 4.10.3.3. Mesma qualidade de atendimento, independentemente do técnico que atender ao chamado: melhora a condução da equipe, pois todos os técnicos possuem a mesma orientação;
 - 4.10.3.4. Aumento da taxa de resolução no primeiro contato: reduz a necessidade de escalar o problema para um técnico experiente;
 - 4.10.3.5. Menor custo para a Central e menor tempo de resposta aos chamados quando o problema é resolvido na primeira ligação, contatos posteriores são dispensados: o técnico atende um leque maior de requisições, incidentes e problemas. O técnico responsável pode solucionar chamados sobre tópicos que não domina completamente por meio de consultas à Base de Conhecimento;
 - 4.10.3.6. A base deve integrar-se a soluções, com versionamento automatizado e workflows aprovados para mudanças de conhecimento: minimiza as exigências iniciais de treinamento e custos, pois, apoiado pelas experiências encontradas na Base de Conhecimento, os técnicos menos experientes resolvem incidentes de maneira mais rápida;
 - 4.10.3.7. A base serve também de ferramenta de treinamento: a consulta à base proporciona ao técnico o aprendizado sobre novos incidentes e produtos;
 - 4.10.3.8. O conhecimento é capturado e se torna um recurso intelectual da Central de Atendimento: esse conhecimento é aproveitado mesmo depois que o técnico que o agregou deixar a equipe e permite a ausência de alguns técnicos; e
 - 4.10.3.9. O problema é pesquisado e resolvido uma única vez: minimiza o custo de suporte para certos problemas. Sem a Base de Conhecimento, diferentes técnicos poderiam utilizar métodos diversos e obter resultados diferentes.
- 4.10.4. Portanto, a contratada deve manter como obrigação à atualização dos registros da base de conhecimento, bem como o vínculo das soluções aplicadas aos procedimentos constantes deste repositório.
- 4.11. Ferramentas de Gerenciamento de Serviços de TIC – ITSM
- 4.11.1. Como prática recomendada, as ferramentas de gestão de demanda (ITSM) podem ser tratadas como solução de TIC independente da operação de infraestrutura. E a PMESP já dispõe de uma ferramenta desse tipo, que deve ser mantida, suportada e utilizada pela contratada como parte integrante da gestão e governança de TIC. Essa ferramenta permite ao contratante planejar e executar o gerenciamento de demandas, incidentes, problemas e requisições com maior eficiência e estabilidade, além de oferecer controle aprimorado sobre melhorias e ajustes necessários nos processos. Isso contribui diretamente para o aumento da maturidade da área de TI no que diz respeito à gestão de seus serviços.
- 4.11.2. O uso de ferramenta sob gestão do contratante permite ainda uma maior proteção ao histórico do gerenciamento do contrato (essencial para a gestão e renovação contratuais), pois a manutenção e a salvaguarda destes dados encontram-se sob a responsabilidade direta da área de TI da PMESP, que acompanha e monitora processos internos de gestão e de governança de TI.
- 4.11.3. Além disso, permite minimizar riscos de manipulações indevidas e adulterações de dados, principalmente no que se refere aos dados utilizados na aferição dos indicadores de níveis de serviço, tais como o tempo de atendimento dos chamados. Consequentemente, evita-se também a ocorrência de pagamentos incorretos ou indevidos.
- 4.11.4. Os processos de gerenciamento de serviços de TIC devem ser suportados por ferramenta automatizada capaz de, no mínimo:
- 4.11.4.1. Implementar as diretrizes constantes dos processos formalizados de requisição de serviços, mudanças, problema e incidentes e configuração;
 - 4.11.4.2. Implementar o fluxo de classificação de chamados, conforme processos formalizados. Além do gerenciamento de incidentes e solicitações, a ferramenta deverá ser utilizada para controle de atividades relacionadas à segurança cibernética, incluindo monitoramento de ameaças, gestão de patches e vulnerabilidades de endpoints, garantindo registro e rastreabilidade de todas as ações corretivas e preventivas.
 - 4.11.4.3. Implementar controles temporais por categoria de chamado;
 - 4.11.4.4. Possibilitar a extração de dados analíticos e consolidados com vistas a permitir a verificação de níveis mínimos de serviço;
 - 4.11.4.5. Assegurar a integridade, autenticidade e disponibilidade dos dados processados e armazenados; e
 - 4.11.4.6. Possibilitar a aferição de satisfação do atendimento pelo demandante do serviço.
- 4.11.5. Todas as demandas devem ser registradas diretamente na ferramenta de gerenciamento de serviços de TIC, com registro automatizado com carimbo de tempo (timestamp), log de alterações e identificação do operador para garantir trilha de auditoria forense conforme ISO/IEC 27037 com fins de mensurar o tempo de atendimento de cada chamado.
- 4.11.6. A contratada será obrigada a utilizar essa ferramenta para documentar e gerenciar todas as suas atividades técnicas, assegurando total rastreabilidade e conformidade com os processos definidos. Demandas atendidas fora da ferramenta não serão aceitas, reforçando a obrigatoriedade de seu uso como canal oficial de registro e controle.
- 4.12. Estrutura dos Serviços a serem contratados
- 4.12.1. Da estrutura
- 4.12.1.1. O modelo é estruturado em Categorias de Serviços, separadas por áreas de atuação e especialidades. Cada Categoria de Serviço é composta por Perfis de Trabalho e possui suas atribuições e atividades de referência.
- 4.12.1.2. As atribuições e atividades listadas em anexo não são exaustivas, mas sim uma referência das atividades a serem desempenhadas de acordo com a especialidade de cada Categoria.
- 4.12.2. Definição do objeto
- 4.12.2.1. O objeto da contratação ficou definido com vistas a atender as necessidades da PMESP. A estrutura do objeto considerou a estratégia mais adequada de contratação com vistas a mitigar riscos e assegurar a prestação dos serviços de infraestrutura com qualidade.
- 4.12.2.2. Agrupamento de categorias e perfil de profissionais em departamentos por localidade e por ambientes, a seguir:

Departamento /Divisão /Seção	Descrição – Categoria de Serviço	Perfil de Trabalho	Atribuição	Qtd	HTS	HTM
------------------------------------	----------------------------------------	-----------------------	------------	-----	-----	-----

DAS/DOI DPC /DIVCIBER	Gerente de infraestrutura de tecnologia da informação	Serviço de Gestão de TIC	Coordenador /Governança /Gestão	1	176	176
	Gerente de suporte técnico de tecnologia da informação	Serviço de Governança de TIC	Projetos /Processos	1	176	176
	Analista de sistemas de automação - Júnior	Serviço de Suporte Técnico de Operação SO /NOC/SOC	SOC/NOC/SO	8	180	1440
	Técnico de suporte ao usuário de tecnologia da informação Júnior	Serviço de Infraestrutura Data Center e Redes	N1/Dispatcher	2	176	352
	Técnico de Rede (Telecomunicações) - Júnior	Serviço de Infraestrutura Data Center e Redes	Cabista	1	176	176
	Gerente de suporte técnico de tecnologia da informação	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	Líder	1	176	176
	Analista de suporte computacional Pleno	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	Windows, Linux - Pleno	4	176	704
		Serviço de Suporte Técnico às				

DAS/DOI /SPD	Administrador de sistemas operacionais Sênior	Demandas e Mudanças de TIC de Data Center	Windows, Linux - Senior	4	176	704
	Administrador de sistemas operacionais Sênior	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	Notes - Senior	3	176	528
	Administrador de banco de dados - Sênior	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	DBA SQL e (Oracle) - Senior	1	176	176
	Administrador de banco de dados - Pleno	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	DBA SQL - Pleno	2	176	352
	Especialista em Cloud Sênior	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	IA - Arquiteto de Solução - Senior	1	176	176
	Gerente de segurança da informação	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	Lider de Segurança	1	176	176
		Serviço de Suporte				

DAS/DOI /SER	Gerente de segurança da informação	Técnico às Demandas e Mudanças de TIC de Data Center	Líder de Infraestrutura	1	176	176
	Analista de redes e de comunicação de dados Sênior	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	N3	4	176	704
	Analista de redes e de comunicação de dados Pleno	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	N2	7	176	1232
DPC /DIVCIBER	Administrador em segurança da informação - Sênior	Serviço de Suporte Técnico de Análise de Threat Hunting	Senior	1	176	176
	Analista de sistemas de automação - Pleno	Serviço de Suporte Técnico de Análise Threat Intelligence	Pleno	1	176	176
	Desenvolvedor de sistemas de tecnologia da informação Sênior	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	Full Stack - DevSecOps - Senior	1	176	176
Total				45		7952

Tabela 1 – Quantitativo de serviços por departamento.

4.13. Definição para Vigência do Contrato

4.13.1. Diante da complexidade técnica e logística, o prazo de vigência contratual é de 30 (trinta) meses para a operação de infraestrutura de TIC e cibersegurança e observa que o objeto do presente projeto tem complexidade elevada que demanda do contratado um período de imersão nos processos, fluxos e operações da PMESP. Outro elemento decisivo no dimensionamento adequado da vigência contratual é o tempo de comissionamento e de eventual substituição dos recursos tecnológicos empregados e de transferência do conhecimento acerca da utilização desses recursos, além do período de internalização dos processos e procedimentos de gerenciamento de TIC do contratante.

4.13.2. Estas são justificativas iniciais para a DTIC/PMESP adotar um prazo de vigência que podem levar em consideração a necessidade de adequação dos recursos humanos e tecnológicos, procedimentos e processos à execução dos serviços, assegurando a estabilidade mínima necessária para que o contratado execute adequadamente os serviços esperados.

4.13.3. Definição de Categorias de Serviços

4.13.3.1. A definição de Categorias de Serviços consiste em realizar o agrupamento das atividades conforme suas características e perfis profissionais similares, garantindo a adequada operação da infraestrutura de TIC da PMESP.

4.13.3.2. A prestação dos serviços poderá ocorrer de forma presencial, remota ou híbrida, conforme as necessidades operacionais. Para atividades presenciais realizadas nas instalações físicas da PMESP, deve-se dimensionar adequadamente a quantidade de profissionais e os perfis necessários, conforme quantitativo da tabela acima. Já para atividades remotas, deve-se garantir que a infraestrutura e os protocolos de segurança da informação sejam adequados ao desempenho eficiente das funções, respeitando a continuidade operacional e os requisitos de segurança e escalabilidade.

4.13.3.3. Considerando que a infraestrutura emprega um modelo híbrido de computação em nuvem, com predominância de recursos on-premises, determinadas funções exigirão presença física, enquanto outras serão executadas remotamente. Em especial, operações de SOC (Security Operations Center) ocorrerá de forma contínua e remota. A contratada será responsável por assegurar a segurança da informação, a conformidade com normas e regulamentos e a disponibilidade ininterrupta dos serviços.

4.13.3.4. Para cada categoria identificada, serão definidos os seguintes aspectos:

4.13.3.4.1. Escopo;

4.13.3.4.2. Níveis mínimos de serviço (SLAs);

4.13.3.4.3. Descrição não exaustiva das atividades;

4.13.3.4.4. Descrição dos requisitos de experiência profissional, formação acadêmica e certificações;

4.13.3.4.5. Previsão do uso de ferramentas de automação.

4.13.4. Forma de demanda dos Serviços:

4.13.4.1. A prestação dos serviços ocorrerá sob o modelo de serviço continuado, garantindo continuidade operacional com foco em Zero Trust, escalabilidade horizontal e observância dos princípios de segurança da informação e conformidade com normativas vigentes.

4.13.4.2. Serviços contínuos: Envolvem atividades ininterruptas, como monitoramento, detecção e resposta a incidentes, operações de SOC e NOC, suporte 24x7 e outras funções críticas. Esses serviços não estão vinculados à abertura de Ordens de Serviço (OS), mas sim à manutenção de SLAs previamente definidos e ao acompanhamento por meio de indicadores (KPIs) e relatórios periódicos.

4.13.4.3. Serviços sob demanda: Atividades específicas que exijam execução pontual e que deverão ser iniciadas por meio da abertura de uma Ordem de Serviço (OS), contendo a descrição das parcelas a serem executadas durante o período de vigência contratual.

4.13.4.4. Para os serviços contínuos, a contratada deverá manter um monitoramento ativo e proativo com foco em métricas de detecção, respostas e falhas, auditáveis mensalmente pela contratante, assegurando a mitigação de riscos e a resposta rápida a incidentes e ameaças. O desempenho desses serviços será avaliado com base em métricas previamente estabelecidas, incluindo tempo de resposta, tempo de resolução e outros indicadores de eficiência.

4.13.4.5. Para os serviços sob demanda, a Ordem de Serviço deverá conter no mínimo: o objetivo da OS, a identificação e os perfis profissionais mínimos, a quantidade mínima de profissionais para cada perfil, os produtos/resultados a serem entregues e o prazo de atendimento.

4.13.4.6. Durante a execução contratual, a contratante poderá abrir chamados que envolvem: requisição de serviços, requisição de mudança, resolução de incidentes ou resolução de problemas.

4.13.4.7. A atuação da contratada deverá ser proativa para assegurar os níveis de serviço exigidos e a qualidade dos serviços prestados. Para tanto, todas as ocorrências deverão ser registradas na ferramenta de gerenciamento de demandas (ITSM), garantindo rastreabilidade e governança dos processos.

4.13.4.8. Outra fonte de informações são os alertas e avisos emitidos pelas ferramentas automatizadas que geram requisições para atuação da contratada.

4.13.4.9. Os serviços deverão ser executados observando-se os processos de gerenciamento de TIC da PMESP.

4.13.4.10. Todos os chamados derivados de requisição de mudança, requisição de serviços, problemas e incidentes devem estar associados ao processo de avaliação da satisfação do usuário, exceto aqueles abertos pela própria contratada.

4.13.4.11. Caso o ambiente de TIC da PMESP adote mecanismos de fluxo de entrega contínua (Deployment Pipeline), deve-se prever fluxos de encaminhamento de demandas de implantação utilizando esses recursos, aproximando as equipes de desenvolvimento e operações. No entanto, deve-se assegurar que os níveis de serviço acompanhem tais práticas ágeis.

4.13.4.12. A contratada deverá seguir as diretrizes operacionais, garantindo a continuidade da operação da infraestrutura de TIC com foco em segurança, integridade e resiliência.

4.14. Forma de Estimativa Prévia do Volume de Serviços;

4.14.1. Dimensionamento das necessidades

4.14.1.1. O dimensionamento das equipes necessárias deverá ser realizado pela licitante com base nos Acordos de Nível de Serviço (SLAs) estabelecidos, garantindo a continuidade operacional da infraestrutura de TIC. Para isso, a contratante fornecerá à licitante a quantidade e a tipologia dos chamados registrados no último ano, conforme detalhado em Apêndice.

4.14.1.2. Com essas informações, a contratante tem visibilidade do real esforço de demanda da equipe para garantir o atendimento aos SLAs, considerando tanto os serviços prestados sob demanda, mediante abertura de tickets, quanto aqueles executados de forma contínua, em execução de mão de obra dedicada, a atuação deve ser proativa, dispensando a abertura de OS, assegurando a conformidade com os requisitos operacionais e a disponibilidade permanente das funções contratadas, incluindo o monitoramento ininterrupto do SOC e do NOC.

4.14.2. Levantamento do ambiente

- 4.14.2.1. O ETP e o Termo de Referência apresentam o parque computacional de TIC atual, abrangendo descritivos e quantitativos de equipamentos, tecnologias, modelos, fabricantes e versões de softwares que o compõem, discriminando-os por localidade (local de execução das atividades e tarefas), conforme detalhado no Apêndice.
- 4.14.2.2. Outras informações sobre a capacidade do ambiente devem ser apuradas, em vistoria técnica, tais como:
- 4.14.2.2.1. Volume de dados armazenados e trafegados;
- 4.14.2.2.2. Capacidades de processamento e memória;
- 4.14.2.2.3. Quantitativo de usuários na rede;
- 4.14.2.2.4. Eventuais mudanças no ambiente, como alterações quantitativas ou qualitativas decorrentes de projetos ou aquisições de hardware ou software previstos ou em andamento no órgão contratante, que possam impactar a prestação dos serviços.
- 4.14.2.2.5. Ainda na vistoria técnica, a licitante deverá, em conjunto com a PMESP, avaliar o nível de complexidade dos serviços a serem prestados, considerando as características do ambiente, os sistemas de missão crítica e outros elementos que demandem maturidade processual conforme ISO/IEC 20.000-1:2020. A análise deve assegurar que o dimensionamento dos serviços contemple a continuidade operacional, a segurança da informação e o atendimento aos requisitos, bem como acessar os documentos sigilosos para entendimento da conexão entre o processo e o serviço, tais documentos são importantes ao licitante para conhecer o ambiente PMESP e propor proposta sólida.
- 4.14.3. Definição do local de prestação dos serviços
- 4.14.3.1. A execução dos serviços seguirá a seguinte distribuição:
- 4.14.3.1.1. A operação do SOC (Security Operations Center) serão realizadas integralmente de forma remota.
- 4.14.3.1.2. A equipe alocada na DTIC (Diretoria de Tecnologia da Informação e Comunicação) atuará em regime 5x8 de forma híbrida.
- 4.14.3.1.3. A operação de NOC (Network Operations Center): A execução do suporte será presencial no SO (Setor Operacional) da DTIC.
- 4.14.4. Para os serviços prestados in loco, a contratante fornecerá a infraestrutura necessária à execução das atividades, bem como adequação do ambiente, garantindo conformidade com os padrões estabelecidos na legislação trabalhista e com as normativas de segurança da informação da PMESP, sujeitando-se, todavia, à homologação da contratante.
- 4.14.5. Definição de experiência profissional e formação de equipe:
- 4.14.5.1. A definição dos requisitos de experiência profissional deverá levar em conta as características e necessidades específicas da infraestrutura de TIC da PMESP, assegurando a qualidade da prestação dos serviços e a aderência aos requisitos estabelecidos neste Termo de Referência.
- 4.14.5.2. A categorização dos perfis profissionais (júnior, pleno ou sênior) será determinada pela natureza, criticidade e complexidade dos serviços a serem prestados, garantindo compatibilidade com os SLAs e a necessidade de atuação contínua para os serviços monitorados.
- 4.14.5.3. A contratada será responsável pela contínua atualização e aprimoramento da capacitação de seus profissionais, garantindo o cumprimento dos SLAs e a adequada prestação dos serviços. Dessa forma, não será permitido que o contratante custeie cursos e/ou treinamentos para os profissionais da contratada.
- 4.14.6. Dimensionamento do volume de serviços.
- 4.14.6.1. O dimensionamento do volume de serviços deverá ser realizado pela licitante com base nos Acordos de Nível de Serviço (SLAs) estabelecidos, garantindo que a prestação dos serviços atenda aos requisitos mínimos de desempenho, disponibilidade e segurança da informação.
- 4.14.6.2. Para auxiliar a licitante na definição da equipe necessária ao cumprimento dos SLAs, a contratante fornecerá o histórico de chamados e serviços prestados no último ano, detalhado no Apêndice, incluindo volumes, tipos e padrões de ocorrência. Além disso, a licitante deverá avaliar, na visita técnica obrigatória, o nível de complexidade dos serviços a serem prestados, considerando as características do ambiente, os sistemas de missão crítica e os processos de operação contínua.
- 4.14.6.3. A licitante será responsável por dimensionar a equipe e os recursos necessários para assegurar o atendimento dos SLAs, considerando tanto os serviços sob demanda, que requerem abertura de Ordem de Serviço (OS), quanto os serviços contínuos, que exigem monitoramento e resposta proativa sem necessidade de OS, apesar da apresentação do quadro de serviços que deverão ser prestados.
- 4.14.7. Quantitativo e perfil Profissional.
- 4.14.7.1. O dimensionamento das equipes será realizado pela licitante, com base nos Acordos de Nível de Serviço (SLAs) estabelecidos, no histórico de chamados e Ordens de Serviço (OS) do último ano e nas características do ambiente da PMESP, bem como na tabela de serviços acima.
- 4.14.7.2. A licitante deverá estimar o quantitativo de profissionais necessários para assegurar o cumprimento dos SLAs, garantindo disponibilidade, tempos de resposta e qualidade dos serviços prestados.
- 4.14.7.3. A definição do quantitativo deve ser compatível com a complexidade e criticidade do ambiente operacional, levando em consideração fatores como a infraestrutura de TIC, os sistemas de missão crítica, o volume de chamados e a necessidade de atuação contínua para os serviços monitorados, bem como apresentado na tabela acima.
- 4.14.7.4. A definição dos perfis profissionais deverá considerar os requisitos técnicos necessários para a execução dos serviços, garantindo compatibilidade com o ambiente, o tipo de serviço, os Acordos de Nível de Serviço (SLAs) estabelecidos e as melhores práticas do mercado.
- 4.14.7.5. A equipe 5x8 presencial na DTIC será obrigatória para o suporte e manutenção contínua das operações de TIC da PMESP. Esta equipe será composta, no mínimo, pelos seguintes profissionais nas áreas de atuação:
- 4.14.7.5.1. Perfil de Suporte técnico de tecnologia da informação;
- 4.14.7.5.2. Gerente de suporte técnico de tecnologia da informação – Analista de Projetos;
- 4.14.7.5.3. Perfil de Infraestrutura de tecnologia da informação;
- 4.14.7.5.4. Gerente de infraestrutura e Operações de Data Center
- 4.14.7.5.5. Perfil Data Center;
- 4.14.7.5.6. Gerente de suporte técnico de tecnologia da informação - Líder;
- 4.14.7.5.7. Especialista em Cloud Sênior;
- 4.14.7.5.8. Administrador de sistemas operacionais Sênior – Notes;
- 4.14.7.5.9. Analista de sistemas de automação – Junior – Monitoramento Windows;
- 4.14.7.5.10. Analista de sistemas de automação – Junior – Monitoramento Linux.
- 4.14.7.5.11. Perfil de Banco de Dados;
- 4.14.7.5.12. Administrador de Banco de Dados – Nível Sênior com atuação em ambientes de alta disponibilidade, replicação, monitoramento e segurança de dados conforme ISO/IEC 27.001 e ISSO/IEC 22.301;

- 4.14.7.5.13. Administrador de banco de dados – Pleno;
- 4.14.7.5.14. Perfil de Redes;
- 4.14.7.5.15. Perfil de Segurança da Informação;
- 4.14.7.5.16. Gerente de segurança da Informação – Lider de Segurança;
- 4.14.7.5.17. Gerente de segurança da Informação – Lider de Infraestrutura;
- 4.14.7.5.18. Analista de Segurança Nível 3;
- 4.14.7.5.19. Analista de Redes Nível 3;
- 4.14.7.5.20. Analista de Segurança de Rede -Nível 2 – Pleno;
- 4.14.7.5.21. Analista de Segurança de Aplicações – Nível 2 – Pleno;
- 4.14.7.5.22. Analista de Redes Nível 2 – Pleno;
- 4.14.7.5.23. Perfil de Cibersegurança;
- 4.14.7.5.24. Analista de sistemas de automação – Pleno – Threat Intelligence;
- 4.14.7.5.25. Administrador em segurança da informação – Sênior – Threat Hunting;
- 4.14.7.5.26. Desenvolvedor de sistemas de tecnologia da informação Sênior – Full Stack – DevSecOps - WebSec;
- 4.14.7.5.27. Perfil de Sistemas Operacionais (Windows);
- 4.14.7.5.28. Administrador de Sistemas Operacionais Sênior;
- 4.14.7.5.29. Analista de suporte computacional Pleno;
- 4.14.7.5.30. Perfil de Sistemas Operacionais Sênior (Linux);
- 4.14.7.5.31. Administrador de Sistemas Operacionais Sênior;
- 4.14.7.5.32. Analista de suporte computacional Pleno;
- 4.14.7.5.33. Técnico de redes;
- 4.14.7.5.34. Técnico de rede (telecomunicações) – Junior – Cabista;
- 4.14.7.6. Os profissionais alocados na DTIC terão as seguintes responsabilidades:
 - 4.14.7.6.1. Atendimento a incidentes críticos que exijam presença física;
 - 4.14.7.6.2. Manutenção de equipamentos e infraestrutura local;
 - 4.14.7.6.3. Suporte presencial a sistemas de missão crítica e serviços essenciais;
 - 4.14.7.6.4. Coordenação com a equipe remota do SOC para resolução de problemas;
 - 4.14.7.6.5. Execução de rotinas operacionais para garantir a continuidade e segurança dos serviços;
 - 4.14.7.6.6. Interação com usuários para suporte técnico avançado em ambiente on-premises;
 - 4.14.7.6.7. Outras atividades que demandem intervenção local para manutenção da operação.
 - 4.14.7.6.8. Estimativa das equipes do SOC.
- 4.14.7.7. Áreas de atuação para os profissionais:
 - 4.14.7.7.1. Perfil de Gerente de suporte técnico de tecnologia da informação -Processos, Governança;
 - 4.14.7.7.2. Perfil de Gerente de suporte técnico de tecnologia da informação -ITSM;
 - 4.14.7.7.3. Perfil de Analista de sistemas de automação – Sênior – Zabbix, Grafana, ITSM, EDR, XDR, SIEM, SYSLOG, APM, NPM e NPB;
 - 4.14.7.7.4. Perfil de Analista de sistemas de automação – Júnior – Monitoramento;
 - 4.14.7.7.5. Perfil de Analista de sistemas de automação – Júnior – Monitoramento;
 - 4.14.7.7.6. Perfil de Analista de sistemas de automação – Júnior – Dispatcher;
- 4.14.7.8. As equipes responsáveis pela operação do SOC e NOC que executarão o trabalho em 24x7, deverão ser ajustadas pela contratada com base nos seguintes fatores:
 - 4.14.7.8.1. Acordos de Nível de Serviço (SLAs) estabelecidos;
 - 4.14.7.8.2. Volume de requisições, registrados no último ano;
 - 4.14.7.8.3. Complexidade, interdependência de sistemas e criticidade operacional dos ambientes da PMESP;
 - 4.14.7.8.4. Processos operacionais e requisitos de monitoramento contínuo;
 - 4.14.7.8.5. Garantia da disponibilidade e integridade dos serviços.
 - 4.14.7.8.6. A categorização dos perfis poderá seguir níveis de complexidade, como júnior, pleno e sênior, conforme aplicável a cada função e de acordo com as exigências técnicas dos serviços a serem executados.
 - 4.14.7.8.7. Importante: Os perfis profissionais definidos neste dimensionamento devem estar diretamente associados à execução técnica dos serviços, que, por sua vez, estão relacionados a critérios de qualidade, níveis mínimos de serviços, critérios de aceitação e resultados esperados.
- 4.14.8. Estimativa das demandas:
 - 4.14.8.1. O modelo de estimativa das demandas para a contratação baseia-se na prestação dos serviços conforme os Acordos de Nível de Serviço (SLAs) estabelecidos, considerando:
 - 4.14.8.1.1. Um dos elementos principais é o quantitativo e o perfil de pessoal estimados pela licitante para cumprir os SLAs. Essa projeção deve considerar o histórico de chamados, o volume de Ordens de Serviço (OS) e a complexidade do ambiente tecnológico da PMESP, garantindo que a equipe proposta esteja dimensionada para atender às demandas com eficiência, além do quadro apresentado acima com o quantitativo de serviços.
 - 4.14.8.1.2. A estimativa dos custos diretos e indiretos, incluindo software, licenças, infraestrutura necessária para execução dos serviços e outras despesas operacionais relevantes;
 - 4.14.8.1.3. Para os serviços sob demanda, a licitante deverá considerar a previsão de execução de Ordens de Serviço (OS) com base na recorrência histórica, sem fixação prévia de volume de atividades, mas garantindo disponibilidade compatível com as necessidades do ambiente da PMESP.
 - 4.14.8.1.4. A composição do TCO (Total Cost of Ownership), incluindo custos de operação, atualização tecnológica, licenciamento, manutenção e segurança cibernética deverá incluir todos os custos operacionais diretos e indiretos, incluindo impostos, lucros e demais encargos, dentro das condições contratuais exigidas.
 - 4.14.8.1.5. A eficiência da contratada pelos serviços prestados será baseado no atendimento dos SLAs, com mensuração fundamentada nos KPIs estabelecidos, visando garantir a operação ininterrupta dos serviços monitorados. Para isso, serão considerados indicadores como SLA, MTTR, FCR, CSAT e taxa de incidentes recorrentes e outros parâmetros descritos no Instrumento de Medição de Resultado (IMR) – anexo A.
- 4.15. Acordo de Nível de Serviço (SLA):

- 4.15.1. Independentemente do escalonamento entre os níveis de suporte e serviços sob responsabilidade da CONTRATADA, o atendimento às requisições e incidentes deverá respeitar os tempos máximos estabelecidos pela CONTRATANTE. A classificação das requisições e incidentes será realizada com base nos critérios de Impacto e Urgência, garantindo o atendimento às prioridades institucionais e à continuidade das operações e a segurança.
- 4.15.2. A urgência e o impacto deverão ser classificados em alto (1), médio (2) e baixo (3):
- 4.15.2.1. Impacto: Determinado pelo alcance da falha e o número de usuários ou sistemas afetados, bem como o impacto na continuidade operacional da CONTRATANTE.
- 4.15.2.2. Urgência: Avaliada com base na necessidade de resolução imediata e no risco de agravamento do incidente.
- 4.15.3. A prioridade será definida por um agrupamento realizado sobre o resultado da multiplicação entre a urgência e o impacto;
- 4.15.4. A Tabela 1, apresentada a seguir, descreve o resultado da multiplicação entre urgência e impacto, de maneira a se obter a prioridade associada:

		Impacto		
		Baixo – 1	Médio - 2	Alto – 3
Urgência	Alta – 3	3	6	9
	Média – 2	2	4	6
	Baixa – 1	1	2	3

- 4.15.5. A Tabela 2 a seguir apresenta a prioridade derivada de um agrupamento realizado sobre o resultado da multiplicação entre urgência e impacto, bem como exemplos de tempo máximo para resolução, relativos a cada um dos níveis de prioridade descritos:

Prioridade	
9	CRÍTICA
6	Alta
3-4	Média
2	Baixa
1	Agendada

- 4.15.5.1. Tempo de Solução
- 4.15.5.1.1. O CONTRATANTE definiu 5 níveis de prioridade demonstrados nos quadros acima e 5 níveis de atendimento, desta forma, o Tempo de Solução para o atendimento é obtido por meio da combinação destes vetores e está demonstrado nos itens a seguir:
- 4.15.5.1.2. Priorização de Incidentes para todos os Serviços Governança, Cibersegurança, SPD e SER.
- 4.15.5.1.3. Deverá ser utilizada a tabela de impacto conforme a Tabela 3, a seguir:

Impacto	Descrição
Alto	Quando atinge a 70% ou mais da organização, 100% de uma localidade ou a IC classificados como críticos.

Médio	Quando atinge a mais de 40% e menos de 70% da organização, afeta a dois ou mais serviços de uma localidade ou a IC classificados como relevantes (de produção e não críticos).
Baixo	Quando atinge a 40% ou menos da organização, a somente 1 (um) serviço de uma localidade ou a IC que não sejam de produção.

4.15.5.1.4. Também deverá ser utilizada a Tabela 4 para a classificação de urgência.

Urgência	Descrição
Alta	Quando os IC ou Serviços (de Negócios) atingidos são classificados como críticos.
Média	Quando os IC ou Serviços (de Negócios) atingidos são classificados como relevantes (de produção e não críticos).
Baixa	Quando os IC ou Serviços (de Negócios) atingidos não são de produção (desenvolvimento, testes, etc.).

4.15.5.1.5. Finalmente, a Tabela 5 apresenta a priorização que deverá ser adotada:

Prioridade	Observação	Tempo de Solução
CRÍTICA (S1)	Devem ser inclusos nessa categoria de priorização todos IC que sustentem os serviços (de Negócio) definidos pelo CONTRATANTE como estratégicos. Dá-se quando o recurso computacional, equipamento ou softwares (programas aplicativos, módulos de sistemas, sistemas aplicativos e suas derivações) está parado (indisponível) em razão de pane, falha ou não-conformidade técnica.	2 horas
Alta (S2)	Devem ser inclusos nessa categoria os incidentes de prioridade média que afetem 70% ou mais das localidades remotas. Dá-se quando o recurso computacional, equipamento ou softwares (programas aplicativos, módulos de sistemas, sistemas aplicativos e suas derivações) apresenta pane, falha ou não-conformidade técnica que prejudica o uso de uma função básica.	4 horas
Média (S3)	Devem ser inclusos nessa categoria os incidentes de prioridade baixa que afetem mais de 40% e menos de 70% das localidades remotas. Dá-se quando o recurso computacional, equipamento ou softwares (programas aplicativos, módulos de sistemas, sistemas aplicativos e suas derivações) apresenta pane, falha ou não-conformidade técnica que provoca restrições ao uso de algumas funções acessórias.	12 horas

Baixa (S4)	Devem ser inclusas nessa categoria mudanças de médio porte (criação de estruturas de rede, reset de servidor de testes, etc.), liberação de acesso, criação de usuário no ambiente AD, etc. Demanda de assistência técnica para a instalação, configuração, customização, otimização ou migração do recurso computacional ou do equipamento de conectividade de rede.	24 horas úteis
Agendada (S5)	Devem ser inclusas nessa categoria mudanças de pequeno porte (movimentação de dados, criação de novo ambiente de desenvolvimento padrão, etc.). Inclui também demanda sazonal de serviços para a instalação, configuração, customização, otimização ou migração simultânea de novos recursos computacionais (hardware e software) ou de equipamentos de conectividade de rede em várias Organizações Policiais Militares (OPM).	Agendada

4.15.5.2. Incidentes de segurança sempre deverão ser atendidos com prioridade CRÍTICA. (e.g.: Infecção de Vírus, atualização de segurança de roteadores e firewalls).

4.15.5.3. Nos casos de impossibilidade da solução de problemas, a contratada deverá demonstrar evidências, por meio de informações diretamente dos fabricantes dos recursos suportados.

4.15.5.4. Para os casos em que a solução dos incidentes/problemas não for possível pelos técnicos da CONTRATADA, há necessidade que a contate o fabricante, mesmo que a Polícia Militar não possua contrato de manutenção;

4.15.6. Priorização de Solicitação de Serviços

4.15.6.1. Além dos Incidentes, a CONTRATADA deverá também atender às solicitações de serviços como criação de usuário, execução de backup, instalação de aplicativos, etc., assim como mudanças pequenas e médias e para isso deverá considerar a Tabela 6, a seguir:

Prioridade	Observação	Tempo de Solução
CRÍTICA (S1)	Ambientes (estações de trabalho) de usuários VIP. Mudanças emergenciais essenciais para manter IC e serviços (de negócios) classificados como críticos.	2 horas
Alta (S2)	Mudanças emergenciais que sejam essenciais para manter IC de produção não críticos ou de 70% ou mais das localidades remotas.	8 horas
Média (S3)	Instalação de aplicativos pré-aprovados. Mudanças que sejam essenciais para manter mais de 40% e menos de 70% das localidades remotas.	24 horas úteis
Baixa (S4)	Mudanças não emergenciais. Manutenção preventiva de ambiente (estações de trabalho) de usuários.	48 horas úteis
	Instalação de aplicativos não homologados (onde seja necessário todo o processo de aprovação da	

Agendada (S5)	<p>aquisição e homologação do mesmo no ambiente do CONTRATANTE).</p> <p>Também devem ser incluídas nessa categoria mudanças de médio porte (movimentação de dados, criação de novo ambiente de desenvolvimento padrão, etc.).</p>	Agendada
----------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------

- 4.15.7. A CONTRATADA deverá garantir a disponibilidade do Ambiente Computacional, por meio do desempenho dos serviços prestados, dimensionados com base nos seguintes padrões mínimos de desempenho:
- 4.15.7.1. Índice de Atendimento de Chamados Técnicos: todos os chamados técnicos encaminhados ao atendimento de terceiro nível devem ser atendidos;
- 4.15.7.2. Taxa de Resolução de Chamados Técnicos e de Ocorrências: o limite mínimo de resolução de chamados técnicos no atendimento de terceiro nível, dentro dos limites de tempo (SLA) dos níveis de severidade, é de 85% (oitenta e cinco por cento) do total mensal;
- 4.16. Gestão e Monitoramento dos Níveis de Serviço
- 4.16.1. Classificação dos chamados: A área de gestão da CONTRATANTE definirá o impacto e a criticidade de cada atendimento com base no catálogo de serviços.
- 4.16.2. Registro e rastreamento: Todos os chamados deverão ser registrados em uma plataforma ITSM com suporte à trilha de auditoria, categorização automática, classificação por criticidade, priorização por tipo de ativo e integração com dashboards operacionais e estratégicos, garantindo rastreabilidade e governança dos processos.
- 4.16.3. Escalonamento: O escalonamento dos atendimentos seguirá os níveis de suporte e serviços sob responsabilidade da CONTRATADA, respeitando os tempos máximos definidos.
- 4.16.4. Avaliação de desempenho: O cumprimento dos SLAs será avaliado por meio de métricas e KPIs, considerando tempo de resposta, tempo de resolução e satisfação do usuário.
- 4.16.5. Melhoria contínua: A CONTRATADA deverá implementar um ciclo contínuo de melhoria (PDCA), com base em análises mensais de desempenho, revisão de incidentes críticos, planos de ação corretivos, e propostas de otimização validadas pela contratante, assegurando a mitigação de riscos e a disponibilidade dos sistemas críticos.
- 4.17. Aspectos de segurança da informação:
- 4.17.1. Deve-se observar, na construção dos artefatos de planejamento da contratação, as diretrizes constantes de Guias e Frameworks de Segurança da Informação e Privacidade, garantindo a conformidade com boas práticas e normativas vigentes.
- 4.17.2. A definição dos requisitos de segurança da informação deve considerar três dimensões e estar alinhada à ISO/IEC 27.701, no tocante à proteção de dados pessoais e privacidade, considerando o impacto da LGPD.
- 4.17.2.1. Prevenção: A capacidade de prevenir a ocorrência de incidentes de segurança;
- 4.17.2.2. Detecção: A capacidade de prover uma resposta rápida na identificação de incidentes de segurança que não puderam ser prevenidos;
- 4.17.2.3. Correção: A capacidade de restaurar ou mitigar o impacto dos incidentes de segurança detectados.
- 4.17.3. As ações das categorias de segurança da informação e banco de dados devem ser supervisionadas por equipe da PMESP. A contratada deverá seguir as diretrizes de segurança estabelecidas e garantir conformidade com políticas internas e SLAs definidos no projeto.
- 4.17.4. A arquitetura de segurança proposta deverá contemplar proteção contra ameaças avançadas e fraudes digitais modernas, como:
- 4.17.4.1. BEC (Business Email Compromise);
- 4.17.4.2. Falsificação de identidade digital (deepfakes, spoofing);
- 4.17.4.3. Ataques de engenharia social com uso de dados públicos e OSINT;
- 4.17.4.4. Ataques à cadeia de suprimentos de software;
- 4.17.4.5. Malware fileless e persistente (APT).
- 4.17.4.6. Para mitigar essas ameaças, recomenda-se a aplicação combinada de:
- 4.17.4.6.1. Autenticação multifator adaptativa (com base em comportamento);
- 4.17.4.6.2. Análise comportamental com inteligência artificial;
- 4.17.4.6.3. Controles de Zero Trust em rede, identidade e dispositivo;
- 4.17.4.6.4. Educação contínua em segurança e campanhas de phishing simuladas para fortalecer a cultura de segurança.
- 4.18. Mecanismos de Controle e Acompanhamento:
- 4.18.1. Por se tratar de uma contratação com pagamento mensal vinculado a mão de obra dedicado, com mecanismo de atendimento de níveis mínimos de serviço (SLAs) por meio do IMR, a execução do contrato deve seguir as diretrizes a seguir:
- 4.18.1.1. O contratado deverá alocar os profissionais com as qualificações exigidas para cada perfil, conforme estabelecido no contrato.
- 4.18.2. A fiscalização do contrato verificará:
- 4.18.2.1. O alcance do objetivo do serviço contratado;
- 4.18.2.2. A qualidade dos produtos/resultados entregues;
- 4.18.2.3. O cumprimento dos SLAs estabelecidos, garantindo conformidade com os níveis mínimos de serviço;
- 4.18.2.4. A execução das Ordens de Serviço (OS), verificando prazos, qualidade da entrega e alinhamento com os requisitos técnicos.
- 4.18.3. O contratado possui gestão sobre a equipe alocada, podendo realizar alterações na quantidade de profissionais, desde que mantenha a qualificação mínima exigida para cada perfil e assegure a execução das Ordens de Serviço (OS) dentro dos prazos e requisitos definidos.
- 4.18.4. As Ordens de Serviço (OS) serão utilizadas para formalizar demandas específicas dentro do contrato, devendo conter, no mínimo:
- 4.18.4.1. A descrição do serviço a ser realizado;
- 4.18.4.2. Os perfis profissionais necessários para a execução da atividade;

- 4.18.4.3. O prazo de atendimento e conclusão;
- 4.18.4.4. Os critérios de aceitação e validação da entrega;
- 4.18.4.5. A associação com os SLAs aplicáveis para avaliação de conformidade.
- 4.19. Fiscalização Técnica do Contrato:
 - 4.19.1. A fiscalização técnica do contrato será conduzida pelo fiscal técnico, que verificará:
 - 4.19.1.1. A qualidade dos serviços prestados;
 - 4.19.1.2. O cumprimento dos prazos máximos definidos nos SLAs;
 - 4.19.1.3. A correta alocação de profissionais, garantindo a qualificação mínima prevista.
 - 4.19.2. Os relatórios de acompanhamento dos serviços devem ser elaborados mensalmente pela equipe de fiscalização do contrato, subsidiando o gestor na apuração do valor mensal a ser autorizado para pagamento.
 - 4.19.3. Esse instrumento de controle deve conter, no mínimo:
 - 4.19.3.1. A apuração dos indicadores de níveis de serviço, conforme definido no item de SLAs;
 - 4.19.3.2. Registros de ocorrências e demais informações necessárias para avaliação da execução contratual.
 - 4.19.4. Os relatórios são ferramentas essenciais para a fiscalização e gestão do contrato, proporcionando acesso a informações estratégicas para a tomada de decisão na área de TI.
 - 4.19.5. A produção dos relatórios deverá ser baseada em dados automatizados provenientes de sistemas sob controle do contratante, evitando dependência exclusiva de declarações da contratada e assegurando integridade, consistência e imparcialidade nas avaliações.
 - 4.19.6. Durante o planejamento da contratação, o órgão contratante deve avaliar processos e mecanismos de governança que assegurem:
 - 4.19.6.1. A integridade das informações utilizadas na fiscalização contratual;
 - 4.19.6.2. A existência de ferramentas adequadas para monitoramento dos níveis de serviço esperados;
 - 4.19.6.3. A viabilidade de geração ágil, precisa e segura dos relatórios de acompanhamento.
- 4.20. Indicador de Medição de Resultado (IMR) e Determinação do Valor Final de Eficiência:
 - 4.20.1. O Indicador de Medição de Resultado (IMR) será utilizado como instrumento para consolidar a avaliação do desempenho da contratada, garantindo que o pagamento mensal seja realizado de acordo com a qualidade dos serviços prestados.
 - 4.20.2. O IMR será calculado com base nos seguintes elementos:
 - 4.20.2.1. O cumprimento dos SLAs estabelecidos;
 - 4.20.2.2. A execução das demandas deverá ser monitorada em tempo real, com SLA específico, incluindo controle de backlog, cancelamentos e reaberturas, além de rastreamento por ticket e responsável técnico;
 - 4.20.2.3. A avaliação dos relatórios de fiscalização técnica;
 - 4.20.2.4. O atendimento aos indicadores de níveis de serviço previamente estabelecidos no contrato.
 - 4.20.3. Reitera que o presente ETP tem por objeto a contratação de empresa especializada para a prestação de serviços continuados, com fornecimento de mão de obra com dedicação exclusiva, distribuída em postos de trabalho previamente dimensionados.
 - 4.20.4. A contratação visa assegurar a execução regular, eficiente e ininterrupta das atividades de apoio necessárias ao adequado funcionamento da cibersegurança, data center e redes da PMESP, garantindo padrões mínimos de qualidade, produtividade e tempestividade.
 - 4.20.5. E considerando a necessidade institucional de aprimorar o controle e a fiscalização da execução contratual, a administração opta pela adoção de modelo de mensuração por desempenho, de acordo com os parâmetros previstos no art. 144 da Lei nº 14.133/2021, vinculando o pagamento mensal ao resultado obtido pela contratada mediante apuração do Índice de Medição de Resultados (IMR), em anexo.
 - 4.20.6. A escolha por este modelo decorre da necessidade de assegurar que os recursos públicos sejam aplicados com eficiência, eficácia e economicidade, observando os princípios previstos no art. 5º da Lei nº 14.133/2021. A remuneração fixa por mão de obra com posto de trabalho, combinada com o ajuste financeiro proporcional ao desempenho aferido mensalmente, reduz riscos de inexecução e incentiva a contratada a manter níveis elevados de qualidade, presença, produtividade e cumprimento de prazos. Tal abordagem contribui para uma gestão contratual mais transparente, objetiva e alinhada ao interesse público, evitando subjetividade na avaliação e garantindo que o pagamento reflita a entrega efetiva dos serviços contratados.
 - 4.20.7. Os serviços deverão ser prestados de forma contínua, com disponibilidade dos profissionais alocados, observadas as qualificações exigidas para cada função e respeitadas todas as normas trabalhistas, previdenciárias, de segurança e saúde ocupacional. A contratada deverá manter coordenação técnica permanente, responsabilizando-se pela orientação operacional das equipes e pela substituição de colaboradores que não atendam às especificações ou apresentem comportamento incompatível com o ambiente institucional.
 - 4.20.8. Caberá ainda à contratada garantir o cumprimento das obrigações legais, apresentar mensalmente documentos comprobatórios de regularidade e atender integralmente às determinações da fiscalização.
 - 4.20.9. O IMR será apurado mensalmente pela fiscalização designada, com base em indicadores como assiduidade, pontualidade, qualidade técnica da execução, produtividade e satisfação do usuário, todos devidamente descritos no ETP e em seus anexos. Cada indicador possuirá metodologia de cálculo, pesos específicos e metas mínimas que deverão ser alcançadas. A pontuação final do SLA definirá o percentual de pagamento devido no mês correspondente, permitindo descontos quando houver desempenho inferior ao pactuado.
 - 4.20.10. O não atendimento das metas instituídas implicará aplicação automática de glosas e descontos na fatura subsequente, sem prejuízo das penalidades previstas nos arts. 155 a 159 da Lei nº 14.133/2021. A contratada será notificada sobre a apuração mensal e poderá apresentar manifestação, contudo a apresentação de defesa não suspenderá a aplicação dos ajustes financeiros.
 - 4.20.11. A fiscalização do contrato será realizada por gestor e fiscais designados pelo Dirigente, observando os procedimentos previstos nos arts. 117 a 120 da Lei nº 14.133/2021. A equipe fiscal registrará ocorrências relevantes, acompanhará a execução dos serviços, verificará o cumprimento das obrigações contratuais e realizará reuniões periódicas com a contratada para alinhamento, correção de desvios e orientação de melhorias.
 - 4.20.12. Diante do exposto, a contratação é necessária, adequada e eficiente, sendo justificável a adoção do modelo de remuneração por mão de obra com dedicação exclusiva combinado com pagamento atrelado ao desempenho por meio de SLA.
 - 4.20.13. Por fim, o presente ETP apresenta os elementos técnicos essenciais para orientar a licitação e a futura gestão contratual, assegurando que os serviços sejam prestados com qualidade, regularidade e observância do interesse público.

5. Necessidades Tecnológicas

- 5.1. O ambiente da CONTRATANTE é baseado em diversas plataformas computacionais, exigindo que os profissionais designados pela CONTRATADA possuam domínio tecnológico adequado para a prestação dos serviços.
- 5.2. O ambiente computacional da CONTRATANTE é composto por um conjunto de soluções que incluem servidores físicos e virtuais, armazenamento de dados (storages), backup, ferramentas de controle e monitoramento, segurança da informação e redes.
- 5.3. A integração dessas soluções no data center garante o uso eficiente dos recursos, proporcionando um ambiente de alta disponibilidade, seguro e capaz de manter o legado de bens e serviços necessários para o atendimento corporativo da CONTRATANTE e seus sistemas de domínio público.
- 5.4. Esses serviços também asseguram a segurança da informação por meio da combinação de ativos de segurança, como NG-Firewalls e IPS, sendo responsáveis por disponibilizar acesso à Internet e Intragov para as redes da CONTRATANTE, e das Organização Policial Militar distribuídas no Estado, através da Unidade Provedora de Acesso (UP) centralizada no Datacenter da CONTRATANTE.
- 5.5. A CONTRATANTE busca continuamente melhorar os serviços de TI já utilizados corporativamente, além de prospectar novas tecnologias que atendam às necessidades dos usuários, realizando um trabalho de governança que envolve instâncias internas e externas.
- 5.6. Os recursos a serem utilizados para a prevenção de vazamentos e perdas de informações sensíveis, mas também uma resposta rápida e eficaz a incidentes de segurança, assegurando a continuidade das operações e a confiança da sociedade nos serviços prestados. Além disso, a adoção dessas tecnologias está em consonância com as normas e regulamentações vigentes, promovendo uma abordagem proativa na gestão da segurança cibernética, essencial para o cumprimento das responsabilidades institucionais e a proteção dos dados da corporação.
- 5.7. Além de proporcionar maior proteção, os serviços e soluções contribuirão para a continuidade das operações da corporação, assegurando que a força policial possa agir com confiança e eficiência em suas atividades diárias. A implementação dessas soluções também está alinhada com as normas e regulamentações vigentes, promovendo uma postura proativa na gestão da segurança cibernética.
- 5.8. O ambiente computacional atual inclui as seguintes tecnologias, sendo que sua composição pode ser ajustada conforme a evolução tecnológica e as necessidades institucionais:
 - 5.8.1. Servidores - Sistemas Operacionais:
 - 5.8.1.1. Microsoft;
 - 5.8.1.2. Linux;
 - 5.8.2. Servidores – Banco de Dados:
 - 5.8.2.1. Microsoft SQL;
 - 5.8.2.2. Microsoft ETL;
 - 5.8.3. Servidores – Aplicação:
 - 5.8.3.1. Microsoft .NET Framework;
 - 5.8.3.2. Microsoft Internet Information Server;
 - 5.8.3.3. Apache;
 - 5.8.4. Servidores – Desenvolvimento e homologação e treinamento:
 - 5.8.4.1. Microsoft Visual Studio .NET (ASP, HTML, JS e C);
 - 5.8.4.2. Azure DevOps;
 - 5.8.4.3. Microsoft SQL Server;
 - 5.8.4.4. ArcMap (ArcGis - Geographic Information System);
 - 5.8.4.5. Kong;
 - 5.8.4.6. GIT;
 - 5.8.5. Clientes – Softwares:
 - 5.8.5.1. Microsoft Windows 10 e Windows 11;
 - 5.8.5.2. Microsoft Office 2016/2019/2021;
 - 5.8.5.3. Tableau.
 - 5.8.6. Equipamentos de Datacenter:
 - 5.8.6.1. Backup (Bacula);
 - 5.8.6.2. Armazenamento de dados (Dell, IBM e Huawei);
 - 5.8.6.3. Servidores Dell;
 - 5.8.6.4. Servidores HPE;
 - 5.8.6.5. Servidores Lenovo;
 - 5.8.6.6. Switches Cisco, HPE e Huawei;
 - 5.8.6.7. Roteador Juniper;
 - 5.8.6.8. ProxMox;
 - 5.8.7. Os serviços infraestrutura – Sala Segura Cofre são suportados por outro contrato especializado em data center;
 - 5.8.8. Nuvem Privada:
 - 5.8.8.1. Nós Appliance Hiperconvergente;
 - 5.8.8.2. X-Rail;
 - 5.8.9. Suite de Virtualização de Servidores:
 - 5.8.9.1. Hiper-V;
 - 5.8.9.2. ProxMox;
 - 5.8.9.3. Citrix
 - 5.8.10. Switch ToR:
 - 5.8.10.1. HPE e Huawei;
 - 5.8.11. Solução de Backup:
 - 5.8.11.1. Bacula;
 - 5.8.12. Suite de Virtualização de Desktops:

- 5.8.12.1. Terminal Server;
- 5.8.13. Ativos de Rede e Segurança:
 - 5.8.13.1. Solução Wi-Fi Cisco;
 - 5.8.13.2. Gestão de acesso da Sala Cofre (Access Control);
 - 5.8.13.3. Gestão de Segurança da Informação - Firewall Cisco, Certificado Digital, Anti-Virus (Kaspersky);
- 5.8.14. Serviços de Gerenciamento, Conhecimento, Rede e Segurança:
- 5.8.15. Active Directory;
- 5.8.16. Monitoramento (Zabbix, Grafana e Elastic);
- 5.8.17. DNS (Cisco Umbrella);
- 5.8.18. Autenticação Integrada SSO (ISE);
- 5.8.19. ITSM (Cherwell);
- 5.9. O ambiente tecnológico poderá ser ajustado, a critério da Diretoria da Tecnologia da Informação e Comunicação - DTIC, durante o período da prestação dos serviços, com a devida comunicação à CONTRATADA sobre a necessidade de realinhamento técnico da equipe, face à evolução tecnológica;
- 5.10. Disponibilização da informação
 - 5.10.1. Antes do início da prestação dos serviços previstos neste ETP, a CONTRATANTE, em conjunto com a atual prestadora de serviços, disponibilizará as informações necessárias para garantir a continuidade operacional. Essas informações incluem, no mínimo:
 - 5.10.1.1. Documentação técnica atualizada dos sistemas e infraestruturas sob gestão;
 - 5.10.1.2. Relatórios históricos de chamados e incidentes críticos registrados no ITSM;
 - 5.10.1.3. Inventário atualizado dos ativos de TIC gerenciados no contrato anterior;
 - 5.10.1.4. Configurações operacionais essenciais que impactem diretamente na execução dos serviços no novo contrato.
 - 5.11. Período de Transição Operacional (PTO)
 - 5.11.1. A transição deverá ser iniciada em até 30 (trinta) dias após a assinatura do contrato, constituindo o Período de Transição Operacional (PTO). Esse período de adaptação terá duração máxima de 2 (dois) meses e deverá garantir a migração gradual das responsabilidades para a nova contratada.
 - 5.11.2. Considerando a criticidade das operações de infraestrutura da PMESP, bem como a necessidade administrativa de encerramento e transição de outros contratos vigentes, a Contratada, em conjunto com a Contratante, poderá realizar o faseamento do Plano de Transição Operacional (PTO) por áreas de atuação. Assim, poderá ser estabelecida, por exemplo, a implantação inicial das verticais de Cibersegurança e Redes, com início da execução dos respectivos serviços, e, após o prazo estimado de 2 (dois) meses, iniciar-se a execução dos serviços relativos ao Data Center, ou outro sequenciamento que se mostrar tecnicamente adequado e aprovado pela Contratante.
 - 5.12. Plano de Transição da Gestão dos Serviços
 - 5.12.1. A nova contratada deverá elaborar um Plano de Transição da Gestão dos Serviços, contendo:
 - 5.12.1.1. Definição dos responsáveis pelo processo de transição, incluindo a composição da Equipe de Transição;
 - 5.12.1.2. Identificação dos profissionais alocados para a administração inicial dos serviços;
 - 5.12.1.3. Estratégias para garantir a continuidade e a estabilidade das operações durante o PTO;
 - 5.12.1.4. Critérios e marcos de aceitação que assegurem que a nova contratada possa assumir integralmente as atividades ao final do PTO.
 - 5.12.2. Ainda em diagnóstico para execução do contrato, a Contratada, em acordo com a Contratante, também poderá fasear os serviços de Governança, gerenciamento e monitoramento das demandas e mudanças de TIC.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

- 6.1. Para uma solução de TIC abrangente para suprir as necessidades tecnológicas da Polícia Militar do Estado de São Paulo (PMESP), é fundamental atender a uma série de requisitos que assegurem utilidade, segurança e conformidade.
- 6.2. A solução deve estar alinhada às normas vigentes, como a Lei nº 14.133/2021, que estabelece diretrizes para licitações e contratos, e a Lei Geral de Proteção de Dados Pessoais (LGPD), garantindo a proteção das informações sensíveis. Adicionalmente, a solução deve seguir padrões técnicos reconhecidos, como as normas ABNT NBR ISO/IEC 20.000:2020 para gestão de serviços de TI e ABNT NBR ISO/IEC 27.001:2022 para segurança da informação, bem como estar em conformidade com as diretrizes da Estratégia Nacional de Segurança Cibernética (E-Ciber) e demais políticas públicas aplicáveis ao setor.
- 6.3. Os serviços a serem prestados devem garantir, de forma ininterrupta, aplicações, produtos e ferramentas que assegurem alta disponibilidade e planos de recuperação de desastres. A arquitetura da solução deve prever redundância geográfica e mecanismos de contingência para evitar interrupções nos serviços críticos da PMESP.
- 6.4. Devem ser adotadas práticas modernas e conhecimento técnico avançado em virtualização e computação em nuvem, utilizando tecnologias recomendadas pelo mercado. A solução deve garantir interoperabilidade com sistemas já existentes na PMESP por meio de APIs abertas e padrões de integração, evitando dependência tecnológica exclusiva de fornecedores específicos (vendor lock-in) e permitindo a evolução contínua da infraestrutura.
- 6.5. No que tange à segurança da informação, deve-se implementar mecanismos avançados, incluindo autenticação multifator, gerenciamento de identidades e monitoramento contínuo de eventos de segurança. A arquitetura de segurança deve seguir o modelo Zero Trust, garantindo proteção desde a borda da rede até os endpoints. Devem ser adotadas soluções avançadas de detecção e resposta a ameaças cibernéticas (XDR, SIEM), além de técnicas baseadas em Inteligência Artificial para análise preditiva e resposta automatizada a incidentes. A criptografia de dados críticos deve ser aplicada em trânsito e em repouso, assegurando a proteção das informações sensíveis da PMESP. A auditoria contínua de logs e trilhas de auditoria deve ser realizada em conformidade com as normativas de segurança, garantindo rastreabilidade e conformidade.
- 6.6. A gestão de serviços deve utilizar plataformas robustas para controle de incidentes, requisições e mudanças, além de ferramentas de monitoramento contínuo para acompanhar a disponibilidade e o desempenho da infraestrutura. A operação de um Centro de Operações de Rede e Segurança (NOC e SOC) operando 24 horas é mandatório para garantir monitoramento constante e resposta rápida a incidentes. O modelo de

governança de TI adotado deve seguir as melhores práticas do ITIL v4 e COBIT, promovendo a gestão eficiente dos serviços e a otimização dos recursos tecnológicos. A adoção de metodologias ágeis, como DevSecOps, deve facilitar a execução de projetos e a implantação de novas soluções.

6.7. O modelo de suporte prevê níveis mínimos de serviço previamente estabelecidos (SLAs) e mecanismos de penalidades em caso de descumprimento, seguindo uma abordagem progressiva de sanções conforme o impacto no serviço prestado. Deve ser necessário oferecer suporte técnico especializado, com equipe certificada e atendimento tanto remoto quanto presencial, conforme a criticidade do serviço. O cumprimento dos SLAs será acompanhado por meio de indicadores de desempenho (KPIs), garantindo a qualidade e disponibilidade dos serviços contratados.

6.8. Em termos de infraestrutura, os recursos devem operar de forma a assegurar alta disponibilidade e redundância dos serviços críticos. Ferramentas de backup e planos de recuperação de desastres devem garantir a integridade dos dados da PMESP.

6.9. A sustentabilidade deve ser considerada na escolha e operação da solução de TIC, priorizando a eficiência energética e a redução do consumo de eletricidade. A recomendação de novos equipamentos deve atender a certificações de eficiência energética, e práticas de reaproveitamento e reciclagem de equipamentos obsoletos devem ser seguidas, garantindo descarte seguro e alinhamento às diretrizes ambientais da administração pública. A adoção de fontes de energia renováveis e o uso otimizado dos recursos computacionais devem ser incentivados para minimizar a pegada de carbono da infraestrutura.

6.10. A CONTRATADA deve fornecer relatórios mensais detalhados sobre os serviços prestados, incluindo métricas de disponibilidade da infraestrutura, tempo médio de resolução de incidentes (MTTR), tempo médio entre falhas (MTBF), taxas de conformidade com os SLAs e análise de tendências. Os mecanismos de governança e compliance devem ser implementados para garantir a conformidade contratual, e dashboards em tempo real devem estar disponíveis para acompanhamento contínuo da execução dos serviços pela fiscalização da PMESP, permitindo uma visão gerencial precisa da operação.

6.11. Os serviços contratados deverão seguir as normas técnicas ISO, de acordo com sua área de atuação:

6.11.1. SOC (Security Operations Center): Deverá cumprir as normas ISO 27001 e 20000, garantindo a segurança da informação, a proteção de dados pessoais e a gestão eficiente dos serviços de TI.

6.11.2. NOC (Network Operations Center): Deverá estar em conformidade com a ISO 20000 para gestão de serviços de TI e implementar controles específicos da ISO 27001 para segurança de redes.

6.11.3. Dispatcher: Deverá seguir a ISO 20000, assegurando a gestão eficiente de incidentes, requisições e suporte técnico, conforme as melhores práticas de ITIL e COBIT.

6.12. A adoção dessas normas é essencial para garantir que a solução atenda aos requisitos operacionais, de segurança e compliance, assegurando um ambiente de TI resiliente, seguro e com alta disponibilidade.

6.13. Todos os custos inerentes à execução dos serviços são de responsabilidade exclusiva da Contratada, a quem compete fornecer os meios necessários à plena execução das atividades, contemplando os requisitos indispensáveis para assegurar a continuidade, a qualidade e a segurança das operações de TIC. Ademais, cabe exclusivamente à Contratada definir a logística e o emprego de seus meios para o efetivo atendimento das obrigações previstas em contrato.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. A estimativa da demanda para a contratação de serviços especializados de suporte técnico de cibersegurança, data center e redes, bem como de governança, gerenciamento e monitoramento, das demandas e mudanças de tecnologia da informação e comunicação e infraestrutura de data center e redes para ambiente computacional e de telecomunicações, de forma a garantir a continuidade dos serviços de Tecnologia da Informação e Comunicação (TIC) foi dimensionada com base nas necessidades operacionais da Polícia Militar do Estado de São Paulo (PMESP), considerando a continuidade e o aprimoramento das atividades críticas de infraestrutura tecnológica. A duração prevista para os serviços é de 30 (trinta) meses, alinhada ao planejamento estratégico da corporação e à substituição dos contratos vigentes, que se encerram em breve. A tabela a seguir demonstra os macros itens e as quantidades dos serviços:

Área	Solução	Qtd
1	Serviços de Coordenação/Governança/Gestão, Projetos /Processos e SOC/NOC /Dipscher de TIC	30 meses
2	Serviços de Cibersegurança	30 meses
3	Serviços de Seção de Processamento de Dados – Data Center	30 meses
4	Serviços de Seção de Engenharia de Redes - Redes	30 meses

- 7.2. Essa estimativa reflete a necessidade de serviços contínuos e especializados para garantir a disponibilidade, segurança e suporte técnico do ambiente de TIC da PMESP.
- 7.3. Os serviços presenciais de gerenciamento de infraestrutura atenderão às demandas locais, enquanto as operações de NOC e SOC assegurarão monitoramento e resposta a incidentes 24x7. Já os serviços de Dispatcher, será executado na modalidade 24x7 (atendimento ininterrupto por acionamento de chamados), com o auxílio das ferramentas de monitoramento e observação para oferecer suporte flexível e adequado à criticidade das operações.
- 7.4. A duração de 30 (trinta) meses visa proporcionar estabilidade contratual e tempo suficiente para a implementação e consolidação das soluções propostas.

8. Infraestrutura de serviços

- 8.1. A disponibilização, pela Contratante, de notebooks devidamente licenciados e padronizados para uso pelos colaboradores da Contratada justifica-se pela necessidade de assegurar conformidade tecnológica, uniformidade operacional e plena aderência às políticas internas de segurança da informação da PMESP. A utilização de equipamentos providos pela própria Contratante garante a aplicação centralizada de configurações, políticas de acesso, atualizações, mecanismos de monitoramento, criptografia e demais controles essenciais para a proteção dos ativos digitais institucionais, mitigando riscos relacionados a incidentes cibernéticos, vulnerabilidades de software, incompatibilidades técnicas e utilização de sistemas não homologados. Além disso, a padronização dos dispositivos proporciona maior eficiência no suporte técnico, melhor desempenho operacional das equipes, redução de custos associados à integração e compatibilidade de ambientes, e maior rastreabilidade das atividades realizadas nos sistemas da PMESP. Dessa forma, o fornecimento de notebooks licenciados pela Contratante é medida necessária para garantir segurança, desempenho, governança tecnológica e a continuidade dos serviços com elevado grau de confiabilidade.
- 8.2. Os equipamentos deverão ter capacidade mínima suficiente para atender todos os requisitos do projeto e incluir a versão mais atual do sistema operacional Microsoft Windows para empresas, as versões mais recentes do Microsoft Office 365, além de software de proteção de endpoint, monitor externo de 27 polegadas, mouse e teclado compatíveis com o ambiente administrativo da CONTRATANTE.
- 8.2.1. Para os profissionais que atuarão como Analista de Monitoramento Windows e Analista de Monitoramento Linux, a CONTRATADA deverá fornecer desktops novos, com capacidade mínima suficiente para atender todos os requisitos do projeto. Os equipamentos deverão contar com a versão mais atual do Microsoft Windows para empresas, versões mais recentes do Microsoft Office 365, software de proteção de endpoint, além de dois monitores de 27 polegadas, mouse e teclado compatíveis com o ambiente administrativo da CONTRATANTE.
- 8.2.2. A CONTRATADA deverá providenciar smartphones novos, na razão de uma unidade por escala de sobreaviso, garantindo o pronto acionamento sempre que necessário. Esses aparelhos deverão contar com garantia e suporte da fabricante até o fim do contrato.
- 8.2.3. Considerando o caráter emergencial de determinados atendimentos, especialmente aqueles realizados nos Centros de Operações de Emergência Policial (COPOM) e nos sites de transmissão de voz por rádio (ERB), a CONTRATADA deverá disponibilizar um veículo destinado à locomoção dos profissionais designados, podendo ser veículo próprio ou locado. A medida é necessária para garantir resposta rápida às ocorrências e assegurar a continuidade operacional dos serviços críticos da PMESP. Na hipótese de o veículo estar em uso para outra atividade contratual, os deslocamentos deverão ser realizados por meio de aplicativos de transporte, táxi ou serviço equivalente disponibilizado pela própria CONTRATADA, de forma a não comprometer a tempestividade dos atendimentos.
- 8.2.4. A CONTRATADA será responsável pelo custeio integral de todas as despesas relacionadas a deslocamentos, hospedagens e demais estadias necessárias à execução dos serviços, incluindo acomodações adequadas que garantam condições apropriadas de conforto, segurança e disponibilidade dos profissionais. A demanda operacional prevê uma estimativa anual de aproximadamente 12.000 km em deslocamentos e até 60 dias de hospedagem por ano, valores que deverão ser integralmente considerados na formação dos preços apresentados pela CONTRATADA.
- 8.2.5. No âmbito da Gestão de Serviços de TI (ITSM), a CONTRATADA deverá adotar e suportar o framework ITSM utilizado pela contratante, garantindo que todas as solicitações de serviço e incidentes sejam registradas e gerenciadas de maneira organizada e rastreável. A exigência de que os analistas atendam exclusivamente às demandas registradas na plataforma ITSM visa assegurar transparência, rastreamento completo das atividades, priorização eficiente, padronização dos processos e aumento da eficiência operacional.
- 8.3. Adequação de Infraestrutura:
- 8.3.1. A CONTRATADA será responsável por apresentar um layout prévio para adequação dos ambientes de trabalho disponibilizados pela Polícia Militar, garantindo conformidade com padrões de salubridade, ergonomia e conforto. O projeto deverá contemplar iluminação, climatização, cabeamento elétrico e de rede, bem como o layout do mobiliário novo. A CONTRATANTE terá o direito de aprovar, rejeitar ou sugerir ajustes no projeto, os quais deverão ser incorporados pela CONTRATADA no planejamento final.
- 8.3.2. A infraestrutura dos ambientes deverá incluir câmeras de monitoramento nas salas onde os profissionais da CONTRATADA desempenharão suas funções, bem como a instalação de cabeamento estruturado conforme normas técnicas vigentes, garantindo estabilidade e eficiência nas conexões de dados e energia.
- 8.3.3. Além disso, a CONTRATADA será responsável pelo fornecimento de mobiliário novo e ergonômico, incluindo mesas, cadeiras, armários e outros itens necessários ao ambiente de trabalho. A instalação de equipamentos e acessórios de escritório deverá assegurar um espaço funcional e eficiente, com itens de qualidade comprovada que atendam aos padrões de conforto, ergonomia e durabilidade.
- 8.3.4. Para assegurar a continuidade e a eficiência das operações, a CONTRATADA deverá fornecer todos os materiais de escritório, bem como os insumos diretos e indiretos necessários à execução dos serviços, garantindo sua reposição regular durante todo o período contratual. Além disso, deverá disponibilizar impressoras multifuncionais coloridas, com capacidade de impressão de alta qualidade, digitalização (scanner) e cópia de documentos, instaladas nos locais físicos de prestação dos serviços. Os equipamentos deverão contar com manutenção preventiva e corretiva sempre que necessário, bem como com o fornecimento contínuo de todos os insumos indispensáveis ao seu funcionamento, incluindo toners, cartuchos e demais componentes consumíveis, de modo a evitar interrupções e assegurar plena disponibilidade operacional.
- 8.3.5. Durante toda a vigência do contrato, a CONTRATADA deverá assegurar a manutenção contínua do ambiente de trabalho, incluindo reparos,

ajustes e substituições sempre que necessário para preservar as condições adequadas. Isso envolve atualização da infraestrutura, reposição de materiais e eventuais adequações no layout ou nos equipamentos, garantindo que o ambiente se mantenha seguro, funcional e em conformidade com as exigências da Polícia Militar.

8.4. Qualificação Técnica dos perfis:

8.4.1. Perfil Gerente de suporte técnico de tecnologia da informação:

8.4.1.1. Cargo - Analista de Projetos:

8.4.1.2. Referência, profissional com responsabilidade de coordenar e gerenciar a atuação dos demais técnicos de suporte e de manutenção, garantindo a adequada prestação dos serviços, bem como controlando e planejando operacionalmente as ações da equipe. Presta também apoio à tomada de decisão do órgão auxiliando na prospecção de soluções de suporte ao usuário, fornecimento de informações táticas e operacionais e proposição de ações de aprimoramento dos serviços de suporte ao usuário.

8.4.1.3. Requisitos básicos:

8.4.1.3.1. Deverá possuir uma das certificações abaixo:

8.4.1.3.2. PMP: Project Management Professional;

8.4.1.3.3. CAPM: Certified Associate in Project Management;

8.4.1.3.4. CSM: Certified ScrumMaster;

8.4.1.3.5. CompTIA Project+;

8.4.1.3.6. PRINCE2 Foundation/PRINCE2 Practitioner;

8.4.1.3.7. CPMP: Certified Project Management Practitioner;

8.4.1.3.8. Associate in Project Management;

8.4.1.3.9. MPM: Master Project Manager;

8.4.1.3.10. PPM: Professional in Project Management;

8.4.1.3.11. PMITS: Project Management in IT Security;

8.4.1.3.12. Certified Project Director;

8.4.1.3.13. IAPM Certified Project Manager;

8.4.1.3.14. ITIL V4 Managing Professional Certificate.

8.4.1.3.15. Deverá possuir Ensino Superior completo em áreas de Tecnologia da Informação, Redes, Engenharia da Computação, Cibersegurança ou áreas correlatas reconhecidas pelo MEC;

8.4.1.3.16. Deverá possuir Pós-Graduação completa na área de na área de Gestão ou Gerenciamento de Projetos;

8.4.1.3.17. Comprovação de experiência profissional de 04 (quatro) anos na área de projetos;

8.4.1.3.18. Deverá ter participado de treinamento formal sobre Liderança ou Gerenciamento de Pessoas com no mínimo 40 horas de duração, com certificado de participação.

8.4.1.4. Os serviços deverão ser prestados presencialmente, com disponibilidade mínima de 40 horas semanais, compatível com o expediente da Polícia Militar, de segunda a sexta-feira, das 09h às 18h, com possibilidade de escalas especiais mediante demanda crítica;

8.4.2. Gerente de Infraestrutura de Tecnologia da Informação

8.4.2.1. Cargo - Gerente de Infraestrutura e Operações de Data Center

8.4.2.2. Referência, profissional com responsabilidade de coordenar e gerenciar a atuação dos demais profissionais alocados no monitoramento, controle e operação da infraestrutura de TIC, garantindo a adequada prestação dos serviços, bem como controlando e planejando operacionalmente as ações dessa equipe. Presta também apoio à tomada de decisão do órgão auxiliando na prospecção de soluções de infraestrutura de TIC, fornecimento de informações táticas e operacionais, e proposição de ações de aprimoramento dos serviços de operações na infraestrutura de TIC.

8.4.2.3. Requisitos básicos:

8.4.2.3.1. Deverá possuir uma das certificações abaixo:

8.4.2.3.2. Project Management Professional (PMP);

8.4.2.3.3. Microsoft Certified: Azure Solutions Architect Expert;

8.4.2.3.4. Microsoft Certified: Cybersecurity Architect Expert;

8.4.2.3.5. Microsoft Certified: DevOps Engineer Expert;

8.4.2.3.6. Microsoft Certified Systems Engineer (MCSE);

8.4.2.3.7. Cisco Certified Network Professional (CCNP);

8.4.2.3.8. Aruba Certified Switching Professional (ACSP);

8.4.2.3.9. Juniper Professional (JNCIP-ENT);

8.4.2.3.10. Huawei Certified ICT Professional Routing & Switching (HCIP-Routing & Switching);

8.4.2.3.11. Certificação de nível Profissional ou equivalente emitida por órgão autorizado ou pelo próprio fabricante;

8.4.2.3.12. Treinamento em Gestão de Pessoas com pelo menos 40 horas semanais, com certificado de participação;

8.4.2.3.13. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;

8.4.2.3.14. Deverá possuir Pós-Graduação completa na área de Tecnologia da Informação, Redes, Segurança, Gestão de Pessoas, Gestão de Projetos ou Governança;

8.4.2.3.15. Comprovação de experiência profissional de 08 (oito) anos na área de tecnologia da informação, redes ou equivalente;

8.4.2.4. Os serviços deverão ser prestados, no mínimo, em horário de expediente administrativo da Polícia Militar, isto é, 08 (oito) horas por dia, 05 (cinco) dias por semana, das 09:00 às 18:00;

8.4.3. Perfil Data Center (Gerente de suporte técnico de tecnologia da informação);

8.4.3.1. Cargo - Arquiteto de Sistemas de Data Center

8.4.3.2. Referência, profissional com responsabilidade de coordenar e gerenciar a atuação dos demais técnicos de suporte e de manutenção, garantindo a adequada prestação dos serviços, bem como controlando e planejando operacionalmente as ações da equipe. Presta também apoio à tomada de decisão do órgão auxiliando na prospecção de soluções de suporte ao usuário, fornecimento de informações táticas e operacionais e proposição de ações de

aprimoramento dos serviços de suporte ao usuário.

8.4.3.3. Requisitos básicos:

8.4.3.3.1. Deverá possuir uma das certificações abaixo:

8.4.3.3.2. Microsoft Certified: Azure Solutions Architect Expert;

8.4.3.3.3. Microsoft Certified: Cybersecurity Architect Expert;

8.4.3.3.4. Microsoft Certified: DevOps Engineer Expert;

8.4.3.3.5. Microsoft Certified Systems Engineer (MCSE);

8.4.3.3.6. Deverá possuir uma das certificações abaixo:

8.4.3.3.7. Linux Professional Institute Certification Level 1 (LPIC-1);

8.4.3.3.8. Certificação CompTIA Linux+;

8.4.3.3.9. SUSE Certified Administrator (SCA);

8.4.3.3.10. Red Hat Certified System Administrator (RHCSA);

8.4.3.3.11. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;

8.4.3.3.12. Deverá possuir Pós-Graduação completa na área de Tecnologia da Informação, Redes ou Segurança;

8.4.3.3.13. Comprovação de experiência mínima de 6 anos em administração de bancos de dados críticos, com ênfase em governança de dados, segurança e continuidade de negócios;

8.4.3.3.14. Deverá ter participado de treinamento formal sobre Liderança ou Gerenciamento de Pessoas com no mínimo 40 horas de duração, com certificado de participação.

8.4.3.3.15. Os serviços deverão ser prestados, no mínimo, em horário de expediente administrativo da Polícia Militar, isto é, 08 (oito) horas por dia, 05 (cinco) dias por semana, das 09:00 às 18:00;

8.4.4. Especialista em Cloud Sênior:

8.4.4.1. Cargo - Arquiteto de Soluções de Inteligência Artificial

8.4.4.2. Referência, profissional responsável pela infraestrutura de nuvem, envolvendo a arquitetura, estruturação, operação, monitoramento, otimização, sustentação e migração de ambientes em nuvem.

8.4.4.3. Requisitos básicos:

8.4.4.3.1. Deverá possuir experiência comprovada em projetos de desenvolvimento, implementação ou suporte à integração de soluções baseadas em Inteligência Artificial, aprendizado de máquina (ML) ou aprendizado profundo (DL), abrangendo desde a concepção até a aplicação prática em ambientes corporativos e de alta complexidade. É desejável que tenha contribuído para o desenvolvimento de pipelines de dados, treinamento e validação de modelos, bem como sua implementação em produção.

8.4.4.3.2. Será necessário demonstrar participação em treinamentos específicos nas áreas de Inteligência Artificial, ciência de dados ou engenharia de dados, com conhecimento prático em frameworks como TensorFlow, PyTorch, Scikit-learn e plataformas de nuvem como AWS, Azure ou Google Cloud. Experiência em manipulação de grandes volumes de dados, criação de modelos preditivos e implementação de arquiteturas de dados também será valorizada.

8.4.4.3.3. Serão consideradas um diferencial, mas não são obrigatórias certificações na área de IA, tais como:

8.4.4.3.3.1. AWS Certified Machine Learning – Specialty.

8.4.4.3.3.2. Google Cloud Professional Machine Learning Engineer.

8.4.4.3.3.3. Microsoft Certified: Azure AI Engineer Associate.

8.4.4.3.3.4. Microsoft Certified: Azure Data Scientist Associate

8.4.4.3.3.5. Microsoft Certified: Fabric Analytics Engineer Associate

8.4.4.3.3.6. Microsoft Certified: Azure Data Engineer Associate

8.4.4.3.3.7. Oracle Cloud Infrastructure 2024 Generative AI Professional

8.4.4.3.3.8. Certificações de aprendizado profundo, como o DeepLearning.AI TensorFlow Developer Professional Certificate.

8.4.4.3.3.9. Certificações equivalentes de nível intermediário, não especificadas neste documento, mas que demonstrem proficiência em tecnologias, frameworks ou metodologias relacionadas à Inteligência Artificial e aprendizado de máquina, também serão aceitas, desde que comprovadas por meio de documentação oficial e relevância para o cargo.

8.4.4.3.4. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;

8.4.4.3.5. Comprovação de experiência profissional de 04 (quatro) anos na área de desenvolvimento, implementação ou arquitetura de soluções baseadas em Inteligência Artificial, aprendizado de máquina, aprendizado profundo ou tecnologias equivalentes.

8.4.4.4. Os serviços deverão ser prestados, no mínimo, em horário de expediente administrativo da Polícia Militar, isto é, 08 (oito) horas por dia, 05 (cinco) dias por semana, das 09:00 às 18:00;

8.4.5. Administrador de sistemas operacionais Sênior

8.4.5.1. Cargo - Analista Correio Eletrônico – Nível 3

8.4.5.2. Referência, profissional atuante em nível 3 em uma central de atendimento ou associado ao centro de dados. Presta serviços de gerenciamento físico e lógico de equipamentos, servidores, storages, entre outros equipamentos do centro de dados ou no ambiente virtualizado. Atua também no gerenciamento de backups, configuração de procedimentos de recuperação de desastres computacionais, gerenciamento de recursos computacionais avançados (a exemplo de servidores de arquivos, de impressão e de comunicação institucional) que demandam alocação, configuração ou instalação de softwares ou construção e execução de scripts para o controle, monitoramento e gerenciamento desses recursos.

8.4.5.3. Requisitos básicos:

8.4.5.3.1. Deverá possuir uma das certificações abaixo:

8.4.5.3.1.1. IBM Certified System Administrator - Notes and Domino;

8.4.5.3.1.2. IBM Certified Advanced System Administrator - Notes and Domino;

8.4.5.3.1.3. HCL Domino Certified Professional;

8.4.5.3.1.4. HCL Domino Associate Administrator;

- 8.4.5.3.1.5. Linux Professional Institute Certification Level 2 (LPIC-2);
- 8.4.5.3.2. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;
- 8.4.5.3.3. Deverá possuir Pós-Graduação completa na área de Tecnologia da Informação, Redes, Segurança ou equivalente;
- 8.4.5.3.4. Comprovação de experiência profissional de 06 (seis) anos na área de tecnologia da informação, redes ou equivalente;
- 8.4.5.4. Os serviços deverão ser prestados, no mínimo entre 07:00 e 22:00, segmentados da seguinte forma:
- 8.4.5.4.1. 1 (um) recurso, no mínimo entre 07:00 à 16:00
- 8.4.5.4.2. 1 (um) recurso, no mínimo entre 09:00 à 18:00
- 8.4.5.4.3. 1 (um) recurso, no mínimo entre 13:00 à 22:00
- 8.4.5.5. A Escala de Sobreaviso Correio Eletrônico deverá ser distribuída entre as posições de Analista Windows – Nível 3 e Analista Windows – Nível 2 de forma que apenas um membro poderá ser acionado a cada semana;
- 8.4.6. Analista de sistemas de automação – Júnior
- 8.4.6.1. Cargo - Analista de Monitoramento Windows
- 8.4.6.2. Referência, profissional responsável por integrar soluções de inteligência de ameaças ao pipeline DevSecOps, assegurando que alertas, indicadores de comprometimento (IoCs) e feeds externos sejam incorporados aos fluxos CI/CD de forma segura e automatizada. Pode atuar como arquiteto de soluções e propor, projetar, executar e aprimorar arquiteturas de soluções necessárias à manutenção e melhoria das operações na infraestrutura de TIC. Poderá atuar como arquiteto em ambientes híbridos (on-premises/cloud), aplicando boas práticas de Zero Trust, segurança em nuvem (CSPM/CNAPP) e conformidade com LGPD e ISO 27017.
- 8.4.6.3. Requisitos básicos:
- 8.4.6.3.1. Deverá possuir uma das certificações abaixo:
- 8.4.6.3.1.1. Certificação Microsoft Certified Fundamentals (MCF);
- 8.4.6.3.1.2. Microsoft Certified Professional (MCP);
- 8.4.6.3.1.3. CompTIA Server+;
- 8.4.6.3.2. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;
- 8.4.6.3.3. Comprovação de experiência profissional de 01 (um) ano na área de tecnologia da informação, redes ou equivalente;
- 8.4.6.4. Os serviços deverão ser prestados em caráter de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- 8.4.7. Analista de sistemas de automação – Júnior
- 8.4.7.1. Cargo - Analista de Monitoramento de Infraestrutura com ênfase em sistemas Linux e ferramentas de observabilidade como Zabbix, Prometheus ou Elastic Stack
- 8.4.7.2. Referência, profissional responsável por assegurar a utilização adequada de soluções de integração - CI ou de entrega contínua - CD. Pode atuar como arquiteto de soluções e propor, projetar, executar e aprimorar arquiteturas de soluções necessárias à manutenção e melhoria das operações na infraestrutura de TIC. Pode atuar também como arquiteto de computação em nuvem, ou ainda como arquiteto de soluções híbridas.
- 8.4.7.3. Requisitos básicos:
- 8.4.7.3.1. Deverá possuir uma das certificações abaixo:
- 8.4.7.3.1.1. Linux Professional Institute Certification Level 1 (LPIC-1);
- 8.4.7.3.1.2. Certificação CompTIA Linux+;
- 8.4.7.3.1.3. SUSE Certified Administrator (SCA);
- 8.4.7.3.1.4. Red Hat Certified System Administrator (RHCSA);
- 8.4.7.3.2. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;
- 8.4.7.3.3. Comprovação de experiência profissional de 01 (um) ano na área de tecnologia da informação, redes ou equivalente;
- 8.4.7.4. Os serviços deverão ser prestados em caráter de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- 8.4.8. Perfil de Banco de Dados (Administrador de Banco de dados – Senior)
- 8.4.8.1. Cargo - Analista Banco de Dados – Nível 3 – Sênior
- 8.4.8.2. Referência, profissional responsável pela administração, operação, gerenciamento, otimização e monitoramento dos recursos de banco de dados. Presta serviços de gerenciamento dos esquemas de banco de dados, alocação e administração de recursos físicos e lógicos, realiza dimensionamentos e prospecções de uso, monitora incidentes e promove adequações, aprimoramentos e expansão dos recursos. Pode atuar na análise de dados propondo padrões e assegurando a normalização e melhor uso dos recursos para armazenamento e utilização de dados corporativos.
- 8.4.8.3. Requisitos básicos:
- 8.4.8.3.1. Deverá possuir uma das certificações abaixo:
- 8.4.8.3.1.1. Microsoft Certified: Azure Database Administrator Associate;
- 8.4.8.3.1.2. Microsoft Certified: Solutions Associate - SQL Server (MCSA SQL);
- 8.4.8.3.1.3. MySQL Database Administrator;
- 8.4.8.3.1.4. Oracle Certified Professional (OCP);
- 8.4.8.3.1.5. Certified PostgreSQL DBA(CPSDBA);
- 8.4.8.3.2. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;
- 8.4.8.3.3. Deverá possuir Pós-Graduação completa na área de Tecnologia da Informação, Redes, Segurança ou equivalente;

- 8.4.8.3.4. Comprovação de experiência profissional de 06 (seis) anos na área de tecnologia da informação, redes ou equivalente;
- 8.4.8.4. Os serviços deverão ser prestados, no mínimo, em horário de expediente administrativo da Polícia Militar, isto é, 08 (oito) horas por dia, 05 (cinco) dias por semana, das 09:00 às 18:00;
- 8.4.9. Cargo - Analista Banco de Dados – Nível 2 - Pleno
- 8.4.9.1. Referência, profissional responsável pela administração, operação, gerenciamento, otimização e monitoramento dos recursos de banco de dados. Presta serviços de gerenciamento dos esquemas de banco de dados, alocação e administração de recursos físicos e lógicos, realiza dimensionamentos e prospecções de uso, monitora incidentes e promove adequações, aprimoramentos e expansão dos recursos. Pode atuar na análise de dados propondo padrões e assegurando a normalização e melhor uso dos recursos para armazenamento e utilização de dados corporativos.
- 8.4.9.2. Requisitos básicos:
- 8.4.9.2.1. Deverá possuir uma das certificações abaixo:
- 8.4.9.2.1.1. Microsoft Certified: Azure Database Administrator Associate;
- 8.4.9.2.1.2. Microsoft Certified: Solutions Associate - SQL Server (MCSA SQL);
- 8.4.9.2.1.3. MySQL Database Administrator;
- 8.4.9.2.1.4. Oracle Certified Associate (OCA);
- 8.4.9.2.2. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;
- 8.4.9.2.3. Comprovação de experiência profissional de 04 (quatro) anos na área de tecnologia da informação, redes ou equivalente;
- 8.4.9.3. Os serviços deverão ser prestados, no mínimo entre 07:00 e 22:00, segmentados da seguinte forma:
- 8.4.9.4. 1 (um) recurso, no mínimo entre 07:00 à 16:00
- 8.4.9.5. 1 (um) recurso, no mínimo entre 13:00 à 22:00
- 8.4.9.6. A Escala de Sobreaviso Banco de Dados deverá ser distribuída entre as posições de Analista Banco de Dados – Nível 3 e Analista Banco de Dados – Nível 2, de forma que apenas um membro poderá ser acionado a cada semana;
- 8.4.10. Perfil de Redes;
- 8.4.10.1. Perfil - Técnico de suporte ao usuário de tecnologia da informação Júnior
- 8.4.10.2. Referência, profissional atuante em centrais de atendimento de TIC (em nível 1) prestando suporte ao usuário, orientando-os na utilização de hardwares e softwares. Pode atuar no monitoramento de aplicações, recursos de rede, banco de dados, servidores entre outros componentes de serviço de TIC.
- 8.4.10.3. Deverá possuir uma das certificações abaixo:
- 8.4.10.3.1. Cisco Certified Network Associate (CCNA);
- 8.4.10.3.2. Aruba Certified Switching Associate (ACSA);
- 8.4.10.3.3. Juniper Associate (JNCIA-Junos);
- 8.4.10.4. Requisitos básicos:
- 8.4.10.4.1. Huawei Certified ICT Associate Routing & Switching (HCIA-Routing & Switching);
- 8.4.10.4.2. Certificação de nível Associate ou equivalente emitida por órgão autorizado ou pelo próprio fabricante.
- 8.4.10.4.3. Deverá ter participado de treinamento formal sobre Cabeamento Estruturado com no mínimo 40 horas de duração, com certificado de participação.
- 8.4.10.4.4. Deverá estar, no mínimo, cursando Ensino Superior na área de Tecnologia da Informação, Redes, Segurança, Engenharias ou equivalente;
- 8.4.10.4.5. Comprovação de experiência profissional de 01 (um) ano na área de tecnologia da informação, redes ou equivalente;
- 8.4.10.4.6. Deverá estar habilitado para condução de veículos automotores, no mínimo, na Categoria B.
- 8.4.10.5. Os serviços deverão ser prestados, no mínimo, em horário de expediente administrativo da Polícia Militar, isto é, 08 (oito) horas por dia, 05 (cinco) dias por semana, das 09:00 às 18:00;
- 8.4.11. Técnico de rede (telecomunicações) – Cabista;
- 8.4.11.1. Perfil - Técnico de Cabeamento Estruturado
- 8.4.11.2. Referência, profissional atuante no monitoramento, configuração, manutenção e otimização de recursos de telecomunicações de dados, áudio e vídeo. Atua também na integração e garantia do desempenho de redes de telecomunicações, centrais de comutação e integração a serviços de telefonia digital.
- 8.4.11.3. Requisitos básicos:
- 8.4.11.3.1. Deverá ter participado de treinamento formal sobre Cabeamento Estruturado com no mínimo 40 horas de duração, com certificado de participação.
- 8.4.11.3.2. Deverá estar habilitado para condução de veículos automotores, no mínimo, na Categoria B.
- 8.4.11.3.3. Comprovação de experiência profissional de 02 (dois) anos na área de tecnologia da informação, redes ou cabeamento estruturado.
- 8.4.11.4. Os serviços deverão ser prestados, no mínimo, em horário de expediente administrativo da Polícia Militar, isto é, 08 (oito) horas por dia, 05 (cinco) dias por semana, das 09:00 às 18:00;
- 8.4.12. Perfil de Segurança da Informação;
- 8.4.12.1. Gerente de segurança da informação
- 8.4.12.2. Perfil - Arquiteto de Segurança da Informação
- 8.4.12.3. Referência, profissional com responsabilidade de coordenar e gerenciar a atuação dos demais profissionais de segurança da informação, garantindo a adequada prestação dos serviços, bem como controlando e planejamento operacionalmente as ações dessa equipe. Presta também apoio à tomada de decisão do órgão auxiliando na prospecção de soluções de segurança da informação, fornecimento de informações táticas e operacionais, e proposição de ações de aprimoramento dos serviços de segurança da informação seja preventiva ou reativa.
- 8.4.12.4. Requisitos básicos:
- 8.4.12.4.1. Deverá possuir uma das certificações abaixo:
- 8.4.12.4.1.1. Cisco Certified Network Professional Security (CCNP Security);

- 8.4.12.4.1.2. Fortinet Certified Professional - Security Operations;
- 8.4.12.4.1.3. Fortinet Certified Professional - Network Security;
- 8.4.12.4.1.4. Juniper Professional (JNCIP-SEC);
- 8.4.12.4.1.5. Check Point Certified Security Expert (CCSE);
- 8.4.12.4.1.6. Palo Alto Networks Certified Network Security Administrator (PCNSA);
- 8.4.12.4.2. Certificação de nível Profissional ou equivalente emitida por órgão autorizado ou pelo próprio fabricante com foco em segurança.
- 8.4.12.4.3. Deverá possuir CompTIA Security+.
- 8.4.12.4.4. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;
- 8.4.12.4.5. Deverá possuir Pós-Graduação completa na área de Tecnologia da Informação, Redes ou Segurança;
- 8.4.12.4.6. Comprovação de experiência profissional de 06 (seis) anos na área de tecnologia da informação, redes, segurança da informação ou equivalente;
- 8.4.12.4.7. Deverá ter participado de treinamento formal sobre Liderança ou Gerenciamento de Pessoas com no mínimo 40 horas de duração, com certificado de participação.
- 8.4.12.5. Os serviços deverão ser prestados, no mínimo, em horário de expediente administrativo da Polícia Militar, isto é, 08 (oito) horas por dia, 05 (cinco) dias por semana, das 09:00 às 18:00;
- 8.4.13. Gerente de segurança da informação
- 8.4.13.1. Perfil - Arquiteto de Infraestrutura
- 8.4.13.2. Referência, profissional com responsabilidade de coordenar e gerenciar a atuação dos demais profissionais de segurança da informação, garantindo a adequada prestação dos serviços, bem como controlando e planejamento operacionalmente as ações dessa equipe. Presta também apoio à tomada de decisão do órgão auxiliando na prospecção de soluções de segurança da informação, fornecimento de informações táticas e operacionais, e proposição de ações de aprimoramento dos serviços de segurança da informação seja preventiva ou reativa.
- 8.4.13.3. Requisitos básicos:
- 8.4.13.3.1. Deverá possuir uma das certificações abaixo:
- 8.4.13.3.1.1. Cisco Certified Network Professional (CCNP);
- 8.4.13.3.1.2. Aruba Certified Switching Professional (ACSP);
- 8.4.13.3.1.3. Juniper Professional (JNCIP-ENT);
- 8.4.13.3.1.4. Huawei Certified ICT Professional Routing & Switching (HCIP-Routing & Switching);
- 8.4.13.3.2. Certificação de nível Profissional ou equivalente emitida por órgão autorizado ou pelo próprio fabricante;
- 8.4.13.3.3. Deverá possuir uma das certificações abaixo:
- 8.4.13.3.3.1. Cisco Certified Specialist - Data Center Core;
- 8.4.13.3.3.2. Cisco Certified Specialist - Data Center Design;
- 8.4.13.3.3.3. Cisco Certified Specialist - Data Center Operations;
- 8.4.13.3.3.4. Juniper Associate (JNCIA-DC);
- 8.4.13.3.3.5. Juniper Specialist (JNCIS-DC);
- 8.4.13.3.4. Certificação de nível Specialist, equivalente ou superior emitida por órgão autorizado ou pelo próprio fabricante;
- 8.4.13.3.5. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;
- 8.4.13.3.6. Deverá possuir Pós-Graduação completa na área de Tecnologia da Informação, Redes ou Segurança;
- 8.4.13.3.7. Comprovação de experiência profissional de 06 (seis) anos na área de tecnologia da informação, redes, segurança da informação ou equivalente;
- 8.4.13.3.8. Deverá ter participado de treinamento formal sobre Liderança ou Gerenciamento de Pessoas com no mínimo 40 horas de duração, com certificado de participação.
- 8.4.13.4. Os serviços deverão ser prestados, no mínimo, em horário de expediente administrativo da Polícia Militar, isto é, 08 (oito) horas por dia, 05 (cinco) dias por semana, das 09:00 às 18:00;
- 8.4.14. Analista de redes e de comunicação de dados Sênior
- 8.4.14.1. Perfil - Analista de Segurança – Nível 3
- 8.4.14.2. Referência, profissional que atua na intercomunicação de redes locais e de longa distância, com ou sem fio, assegurando a operação, desempenho e qualidade dos serviços de rede e comunicação de dados, bem como no aprimoramento e funcionamento adequados dos ativos de redes. Presta serviços de execução, aprimoramento e manutenção dos projetos de redes, além da configuração e otimização de recursos de interconexão de dados.
- 8.4.14.3. Deve possuir conhecimento em ferramentas de WEBSEC (Web Security) para proteger aplicações web acessadas pela rede, mitigando vulnerabilidades como XSS e injeção de SQL. Também será responsável por conduzir testes de DAST (Dynamic Application Security Testing) para identificar falhas de segurança em aplicações em tempo real
- 8.4.14.4. Requisitos básicos:
- 8.4.14.4.1. Deverá possuir uma das certificações abaixo:
- 8.4.14.4.1.1. Cisco Certified Network Professional Security (CCNP Security);
- 8.4.14.4.1.2. Fortinet Certified Professional - Security Operations;
- 8.4.14.4.1.3. Fortinet Certified Professional - Network Security;
- 8.4.14.4.1.4. Juniper Professional (JNCIP-SEC);
- 8.4.14.4.1.5. Check Point Certified Security Expert (CCSE);
- 8.4.14.4.1.6. Palo Alto Networks Certified Network Security Administrator (PCNSA);
- 8.4.14.4.2. Certificação de nível Profissional ou equivalente emitida por órgão autorizado ou pelo próprio fabricante com foco em segurança.
- 8.4.14.4.3. Deverá possuir CompTIA Security+.
- 8.4.14.4.4. Deverá possuir conhecimento comprovado em WEBSEC (Web Security), com experiência na aplicação de práticas de segurança baseadas no OWASP Top 10.

- 8.4.14.4.5. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;
- 8.4.14.4.6. Deverá estar, no mínimo, cursando Pós-Graduação na área de Tecnologia da Informação, Redes, Segurança ou equivalente;
- 8.4.14.4.7. Comprovação de experiência profissional de 04 (quatro) anos na área de tecnologia da informação, redes ou equivalente;
- 8.4.14.5. Os serviços deverão ser prestados, no mínimo, em horário de expediente administrativo da Polícia Militar, isto é, 08 (oito) horas por dia, 05 (cinco) dias por semana, das 09:00 às 18:00.
- 8.4.14.6. A Escala de Sobreaviso Segurança deverá ser distribuída entre as posições de Analista de Segurança – Nível 3 e Analista de Segurança – Nível 2, de forma que apenas um membro poderá ser acionado a cada semana;
- 8.4.15. Analista de redes e de comunicação de dados Sênior
- 8.4.15.1. Perfil - Analista de Redes – Nível 3
- 8.4.15.2. Referência, profissional que atua na intercomunicação de redes locais e de longa distância, com ou sem fio, assegurando a operação, desempenho e qualidade dos serviços de rede e comunicação de dados, bem como no aprimoramento e funcionamento adequados dos ativos de redes. Presta serviços de execução, aprimoramento e manutenção dos projetos de redes, além da configuração e otimização de recursos de interconexão de dados.
- 8.4.15.3. Requisitos básicos:
- 8.4.15.3.1. Deverá possuir uma das certificações abaixo:
- 8.4.15.3.1.1. Cisco Certified Network Professional (CCNP);
- 8.4.15.3.1.2. Aruba Certified Switching Professional (ACSP);
- 8.4.15.3.1.3. Juniper Professional (JNCIP-ENT);
- 8.4.15.3.1.4. Huawei Certified ICT Professional Routing & Switching (HCIP-Routing & Switching);
- 8.4.15.3.2. Certificação de nível Profissional ou equivalente emitida por órgão autorizado ou pelo próprio fabricante
- 8.4.15.3.3. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;
- 8.4.15.3.4. Deverá estar, no mínimo, cursando Pós-Graduação na área de Tecnologia da Informação, Redes, Segurança ou equivalente;
- 8.4.15.3.5. Comprovação de experiência profissional de 04 (quatro) anos na área de tecnologia da informação, redes ou equivalente;
- 8.4.15.4. Os serviços deverão ser prestados, no mínimo, em horário de expediente administrativo da Polícia Militar, isto é, 08 (oito) horas por dia, 05 (cinco) dias por semana, das 09:00 às 18:00.
- 8.4.15.5. A Escala de Sobreaviso Redes deverá ser distribuída entre as posições de Analista de Redes – Nível 3 e Analista de Redes – Nível 2, de forma que apenas um membro poderá ser acionado a cada semana;
- 8.4.15.6. Analista de redes e de comunicação de dados Pleno
- 8.4.15.7. Perfil - Analista de Segurança de Rede – Nível 2
- 8.4.15.8. Referência, profissional que atua na intercomunicação de redes locais e de longa distância, com ou sem fio, assegurando a operação, desempenho e qualidade dos serviços de rede e comunicação de dados, bem como no aprimoramento e funcionamento adequados dos ativos de redes. Presta serviços de execução, aprimoramento e manutenção dos projetos de redes, além da configuração e otimização de recursos de interconexão de dados.
- 8.4.15.9. Requisitos básicos:
- 8.4.15.9.1. Deverá possuir uma das certificações abaixo:
- 8.4.15.9.1.1. Certificação Cisco Certified Specialist - Security Core;
- 8.4.15.9.1.2. Juniper Associate (JNCIA-SEC);
- 8.4.15.9.1.3. Palo Alto Networks Certified Cybersecurity Associate (PCCSA);
- 8.4.15.9.1.4. Check Point Certified Security Administrator (CCSA) ou alguma certificação de nível;
- 8.4.15.9.2. Certificação de nível Associate ou equivalente emitida por órgão autorizado ou pelo próprio fabricante com foco em segurança de redes.
- 8.4.15.9.3. Deverá possuir CompTIA Security+.
- 8.4.15.9.4. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;
- 8.4.15.9.5. Comprovação de experiência profissional de 02 (dois) anos na área de tecnologia da informação, redes ou equivalente;
- 8.4.15.10. Os serviços deverão ser prestados, no mínimo entre 07:00 e 22:00, segmentados da seguinte forma:
- 8.4.15.10.1. 1 (um) recurso, no mínimo entre 07:00 à 16:00;
- 8.4.15.10.2. 1 (um) recurso, no mínimo entre 09:00 à 18:00;
- 8.4.15.10.3. 1 (um) recurso, no mínimo entre 13:00 à 22:00;
- 8.4.15.11. A Escala de Sobreaviso Segurança deverá ser distribuída entre as posições de Analista de Segurança – Nível 3 e Analista de Segurança – Nível 2, de forma que apenas um membro poderá ser acionado a cada semana;
- 8.4.16. Analista de redes e de comunicação de dados Pleno
- 8.4.16.1. Cargo - Analista de Segurança de Aplicações – Nível 2
- 8.4.16.2. Referência, profissional que atua na intercomunicação de redes locais e de longa distância, com ou sem fio, assegurando a operação, desempenho e qualidade dos serviços de rede e comunicação de dados, bem como no aprimoramento e funcionamento adequados dos ativos de redes. Presta serviços de execução, aprimoramento e manutenção dos projetos de redes, além da configuração e otimização de recursos de interconexão de dados.
- 8.4.16.3. Deverá aplicar práticas de WEBSEC (Web Security) para proteger aplicações web contra ameaças como injeção de código e ataques de força bruta, além de realizar testes de DAST (Dynamic Application Security Testing) para identificar vulnerabilidades em aplicações em produção;
- 8.4.16.4. Requisitos básicos:
- 8.4.16.4.1. Deverá possuir uma das certificações abaixo:
- 8.4.16.4.1.1. Certificação Information Security Foundation based on ISO/IEC 27.001;
- 8.4.16.4.1.2. SC-900: Microsoft Security, Compliance, and Identity Fundamentals;
- 8.4.16.4.2. Certificação de nível Associate ou equivalente emitida por órgão autorizado ou pelo próprio fabricante com foco em segurança de redes.
- 8.4.16.4.3. Deverá possuir CompTIA Security+.

- 8.4.16.4.4. Deverá possuir certificação ou treinamento em WEBSEC (Web Security), como o OWASP Top 10 Awareness ou equivalente;
- 8.4.16.4.5. Deverá ter experiência prática com ferramentas de DAST (Dynamic Application Security Testing), como OWASP ZAP ou Burp Suite, para testes de segurança em aplicações web.
- 8.4.16.4.6. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;
- 8.4.16.4.7. Comprovação de experiência profissional de 02 (dois) anos na área de tecnologia da informação, redes ou equivalente;
- 8.4.16.5. Os serviços deverão ser prestados, no mínimo entre 07:00 e 22:00, segmentados da seguinte forma:
- 8.4.16.5.1. 1 (um) recurso, no mínimo entre 07:00 à 16:00
- 8.4.16.5.2. 1 (um) recurso, no mínimo entre 13:00 à 22:00;
- 8.4.17. Analista de redes e de comunicação de dados Pleno
- 8.4.17.1. Cargo - Analista de Redes – Nível 2
- 8.4.17.2. Referência, profissional que atua na intercomunicação de redes locais e de longa distância, com ou sem fio, assegurando a operação, desempenho e qualidade dos serviços de rede e comunicação de dados, bem como no aprimoramento e funcionamento adequados dos ativos de redes. Presta serviços de execução, aprimoramento e manutenção dos projetos de redes, além da configuração e otimização de recursos de interconexão de dados.
- 8.4.17.3. Requisitos básicos:
- 8.4.17.3.1. Deverá possuir uma das certificações abaixo:
- 8.4.17.3.1.1. Cisco Certified Network Associate (CCNA);
- 8.4.17.3.1.2. Aruba Certified Switching Associate (ACSA);
- 8.4.17.3.1.3. Juniper Associate (JNCIA-Junos);
- 8.4.17.3.1.4. Huawei Certified ICT Associate Routing & Switching (HCIA-Routing & Switching);
- 8.4.17.3.1.5. Cisco Certified Specialist - Data Center Core
- 8.4.17.3.1.6. Cisco Certified Specialist - Data Center Design
- 8.4.17.3.1.7. Cisco Certified Specialist - Data Center Operations
- 8.4.17.3.1.8. Juniper Associate (JNCIA-DC)
- 8.4.17.3.1.9. Juniper Specialist (JNCIS-DC)
- 8.4.17.3.2. Certificação de nível Specialist, equivalente ou superior emitida por órgão autorizado ou pelo próprio fabricante
- 8.4.17.3.3. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;
- 8.4.17.3.4. Comprovação de experiência profissional de 02 (dois) anos na área de tecnologia da informação, redes ou equivalente;
- 8.4.17.3.5. Deverá estar habilitado para condução de veículos automotores, no mínimo, na Categoria B.
- 8.4.17.4. Os serviços deverão ser prestados, no mínimo entre 07:00 e 22:00, segmentados da seguinte forma:
- 8.4.17.4.1. 1 (um) recurso, no mínimo entre 07:00 à 16:00
- 8.4.17.4.2. 1 (um) recurso, no mínimo entre 13:00 à 22:00
- 8.4.17.5. A Escala de Sobreaviso Redes deverá ser distribuída entre as posições de Analista de Redes – Nível 3 e Analista de Redes – Nível 2, de forma que apenas um membro poderá ser acionado a cada semana;
- 8.4.18. Perfil de Cibersegurança;
- 8.4.18.1. Perfil: Analista de Inteligência Cibernética (Threat Intelligence Analyst)
- 8.4.18.2. Profissional responsável por assegurar a utilização adequada de soluções de integração - CI ou de entrega contínua - CD. Pode atuar como arquiteto de soluções e propor, projetar, executar e aprimorar arquiteturas de soluções necessárias à manutenção e melhoria das operações na infraestrutura de TIC. Pode atuar também como arquiteto de computação em nuvem, ou ainda como arquiteto de soluções híbridas.
- 8.4.18.3. Deverá utilizar técnicas de OSINT (Open Source Intelligence) para coletar e analisar dados de fontes abertas, como deep e dark web, visando identificar ameaças cibernéticas e indicadores de comprometimento (IoCs). Pode atuar como arquiteto de soluções e propor, projetar, executar e aprimorar arquiteturas de soluções necessárias à manutenção e melhoria das operações na infraestrutura de TIC
- 8.4.18.4. Requisitos básicos:
- 8.4.18.4.1. Deverá possuir uma das certificações abaixo:
- 8.4.18.4.1.1. CompTIA Cybersecurity Analyst (CySA+), preferencialmente com foco em detecção comportamental e correlação baseada em UEBASplunk Core Certified User;
- 8.4.18.4.1.2. MITRE ATT&CK Defender (MAD);
- 8.4.18.4.1.3. Certified Threat Intelligence Analyst (CTIA);
- 8.4.18.4.1.4. GIAC Cyber Threat Intelligence (GCTI);
- 8.4.18.4.1.5. CREST Threat Intelligence Analyst (CCTIM)
- 8.4.18.4.2. Certificação de nível Associate ou equivalente emitida por órgão autorizado ou pelo próprio fabricante com foco em segurança de redes.
- 8.4.18.4.3. Deverá possuir CompTIA Security+.
- 8.4.18.4.4. Deverá possuir certificação ou treinamento em ferramentas OSINT (Open Source Intelligence), como o Certified Threat Intelligence Analyst (CTIA) ou equivalente, com experiência em ferramentas como por exemplo: “ Maltego, SpiderFoot, Recon-ng, IntelligenceX, OpenCTI ou similares;
- 8.4.18.4.5. Deverá possuir o Ensino Superior completo em cursos reconhecidos pelo MEC nas áreas de tecnologia da informação, redes, ciência de dados, segurança da informação ou engenharia da computação ou equivalentes;
- 8.4.18.4.6. Comprovação de experiência profissional de 04 (quatro) anos na área de tecnologia da informação, redes, segurança da informação ou equivalente;
- 8.4.18.5. Os serviços deverão ser prestados, no mínimo, em horário de expediente administrativo da Polícia Militar, isto é, 08 (oito) horas por dia, 05 (cinco) dias por semana, das 09:00 às 18:00;
- 8.4.19. Administrador em segurança da informação – Sênior
- 8.4.19.1. Perfil - Analista de Threat Hunting
- 8.4.19.2. Referência, profissional responsável pela infraestrutura de nuvem, envolvendo a arquitetura, estruturação, operação, monitoramento,

otimização, sustentação e migração de ambientes em nuvem. Deverá conduzir e apoiar atividades de PENTEST (Penetration Testing) para simular ataques cibernéticos e identificar vulnerabilidades em ambientes de nuvem, além de utilizar OSINT (Open Source Intelligence) para mapear ameaças externas e fortalecer as defesas da CONTRATANTE;

8.4.19.3. Requisitos básicos:

8.4.19.3.1. Deverá possuir uma das certificações abaixo:

8.4.19.3.1.1. eCTHP (Certified Threat Hunting Professional);

8.4.19.3.1.2. eJPT (Junior Penetration Tester);

8.4.19.3.1.3. CompTIA Cybersecurity Analyst (CySA+);

8.4.19.3.2. Deverá ter experiência comprovada em OSINT (Open Source Intelligence), com conhecimento em coleta de dados em fontes abertas para análise de ameaças.

8.4.19.3.3. Microsoft Certified: Security, Compliance, and Identity Fundamentals;

8.4.19.3.4. Certificação de nível Associate ou equivalente emitida por órgão autorizado ou pelo próprio fabricante com foco em segurança de redes.

8.4.19.3.5. Deverá possuir certificação CompTIA Security+.

8.4.19.3.6. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;

8.4.19.3.7. Comprovação de experiência profissional de 04 (quatro) anos na área de tecnologia da informação, redes, segurança da informação ou equivalente;

8.4.19.4. Os serviços deverão ser prestados, no mínimo, em horário de expediente administrativo da Polícia Militar, isto é, 08 (oito) horas por dia, 05 (cinco) dias por semana, das 09:00 às 18:00;

8.4.20. Desenvolvedor de sistemas de tecnologia da informação Sênior

8.4.20.1. Perfil - Desenvolvedor de Software Seguro

8.4.20.2. Referência, profissional com a responsabilidade de assegurar a implantação adequada dos entregáveis de softwares. Pode atuar como analista de teste de aplicações executando testes automatizados e assegurando a cobertura mínima de testes nas soluções entregues. Pode atuar como analista de qualidade dos produtos a serem implantados.

8.4.20.3. Requisitos básicos:

8.4.20.3.1. Deverá possuir uma das certificações abaixo:

8.4.20.3.1.1. Cisco Certified DevNet Associate

8.4.20.3.1.2. Microsoft Certified: Azure Developer Associate

8.4.20.3.1.3. Certified Kubernetes Application Developer (CKAD)

8.4.20.3.1.4. DevSecOps Foundation

8.4.20.3.1.5. Certified DevSecOps Professional (CDP);

8.4.20.3.2. Deverá possuir certificação ou treinamento em WEBSEC (Web Security), como o OWASP Top 10 Awareness ou equivalente;

8.4.20.3.3. Deverá ter experiência com ferramentas de DAST (Dynamic Application Security Testing), como OWASP ZAP ou Burp Suite, para testes de segurança em aplicações;

8.4.20.3.4. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;

8.4.20.3.5. Comprovação de experiência profissional de 06 (seis) anos na área de tecnologia da informação, redes, segurança da informação ou equivalente;

8.4.20.4. Os serviços deverão ser prestados, no mínimo, em horário de expediente administrativo da Polícia Militar, isto é, 08 (oito) horas por dia, 05 (cinco) dias por semana, das 09:00 às 18:00;

8.4.21. Perfil de Analista de Sistemas Operacionais (Windows);

8.4.21.1. Cargo - Analista Windows

8.4.21.2. Referência, profissional atuante em nível 3 em uma central de atendimento ou associado ao centro de dados. Presta serviços de gerenciamento físico e lógico de equipamentos, servidores, storages, entre outros equipamentos do centro de dados ou no ambiente virtualizado. Atua também no gerenciamento de backups, configuração de procedimentos de recuperação de desastres computacionais, gerenciamento de recursos computacionais avançados (a exemplo de servidores de arquivos, de impressão e de comunicação institucional) que demandam alocação, configuração ou instalação de softwares ou construção e execução de scripts para o controle, monitoramento e gerenciamento desses recursos.

8.4.21.3. Requisitos básicos:

8.4.21.3.1. Deverá possuir uma das certificações abaixo:

8.4.21.3.1.1. Microsoft Certified: Azure Solutions Architect Expert;

8.4.21.3.1.2. Microsoft Certified: Cybersecurity Architect Expert;

8.4.21.3.1.3. Microsoft Certified: DevOps Engineer Expert;

8.4.21.3.1.4. Microsoft Certified Systems Engineer (MCSE);

8.4.21.3.2. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;

8.4.21.3.3. Deverá possuir Pós-Graduação completa na área de Tecnologia da Informação, Redes, Segurança ou equivalente;

8.4.21.3.4. Comprovação de experiência profissional de 06 (seis) anos na área de tecnologia da informação, redes ou equivalente;

8.4.21.4. Os serviços deverão ser prestados, no mínimo, em horário de expediente administrativo da Polícia Militar, isto é, 08 (oito) horas por dia, 05 (cinco) dias por semana, das 09:00 às 18:00;

8.4.22. Analista de suporte computacional Pleno

8.4.22.1. Perfil- Analista Windows – Nível 2

8.4.22.2. Referência, profissional que atua na camada de virtualização e orquestração de sistemas operacionais de servidores de dados. Presta serviços de configuração, instalação e ampliação de ambientes de containers. Responsável pela adequada operação, desempenho e uso racional de recursos utilizados pelos softwares básicos, orquestradores de containers e virtualizadores.

8.4.22.3. Requisitos básicos:

8.4.22.3.1. Deverá possuir uma das certificações abaixo:

- 8.4.22.3.1.1. Microsoft Certified: Azure Network Engineer Associate;
- 8.4.22.3.1.2. Microsoft Certified: Security Operations Analyst Associate;
- 8.4.22.3.1.3. Microsoft Certified: Identity and Access Administrator Associate;
- 8.4.22.3.1.4. Microsoft Certified: Azure Security Engineer Associate;
- 8.4.22.3.1.5. Microsoft Certified: Windows Server Hybrid Administrator Associate;
- 8.4.22.3.1.6. Microsoft Certified: Azure Administrator Associate;
- 8.4.22.3.2. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;
- 8.4.22.3.3. Comprovação de experiência profissional de 04 (quatro) anos na área de tecnologia da informação, redes ou equivalente;
- 8.4.22.4. Os serviços deverão ser prestados, no mínimo entre 07:00 e 22:00, segmentados da seguinte forma:
 - 8.4.22.4.1. 1 (um) recurso, no mínimo entre 07:00 à 16:00
 - 8.4.22.4.2. 1 (um) recurso, no mínimo entre 13:00 à 22:00
- 8.4.22.5. A Escala de Sobreaviso Windows deverá ser distribuída entre as posições de Analista Windows – Nível 3 e Analista Windows – Nível 2 de forma que apenas um membro poderá ser acionado a cada semana;
- 8.4.23. Perfil de Sistemas Operacionais (Linux);
 - 8.4.23.1. Perfil - Analista Linux
 - 8.4.23.2. Referência, profissional atuante em nível 3 em uma central de atendimento ou associado ao centro de dados. Presta serviços de gerenciamento físico e lógico de equipamentos, servidores, storages, entre outros equipamentos do centro de dados ou no ambiente virtualizado. Atua também no gerenciamento de backups, configuração de procedimentos de recuperação de desastres computacionais, gerenciamento de recursos computacionais avançados (a exemplo de servidores de arquivos, de impressão e de comunicação institucional) que demandam alocação, configuração ou instalação de softwares ou construção e execução de scripts para o controle, monitoramento e gerenciamento desses recursos.
 - 8.4.23.3. Requisitos básicos:
 - 8.4.23.3.1. Deverá possuir uma das certificações abaixo:
 - 8.4.23.3.1.1. Linux Professional Institute Certification Level 2 (LPIC-2);
 - 8.4.23.3.1.2. SUSE Certified Engineer (SCE);
 - 8.4.23.3.1.3. Red Hat Certified Engineer (RHCE);
 - 8.4.23.3.2. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;
 - 8.4.23.3.3. Deverá possuir Pós-Graduação completa na área de Tecnologia da Informação, Redes, Segurança ou equivalente;
 - 8.4.23.3.4. Comprovação de experiência profissional de 06 (seis) anos na área de tecnologia da informação, redes ou equivalente;
 - 8.4.23.4. Os serviços deverão ser prestados, no mínimo, em horário de expediente administrativo da Polícia Militar, isto é, 08 (oito) horas por dia, 05 (cinco) dias por semana, das 09:00 às 18:00;
- 8.4.24. Analista de suporte computacional Pleno
 - 8.4.24.1. Perfil - Analista Linux – Nível 2
 - 8.4.24.2. Referência, profissional que atua na camada de virtualização e orquestração de sistema operacionais de servidores de dados. Presta serviços de configuração, instalação e ampliação de ambientes de containers. Responsável pela adequada operação, desempenho e uso racional de recursos utilizados pelos softwares básicos, orquestradores de containers e virtualizadores.
 - 8.4.24.3. Requisitos básicos:
 - 8.4.24.3.1. Deverá possuir uma das certificações abaixo:
 - 8.4.24.3.1.1. Linux Professional Institute Certification Level 1 (LPIC-1);
 - 8.4.24.3.1.2. Certificação CompTIA Linux+;
 - 8.4.24.3.1.3. SUSE Certified Administrator (SCA);
 - 8.4.24.3.1.4. Red Hat Certified System Administrator (RHCSA);
 - 8.4.24.3.2. Deverá possuir o Ensino Superior completo ou equivalente na área de tecnologia da informação, redes, segurança, engenharias ou equivalente;
 - 8.4.24.3.3. Comprovação de experiência profissional de 04 (quatro) anos na área de tecnologia da informação, redes ou equivalente;
 - 8.4.24.4. Os serviços deverão ser prestados, no mínimo entre 07:00 e 22:00, segmentados da seguinte forma:
 - 8.4.24.4.1. 1 (um) recurso, no mínimo entre 07:00 a 16:00
 - 8.4.24.4.2. 1 (um) recurso, no mínimo entre 13:00 à 22:00
 - 8.4.24.5. A Escala de Sobreaviso Linux deverá ser distribuída entre as posições de Analista Linux – Nível 3 e Analista Linux – Nível 2 de forma que apenas um membro poderá ser acionado a cada semana;
 - 8.4.25. Perfil Técnico de redes;
 - 8.4.25.1. Cargo - Técnico de Cabeamento Estruturado
 - 8.4.25.2. Referência, profissional atuante no monitoramento, configuração, manutenção e otimização de recursos de telecomunicações de dados, áudio e vídeo. Atua também na integração e garantia do desempenho de redes de telecomunicações, centrais de comutação e integração a serviços de telefonia digital.
 - 8.4.25.3. Requisitos básicos:
 - 8.4.25.3.1. Deverá ter participado de treinamento formal sobre Cabeamento Estruturado com no mínimo 40 horas de duração, com certificado de participação.
 - 8.4.25.3.2. Deverá estar habilitado para condução de veículos automotores, no mínimo, na Categoria B.
 - 8.4.25.3.3. Comprovação de experiência profissional de 02 (dois) anos na área de tecnologia da informação, redes ou cabeamento estruturado.
 - 8.5. Os serviços deverão ser prestados, no mínimo, em horário de expediente administrativo da Polícia Militar, isto é, 08 (oito) horas por dia, 05 (cinco) dias por semana, das 09:00 às 18:00;

9. Levantamento de soluções

9. Levantamento de Soluções:

9.1. Ferramentas e Tecnologias Aplicadas

9.1.1. Para otimizar o processo de operação e reduzir a necessidade de efetivo técnico, a contratada deverá aplicar ferramentas e softwares especializados que monitorarão e munirão os analistas com informações detalhadas e em tempo real. Essas ferramentas permitirão análises automatizadas e precisas, facilitando a tomada de decisão, maximizando a eficiência dos serviços.

9.1.2. As ferramentas utilizadas para a prestação dos serviços deverão ser plenamente compatíveis com o ambiente tecnológico da CONTRATANTE, assegurando integração, escalabilidade, desempenho e conformidade com os requisitos de segurança da informação. A CONTRATADA deverá utilizar exclusivamente ferramentas licenciadas, onde a Contratada possuir também ferramentas licenciadas, a exemplo EDR, devidamente licenciadas e reconhecidas pelo mercado, garantindo níveis adequados de suporte, atualização contínua, confiabilidade, auditoria e segurança, bem como ferramentas open onde a Contratada utiliza ferramenta open, a exemplo Zabbix,. Não haverá imposição de fabricante, marca ou modelo específico; contudo, todas as licenças, assinaturas, renovações e demais custos associados às ferramentas utilizadas deverão estar integralmente incluídos na proposta comercial da CONTRATADA e mantidos durante todo o período contratual.

9.1.3. As ferramentas devem ser tecnicamente reconhecidas pelo mercado e amplamente adotadas por organizações de grande porte, garantindo suporte e atualizações regulares das ferramentas.

9.1.4. Todas as ferramentas utilizadas deverão possuir suporte técnico e manutenção garantidos pela CONTRATADA, incluindo correções de segurança, patches e atualizações durante toda a vigência do contrato.

9.1.5. As soluções devem oferecer capacidade de integração via APIs abertas ou conectores seguros, permitindo interoperabilidade com os sistemas e infraestruturas já existentes da CONTRATANTE, principalmente o ITSM, sistema que irá proporcionar padrão no atendimento dos SLAs.

9.1.6. As ferramentas escolhidas devem atender requisitos normativos e boas práticas.

9.1.7. A CONTRATANTE não exigirá métricas de desempenho ou KPIs específicos das ferramentas, mas o desempenho final dos serviços prestados deverá atender aos SLA e níveis de serviço estabelecidos no contrato principal.

9.1.8. A CONTRATADA será responsável por dimensionar corretamente as ferramentas, garantindo que possuam capacidade suficiente para suportar o ambiente da CONTRATANTE, conforme o escopo dos serviços contratados.

9.1.9. A CONTRATADA deverá executar Testes de Penetração da rede (Pentest) internos e externos para identificação de vulnerabilidades;

9.1.10. Executar testes de penetração em sistemas, redes e aplicações: para identificar vulnerabilidades exploráveis e avaliar a postura de segurança da infraestrutura da CONTRATANTE.

9.2. Ferramentas para o SOC (Security Operations Center)

9.2.1. A operação do SOC deverá ser sustentada por uma suíte de ferramentas integradas para detecção, análise e resposta a incidentes, correlação em tempo real, e integração com feeds de Threat Intelligence externos e internos.

9.2.2. A CONTRATADA poderá adotar outras ferramentas adicionais, conforme necessário, desde que respeitem as diretrizes e políticas de segurança da PMESP e que sejam compatíveis com os serviços prestados.

9.2.3. Para garantir um nível mínimo de segurança e capacidade operacional, as seguintes ferramentas são exigidas:

9.2.3.1. Módulo de Gestão e Correlação de Eventos (SIEM);

9.2.3.2. Módulo de Sistema de Logs (SysLog);

9.2.3.3. Módulo de Detecção em Endpoint (EDR);

9.2.3.4. Módulo Avançado de Detecção e Resposta (XDR);

9.2.3.5. Módulo de Teste de Penetração (PENTEST);

9.2.3.6. Módulo de Threat Intelligence (OSINT);

9.3. Módulo de Gestão e Correlação de Eventos (SIEM) e Módulo de Sistema de Logs (SysLog):

9.3.1. A CONTRATADA deverá fornecer o serviço de Security Information and Event Management (SIEM), contemplando a coleta, armazenamento, análise, classificação e correlação de logs de segurança provenientes de diversas fontes, garantindo auditoria, compliance e detecção de incidentes.

9.3.2. A ferramenta de SIEM deverá ser uma solução utilizada no âmbito público, adotada em serviços de SOC, e capaz de atender a requisitos de segurança da informação. A solução deverá oferecer funcionalidades de monitoramento, detecção de ameaças e resposta a incidentes, suportando, no mínimo, 3.000 (três mil) eventos por segundo e ou 133GB/DIA, com garantia de escalabilidade e desempenho adequados às demandas do CONTRATANTE.

9.3.3. A ferramenta de SIEM, como elemento central para processamento e armazenamento de logs e eventos, com histórico comprovado em ambientes governamentais, e capacidade de ingestão superior a 1.000 EPS (Eventos por Segundo).

9.3.4. É importante destacar que o licenciamento deverá suportar até 3.000 (três mil) EPS com 30 dias de retenção. E quanto ao Syslog 5 (cinco) anos de retenção. E o custo do software será apurado mensalmente, de modo a permitir o correto dimensionamento dos pagamentos.

9.3.5. O serviço deverá ser contínuo e ininterrupto (24x7x365), garantindo a ingestão e o tratamento adequado dos eventos de segurança do ambiente computacional do CONTRATANTE.

9.3.6. A prestação do serviço deve incluir, no mínimo:

9.3.6.1. Administração e operação da solução de SIEM.

9.3.6.2. Monitoramento contínuo e análise de eventos de segurança.

9.3.6.3. Suporte técnico e manutenção evolutiva e corretiva da solução.

9.3.6.4. Implementação de processos para avaliação e otimização da ingestão de logs.

9.3.6.5. Atualizações regulares, garantindo segurança, patches e melhorias contínuas.

9.3.6.6. A ferramenta de SIEM deverá incorporar tecnologias, alinhadas às melhores práticas do mercado, para identificar eventos de segurança e comportamentos anômalos com maior assertividade, superando limitações de tecnologias tradicionais, aprimorando a detecção de ameaças com alta precisão, reduzindo falsos positivos.

9.3.7. Integração e Compatibilidade

9.3.7.1. A ferramenta de SIEM deverá possuir integração nativa com as demais ferramentas da SOLUÇÃO, ou via APIs seguras, garantindo a interoperabilidade e a cobertura completa das funcionalidades necessárias.

- 9.3.7.2. Deve ser capaz de coletar, normalizar e correlacionar logs de diversas fontes, incluindo sistemas operacionais, aplicações, dispositivos de rede, firewalls, sistemas de autenticação e demais sistemas de segurança.
- 9.3.7.3. A solução deverá permitir a ingestão de eventos utilizando padrões como:
 - 9.3.7.3.1. Syslog RFC 3164 e RFC 5424
 - 9.3.7.3.2. CEF (Common Event Format)
 - 9.3.7.3.3. JSON, XML, CSV e logs estruturados
 - 9.3.7.3.4. Microsoft Windows Event Logs
 - 9.3.7.3.5. ODBC/JDBC para bancos de dados
 - 9.3.7.3.6. NetFlow/IPFIX para análise de tráfego de rede
- 9.3.7.4. Deverá possuir painéis de análise, com dashboards interativos e personalizáveis, classificação de incidentes por criticidade, apresentação das evidências associadas e possibilidade de integração com ferramentas externas para implementação de workflow de tratamento e escalonamento.
- 9.3.7.5. Deve permitir a criação e personalização de regras de correlação de eventos, permitindo ajustes conforme o ambiente do CONTRATANTE, incluindo:
 - 9.3.7.6. Definição de alertas customizados.
 - 9.3.7.7. Aplicação de regras para detectar padrões de ataques e ameaças persistentes.
 - 9.3.7.8. Filtragem e categorização de eventos de segurança.
- 9.3.8. Infraestrutura e Segurança
 - 9.3.8.1. A ferramenta de SIEM deverá ser disponibilizada em infraestrutura própria da CONTRATADA ou em ambiente de nuvem, podendo ser ofertada na modalidade SaaS (Software as a Service), PaaS (Platform as a Service) ou hospedagem dedicada, desde que atenda aos requisitos de segurança e desempenho estabelecidos.
 - 9.3.8.2. O ambiente utilizado pela CONTRATADA para hospedagem da solução deverá atender aos seguintes requisitos mínimos:
 - 9.3.8.3. Infraestrutura de alta disponibilidade e resiliência, garantindo continuidade dos serviços e recuperação de desastres.
 - 9.3.8.4. Armazenamento e processamento dos dados do CONTRATANTE em conformidade com regulamentações de proteção de dados aplicáveis.
 - 9.3.8.5. Isolamento adequado dos dados do CONTRATANTE para evitar concorrência de recursos críticos com outros clientes.
 - 9.3.8.6. A CONTRATADA deverá garantir que a comunicação entre os elementos locais do CONTRATANTE e o SIEM seja realizada por meio de conexões seguras, utilizando TLS 1.2 ou superior, com protocolos criptográficos robustos que assegurem a integridade e a confidencialidade dos dados.
- 9.3.9. Gestão de Eventos e Resposta a Incidentes
 - 9.3.9.1. A ferramenta de SIEM deverá permitir:
 - 9.3.9.1.1. Detecção e categorização automática de ameaças.
 - 9.3.9.1.2. Geração de alertas e notificações em tempo real sobre eventos suspeitos.
 - 9.3.9.1.3. A solução deverá permitir o encaminhamento automático de alertas para plataformas externas de orquestração de resposta, possibilitando a execução de playbooks automatizados, enriquecimento com fontes de Threat Intelligence e acionamento escalonado por severidade, com suporte a integrações que permitam gestão baseada em SLA.
 - 9.3.9.2. A solução deverá possuir interface gráfica para análise forense, permitindo:
 - 9.3.9.2.1. Busca avançada com suporte a expressões regulares (regex) e filtros adaptativos, utilizando sintaxe de consulta compatível com ferramentas de mercado, e possibilidade de integração com mecanismos externos para execução de consultas YARA, quando aplicável.
 - 9.3.9.2.2. Visualização centralizada dos eventos e alertas de segurança.
 - 9.3.9.2.3. Geração de relatórios detalhados e gráficos interativos para auditoria e investigação.
 - 9.3.9.2.4. Retenção de dados configurável, com possibilidade de exportação segura e integridade garantida por mecanismos de criptografia e/ou assinatura digital, incluindo integração com ferramentas externas quando necessário para atender à cadeia de custódia.
 - 9.3.9.3. A ferramenta de SIEM deverá permitir a configuração de políticas de retenção de logs, suportando pelo menos dois níveis de armazenamento:
 - 9.3.9.3.1. SIEM: Retenção de logs ativos por até 30 dias.
 - 9.3.9.3.2. SISLOG: Arquivamento de logs de longo prazo por pelo menos 60 meses.
 - 9.3.9.4. Deve suportar a exportação de logs e incidentes, permitindo que o CONTRATANTE migre os dados para outro prestador de serviço, sem custo adicional e sem perda de integridade.
- 9.3.10. Responsabilidades da CONTRATADA
 - 9.3.10.1. A CONTRATADA será integralmente responsável pelo fornecimento, suporte e manutenção da solução.
 - 9.3.10.2. Licenciamento oficial e vigente da ferramenta durante toda a vigência do contrato.
 - 9.3.10.3. Monitoramento contínuo e atualizações regulares de segurança.
 - 9.3.10.4. Treinamento operacional para os responsáveis pelo uso da solução.
 - 9.3.10.5. A CONTRATADA deve promover a automação de processos e fluxos de trabalho, que por sua vez, deverá ser capaz de criá-los por meio de interface low-code/no-code com biblioteca de conectores prontos (REST/SOAP) e integração a ferramentas como EDR, Firewall, DLP e antivírus.
 - 9.3.10.6. Possuir recursos gráficos de workflow interativos para criação e processos e rotinas operacionais, que permita operações como arrastar-e-soltar para o desenho dos fluxos de trabalho;
 - 9.3.10.7. Apresentar componente próprio para a modelagem gráfica e a automação de processos e fluxos de trabalho da solução;
 - 9.3.10.8. Permitir a automação de fluxos de automação de forma gráfica, incluindo estágios, tarefas paralelas ou sequenciais, regras de decisão e aprovação, sem a necessidade de programação ou alteração de código fonte;
 - 9.3.10.9. Possuir ferramenta de criação de formulários com campos específicos de cada processo e fluxo de trabalho, a fim de personalizar a inserção de informações e controles de acordo com a necessidade, sem a necessidade de programação ou alteração do código-fonte;
 - 9.3.10.10. Dispensar a necessidade da criação de tabelas, colunas e campos de banco de dados na solução, ou a necessidade de programação ou alteração do código-fonte, tornando estas alterações, quando necessárias, transparentes aos operadores e administradores que implementam os fluxos de trabalho;
 - 9.3.10.11. Permitir a criação de campos compartilhados que possam ser utilizados em quaisquer outras entidades da solução, sem a necessidade de programação ou alteração do código-fonte;
 - 9.3.10.12. Disponibilizar recursos tecnológicos de catálogo de serviços que possibilitem a automação de processos de gestão de TI;
 - 9.3.10.13. Permitir a customização de menus, formulários, labels, automatizações de fluxos de trabalho e processos de TI, desenvolvidos na solução,

- permitindo a adequação às necessidades de uso de cada usuário, sem a necessidade de programação ou alteração do código-fonte;
- 9.3.10.14. Permitir a criação e automação de processos e fluxos de trabalho de forma segregada e independente a fim de permitir a personalização para cada departamento;
- 9.3.10.15. Permitir a automação de processos e fluxos de trabalho;
- 9.3.10.16. Permitir a criação de painéis e dashboards com gráficos de gestão, de forma ágil e intuitiva, sem a necessidade de programação e alteração do código-fonte;
- 9.3.10.17. Permitir a criação de painéis e dashboards com gráficos do tipo pizza, linha, colunas, barras e tabelas dinâmicas, sem a necessidade de programação e alteração do código-fonte. E que contemple as diversas necessidades de visão gerencial com agilidade e flexibilidade de ajustes necessários;
- 9.3.10.18. Permitir alterações de atributos de forma dinâmica em gráficos de gestão, contidos em painéis e dashboards da solução, possibilitando a alteração de eixos, título do gráfico, legenda, escala, rótulos de dados, tamanho do gráfico, de forma gráfica na solução e sem a necessidade de alterações do código-fonte;
- 9.3.10.19. Permitir aos atendentes e solucionadores de chamados criarem seus próprios painéis e gráficos dentro da solução e compartilharem com grupos ou usuários específicos da solução, permitindo gerenciar as permissões de compartilhamento de acordo com os perfis de usuários da solução;
- 9.3.10.20. Permitir a criação de gráficos com informações de diferentes entidades da solução, permitindo a sobreposição e cruzamento de informações e delimitação de linhas de tendência;
- 9.3.10.21. Permitir geração de relatórios com metadados, trilha de auditoria, hash de integridade, e exportação nos formatos .csv, .html, .pdf, .xml, .json e integração com ferramentas BI;
- 9.3.10.22. Prover informação em “real-time” de maneira gráfica por meio de dashboards;
- 9.3.10.23. Permitir configurar o envio automático e agendado de relatórios e gráficos gerenciais para grupos de usuários ou usuários específicos.
- 9.3.10.24. A CONTRATADA é responsável por desenvolver, implementar e aprimorar continuamente fluxos de trabalho automatizados para detecção, investigação e resposta a incidentes de segurança. Isso inclui a identificação de processos que podem ser automatizados, a criação de scripts e integrações necessárias, e a validação da eficácia desses fluxos de trabalho.
- 9.3.10.25. A CONTRATADA deve manter uma biblioteca de playbooks e scripts atualizados, os quais são essenciais para automatizar a resposta a incidentes, incluindo o desenvolvimento de novos playbooks conforme necessário, bem como a revisão e atualização periódica dos existentes para garantir sua eficácia e relevância.
- 9.3.10.26. A CONTRATADA deve designar o grupo técnico responsável pela gestão, definição de fluxos de trabalho, análise de processos de segurança, automação, otimização de processos para garantir a eficácia na detecção e resposta a incidentes.
- 9.3.11. Características gerais:
- 9.3.11.1. Deve utilizar de inteligência artificial e algoritmos de aprendizado de máquina para fornecer detecção aprimorada de ameaças, resposta a incidentes de segurança, análise de comportamentos anômalos para tomada de decisão de forma automatizada, reduzindo o tempo de resposta;
- 9.3.11.2. A orquestração deverá permitir a criação de scripts, playbooks, e fluxos de trabalho para execução de tarefas corretivas, ou escalção para equipes especializadas, com objetivo de atender a diversos tipos de incidentes;
- 9.3.11.3. Deve possuir processos, scripts e automações baseados em casos de uso em sua base de orquestração com capacidade de adaptação ao ambiente da PMESP, permitindo maior agilidade na implantação;
- 9.4. Módulo de Detecção em Endpoint (EDR):**
- 9.4.1. A proteção de terminais e a prevenção contra vazamento de informações são componentes essenciais para a segurança cibernética da PMESP. Para isso, a CONTRATADA deverá adotar soluções eficazes para monitoramento de ameaças e controle de dados sensíveis.
- 9.4.2. É importante destacar que o licenciamento dos EDR poderá chegar a até 20.000 (vinte mil) unidades, conforme a necessidade e a estratégia de implantação. O custo do software será apurado mensalmente, de modo a permitir o correto dimensionamento dos pagamentos.
- 9.4.3. As ferramentas implementadas devem ser compatíveis com os demais sistemas de segurança e permitir integração com a estrutura do SOC, garantindo uma visão centralizada dos eventos de segurança.
- 9.4.4. Deverá preencher os seguintes requisitos:
- 9.4.4.1. O Servidor de Administração e Console Administrativa.
- 9.4.4.1.1. Compatibilidade: Microsoft Windows Server 2012 (Todas edições x64); Microsoft Windows Server 2012 R2 (Todas edições x64); Microsoft Windows Server 2016 x64; Windows Server 2022 Core Standard/ Datacenter; Windows Server 2022 Core Standard/ Datacenter; Microsoft Windows 10 (Todas edições x32); Microsoft Windows 10 (Todas edições x64);
- 9.4.4.2. Suporta as seguintes plataformas virtuais:
- 9.4.4.2.1. VMware: Workstation 14.x Pro, vSphere 6. vSphere 6.5; Microsoft Hyper-V: 2008, 2008 R2, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 e 2022; Citrix;
- 9.4.4.3. Estações Windows
- 9.4.4.3.1. Compatibilidade: Microsoft Windows 10 Pro / Enterprise x86 / x64; Microsoft Windows Server 2012 R2 Standard x64; Microsoft Windows Server 2012 Foundation x64; Microsoft Windows Server 2012 Standard x64; Microsoft Windows Server 2008 R2 Standard/Enterprise x64 SP1; Microsoft Windows Server 2016 x64; Windows Server 2019 Core Standard/ Datacenter; Windows Server 2022 Core Standard/ Datacenter; Estações Mac OS X; Mac OS macOS 13.X Ventura e posteriores; Ubuntu 18.04; Ubuntu 20.04 LTS; CentOS-6.9; CentOS-7.4; CentOS-8; CentOS-9 stream; Debian GNU/Linux 9.4; OracleLinux 7.4;
- 9.4.4.4. Servidores Windows
- 9.4.4.4.1. Compatibilidade: Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter; Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter; Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter; Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter; Windows Server 2016 Essentials/Standard/Datacenter/MultiPoint Premium Server; Windows Server 2016 Core Standard / Datacenter; Windows Server 2019 Core Standard/ Datacenter; Windows Server 2022 Core Standard/ Datacenter.
- 9.4.4.5. Servidores Linux:
- 9.4.4.5.1. Compatibilidade: Plataforma 64-bits: Red Hat® Enterprise Linux® 6.9 Server; Red Hat® Enterprise Linux® 7.4 Server; Red Hat® Enterprise Linux® 7.5 Server; CentOS-6.9; CentOS-7.4; CentOS-7.5; CentOS-8; CentOS-9; Ubuntu 18.04; Ubuntu 24; Ubuntu Server 20.04.1 LTS.
- 9.4.5. Deve prover as seguintes proteções:

- 9.4.5.1. Varredura de arquivos residente que verifique qualquer arquivo criado, copiado (de fonte interna ou externa), acessado ou modificado, sendo realizado em tempo real, e também agendada ou solicitada;
- 9.4.5.2. Autoproteção contra-ataques aos serviços/processos do antivírus;
- 9.4.5.3. Capacidades de detecção e priorização de vulnerabilidades do Windows e de aplicativos instalados, fornecendo visibilidade detalhada para ação imediata de correção ou mitigação;
- 9.4.5.4. Detecção e bloqueio de tentativas de exploração no endpoint, utilizando análise comportamental, inteligência de ameaças e prevenção de execução de código malicioso;
- 9.4.6. Deve ter as seguintes capacidades:
 - 9.4.6.1. As atualizações de conteúdo e assinaturas devem ser disponibilizadas e aplicadas automaticamente pelo fabricante, diariamente.
 - 9.4.6.2. Ter a capacidade para importação e distribuição automática e manual de atualizações a partir da console do produto;
 - 9.4.6.3. Não deve haver a necessidade de reinicialização do computador ou serviço e sem a necessidade de instalação de ou módulos adicionais à solução de antivírus ofertada;
 - 9.4.6.4. Notificar automaticamente por meio de mensagem na tela a detecção de vírus ou de falha no processo de “limpeza”/“ exclusão” dos arquivos infectados, com exibição da ação tomada. Esta mensagem deverá ser configurável permitindo a inserção de textos personalizados pela PMESP e/ou uma mensagem de notificação enviada por e-mail;
 - 9.4.6.5. Disponibilizar ao menos um console central de gerenciamento hospedado em ambiente cloud, na modalidade SaaS, sem limitação de processadores ou quantidade de dispositivos gerenciados;
 - 9.4.6.6. Permitir administração descentralizada com base em perfis e permissões configuráveis, integrados ao Active Directory da PMESP quando aplicável;
 - 9.4.6.7. Possuir capacidade para configurar como serão distribuídas as atualizações de conteúdo, produto e configurações, de forma centralizada via console de gerenciamento;
 - 9.4.6.8. Permitir definir grupos de endpoints para aplicação de políticas e atualizações conforme critérios da contratante;
 - 9.4.6.9. Permitir acesso a console de gerenciamento por meio da tecnologia MMC (Microsoft Management Console) ou da tecnologia Web com acesso seguro (HTTPS);
 - 9.4.6.10. Capacidade para configurar manualmente e/ou automaticamente repositórios distribuídos principais e secundários, de forma para que no caso de o repositório principal ficar indisponível, o computador de ponta irá buscar atualizações em repositórios secundários;
 - 9.4.6.11. Ter a capacidade de implementação de senha em todos os softwares (agentes) adquiridos, de forma que operações que resultam na desinstalação, alteração de parâmetros de configuração ou desativação do software, sejam restritas pelo uso de senha;
 - 9.4.6.12. Permitir o agrupamento dos computadores (que estiverem com o software (agente) instalado) em grupos lógicos e independentes da estrutura de domínio de rede, conforme política e critérios de definição fixados pela Contratada na console de gerenciamento;
 - 9.4.6.13. Ter a capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
 - 9.4.6.14. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
 - 9.4.6.15. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
 - 9.4.6.16. Leitura de configurações;
 - 9.4.6.17. Modificação de configurações;
 - 9.4.6.18. Gerenciamento de Backup;
 - 9.4.6.19. Visualização de relatórios;
 - 9.4.6.20. Gerenciamento de relatórios;
 - 9.4.6.21. Gerenciamento de chaves de licença;
 - 9.4.6.22. Gerenciamento de permissões (adicionar/excluir permissões acima);
 - 9.4.6.23. Possuir capacidade de monitorar e inspecionar continuamente todos os processos em execução no endpoint, aplicando análise comportamental e baseada em machine learning para detectar e prevenir atividades maliciosas em tempo real, sem impacto perceptível ao usuário final;
 - 9.4.6.24. Bloquear malwares tais como ransomwares mesmo quando o ataque vier de um computador sem antivírus na rede;
 - 9.4.6.25. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa;
 - 9.4.6.26. Garantir continuidade da proteção mesmo após interrupções inesperadas, retomando automaticamente os processos de monitoramento em tempo real e análise comportamental assim que o sistema estiver operacional;
 - 9.4.6.27. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (Uninterruptible Power supply – UPS);
 - 9.4.6.28. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
 - 9.4.6.29. Ter capacidade de configurar políticas de verificação diferentes para grupos de dispositivos permitindo ainda exceções e exclusões de pastas e arquivos;
 - 9.4.6.30. Ter capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
 - 9.4.6.31. Ter capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan. banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
 - 9.4.6.32. Ter capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
 - 9.4.6.33. Ter capacidade de verificar somente arquivos novos e alterados;
 - 9.4.6.34. Ter capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .pst, arquivos compactados por compactadores binários, etc.);
 - 9.4.6.35. Ter capacidade de verificar objetos usando heurística;
 - 9.4.6.36. Ter capacidade de configurar diferentes ações para diferentes tipos de ameaças;
- 9.4.7. O antivírus, ao encontrar um arquivo potencialmente perigoso, deve:
 - 9.4.7.1. Bloquear acesso ao objeto;
 - 9.4.7.2. Quarentenar ou excluir automaticamente o arquivo, conforme política previamente definida pelo administrador;
 - 9.4.7.3. A solução deve ser projetada para funcionar no modo off-line.

- 9.4.7.4. A comunicação entre agente e console de gerenciamento deve ser criptografada.
- 9.4.8. Manutenção / Subscrição de Software
- 9.4.8.1. Manutenção para Atualizações e Correções dos Softwares
- 9.4.8.2. A subscrição terá prazo de vigência do contrato.
- 9.4.8.3. Consiste no fornecimento das atualizações da solução (engine), perfis de comportamento, assinaturas de ameaças, bem como, das correções, atualizações, novas versões, qualquer alteração do software ou de suas bases complementares (listas, assinaturas, métodos de funcionamento, etc.) e novos releases de todos os softwares que compõe a solução fornecida e que forem lançadas no mercado pelo fabricante do produto, devendo ser prestada na seguinte conformidade:
- 9.4.8.4. Durante toda vigência do contrato, por vinte e quatro horas/dia para todos os dias da semana, deverá;
- 9.4.8.5. Fornecer as novas versões, novos releases, correções, alterações, bases acessórias do software (qualquer lista ou base de dados que seja necessária para o perfeito funcionamento do software ou para mantê-lo em níveis recentes de atualização) e atualizações desenvolvidas para todos os softwares que compõe a solução fornecida e que forem lançadas no mercado pelo fabricante do produto;
- 9.4.8.6. Fornecer a correção de erros e defeitos de todos os softwares que compõe a solução fornecida sempre que forem identificados erros ou defeitos de programação prejudiciais ao seu perfeito uso, funcionamento e administração no ambiente da PMESP;
- 9.4.8.7. Fornecedor contínuo de novas assinaturas, regras de detecção e indicadores de ameaças assim que liberados pelo fabricante, garantindo que a solução permaneça atualizada frente a novas técnicas de ataque;
- 9.4.8.8. A retirada de circulação comercial ou a exclusão da lista de produtos suportados pelo fabricante não excluirá as obrigações da contratada sobre os softwares fornecidos;
- 9.4.8.9. Caso o software seja descontinuado durante a vigência do Contrato, sendo entendido que software descontinuado é aquele que tenha sido excluído da lista de produtos suportados e que o seu desenvolvimento, aperfeiçoamento e manutenção foi encerrado pelo fabricante, as obrigações da contratada serão mantidas até a data final de vigência do contrato.
- 9.4.9. Suporte Técnico dos Softwares
- 9.4.9.1. A CONTRATADA deverá possuir de forma permanente durante 24h em todos os dias da semana, setor de suporte para atendimento da Contratante, sendo que:
- 9.4.9.2. Consiste no atendimento dos chamados técnicos da Contratante, na resolução de dúvidas, panes, falhas e não conformidades técnicas prejudiciais ao uso, instalação, administração, funcionamento, desempenho e à performance dos softwares fornecidos, sendo prestada em duas modalidades:
- 9.4.9.3. Remoto (telefônico, em língua portuguesa): Atendimento feito por meio de Central de Serviços (Service Desk), com posições de atendimento (PAs) suficientes para o atendimento, registro, resolução e/ou direcionamento dos chamados técnicos do Contratante.
- 9.4.9.4. Local (on site): Atendimento feito por meio de analistas de campo devidamente habilitados e capacitados, que atuarão diretamente no local de instalação do software fornecido.
- 9.4.9.5. O Suporte Técnico dos Softwares, remoto e local, deve ser prestada na seguinte conformidade:
- 9.4.9.6. Durante toda vigência do contrato, por vinte e quatro horas/dia para todos os dias da semana, deverá:
- 9.4.9.7. Diagnosticar erros e defeitos dos softwares fornecidos;
- 9.4.9.8. Identificar as correções necessárias para a resolução de problemas gerados pelos erros e defeitos diagnosticados;
- 9.4.9.9. Identificar as soluções de contorno para a resolução de problemas gerados por erros e defeitos apresentados no software fornecido;
- 9.4.9.10. Efetuar a solicitação de correções para erros e defeitos do software;
- 9.4.9.11. Efetuar a solução de dúvidas, panes, falhas e não-conformidades técnicas relacionadas com a execução de todas as operações e intervenções técnicas necessárias à instalação, configuração, teste, otimização, operacionalização, aplicação de atualizações, correção de erros, operacionalização, uso e administração da solução contratada;
- 9.4.9.12. Prover a infraestrutura presencial ou de Help Desk em língua portuguesa necessária para o atendimento dos chamados técnicos;
- 9.4.9.13. As atividades relativas serão executadas nos locais de instalação dos softwares, limitando-se somente ao município de São Paulo e sua região metropolitana.
- 9.4.10. Condições de Atendimento
- 9.4.10.1. Define as principais metas e responsabilidades da Contratada para o atendimento das Obrigações da Contratada – Subscrição de Software. O atendimento será feito pela contratante por meio da abertura de chamados técnicos pela contratada, que serão classificados por grau de severidade, devendo ser prestados dentro dos padrões mínimos de atendimento abaixo:
- 9.4.10.1.1. Severidade 1 (S1): software apresenta pane, falha ou não-conformidade técnica que o torna total ou parcialmente inoperante. O primeiro retorno telefônico da Contratada deve ser realizado em no máximo 02 (duas) horas e a solução técnica, definitiva ou de contorno, não poderá exceder a 8 (oito) horas, contadas do chamado técnico;
- 9.4.10.1.2. Severidade 2 (S2): software apresenta pane, falha ou não-conformidade técnica que prejudica a operação, uso ou acesso de função(s) básica(s). O primeiro retorno telefônico da Contratada deve ser realizado em no máximo 02 (duas) horas e a solução técnica, definitiva ou de contorno, não poderá exceder a 24 (vinte e quatro) horas, contadas do chamado técnico;
- 9.4.10.1.3. Severidade 3 (S3): software apresenta pane, falha ou não-conformidade técnica que causa restrições de operação de funções acessórias. O primeiro retorno telefônico da Contratada deve ser realizado em no máximo 02 (duas) horas e a solução técnica, definitiva ou de contorno, não poderá exceder a 48 (quarenta e oito) horas, contadas do chamado técnico;
- 9.4.11. Condições Gerais
- 9.4.11.1. A contratada deverá fornecer todo e qualquer software necessário ao perfeito funcionamento, uso e administração da solução proposta.
- 9.4.11.2. Todos os softwares fornecidos deverão ter as funcionalidades já disponíveis em mercado, não sendo permitida a adequação destes softwares para atender requisitos específicos exigidos neste projeto básico, não será admitido o desenvolvimento de software para atender as demandas específicas definidas neste projeto básico;
- 9.4.11.3. O licenciamento dos softwares deverá ser feito sem limites quanto ao número de processadores existentes no microcomputador onde estiver sendo processado o módulo;
- 9.4.11.4. Compatibilidade para a instalação, funcionamento e utilização plena de todos os recursos em microcomputadores do tipo servidores, estações de trabalho, notebooks e netbooks;
- 9.4.12. Instalação:

- 9.4.12.1. A instalação compreende as atividades de preparação da infraestrutura, instalação lógica do software e testes;
- 9.4.12.2. Incluem-se na instalação as atividades de: Levantamento de dados; Adequação da solução à infraestrutura apresentada; Execução dos testes dos testes de funcionamento do software; A contratada deverá prover todos os materiais necessários à instalação da solução fornecida;
- 9.4.12.3. Durante a fase preparatória e de execução da instalação, a CONTRATADA deverá observar as indicações técnicas do Fabricante, as normas de segurança aplicáveis à espécie.
- 9.4.12.4. Os serviços de instalação compreendem a execução direta, pelos técnicos da contratada, das operações e intervenções necessárias à instalação da solução de Endpoint Protection, visando o seu perfeito funcionamento, uso, administração e a sua total interligação, integração e compatibilidade com o ambiente computacional da Contratada, observadas as seguintes condições:
- 9.4.12.5. Integrar e compatibilizar a solução com os demais ativos do ambiente computacional da Contratada.
- 9.4.12.6. Integrar com a solução de SIEM, atual ou ofertada na estrutura de SOC.

9.5. Módulo Avançado de Detecção e Resposta - XDR:

- 9.5.1. A plataforma deve ser entregue na modalidade Software-as-a-Service com alta disponibilidade;
- 9.5.2. É importante destacar que o licenciamento dos XDR poderá chegar a até 200 (duzentas) unidades, conforme a necessidade e a estratégia de implantação. O custo do software será apurado mensalmente, de modo a permitir o correto dimensionamento dos pagamentos.
- 9.5.3. O acesso a plataforma deve ser realizado via browser, ao menos: Google Chrome, Mozilla Firefox e Microsoft Edge;
- 9.5.4. Deve receber telemetria dos demais sensores existentes, de forma centralizar a visão de logs, alertas e incidentes;
- 9.5.5. Deve permitir que as detecções vindas dos sensores sejam correlacionadas, permitindo investigação multicamadas.
- 9.5.6. A plataforma deve ser entregue em nuvem como um serviço (SaaS), sendo o fabricante responsável por todas as manutenções, atualizações e garantia de disponibilidade;
- 9.5.7. Deve possuir capacidade centralizar a visibilidade dos logs coletados, criando uma relação de objetos que apresente as ações envolvidas no alerta de fim a fim;
- 9.5.8. A plataforma deve possuir os seguintes módulos de forma:
 - 9.5.8.1. Módulo de investigação de incidentes;
 - 9.5.8.2. Módulo de análise forense de ameaças digitais;
 - 9.5.8.3. Módulo de inteligência de ameaças;
 - 9.5.8.4. Módulo de gestão de vulnerabilidades;
- 9.5.9. Serviço de monitoramento avançado especializado da plataforma 24x7;
 - 9.5.9.1. Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias e suportar extensão deste prazo para até 60 meses totais;
 - 9.5.9.2. A plataforma de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;
 - 9.5.9.3. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;
 - 9.5.9.4. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total, permissão para realizar investigações e permissão de apenas leitura;
 - 9.5.9.5. Deve permitir a criação de perfis de acesso customizados, sendo possível vincular a visão de menus da plataforma de acordo com grupos de dispositivos e contas de usuários;
 - 9.5.9.6. Deve permitir que o administrador atribua acesso ao grupo de funcionalidades da console para cada usuário;
 - 9.5.9.7. A console deve suportar limitação de sessões concorrentes de acesso via navegador;
 - 9.5.9.8. A console deve restringir acesso por meio de endereço de IP e range de IP;
 - 9.5.9.9. Deve listar os logs de auditoria da console dos últimos 30 dias;
 - 9.5.9.10. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;
 - 9.5.9.11. Deve possibilitar adição de MFA para acesso a plataforma, da Contratante;
 - 9.5.9.12. Deve permitir o envio de notificações para os administradores através de e-mail, API e integrações com sistemas de ITSM;

9.5.10. Módulo de investigação de incidentes;

- 9.5.10.1. Deve gerar visibilidade de todos os alertas vindos dos demais sensores de telemetria da plataforma, a saber: Rede, Endpoint, Cloud e Identidade;
- 9.5.10.2. Deve correlacionar tais alertas de forma a indicar por meio de relação de objetos quais são os dispositivos, IPs, usuários e servidores envolvidos no contexto do alerta gerado;
- 9.5.10.3. Deve apresentar arquivos, caminhos de pastas, comandos, URLs e Hashs envolvidos nos alertas;
- 9.5.10.4. Deve associar a técnica identificada com base na matriz do framework MITRE ATT&CK;
- 9.5.10.5. Deve ser possível assignar um usuário responsável para tratar e analisar o alerta gerado;
- 9.5.10.6. Deve ser possível categorizar os alertas de acordo as análises realizadas, de forma a ser possível apontar que o alerta se trata de um:
 - 9.5.10.6.1. Verdadeiro positivo;
 - 9.5.10.6.2. Falso positivo;
 - 9.5.10.6.3. Incidente notável;
- 9.5.10.7. Deve ser possível inserir informações a respeito do alerta analisado;
- 9.5.10.8. Cada alerta gerado deve apresentar um nível de severidade de risco ao ambiente da CONTRATANTE, segundo categorização:
 - 9.5.10.8.1.1. Risco Baixo;
 - 9.5.10.8.1.2. Risco Médio;
 - 9.5.10.8.1.3. Risco Alto;
 - 9.5.10.8.1.4. Risco Crítico.
- 9.5.10.9. Dentro da tela de visibilidade dos alertas, deve ser possível tomar ações de resposta imediata perante o contexto do possível ataque:
 - 9.5.10.9.1. Acesso remoto a máquina sessão da própria solução;
 - 9.5.10.9.2. Isolamento de máquina – Essa ação deve restringir completamente a comunicação da máquina com dispositivos da rede local e endereços da internet, permitindo apenas a conexão com a plataforma XDR;
 - 9.5.10.9.3. Reset senha do usuário;
 - 9.5.10.9.4. Bloqueio de conta do usuário;

- 9.5.10.9.5. Envio de script customizado;
- 9.5.10.10. Deve prover visualização em linha do tempo com informações dos eventos monitorados;
- 9.5.10.11. Deve possuir funcionalidade de busca inteligente aos dados coletados advindos dos sensores da plataforma, suportando buscas via operadores lógicos;
- 9.5.10.12. Deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque;
- 9.5.10.13. Deve permitir a visualização entre usuários, máquinas, processos, comandos, arquivos e demais componentes correlacionados em determinado ataque;
- 9.5.10.14. O módulo de investigação de incidentes deve atuar baseado em modelos de detecção de ataques avançados e furtivos;
- 9.5.10.15. Deve implementar e organizar os ataques baseados no framework MITRE ATT&CK, identificando técnicas e táticas dos ataques;
- 9.5.10.16. Deve possuir capacidades de criação de modelos de detecção customizados;
- 9.5.10.17. Deve informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;
- 9.5.10.18. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscas específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.
- 9.5.10.19. A partir da identificação de uma exploração de vulnerabilidade em determinadas máquinas, a solução deve ser capaz de fornecer recomendações de mitigação, permitindo aplicar políticas de proteção diretamente ou via integrações;
- 9.5.10.20. Com base na telemetria gerada, deve apresentar de forma gráfica fases de um possível ataque, por meio das correlações aplicadas;
- 9.5.10.21. Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;
- 9.5.10.22. Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;
- 9.5.10.23. Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;
- 9.5.10.24. Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;
- 9.5.10.25. Possuir capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;
- 9.5.10.26. Capacidade de construir sequências de buscas para localizar os dados ou objetos no ambiente que será feita a análise;
- 9.5.10.27. Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta para identificar, categorizar e recuperar os resultados da pesquisa;
- 9.5.10.28. Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais;
- 9.5.10.29. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise de impacto e análise de causa-raiz;
- 9.5.10.30. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;
- 9.5.10.31. Deve exibir os eventos de forma a priorizar os alertas mais críticos para otimizar o tempo de investigação, como pontuações ou níveis de prioridade;
- 9.5.10.32. Atuar com ações planejadas, por meio de roteiros customizáveis, quando da detecção de alto risco de máquinas presentes no ambiente da CONTRATANTE;
- 9.5.10.33. Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;
- 9.5.10.34. Deve prover visualização em linha do tempo com informações dos eventos monitorados em dispositivo;
- 9.5.10.35. Deve associar cada alerta gerado a um incidente macro, a fim de correlacionar os alertas gerando visão de impacto e criticidade;
- 9.5.10.36. Deve ser possível assignar um alerta a um incidente;
- 9.5.10.37. Deve ser possível correlacionar um alerta a um caso no ITSM;

9.5.11. Módulo de análise forense de ameaças digitais;

- 9.5.11.1. Deve possuir módulo de análise forense de ameaças digitais, sendo possível a investigação em tempo real nas máquinas por meio de queries avançadas;
- 9.5.11.2. Deve ser possível a criação de espaços de investigação dentro da plataforma, para que informações de máquinas e evidências sejam coletadas;
- 9.5.11.3. Deve possuir capacidades de coleta de arquivos conforme alvos detectados;
- 9.5.11.4. Deve possuir suporte à coleta de grandes volumes de evidências digitais, permitindo a extração e transferência eficiente de artefatos para análise forense;
- 9.5.11.5. A coleta de arquivos e evidências devem ser de forma remota via ações automáticas e manuais, quando necessário;
- 9.5.11.6. Deve suportar a coleta de evidências com base em informações de sistema das máquinas, linha do tempo de arquivos, dispositivos externos conectados, informações de serviço, processos e tarefas agendadas.
- 9.5.11.7. Deve possuir ambiente isolado para análise de artefatos, tal ambiente de estar hospedado na própria nuvem do fabricante e integrado a plataforma, suportando a execução de URLs e arquivos suspeitos;
- 9.5.11.8. Tais objetos advindos das análises devem ser adicionados automaticamente na lista de objetos suspeitos;
- 9.5.11.9. Deve suportar no mínimo a análise de 50 artefatos por dia;

9.5.12. Módulo de Inteligência de Ameaças

- 9.5.12.1. A solução deve contar com módulo dedicado a inteligência de ameaças;
- 9.5.12.2. Deve gerar alertas de indicadores de comprometimento (IOCs) presentes no ambiente da CONTRATANTE e que possam estar correlacionados a companhias globais de ameaças;
- 9.5.12.3. Deve gerar relatórios com base nas fontes de inteligência do fabricante e de terceiros, a fim de identificar possíveis IOCs no ambiente;
- 9.5.12.4. Deve ter suporte a customização das buscas por IOCs no ambiente;
- 9.5.12.5. Deve possuir lista customizável de indicadores de comprometimento e objetos suspeitos;
- 9.5.12.6. Deve permitir adicionar arquivos SHA-1, SHA-256, URLs, IPs, domínios e endereços de e-mail a lista de objetos suspeitos;
- 9.5.12.7. Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de objetos suspeitos.
- 9.5.12.8. Deve ser possível determinar o tempo de vida da existência de um IOC;

- 9.5.12.9. Deve ser capaz de configurar o nível de risco de cada IOC;
- 9.5.12.10. Deve ter suporte ao consumo de fontes externas de IOCs, por meio de integração nativa ou via API;
- 9.5.12.11. Quando um IOC é inserido na lista de objetos, o módulo deve enviar tal informação a todos os agentes que compõem a solução, unificando a informação;
- 9.5.13. Módulo de Gestão de Vulnerabilidade**
- 9.5.13.1. A solução deve ser entregue como um serviço Software-as-a-Service (SaaS) em uma nuvem proprietária do fabricante para todos os seus serviços e aplicativos exigidos neste documento. Serviços fornecidos por nuvens de terceiros não são aceitos;
- 9.5.13.2. A gestão de todos os módulos considerados neste termo deve ser feita através de uma console única;
- 9.5.13.3. A solução deverá possuir no mínimo, duas das seguintes certificações de privacidade e segurança: EU-U.S. Privacy Shield Framework, Swiss-U.S. Privacy Shield Framework, Cloud Security Alliance e (CSA) STAR.
- 9.5.13.4. Todos os serviços da plataforma devem estar disponíveis sob o mesmo padrão de qualidade de serviço 24x7x365 e garantir 99% de disponibilidade;
- 9.5.13.5. O ofertante deve oferecer manutenção e atualização constante da plataforma durante todo o período de vigência do contrato de serviço;
- 9.5.13.6. As atualizações de serviço devem ser transparentes para o administrador da solução, sem afetar nenhum dos dados armazenados - serviços fornecidos;
- 9.5.13.7. Todas as comunicações entre componentes, transferência de dados e sincronização da solução devem ser criptografadas de ponta a ponta, fazendo uso de no mínimo TLS 1.2, certificados assinados com RSA 2048 bits e algoritmo de assinatura SHA256;
- 9.5.13.8. A solução deve permitir criação de usuários distintos;
- 9.5.13.9. Deve permitir separação de funções e permissões na console;
- 9.5.13.10. Deve permitir integração através de SSO com, pelo menos, Active Directory;
- 9.5.13.11. A console deve ser acessível a partir de, pelo menos, um dos navegadores comerciais dentre Google Chrome, Microsoft Edge e Firefox;
- 9.5.13.12. A solução proposta deve oferecer um agente de baixo impacto nos sistemas operacionais onde está instalado e no consumo de largura de banda que utilizará na rede;
- 9.5.13.13. A solução deve ser instalada em servidores, estações de trabalho, e máquinas virtuais, suportando sua implantação em rede local, em rede doméstica e na nuvem;
- 9.5.13.14. A solução deve oferecer suporte para sua implantação em pelo menos os seguintes sistemas operacionais: Windows 7/Windows Server 2003 SP2 e posterior (x86, x64), Red Hat Enterprise Linux/CentOS 6.5+, 7.x (x64), 8.x (x64), Ubuntu 14, 16,18,19,20 (x64), Oracle Enterprise Linux 8, Oracle Enterprise Linux (OEL) 7 até 7.5, Oracle Enterprise Linux (OEL) 6, Amazon Linux 2, Amazon Linux 2018.03, Amazon Linux 2017.09, Amazon Linux 2017.03, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 11.
- 9.5.13.15. O agente da solução deve se atualizar automaticamente e gerir as suas atualizações automaticamente;
- 9.5.13.16. A solução deve suportar plataformas de nuvem AWS, GCP, Azure;
- 9.5.13.17. A solução deve ser capaz de coletar informações sobre o inventário de ativos;
- 9.5.13.18. As funcionalidades de gestão de ativos, gestão de vulnerabilidade e detecção de patches devem ser fornecidas pelo mesmo agente de gerenciamento, não serão aceitas soluções com múltiplos agentes;
- 9.5.13.19. O agente de gerenciamento deve suportar o uso de proxy;
- 9.5.13.20. Deve ser possível definir o intervalo de comunicação entre o agente e a console de gerenciamento;
- 9.5.13.21. Deve ser possível limitar o consumo de CPU ou memória do agente;
- 9.5.13.22. Deve permitir a definição de um período global de inatividade dos agentes;
- 9.5.13.23. A solução deve permitir o uso de scanners capazes de identificar vulnerabilidades através de varreduras em ranges de IP definidos pelo administrador;
- 9.5.13.24. Não deverá haver restrições para instalação de scanners virtuais no ambiente;
- 9.5.13.25. Deve ser permitido o uso de scanners externos, sem necessidade de instalação, em nuvem própria do fabricante para varreduras de ativos publicados na internet;
- 9.5.13.26. Os scanners virtuais devem suportar pelo menos um dos hypervisors: Hyper-V, ProxMox.
- 9.5.13.27. Os Scanners devem suportar a varredura de ambientes em nuvem para pelo menos dois dos seguintes provedores: Azure; AWS; Google Cloud Platform; Oracle;
- 9.5.13.28. Os scanners devem reportar vulnerabilidades para console em nuvem, permitindo uma visão consolidada de vulnerabilidades;
- 9.5.13.29. Deve ser permitido a configuração de varreduras periódicas (com intervalo mínimo de 4 horas) para máquinas identificadas manualmente por meio de perfil de configuração ou tags associadas a uma versão específica de banco de dados em execução;
- 9.5.13.30. Deve ser permitido a varredura sob demanda para um ou mais ativos de rede;
- 9.5.13.31. O mesmo scanner deve ser capaz de varrer por falhas de conformidade e também por vulnerabilidades;
- 9.5.13.32. O scanner deverá consolidar vulnerabilidades encontradas em um ativo que possua agente instalado;
- 9.5.13.33. A solução deve permitir a configuração do tipo de varredura a ser realizada, permitindo pelo menos definir as seguintes configurações ao defini-la:
- 9.5.13.33.1. Configuração de quantidades de portas TCP/UDP a serem validadas;
- 9.5.13.33.2. Consumo de largura de banda e recursos (alto, médio, baixo);
- 9.5.13.33.3. Digitalize para dispositivos que não suportam ping - traceroute;
- 9.5.13.33.4. Detecção de balanceadores de carga;
- 9.5.13.33.5. Configuração de força bruta para usar em senhas;
- 9.5.13.33.6. Uso de um cabeçalho HTTP personalizado;
- 9.5.13.33.7. Ignorar pacotes;
- 9.5.13.33.8. Instalação de agente temporário para validação de registro local;
- 9.5.13.34. A solução proposta deve permitir a coleta de informações detalhadas sobre o ativo gerenciado, deve detalhar pelo menos os seguintes dados para cada ativo: Serviços em execução; Software instalado; Usuários; Portas abertas; Nome do host; FQDN; IP v4 / v6; Endereço MAC; Processador; Memória; Volumes de disco; BIOS;
- 9.5.13.35. A solução deve classificar automaticamente os ativos por famílias de tecnologia, tipo de dispositivo, tipo de plataforma e fabricante;

- 9.5.13.36. A solução deve normalizar automaticamente os nomes dos fabricantes de HW e SW com seus dados relevantes, como o nome dos aplicativos e versões, para facilitar sua posterior busca na solução;
- 9.5.13.37. A solução deve possuir a habilidade de etiquetagem (Tags) de ativos para facilitar a identificação, deve permitir a geração de Tags, pelo menos, usando os seguintes parâmetros: Palavras-chaves; Endereço IP e intervalos de IP; Segmento de rede; Portas abertas;
- 9.5.13.38. Informações de inventário considerando, no mínimo: Sistema operacional; Presença ou ausência de determinado software instalado ou serviço em execução;
- 9.5.13.39. A solução deve permitir agrupamento manual a critério do administrador da solução;
- 9.5.13.40. A solução deve permitir atribuir criticidade ao ativo para priorizá-lo durante o processo de gerenciamento.;
- 9.5.13.41. Deve permitir criação de Dashboards personalizados que sejam capazes de trazer as seguintes informações sobre os ativos: Categorias de softwares instalados nos ativos; Hosts que executam máquinas virtuais; Sistemas operacionais utilizados; Serviços e portas TCP ou UDP abertas; Softwares de segurança instalados;
- 9.5.13.42. A solução deve permitir uma interface de busca de ativos que utilize uma sintaxe lógica baseados, no mínimo, nos critérios abaixo: Fabricante de hardware; Último usuário logado; Categoria de software instalado;
- 9.5.13.43. A solução deve permitir a visualização de quantidade de máquinas com um determinado software instalado;
- 9.5.13.44. Deve permitir visualização de recursos em nuvem AWS ou Azure tais como VPCs, Virtual Networks, Security Group, S3 buckets, RDS, SQL Server, através de conectores ou via agente;
- 9.5.13.45. Deve permitir visibilidade a respeito de hosts que executam containers e containers em execução;
- 9.5.13.46. A solução deve permitir descobrir, avaliar, priorizar e auxiliar na correção de vulnerabilidades/ configurações em toda a infraestrutura de rede, incluindo estações de trabalho, servidores, dispositivos de rede, dispositivos de telecomunicações e dispositivos de segurança, hypervisors, máquinas virtuais, orquestradores de contêineres, contêineres e nuvens (Azure, GCP, AWS), proporcionando através de única interface para o administrador via um portal web para gerenciamento de todos os ativos, permitindo o gerenciamento centralizado de todos os componentes da solução a partir de um único ponto, sem a necessidade de incorrer em consoles - componentes adicionais fora dele para a administração dos serviços oferecidos
- 9.5.13.47. A solução deve ser oferecida na modalidade SaaS em nuvem própria do fabricante, sem necessidade de instalação de componentes locais para a gerência;
- 9.5.13.48. A solução deve ser licenciada por Asset (IP - HOST) para ativos de infraestrutura;
- 9.5.13.49. A solução deve ser licenciada com foco em servidores, de acordo com as quantidades especificadas na tabela de quantitativos;
- 9.5.13.50. A CONTRATANTE poderá solicitar a cobertura de desktops considerados críticos, a serem acionados sob demanda;
- 9.5.13.51. A solução deve permitir varreduras de vulnerabilidade com base em: Sistemas Operacionais; Portas TCP e UDP; Serviços; Bancos de dados; Dispositivos de rede como switches, roteadores e balanceadores de carga;
- 9.5.13.52. No mínimo, a ferramenta deve abranger os seguintes sistemas operacionais, bancos de dados e aplicativos: Microsoft Windows, UNIX, LINUX, MacOS e VMware.
- 9.5.13.53. Detectar e analisar vulnerabilidades nas principais versões de Bancos de Dados, pelo menos: Microsoft SQL Server, MySQL e Oracle.
- 9.5.13.54. Detectar e analisar vulnerabilidades em plataformas WEB, pelo menos: IIS, Apache Tomcat, Detectar e analisar vulnerabilidades em porta e serviços TCP e UDP.
- 9.5.13.55. Detectar vulnerabilidades em pelo menos os seguintes aplicativos ou plataformas: Adobe, Apple, Microsoft (Office, IIS, Exchange), Oracle e Java.
- 9.5.13.56. Permitir a descoberta de vulnerabilidades na rede, oferecendo as seguintes alternativas de varredura: Varredura ativa de rede não autenticada, Varredura ativa de rede autenticada, Agente, Varreduras externas e O mecanismo de varredura deve ter uma taxa de precisão de detecção de vulnerabilidade de 99,99966% (seis sigma) durante os últimos 10 anos.
- 9.5.13.57. A base de conhecimento de vulnerabilidade deve ser atualizada semanalmente, garantindo a incorporação de pelo menos 20 CVEs a ela e deve ter pelo menos uma base de conhecimento de 35.000 CVEs relacionados incluindo tecnologias legadas e atuais;
- 9.5.13.58. A solução deve oferecer suporte ao padrão da indústria para pontuação de vulnerabilidade do Common Vulnerability Scoring System (CVSS);
- 9.5.13.59. A solução deve oferecer suporte ao padrão da indústria para adicionar detecções personalizadas usando Open Vulnerability Assessment Language (OVAL);
- 9.5.13.60. A solução deve permitir vincular as vulnerabilidades detectadas e indicar sua relação com ameaças como Vírus, Trojan e Malware;
- 9.5.13.61. A solução deve ser capaz de indicar explorações disponíveis e códigos disponíveis para uma vulnerabilidade, quando aplicável;
- 9.5.13.62. O banco de dados deve relacionar a maioria das vulnerabilidades ao CVE e Bugtraq;
- 9.5.13.63. A solução deve oferecer suporte à integração para autenticação por ferramentas de cofres de senha;
- 9.5.13.64. A solução deve permitir buscas interativas de vulnerabilidade utilizando filtros como severidade, categoria, sistema operacional, status, classificação do CVSS, CVE ou KB;
- 9.5.13.65. A solução deve permitir a utilização de operadores lógicos na busca de vulnerabilidades para que seja possível encontrar, no mínimo, as seguintes informações: Vulnerabilidades associadas a ransomware e que possuem patches disponíveis, Vulnerabilidades detectadas em um segmento de rede, Vulnerabilidades detectadas em serviços específicos, Vulnerabilidades detectadas por um usuário específico, Vulnerabilidades detectadas em hardware específico e Vulnerabilidades detectadas por tag AWS ou Azure específicas.
- 9.5.13.66. Na busca de vulnerabilidades deve permitir agrupamento para mostrar, no mínimo, as seguintes visualizações: Quantidade de ocorrências de uma mesma vulnerabilidade, Quantidade de vulnerabilidades por sistema operacional, Quantidade de vulnerabilidades por host, Quantidade de vulnerabilidades por Exploit disponível e Quantidade de vulnerabilidades por produto/software vulnerável.
- 9.5.13.67. A solução deve permitir exportar buscas e filtros criados para um dashboard;
- 9.5.13.68. A solução deve permitir salvar filtros criados em buscas para reutilização;
- 9.5.13.69. Deve mostrar dashboards que consigam mostrar variação histórica de vulnerabilidades novas, corrigidas, reabertas;
- 9.5.13.70. Deve permitir mostrar dashboards que contenham quantidades de vulnerabilidades associadas a ransomware, que contém exploits públicos e que permitem exploração sem autenticação;
- 9.5.13.71. Deve mostrar dashboards que mostrem o racional de vulnerabilidades que podem ser corrigidas através de patches;
- 9.5.13.72. Deve mostrar patches faltantes em sistemas operacionais independente da relação com uma vulnerabilidade existente;
- 9.5.13.73. A solução deve oferecer a possibilidade de monitorar dispositivos móveis Android, iOS;

- 9.5.13.74. A solução deve permitir a avaliação, o relatório e o relatório de problemas de configuração, com base nas referências do padrão da indústria do Centro de Segurança da Internet (CIS);
- 9.5.13.75. O fabricante deve ser oficialmente certificado pelo CIS para fornecer este nível de controles;
- 9.5.13.76. A solução deve oferecer avaliação de configuração com base no benchmark CIS padrão da indústria, cobrindo esta funcionalidade nas seguintes categorias: Sistemas operacionais, Software de servidor, Provedores de nuvem, Dispositivos de rede e Software de desktop.
- 9.5.13.77. A solução deve suportar detecção de falhas de conformidades através de varreduras autenticadas ou através de agente instalado diretamente no ativo monitorado;
- 9.5.13.78. A solução deve permitir que os administradores recebam informação de conformidade de sistemas operacionais Windows e Linux, mesmo que não estejam conectados a rede corporativa;
- 9.5.13.79. A solução deve permitir a avaliação de certificados digitais (internos e externos) e configurações de TLS em busca de problemas e vulnerabilidades de certificados, resultando em diferentes graus de conformidade de acordo com os resultados da avaliação de seu emissor, prazo de validade, tipo de certificado, robustez do o algoritmo e o conjunto de criptografia usados;
- 9.5.13.80. A solução proposta deve permitir enviar alertas em tempo real sobre irregularidades na rede, identificar ameaças e monitorar mudanças inesperadas que ocorram na mesma;
- 9.5.13.81. A solução deve permitir enviar notificações para usuários específicos e grupos de usuários para o perfil de monitoramento - perfis de monitoramento múltiplos;
- 9.5.13.82. A solução deve permitir a personalização do perfil de monitoramento associado a uma lista específica de critérios;
- 9.5.13.83. A solução deve permitir que os alertas sejam personalizados para uma ampla variedade de condições que afetam sistemas, certificados, vulnerabilidades, portas, serviços e software. Cada regra deve permitir que seja configurada para detectar mudanças gerais comuns - para se ajustar a circunstâncias muito específicas;
- 9.5.13.84. A solução deve permitir a atribuição de destinatários diferentes para cada alerta;
- 9.5.13.85. A solução deve enviar alertas de monitoramento sobre vulnerabilidades, configurações incorretas e outros parâmetros definidos pelo administrador da solução:
- 9.5.13.85.1. Ativos com sistemas operacionais não aprovados;
- 9.5.13.85.2. Certificados expirados - expirando;
- 9.5.13.85.3. Portas abertas;
- 9.5.13.85.4. Vulnerabilidades graves;
- 9.5.13.85.5. Tickets de correção abertos, resolvidos e fechados;
- 9.5.13.85.6. Software não aprovado;
- 9.5.13.86. A solução proposta deve fornecer fontes de inteligência de ameaças em tempo real e técnicas de aprendizado de máquina para fornecer controle de administrador sobre a evolução das ameaças relacionadas a vulnerabilidades encontradas nos ativos da organização e identificar quais corrigir primeiro;
- 9.5.13.87. A solução deve permitir consultas ad-hoc com múltiplas variáveis e critérios, como classe de ativo, tipo de vulnerabilidade, indicadores de ameaça em tempo real, etiqueta de ativo e o sistema operacional, de modo que, por exemplo, seja possível pesquisar todas as vulnerabilidades que tenham uma alta classificação de gravidade, são fáceis de explorar e foram lançados na semana passada;
- 9.5.13.88. A solução deve permitir que se faça uma correlação em tempo real das ameaças ativas contra as vulnerabilidades detectadas nos ativos corporativos;
- 9.5.13.89. A solução deve incluir indicadores de ameaças em tempo real que ajudam a avaliar e priorizaras vulnerabilidades detectadas, categorizados da seguinte forma:
- 9.5.13.89.1. Dia Zero: vulnerabilidades para as quais não há patch disponível e para as quais um ataque ativo foi observado;
- 9.5.13.89.2. Exploração pública: Vulnerabilidades cujo mecanismo de exploração é conhecido, para o qual existe um código de exploração e está disponível publicamente;
- 9.5.13.89.3. Ataques ativos: vulnerabilidades que estão sendo atacadas ativamente;
- 9.5.13.89.4. Movimento lateral: vulnerabilidades que permitem ao invasor espalhar o ataque amplamente pela rede violada;
- 9.5.13.89.5. Fácil exploração: vulnerabilidades que podem ser facilmente exploradas, exigindo poucas habilidades e pouco conhecimento;
- 9.5.13.89.6. Perda de dados: vulnerabilidades cuja exploração causará perda massiva de dados;
- 9.5.13.89.7. Negação de serviço: vulnerabilidades cuja carga útil pode sobrecarregar - impedir que sistemas comprometidos estejam permanentemente - temporariamente disponíveis;
- 9.5.13.89.8. No Patch: Vulnerabilidades para as quais não há solução do provedor;
- 9.5.13.89.9. Malware: vulnerabilidades associadas a infecções por malware;
- 9.5.13.89.10. Kit de exploração: vulnerabilidades para as quais um kit de exploração está disponível;
- 9.5.13.90. A solução deve atribuir uma pontuação a cada vulnerabilidade de forma contextual de forma a quantificar o risco associado a esta vulnerabilidade;
- 9.5.13.91. Os fatores de risco devem considerar, pelo menos 3 dos fatores abaixo:
- 9.5.13.91.1. Malwares associados;
- 9.5.13.91.2. Atores maliciosos associados;
- 9.5.13.91.3. Possibilidade de remediação;
- 9.5.13.92. A solução proposta deve fornecer um workflow de correção baseado em políticas de criação e atribuição, atribuindo tickets de acordo com as condições definidas pelo administrador da solução através de políticas ou manualmente;
- 9.5.13.93. A solução deve permitir a criação de tickets com status aberto, fechado, ignorado, com base nos seguintes critérios:
- 9.5.13.93.1. Host(s) a quem a regra se aplica;
- 9.5.13.93.2. Vulnerabilidade (s) a que a regra se aplica;
- 9.5.13.93.3. Usuário atribuído;
- 9.5.13.93.4. Data de criação - expiração;
- 9.5.13.93.5. Mudança de estado;
- 9.5.13.94. A solução deve permitir a criação de tickets de correção automaticamente a partir do resultado de uma varredura de vulnerabilidade - com

base nas informações de um host específico e também manualmente por um administrador de solução;

9.5.13.95. A solução proposta deve correlacionar vulnerabilidades e patches automaticamente para os hosts da sua organização;

9.5.13.96. A solução deve mapear automaticamente os patches com CVEs associados às vulnerabilidades detectadas;

9.5.13.97. Deve mostrar patches faltantes mesmo que não exista correlação com uma vulnerabilidade existente;

9.5.13.98. Deve mostrar patches faltantes para no mínimo as seguintes categorias: Navegadores, Ferramentas de compressão de arquivos, Visualizadores de PDF e Sistemas operacionais.

9.5.13.99. A solução proposta deve permitir administração centralizada via interface gráfica WEB usando HTTPS;

9.5.13.100. A solução deve possibilitar o acesso a console de todos os componentes do serviço a partir de um único ponto;

9.5.13.101. A solução deve permitir a definição de diferentes perfis de usuários e funções para administração;

9.5.13.102. A solução deve fornecer controles de acesso de usuário hierárquicos e baseados em funções que permitem a delegação de responsabilidades para refletir a estrutura organizacional;

9.5.13.103. A solução deve permitir o acesso de um usuário autorizado de qualquer local;

9.5.13.104. A solução deve suportar integração com uma biblioteca API XML extensível;

9.5.13.105. A solução deve suportar autenticação de dois fatores para usuários e login;

9.5.13.106. A solução deve suportar configurações de segurança de senha;

9.5.13.107. A solução deve suportar personalizar a política de segurança para configurações de gerenciamento de senha, por:

9.5.13.107.1. Idade e expiração da senha;

9.5.13.107.2. Conta do usuário bloqueada após uma série de logins com falha;

9.5.13.107.3. Comprimento mínimo da senha;

9.5.13.107.4. Complexidade da senha, caracteres alfanuméricos e numéricos a serem usados;

9.5.13.107.5. Forçar mudança de senha no login inicial

9.5.13.107.6. Notificação de senha expirada antes de vários dias;

9.5.13.108. A solução deve suportar a capacidade de restringir o acesso apenas de rede interna da empresa;

9.5.13.109. A solução deve suportar a capacidade de rastrear a atividade do usuário por nome da conta do usuário, data, ação e informações sobre a ação;

9.5.13.110. A solução deve suportar acesso por SSO (Single Sign-on) usando SAML 2.0;

9.5.13.111. A solução proposta deve gerar relatórios por IPs, Grupo e Tags

9.5.13.112. A solução deve permitir a geração de relatórios de qualquer IP - Host previamente verificado;

9.5.13.113. A solução deve permitir agendar relatórios diários, semanais, mensais e sob demanda;

9.5.13.114. A solução deve permitir o envio de notificações por email sempre que um relatório estiver disponível para o administrador da solução, usuários específicos e perfis diferentes criados na ferramenta;

9.5.13.115. A Solução deve permitir pelo menos os seguintes tipos de relatórios: Relatório de correção; Relatório de vulnerabilidades altamente críticas; Relatório Executivo; Relatório de autenticação; Relatório de conformidade normativa e regulatória; e Relatório de remediação.

9.5.13.116. A solução deve fornecer relatórios de correção por grupo de ativos, usuário e vulnerabilidade;

9.5.13.117. A solução deve permitir a criação de relatórios baseados em IPv4, endereços IPv6, nome do host, grupo de ativos e rótulos personalizados pelo administrador;

9.5.13.118. A solução deve permitir relatórios com cálculo de risco de segurança, permitindo um cálculo de risco global para todos os ativos incluídos no relatório;

9.5.13.119. A solução deve permitir relatórios que possibilitem o cálculo do risco do negócio, utilizando como base para o cálculo do risco de impacto ao negócio e do risco de segurança dos ativos incluídos no relatório;

9.5.13.120. A solução deve permitir relatar as descobertas com base no status das vulnerabilidades detectadas e seu status, conforme lista abaixo: Novo, Resolvido, Reaberto e Ativo.

9.5.13.121. A solução deve permitir relatórios que incluam vulnerabilidades com base na data de publicação;

9.5.13.122. A solução deve permitir excluir vulnerabilidades que não são exploráveis devido à configuração do sistema / plataforma onde foi detectada;

9.5.13.123. A solução deve permitir a exclusão de patches da Microsoft que foram substituídos por um novo patch ou um patch cumulativo do mesmo fabricante;

9.5.13.124. A solução deve fornecer relatórios automatizados de tendências e diferenciais;

9.5.13.125. A solução deve fornecer várias opções de distribuição de relatórios, incluindo PDF criptografado;

9.5.13.126. A solução deve dar suporte à personalização do modelo de relatório conforme necessário;

9.5.13.127. A solução deve permitir a exportação de relatórios para dois dos formatos HTML, MHT, PDF, DOC, CSV e XML;

9.5.13.128. A solução deve permitir que relatórios sejam apresentados em tabelas e gráficos com as ocorrências ocorridas, permitindo a customização detalhada de cada relatório;

9.5.13.129. A solução deve possuir um painel (dashboard) que, por padrão, permite que você veja as tendências de vulnerabilidades por gravidade, plataforma, idade e status de remediação;

9.5.13.130. A solução deve permitir a customização dos painéis fazendo uso de qualquer um dos dados disponíveis associados aos ativos varridos para selecionar diferentes tipos de gráficos, tabelas e visualizações sobre a priorização de vulnerabilidades;

9.5.13.131. A solução deve fornecer painéis executivos personalizáveis com uma visão unificada de todos os componentes da solução;

9.5.13.132. Deve ser possível criar dashboards que mostrem a pontuação de risco global de ativos e sua variação ao longo do tempo;

9.6. Módulo de Teste de Penetração - Pentest:

9.6.1. Objetivo dos Testes:

9.6.2. Executar testes de penetração em sistemas, redes e aplicações da CONTRATANTE, com o objetivo de identificar vulnerabilidades exploráveis, avaliar a postura de segurança da infraestrutura e fornecer recomendações práticas para mitigar riscos identificados.

9.6.3. Os testes devem ser realizados com ferramentas desenvolvidas pelo próprio analista ou ferramentas reconhecidas no mercado: Nmap, Metasploit, Cobalt Strike, Kali Linux, BloodHound, CrackMapExec, além de técnicas personalizadas em Python/Bash entre outras linguagens;

9.6.4. Os testes devem ser realizados sem comprometer a confidencialidade, disponibilidade ou integridade dos sistemas, salvo acordo prévio, e culminar na entrega de um relatório final detalhado com os resultados, impactos e sugestões de correção.

9.6.5. É importante destacar que o PENTEST poderá ser realizado 3 (três) vezes durante a execução do contrato e custo do teste será apurado mensalmente, de modo a permitir o correto dimensionamento dos pagamentos.

9.6.6. Escopo dos Testes:

9.6.6.1. Ambientes a Serem Testados

9.6.6.1.1. Definir os ambientes a serem testados, incluindo, mas não se limitando a: redes internas e externas, serviços expostos, aplicações web, APIs, dispositivos IoT, sistemas legados, bancos de dados, serviços em nuvem (ex.: AWS, Azure) e aplicações móveis.

9.6.6.1.2. O escopo deve ser detalhado em conjunto com a CONTRATANTE, com base em uma lista de ativos ou diagrama de infraestrutura previamente fornecidos.

9.6.6.2. Simulações de Ataque

9.6.6.2.1. O testes devem incluir simulações de ataques internos e externos, explorando diferentes vetores de ameaça, como phishing, escalonamento de privilégios, injeção de código e exploração de configurações incorretas. Os testes podem ser realizados nos formatos black-box (sem informações prévias) ou gray-box (informações parciais), conforme definido no escopo acordado com a CONTRATANTE.

9.6.6.3. Frequência e Agendamento

9.6.6.4. Periodicidade dos Testes

9.6.6.4.1. Determinar a periodicidade dos testes (trimestral, semestral, anual ou conforme demanda específica), considerando a criticidade dos sistemas testados, requisitos regulatórios ou políticas internas da CONTRATANTE.

9.6.6.5. Testes Adicionais

9.6.6.5.1. Estabelecer critérios para a execução de testes adicionais em caso de grandes mudanças na infraestrutura (como implementação de novos sistemas, atualizações críticas ou expansões significativas) ou incidentes relevantes, com prazo de execução definido em até 7 (sete) dias após o evento, conforme acordado com a CONTRATANTE.

9.6.7. Metodologias e Padrões de Segurança

9.6.7.1. Metodologias Reconhecidas

9.6.7.1.1. Indicar metodologias reconhecidas para a realização dos testes, como OWASP (Open Web Application Security Project) para aplicações web e APIs, NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment) para diretrizes de avaliação técnica, MITRE ATT&CK para simulações de Red Team, PTES (Penetration Testing Execution Standard) para testes abrangentes, OSSTMM (Open Source Security Testing Methodology Manual) e, quando aplicável, alinhamento com a ISO/IEC 27001. As metodologias podem ser combinadas ou adaptadas ao contexto da CONTRATANTE, utilizando ferramentas reconhecidas, conforme especificado no plano de teste.

9.6.7.2. Os testes devem ser conduzidos por equipe técnica qualificada, com experiência comprovada e, preferencialmente, certificações reconhecidas na área de segurança da informação, como CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional) ou CISSP (Certified Information Systems Security Professional).

9.6.7.3. Exploração de Vulnerabilidades:

9.6.7.4. A ferramenta deve permitir a exploração controlada de vulnerabilidades identificadas, com as seguintes capacidades:

9.6.7.5. O analista deverá utilizar ferramentas que permitam a exploração controlada das vulnerabilidades identificadas, sem colocar em risco a integridade ou disponibilidade do ambiente, atendendo algumas premissas básicas de pentest, como por exemplo:

9.6.7.6. Execução de Exploits: Suporte à execução segura e documentada de exploits para validar a explotabilidade de falhas.

9.6.7.7. Criação de Payloads Personalizados: Funcionalidade para gerar sessões reversas, shells e payloads customizados (ex.: reverse shell para acesso remoto).

9.6.7.8. Integração com Bases de Exploits: Conexão com repositórios atualizados, como Exploit-DB, para acesso a exploits relevantes e recentes.

9.6.7.9. Testes em Diferentes Perspectivas: Capacidade de realizar testes de intrusão em redes internas e externas, simulando cenários de ataque realistas.

9.6.7.10. As vulnerabilidades identificadas devem ser classificadas conforme o sistema CVSS (Common Vulnerability Scoring System), acompanhadas de recomendações detalhadas e prazos sugeridos para mitigação. Deve ser oferecida a opção de retestes para validação das correções implementadas pela CONTRATANTE.

9.6.8. Conformidade Legal e Ética

9.6.8.1. Os testes devem ser realizados em conformidade com a legislação aplicável, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, e mediante autorização formal da CONTRATANTE, garantindo que todas as ações sejam éticas e legais.

9.6.8.2. Comunicação e Notificação, vulnerabilidades críticas devem ser comunicadas à CONTRATANTE em até 24 horas após a identificação, com relatórios preliminares, se necessário. Relatórios detalhados, contendo todas as descobertas, análises e recomendações, devem ser entregues ao final dos testes, em formato acordado com a CONTRATANTE

9.6.9. Suporte a Criptografia e Força Bruta:

9.6.9.1. A ferramenta deve oferecer recursos para testar a robustez de sistemas de autenticação e criptografia, incluindo:

9.6.9.2. Ataques a Senhas: Capacidade de quebrar senhas por meio de ataques de dicionário, força bruta ou métodos híbridos.

9.6.9.3. Compatibilidade com Protocolos: Suporte a testes em serviços como SSH, FTP, HTTP Auth, SMB, entre outros.

9.6.10. Para avaliação da segurança de ativos computacionais, redes, aplicações e serviços, com capacidade de identificar, explorar e relatar vulnerabilidades, conforme boas práticas reconhecidas internacionalmente, a CONTRATADA deverá em seu ambiente de SOC utilizar ferramenta com a capacidade mínimas para estes objetivos:

9.6.11. Coleta de Informações (Reconhecimento Passivo e Ativo)

9.6.11.1. A ferramenta deve oferecer capacidades robustas de reconhecimento, incluindo:

9.6.11.2. Varredura de Portas e Serviços: Capacidade de escanear portas e identificar serviços ativos em protocolos TCP, UDP e ICMP, detectando pontos de entrada em hosts-alvo.

9.6.11.3. Deve realizar a identificação de sistemas e serviços, com a Detecção automática de sistemas operacionais (ex.: Windows, Linux) e versões de serviços (ex.: Apache, SSH) em execução nos alvos.

9.6.11.4. Coleta de Informações Públicas (OSINT): Suporte à obtenção de metadados e dados públicos a partir de fontes abertas, como WHOIS, registros DNS e plataformas OSINT, sem interação direta com o alvo.

9.6.11.5. Descoberta de Subdomínios e DNS: Funcionalidade para identificar subdomínios e servidores DNS associados ao domínio-alvo;

9.6.11.6. Todas as ferramentas utilizadas pelo time técnico deverão ser fornecidas pela CONTRATADA, como exemplo cito ferramentas para

realização de pentest web, máquinas para quebra de senha e ferramentas para engenharia reversa, variando de acordo com o escopo do teste definido pelo CONTRATANTE.

9.6.12. Análise de Vulnerabilidades:

9.6.12.1. A ferramenta deve possuir recursos avançados para identificação e classificação de vulnerabilidades, incluindo:

9.6.12.2. Detecção de Vulnerabilidades Conhecidas: Capacidade de detectar falhas catalogadas no banco CVE, com classificação baseada no CVSS (ex.: crítico, alto, médio).

9.6.12.3. Suporte a Múltiplos Alvos: Análise de vulnerabilidades em aplicações web, APIs, infraestrutura de rede e sistemas tradicionais.

9.6.12.4. Filtros de Severidade: Opções para filtrar resultados por nível de criticidade e severidade, facilitando a priorização de correções.

9.6.12.5. Exportação de Resultados: Geração de relatórios exportáveis em formatos abertos, como XML, JSON, CSV e PDF, para integração com outros sistemas ou entrega à CONTRATANTE;

9.6.13. Armazenamento e descarte de Relatórios e Evidências

9.6.13.1. Com base no NIST e OWASP todas as evidências técnicas, relatórios preliminares, finais e demais artefatos gerados durante a execução do serviço de teste de intrusão (pentest) deverão ser, obrigatoriamente, armazenados exclusivamente na infraestrutura da CONTRATANTE, seja em ambiente local ou em seus serviços próprios de nuvem.

9.6.13.2. É vedado ao contratado manter cópias desses documentos ou evidências em qualquer outro meio físico ou digital após a conclusão do projeto, salvo autorização expressa e formal da CONTRATANTE.

9.6.13.3. Após a conclusão da atividade as evidências coletadas nos computadores, dispositivo utilizado no pentest deverão ser apagados mantendo apenas as cópias na infraestrutura da CONTRATANTE.

9.6.14. Escopo de pentest

9.6.14.1. O escopo do pentest será definido pelo CONTRATANTE e será dividido em 3 diferentes fases:

9.6.14.1.1. Pentest Blackbox/Graybox na(s) aplicações, infraestrutura ou serviços definidos pelo cliente. Com base de 160 horas de execução seguindo as melhores práticas de mercado: 1. Reconhecimento, 2. Escaneamento e Exploração, 3. Movimentação Lateral, 4. Manutenção de Acesso, 5. Exfiltração de Dados.

9.6.14.1.2. Pentest Blackbox/Graybox na(s) aplicações, infraestrutura ou serviços definidos pelo cliente. Com base de 80 horas de execução seguindo as melhores práticas de mercado: 1. Reconhecimento, 2. Escaneamento e Exploração, 3. Movimentação Lateral, 4. Manutenção de Acesso, 5. Exfiltração de Dados.

9.6.14.1.3. Pentest Blackbox/Graybox na(s) aplicações, infraestrutura ou serviços definidos pelo cliente. Com base de 80 horas de execução seguindo as melhores práticas de mercado: 1. Reconhecimento, 2. Escaneamento e Exploração, 3. Movimentação Lateral, 4. Manutenção de Acesso, 5. Exfiltração de Dados.

9.7. Modulo de Threat Intelligence (OSINT):

9.7.1. Deverá ser fornecido o serviço de Inteligência em Ameaças Cibernéticas (Threat Intelligence), com foco em coleta, correlação e análise de dados públicos e fontes abertas (OSINT), através de uma solução que atenda aos requisitos abaixo:

9.7.1.1. Capacidade para operação simultânea de, no mínimo, 03 usuários autenticados,

9.7.1.2. A operação da ferramenta será realizada pelo time de SOC da empresa CONTRATADA em regime 24x7.

9.7.1.3. O funcionamento da plataforma deverá ser em nuvem, acessível via web no modelo SaaS (Software-as-a-Service), com disponibilidade mínima de 99,9%.

9.7.1.4. A solução deverá operar em cloud pública, com arquitetura redundante e escalável.

9.7.1.5. Compatibilidade com navegadores modernos (Firefox 60+, Chrome 65+), incluindo suporte a autenticação multifator.

9.7.2. Integração e API:

9.7.2.1. Integração por API RESTful e/ou SDK, com respostas em formato JSON e documentação acessível.

9.7.2.2. Suporte a webhooks e integração com plataformas de SIEM, SOAR, e Threat Intelligence Platform (TIP).

9.7.2.3. Controle granular de acesso por usuário, times e perfis de operação.

9.7.2.4. Integração com MISP (Malware Information Sharing Platform), com importação/exportação de IOCs.

9.7.3. Armazenamento e Logs:

9.7.3.1. Retenção ilimitada de eventos OSINT, mesmo após exclusão da fonte original.

9.7.3.2. Armazenamento mínimo de 5 bilhões de eventos e 25 milhões de entidades maliciosas (atores, domínios, IPs, etc.).

9.7.3.3. Logs de acesso detalhados (usuário, atividade, IP, data/hora, user-agent), armazenados por no mínimo 1 ano.

9.7.4. Processamento, Enriquecimento e Inteligência Artificial:

9.7.4.1. Capacidade de enriquecimento automático de dados coletados com IA/ML.

9.7.4.2. Detecção com IA de cartões de crédito expostos, credenciais vazadas, perfis falsos de executivos, menções a VIPs.

9.7.4.3. Correlação automática entre dados coletados (rede social, domínio, e-mail, telefone, endereço IP).

9.7.4.4. Apoio a técnicas de fingerprinting e clusterização de entidades maliciosas.

9.7.4.5. Identificação de links de phishing, typosquatting e infraestruturas de comando e controle (C2).

9.7.5. Metadados dos Eventos:

9.7.5.1. Cada evento OSINT deverá conter:

9.7.5.1.1. Data da coleta e data de indexação

9.7.5.1.2. Hash do conteúdo (SHA-256)

9.7.5.1.3. Fonte original (URL, domínio, plataforma)

9.7.5.1.4. Nome do robô/coletor

9.7.5.1.5. Classificação por tipo e severidade

9.7.6. Mecanismos de Busca e Visualização OSINT

9.7.6.1. Busca avançada por data, metadados, fontes, palavras-chave, atores, campanhas, hashtags e IOC.

9.7.6.2. Suporte a filtros avançados: proximidade, fuzzy search, lógica binária, regex, operadores lógicos, wildcard.

9.7.6.3. Capacidade de drill-down exploratório com filtros dinâmicos (inclusão/exclusão).

9.7.6.4. Identificação automática de campanhas de phishing, perfis falsos, vulnerabilidades exploradas (zeroday), defacements, malspam, scam e fraude.

9.7.6.5. Monitoramento e análise de domínios, certificados SSL, URLs, arquivos suspeitos e infraestrutura relacionada.

- 9.7.7. Dashboards e Visualização Analítica
 - 9.7.7.1. Painéis interativos com gráficos de tendências, volume de ameaças, fontes monitoradas e perfis observados.
 - 9.7.7.2. Busca de perfis e entidades por nome, apelido, e-mail, telefone, CPF/CNPJ, usernames e handles.
 - 9.7.7.3. Visualização de pesquisas salvas com filtros organizacionais e exportação em diversos formatos (XLSX, JSON, CSV, DOCX, PDF).
- 9.7.8. Gerenciamento de Ocorrências e Casos de Investigação:
 - 9.7.8.1. Associação de eventos OSINT a ocorrências específicas ou incidentes internos.
 - 9.7.8.2. Campos com suporte a imagens embutidas, anexos, histórico de alterações e adição de comentários colaborativos.
 - 9.7.8.3. Notificações configuráveis por e-mail e WebHook com base em palavras-chave, nível de risco e origem.
 - 9.7.8.4. Ferramentas de triagem por criticidade, categoria, período, responsável e organização.
 - 9.7.8.5. Inclusão de IOCs, marcadores e histórico de modificações em cada ocorrência.
- 9.7.9. Relatórios de Inteligência:
 - 9.7.9.1. Mínimo de relatórios desenvolvidos por analistas humanos e IA, com foco em, sob demanda:
 - 9.7.9.1.1. Ameaças emergentes
 - 9.7.9.1.2. Infraestruturas maliciosas
 - 9.7.9.1.3. Hacktivismo, geopoliticamente motivado
 - 9.7.9.1.4. Deep e Dark Web
 - 9.7.9.1.5. Detecção de novos TTPs e ferramentas ofensivas
 - 9.7.9.2. Base histórica de 3.000 relatórios com pesquisa por palavras-chave, categoria, autor e data.
 - 9.7.9.3. Relatórios exportáveis em PDF criptografado para casos confidenciais.
- 9.7.10. Fontes Monitoradas e Coleta OSINT:
 - 9.7.10.1. Coleta automatizada de:
 - 9.7.10.1.1. Mídias sociais (Facebook, Twitter, LinkedIn, Instagram, TikTok, Reddit)
 - 9.7.10.1.2. Deep Web (fóruns, pastebins, marketplaces)
 - 9.7.10.1.3. Dark Web (Tor, I2P, ZeroNet)
 - 9.7.10.1.4. Blogs, sites de notícias, grupos públicos de Telegram e Discord
 - 9.7.10.2. Suporte a crawlers personalizados, scraping de páginas públicas, monitoramento de canais fechados com autorização.
 - 9.7.10.3. Web beacon para rastreamento de acessos a sites da CONTRATANTE.
 - 9.7.10.4. Scripts para detecção de clonagem de sites, redirecionamentos maliciosos e alterações de DNS.
- 9.7.11. Solicitação e Gestão de Takedowns
 - 9.7.11.1. Serviço integrado de takedown, com opção para remoção automatizada de conteúdos maliciosos.
 - 9.7.11.2. Mínimo de 10 remoções/mês durante a vigência contratual.
 - 9.7.11.3. Tela dedicada para solicitação de takedowns com os campos:
 - 9.7.11.3.1. URL
 - 9.7.11.3.2. Empresa
 - 9.7.11.3.3. Prioridade
 - 9.7.11.3.4. Categoria
 - 9.7.11.4. Possibilidade de feedback para cada ocorrência encerrada.
 - 9.7.11.5. Painel com visualização por data, prioridade, status e número de ocorrências.
 - 9.7.11.6. Filtros por empresa, período, categoria, responsável e status.
- 9.7.12. Takedown Automatizado e Dashboard
 - 9.7.12.1. Recurso de takedown automatizado para perfis e páginas em:
 - 9.7.12.1.1. Instagram, Facebook, TikTok
 - 9.7.12.1.2. Hospedagens como Hostgator, GoDaddy
 - 9.7.12.1.3. Compartilhadores de arquivos (ex: Scribd, MediaFire).
 - 9.7.12.2. Dashboard com:
 - 9.7.12.2.1. Volume de takedowns solicitados
 - 9.7.12.2.2. Status atual por categoria
 - 9.7.12.2.3. Tempo médio de resposta
 - 9.7.12.2.4. Lista com filtros avançados por empresa, período e responsável.
- 9.8. Ferramentas para o NOC (Network Operations Center) e SO (Setor Operacional)**
 - 9.8.1. O NOC e SO deverá dispor de soluções de observabilidade de rede e sistemas, análise de fluxo, análise de pacotes e correlacionadores de performance com alertas baseados em políticas e IA.
 - 9.8.2. As soluções adotadas devem proporcionar visibilidade detalhada do tráfego de rede, permitir a análise avançada de pacotes e facilitar a identificação de problemas de desempenho e segurança.
 - 9.8.3. A CONTRATADA poderá utilizar outras ferramentas adicionais, conforme necessário, desde que respeitem as diretrizes acordadas com a contratante e sejam compatíveis com os serviços prestados.
 - 9.8.4. Para garantir um nível mínimo de capacidade operacional e eficiência na ações de rede, o NOC e SO deve contar com as seguintes ferramentas modulares:
 - 9.8.4.1. Módulo de observabilidade de rede e sistemas - APM (Application Performance Monitoring) e NPM (Network Performance Monitoring);
 - 9.8.4.2. Módulo de visibilidade de tráfego - NPB (Network Packet Broker) agregação e distribuição de tráfego;
 - 9.8.4.3. Módulo de gerenciamento e monitoramento – ITSM (Cherwell) e Zabbix/ Grafana.
 - 9.8.4.4. Módulo de observabilidade de rede e sistemas - APM (Application Performance Monitoring) e NPM (Network Performance Monitoring)
- 9.8.5. Monitoramento por APM (Application Performance Monitoring)**
 - 9.8.5.1. A CONTRATADA deverá disponibilizar, configurar e customizar uma solução de Observabilidade baseada em padrões como OpenTelemetry, Prometheus e Grafana, capaz de coletar logs, métricas e traces distribuídos. A solução deverá contemplar integração com ambientes críticos de segurança pública e permitir a geração de alertas correlacionados por AI/ML para antecipação de falhas e incidentes. O sistema deverá possibilitar o monitoramento

contínuo do tempo de resposta de chamadas de API, uso de recursos por diferentes componentes de aplicações e detecção de anomalias, garantindo eficiência operacional e alta disponibilidade dos sistemas da CONTRATANTE.

9.8.5.2. O monitoramento contínuo da infraestrutura e das aplicações da CONTRATANTE deverá contar com ferramentas especializadas para identificar gargalos de desempenho, falhas, impactos na experiência do usuário e incidentes de segurança.

9.8.5.3. A solução adotada deverá garantir visibilidade completa do ciclo de vida das aplicações e serviços, permitindo análise detalhada dos tempos de resposta, consumo de recursos, comportamento transacional e correlação de eventos em tempo real.

9.8.5.4. O monitoramento deverá abranger todas as aplicações críticas da CONTRATANTE, incluindo aquelas hospedadas no Datacenter, bem como serviços distribuídos em ambientes híbridos ou na nuvem.

9.8.5.5. A solução deverá oferecer recursos avançados para detecção de anomalias, diagnóstico proativo e resposta automatizada a incidentes de TI, garantindo resiliência operacional.

9.8.5.6. A CONTRATADA poderá adotar outras ferramentas adicionais, conforme necessário, desde que respeitem as diretrizes da contratante e que sejam compatíveis com os serviços prestados.

9.8.5.7. A CONTRATADA será responsável pela hospedagem, operação e gerenciamento da solução de monitoramento e observabilidade, garantindo que os serviços sejam prestados de forma contínua e segura, com alta disponibilidade e redundância. A CONTRATANTE deverá ter acesso remoto, contínuo e seguro às informações estratégicas, dashboards, relatórios e alertas, sem a necessidade de operação direta do sistema. A CONTRATADA deverá garantir a exportação e consulta dos dados históricos, conforme prazos e formatos definidos pela CONTRATANTE, incluindo a possibilidade de solicitações eventuais de extração de dados pela CONTRATANTE para auditoria ou análise detalhada.

9.8.5.8. Requisitos Gerais da Solução

9.8.5.9. A solução deverá ser disponibilizada e operada pela CONTRATADA, garantindo conformidade com normas de proteção de dados, incluindo a Lei Geral de Proteção de Dados (LGPD) e regulamentações internacionais compatíveis.

9.8.5.10. A CONTRATADA deverá assegurar que a CONTRATANTE tenha acesso seguro e contínuo aos dashboards, relatórios e métricas necessárias para acompanhamento dos serviços, incluindo dados históricos e exportáveis.

9.8.5.11. A CONTRATADA deverá fornecer mecanismos para contingência e continuidade operacional, incluindo arquitetura ativa-ativa ou ativa-passiva com failover automático, RTO inferior a 15 minutos e RPO de no máximo 5 minutos, replicação geográfica de dados críticos, e testes mensais de resiliência com relatórios auditáveis.

9.8.5.12. A ferramenta deverá fornecer integração ampla com soluções de terceiros por meio de APIs abertas e suporte a padrões de mercado, como REST, Webhooks e OpenTelemetry.

9.8.5.13. A solução deverá ser compatível com ambientes híbridos e multicloud, permitindo o monitoramento de aplicações distribuídas e infraestrutura localizada no Datacenter da CONTRATANTE.

9.8.5.14. A plataforma deverá utilizar inteligência artificial e aprendizado de máquina para detecção de anomalias, com capacidade de construir perfis comportamentais baseados em séries temporais, identificar padrões de degradação e recomendar ações proativas com base em modelos supervisionados e não supervisionados.

9.8.5.15. A ferramenta deverá oferecer suporte a análise preditiva de falhas utilizando modelos supervisionados e não supervisionados, com detecção de comportamento anômalo, previsão de picos de uso e sugestão de remediações preventivas baseadas em incidentes históricos.

9.8.5.16. A solução deverá permitir a criação de métricas de negócio personalizáveis, incluindo volume de transações e tempo médio de processamento, garantindo flexibilidade para monitoramento de desempenho operacional.

9.8.5.17. Requisitos Técnicos e Funcionalidades Mínimas

9.8.5.17.1. A plataforma deverá integrar logs, métricas e rastreamentos (traces) de forma nativa, seguindo a especificação do Three Pillars of Observability, e permitir correlação contextual em tempo real. Deverá suportar ingestão via agentes leves e coleta via API para ambientes híbridos, com disponibilidade mínima de 99,9%, replicação de dados e escalabilidade horizontal, permitindo correlação automática entre eventos de diferentes fontes.

9.8.5.17.2. A solução deverá prover visibilidade detalhada do uso de CPU, consumo de memória, rede e armazenamento, com série temporal de métricas, coleta via agentes leves e exportação em dashboards de análise comparativa por componente, host e serviço, além de permitir criação de alertas threshold e análise preditiva de capacidade, permitindo diagnóstico preciso de degradação de performance.

9.8.5.17.3. O sistema deve permitir a criação de alertas automatizados com base em limiares configuráveis, anomalias detectadas e tendências históricas.

9.8.5.17.4. A ferramenta deverá fornecer dashboards interativos e personalizáveis, permitindo filtragem de dados e visualizações detalhadas em tempo real.

9.8.5.17.5. A solução deverá fornecer suporte ao monitoramento de banco de dados, incluindo tempo de resposta de queries, taxa de acertos em cache, consumo de CPU por sessão e detecção de anomalias em acessos concorrentes.

9.8.5.17.6. A solução deverá permitir a análise detalhada do desempenho de aplicações, garantindo visibilidade fim a fim por meio da coleta, processamento e correlação de eventos.

9.8.5.17.7. A ferramenta deverá fornecer integração com soluções de ITSM, facilitando a abertura e acompanhamento de incidentes.

9.8.5.17.8. A solução deverá suportar armazenamento de logs e métricas históricos para análise forense e auditorias de segurança.

9.8.5.17.9. A solução deverá incluir mecanismos para detecção proativa de falhas de segurança em aplicações monitoradas, integrando-se com bases públicas de vulnerabilidades e permitindo alertas automatizados para atividades suspeitas.

9.8.5.18. Requisitos de Implantação e Suporte

9.8.5.19. A solução deverá garantir conformidade com a Lei Geral de Proteção de Dados (LGPD), assegurando a privacidade e integridade das informações monitoradas.

9.8.5.20. A solução deverá permitir integração segura com sistemas externos, utilizando protocolos de comunicação criptografados.

9.8.5.21. A CONTRATADA deverá garantir a alta disponibilidade da solução, assegurando que incidentes internos da sua infraestrutura não impactem a continuidade do monitoramento da CONTRATANTE. Deverão ser implementados mecanismos de redundância e contingência para evitar interrupções nos serviços prestados. Caso ocorra falha de comunicação entre os agentes e a plataforma da CONTRATADA, os dados coletados localmente deverão ser armazenados e sincronizados assim que a conectividade for restabelecida, garantindo integridade e continuidade do monitoramento. Em casos de falhas prolongadas na infraestrutura da CONTRATADA, a mesma deverá disponibilizar à CONTRATANTE um plano de contingência que permita acesso emergencial aos dados críticos e relatórios previamente coletados.

9.8.5.22. A CONTRATADA deverá fornecer documentação técnica sobre a operação e utilização da plataforma, incluindo a definição dos fluxos de

monitoramento e análise.

9.8.5.23. A CONTRATADA deverá fornecer capacitação para usuários da CONTRATANTE, abordando a navegação em dashboards, geração de relatórios e interpretação de métricas relevantes ao acompanhamento dos serviços prestados.

9.8.5.24. A CONTRATANTE poderá solicitar capacitação adicional para novos usuários ou atualizações da ferramenta, sempre que forem implementados novos recursos ou alterações significativas na plataforma.

9.8.5.25. A CONTRATADA deverá fornecer documentação técnica e de usuário, contendo instruções detalhadas sobre a utilização dos recursos disponíveis para a CONTRATANTE.

9.8.5.26. O suporte da ferramenta deverá ser prestado na modalidade 8x5 NBD (Next Business Day), garantindo tempo de resposta de até 4 horas para incidentes críticos.

9.8.5.27. A contratada deverá realizar a implementação e tuning do monitoramento para os seguintes sistemas críticos da CONTRATANTE: COPOM Online; SIOPM Web; SIOPM Corp/V; Citrix App and Desktop Virtualization; Microsoft SQL Server.

9.8.5.28. Além desses sistemas, a CONTRATANTE poderá solicitar a inclusão de outras aplicações e infraestruturas críticas, devendo a solução ofertada ser capaz de monitorar qualquer ativo demandado, independentemente do fabricante e da arquitetura.

9.8.5.29. Ao final da implementação a CONTRATADA deverá entregar um documento técnico detalhado (LLD - Low-Level Design), contendo: Topologia dos sistemas monitorados, Relação dos componentes monitorados, incluindo endereços IP e hostnames, Passo a passo de cada configuração realizada e Capturas de tela e logs de configuração e dashboards principais.

9.8.5.30. O LLD deverá ser entregue de forma faseada, acompanhando a implementação da solução, garantindo visibilidade à CONTRATANTE sobre as configurações realizadas ao longo do projeto.

9.8.5.31. A Plataforma de Observabilidade deverá permitir a correlação automatizada de eventos em aplicações, infraestrutura e serviços, fornecendo uma visão fim a fim do ambiente monitorado.

9.8.5.32. A solução deverá integrar logs, métricas e rastreamentos (traces) de forma nativa, permitindo análise unificada e identificação de falhas em tempo real.

9.8.5.33. A A ferramenta deverá suportar descoberta automática e remota de componentes de TI, incluindo servidores, bancos de dados, aplicações, APIs e microsserviços, gerando um mapa dinâmico das dependências. A solução deverá ser compatível com arquiteturas distribuídas, garantindo que componentes monitorados na infraestrutura da CONTRATANTE sejam corretamente identificados e correlacionados dentro da plataforma da CONTRATADA.

9.8.5.34. A solução deverá incluir análise preditiva baseada em inteligência artificial e aprendizado de máquina para identificar padrões, prever falhas e recomendar ações corretivas.

9.8.5.35. O sistema deverá ser compatível com ambientes on-premises, híbridos e multicloud, permitindo o monitoramento centralizado de infraestruturas distribuídas.

9.8.5.36. A plataforma deverá incluir detecção automática de anomalias e alertas inteligentes, ajustando-se dinamicamente ao comportamento esperado dos sistemas.

9.8.5.37. O sistema deverá fornecer dashboards interativos e personalizáveis, com suporte à criação de painéis customizados para diferentes equipes e necessidades.

9.8.5.38. A solução deverá oferecer integração com ferramentas de ITSM e SIEM, facilitando a resposta a incidentes e a rastreabilidade de eventos críticos.

9.8.5.39. A plataforma deverá possuir APIs abertas e documentadas, permitindo integração com sistemas existentes da CONTRATANTE e soluções de terceiros.

9.8.5.40. A ferramenta deverá fornecer suporte a consulta histórica de dados, permitindo auditoria e análise forense de eventos passados.

9.8.5.41. A plataforma deverá contar com mecanismos de alta disponibilidade e escalabilidade, garantindo desempenho adequado para grandes volumes de dados e comunicação eficiente com ambientes distribuídos e remotos. A infraestrutura da CONTRATADA deverá ser dimensionada para suportar picos de demanda, garantindo que o monitoramento da CONTRATANTE ocorra sem degradação de desempenho ou perda de eventos críticos. A solução deverá assegurar baixa latência na comunicação entre os agentes de monitoramento da CONTRATANTE e a plataforma hospedada na infraestrutura da CONTRATADA, garantindo a entrega de eventos em tempo real para serviços críticos.

9.8.5.42. A Plataforma deverá ser capaz de monitorar qualquer aplicação ou infraestrutura crítica que venha a ser adicionada no ambiente da CONTRATANTE, garantindo escalabilidade e compatibilidade com múltiplos fabricantes.

9.8.5.43. O APM deverá fornecer monitoramento contínuo do desempenho das aplicações, identificando gargalos e falhas em tempo real.

9.8.5.44. A ferramenta deverá medir e analisar tempo de resposta de chamadas de API, execução de queries em banco de dados, consumo de CPU /memória e latência de serviços.

9.8.5.45. O sistema deverá ser capaz de mapear automaticamente dependências entre aplicações, serviços e infraestrutura, fornecendo visão fim a fim do ambiente, incluindo a comunicação entre os agentes remotos e a plataforma da CONTRATADA.

9.8.5.46. A solução deverá incluir rastreamento distribuído de transações, permitindo identificar onde ocorre degradação de desempenho em arquiteturas baseadas em microsserviços.

9.8.5.47. A ferramenta deverá oferecer baselines dinâmicos, ajustando automaticamente os limiares de alerta com base no comportamento normal da aplicação.

9.8.5.48. O sistema deverá permitir análise detalhada de código, identificando métodos e consultas SQL com maior impacto no tempo de resposta.

9.8.5.49. A solução deverá gerar alertas proativos, notificando automaticamente equipes responsáveis quando ocorrerem degradações de desempenho.

9.8.5.50. A ferramenta deverá suportar testes sintéticos, permitindo simular interações de usuários para detectar falhas antes que impactem o ambiente produtivo.

9.8.5.51. O APM deverá ser compatível com diversas tecnologias e linguagens de desenvolvimento, incluindo Java, .NET, Python, Node.js, PHP, entre outras.

9.8.5.52. A Solução deverá ser integrada à Plataforma de Observabilidade, permitindo correlação de eventos e análise conjunta de métricas, logs e traces.

9.8.5.53. A solução deve ser capaz de monitorar a experiência de usuários finais da aplicação, através de um código JavaScript injetado no front-end da aplicação de maneira automática. A coleta de dados não deve requerer alteração de arquivos da aplicação ou alteração de código da aplicação. Novas configurações na UI devem ser propagadas automaticamente para o agente, sem requerer alterações ao código JavaScript. Não deve requerer alterações

no ambiente/navegador do usuário final e também não serão permitidas alterações nos servidores HTTP assim como inserções manuais de URL via interface.

9.8.5.54. Deverá permitir a configuração de capturas de informações a partir de pelo menos Meta Tag, componentes CSS e JavaScript Variables, na página executada no navegador do usuário. O objetivo identificar o usuário logado ou enriquecer as transações de negócio. Não será permitido a alteração de código para captura de informações

9.8.5.55. A solução deverá permitir a consulta (queries) de informações capturadas no monitoramento da experiência do usuário, podendo ser visualizadas em dashboards e utilizá-las como métricas de negócio.

9.8.5.56. "Deverá realizar a monitoração fim-a-fim das aplicações hospedadas no DataCenter, registrando e avaliando, no mínimo:

9.8.5.56.1. A requisição feita pelo usuário no navegador (click e carregamento de páginas ou ação do usuário na aplicação, gerando tráfego no servidor).

9.8.5.56.2. A execução do código nos servidores de aplicação.

9.8.5.56.3. As consultas aos servidores de banco de dados.

9.8.5.56.4. O retorno do resultado ao navegador do usuário.

9.8.5.56.5. Tempo de execução total da sessão/visita;

9.8.5.56.6. Tempo gasto em rede;

9.8.5.56.7. Tempo de servidor (execução transacional da aplicação)

9.8.5.56.8. Tempo de download do HTML e outros recursos da página;

9.8.5.56.9. Tempo de renderização do browser (DOM Build);

9.8.5.56.10. Tempo de pós-load;

9.8.5.56.11. Identificar webservices e chamadas a serviços externos das transações de uma aplicação."

9.8.5.57. O módulo de experiência de usuário deve permitir, nativamente, a configuração de capturas de dados na página executada no navegador do usuário de forma anonimizada, com objetivo de reproduzir a sessão do usuário a partir da captura de eventos do navegador que permitam a visualização em formato de vídeo do ponto de vista do usuário a navegação realizada. Estas visualizações devem estar disponíveis para reprodução por, no mínimo, 30 dias após a sua realização;

9.8.5.58. A solução de reprodução de sessão do usuário deve vir com mascaramento de informações sensíveis do usuário por padrão e também permitir a configuração customizada deste mecanismo de privacidade de dados., permitindo, a nível de permissões de perfis de analistas, visualizar ou não as informações sensíveis.

9.8.6. Dimensionamento do volume:

	1 VM Linux	4 vCPU 8Gb memória
	1 VM Linux	5 vCPU 8Gb memória
	1 VM Windows	2 vCPU 2Gb memória
	6 VM Windows	6 vCPU 8Gb memória
	2 VM Windows	5 vCPU 20Gb memória
	25 VM Windows	6 vCPU 20Gb memória
	1 VM Windows	2 VCPU 2Gb memória
	3 VM Windows	4 VCPU 4Gb memória

Módulo de observabilidade de sistemas (APM)	1 VM Windows	8 VCPU 4Gb memória
	4 VM Windows	16 VCPU 5Gb memória
	3 VM Windows	4 VCPU 8Gb memória
	6 VM Windows	8 VCPU 8Gb memória
	2 VM Windows	4 VCPU 16Gb memória
	1 VM Windows	10 VCPU 16Gg memória
	5 VM Windows	12 VCPU 16Gb memória
	1 VM Windows	16 VCPU 16Gb memória
	2 VM Windows	6 VCPU 32Gb memória
	6 VM Windows	32 VCPU 32Gb memória
	4 VM Windows	16 VCPU 78Gb memória
	4 SQL BD	80 VCPU 4Tb memória

9.9. Módulo de Network Performance Monitoring - NPM

9.9.1. A solução deve ser composta por equipamentos físicos e virtuais independentes de um único fabricante.

9.9.2. É importante destacar que o licenciamento dos NPM poderá chegar a a 100 (cem) unidades, conforme a necessidade e a estratégia de

implantação. O custo do software será apurado mensalmente, de modo a permitir o correto dimensionamento dos pagamentos.

9.9.3. Os equipamentos ofertados devem possuir memória e capacidade de processamento suficientes para garantir o atendimento a todos os requisitos desta especificação, mesmo sob uso máximo.

9.9.4. A solução deve suportar alta disponibilidade, adotando mecanismos de clusterização ou similares, ou permitir balanceamento de tráfego por meio de solução Network Packet Broker.

9.9.5. Não será aceita administração por meio de aplicação cliente ou solução executada em JVM (Java Virtual Machine).

9.9.6. Todos os equipamentos fornecidos devem ser novos, sem uso anterior, e compatíveis com a linha de produção atual do fabricante na data de entrega.

9.9.7. Os equipamentos devem implementar mecanismos nativos de monitoramento e detecção de falhas internas.

9.9.8. Todos os ativos gerenciáveis devem possuir pelo menos uma interface dedicada 1GbE RJ45 para gerenciamento.

9.9.9. Os discos rígidos devem suportar tecnologia hot swappable e RAID para proteção contra perda de dados.

9.9.10. A administração remota deve ser realizada por meio de interface gráfica (GUI) via canal seguro.

9.9.11. Deve haver suporte à interface de gerenciamento Web (HTTPS) e CLI.

9.9.12. Devem ser implementados os protocolos de gerenciamento SNMPv2c, SNMPv3, incluindo geração de traps.

9.9.13. Deve ser implementado o protocolo NTP (Network Time Protocol).

9.9.14. Deve permitir acesso via SSHv2, com proteção por senha.

9.9.15. Deve permitir autenticação com base em servidores RADIUS ou LDAP.

9.9.16. Deve permitir envio de logs para servidores externos (syslog).

9.9.17. Deve permitir auditoria de alterações de configuração por meio de logs.

9.9.18. Deve permitir atualização remota do sistema operacional e arquivos de configuração via interface de gerenciamento.

9.9.19. Deve implementar controle de acesso baseado em funções (RBAC) com perfis de acesso configuráveis.

9.9.20. A solução deve coletar dados em tempo real da solução Network Packet Broker, sem impactar o desempenho da rede ou das aplicações.

9.9.21. A solução deve fornecer métricas de desempenho na camada de rede, incluindo: Taxa de Bits, Largura de Banda, Conexões Simultâneas, Atraso de Rede, Atraso no Servidor, Tempo de Transmissão de Dados, Perda de Pacotes, Retransmissão, Janela TCP Zero, Desconexão Anormal TCP, etc.

9.9.22. Deve haver suporte à personalização de aplicações agrupadas por portas TCP/UDP, URLs, endereços IPv4/IPv6 e marcações DSCP.

9.9.23. Deve ser capaz de identificar e eliminar instâncias duplicadas de pacotes durante a coleta.

9.9.24. Deve permitir gravação e exportação de arquivos capturados em formato .pcap.

9.9.25. Deve fornecer visualizações personalizadas por login de usuário.

9.9.26. Deve permitir renomear aplicações inspecionadas com base no número da porta TCP/UDP e/ou endereço IP.

9.9.27. Deve fornecer análise de comportamento de rede com alertas de baseline para anomalias nas métricas selecionadas.

9.9.28. Deve suportar integração de alertas via SNMP Trap, SNMP GET, API ou outros meios de integração.

9.9.29. Deve montar um mapeamento dinâmico da rede com base nos pacotes capturados da rede.

9.9.30. Este mapeamento deve ter como referência os endereços IP dos servidores e apresentar as condições dos segmentos de rede, das aplicações e a causa raiz de falhas, permitindo uma análise aprofundada da comunicação.

9.9.31. Deve emitir alertas para desvios de desempenho da rede e aplicações, bem como variações sazonais, com base em análise detalhada de cada aplicação existente.

9.9.32. Deve permitir inventariar sub-redes e VLANs, visualizando cada uma como localidade distinta.

9.9.33. Todas as licenças de software necessárias devem ser fornecidas para cumprimento integral desta especificação, incluindo atualizações durante o período contratual.

9.9.34. Deve permitir acesso simultâneo de múltiplos usuários à interface gráfica (GUI) da solução, por navegadores populares ou aplicação proprietária.

9.9.35. Todas as funcionalidades de gráficos, relatórios, buscas e gerenciamento devem estar acessíveis em formato de página web.

9.9.36. Deve permitir integração com outras plataformas por meio de APIs para consultas automatizadas.

9.9.37. A solução deve suportar, no mínimo, os seguintes tipos de contas de usuário:

9.9.37.1. Administrador: configuração de hardware, criação de contas de usuário, monitoramento de dispositivos, backup, acesso completo às funcionalidades, gerenciamento de contas, etc.

9.9.37.2. Operador: gerenciamento de grupos, alertas, relatórios de tráfego/eventos e configuração de detecção de eventos.

9.9.37.3. Monitor: consultas a relatórios e acompanhamento do status de eventos.

9.9.38. Probe de Captura de Dados de Rede:

9.9.38.1. A solução ofertada deve ser estruturada em hardware próprio e dedicado, visando garantir a disponibilidade e o desempenho do serviço.

9.9.38.2. Deve ser completamente passiva na rede existente, garantindo que qualquer interrupção na solução não leve à indisponibilidade dos serviços.

9.9.38.3. Toda nova aplicação configurada na rede deve ser capaz de ser capturada e inspecionada sem a necessidade de desenvolvimento da ferramenta.

9.9.38.4. Os pacotes capturados devem ser armazenados por um determinado período de tempo, conforme solicitado no Período de Retenção, e deve ser permitido extrair esses pacotes, no mínimo, nos formatos PCAP.

9.9.38.5. Os ativos utilizados para captura de pacotes devem possuir alta velocidade de processamento e placas de captura de ultra-baixa latência com, no mínimo, 2 interfaces 40/100 Gbps QSFP/QSFP28.

9.9.38.6. Para atender ao período de retenção com armazenamento de dados brutos e metadados, a solução deve possuir, no mínimo, 240 TB de armazenamento sem expansão, operando em RAID 5 ou superior, que forneça desempenho e proteção contra perda de dados.

9.9.38.7. Deve suportar o armazenamento de dados brutos da rede por, no mínimo, 3 dias.

9.9.38.8. A solução de captura de pacotes deve armazenar e ser capaz de sobrescrever/excluir automaticamente dados antigos.

9.9.38.9. Deve ser capaz de capturar dados brutos automaticamente, de forma contínua, 24 horas por dia, 7 dias por semana, sobrescrevendo dados antigos quando atingir 100% de utilização do disco.

9.9.38.10. Os pacotes brutos da rede capturados podem ser armazenados em tempo real em formato comprimido, reduzindo a utilização do espaço em disco.

- 9.9.38.11. Deve possuir, no mínimo, 256 GB de RAM.
- 9.9.38.12. A solução deve coletar pacotes em fluxo constante com, no mínimo, 40 Gbps de throughput em um único appliance.
- 9.9.38.13. A solução deve possuir capacidade de gravação em disco de, no mínimo, 40 Gbps, de forma constante e sem perdas e/ou interrupções.
- 9.9.38.14. A solução pode identificar inteligentemente o comprimento do cabeçalho de diferentes tipos de pacotes (como VLAN, VXLAN, VXLAN over VXLAN) e remover com precisão as informações de carga útil, garantindo a segurança dos dados sem perder informações da camada de rede.
- 9.9.38.15. Deve operar de forma independente da console central fornecida, no que diz respeito à captura de pacotes de rede.
- 9.9.38.16. Capacidade de apresentar análises graficamente.
- 9.9.38.17. Deve então enviar esses dados e métricas para a console central fornecida, para compilar estatísticas e gerar relatórios.
- 9.9.38.18. Deve capturar pacotes em múltiplas interfaces de rede em modo ininterrupto, com a opção de gravação em disco rígido por meio de capture jobs ou filtros.
- 9.9.38.19. Deve ser capaz de armazenar os pacotes de forma indexada, permitindo examiná-los no próprio dispositivo, sem necessidade de transferência para analisador externo.
- 9.9.38.20. Deve permitir a implementação da função de agregação de suas diversas interfaces de rede ou link aggregation.
- 9.9.38.21. Deve permitir a criação de arquivos de captura para porções definidas dos capture jobs ou filtros. Esses arquivos devem ser definidos por horário de início e término. Além disso, deve permitir que esses arquivos sejam exportados para estudo através de analisadores de protocolo no formato de dados "pcap".
- 9.9.38.22. Deve permitir a nomeação de portas e protocolos nos casos em que o dispositivo não os classifique automaticamente.
- 9.9.38.23. Deve permitir o agrupamento de portas em grupos lógicos, a fim de criar categorias e enriquecer relatórios.
- 9.9.38.24. A solução ofertada pode ser baseada em appliance dedicado (hardware) ou por software via virtual appliance. Caso seja ofertada por software, o proponente deve fornecer o hardware (servidor), bem como o sistema operacional e as licenças necessárias para executar a máquina virtual.
- 9.9.38.25. Os servidores utilizados para captura de fluxo devem possuir, no mínimo, 1 interface de gerenciamento Gigabit Ethernet e armazenamento interno com arranjo RAID 5 ou superior, que garanta proteção contra perda de dados, com área compatível com o volume de dados desta solução.
- 9.9.38.26. Deve ser fornecida uma licença que permita o processamento, no mínimo, da taxa de 200.000 (duzentos mil) registros de fluxo por minuto.
- 9.9.38.27. Deve suportar o recebimento de informações via fluxos de, no mínimo, 2.000 fontes.
- 9.9.38.28. A solução ofertada deve permitir a coleta de dados por NetFlow v5, v9 e IPFIX.
- 9.9.38.29. A solução ofertada deve apresentar os fluxos. Parâmetros mínimos a serem exibidos:
 - 9.9.38.29.1. IP de origem e destino;
 - 9.9.38.29.2. Porta e aplicações de rede utilizadas;
 - 9.9.38.29.3. Número de pacotes e total de bytes.

9.9.39. Plataforma de Gerenciamento de Análise de Desempenho de Rede

- 9.9.39.1. A solução oferecida pode ser baseada em appliance dedicado (hardware) ou por software por meio de máquina virtual (virtual appliance). Caso seja oferecida por software, o proponente deve fornecer o hardware, bem como o sistema operacional e as licenças necessárias para execução da máquina virtual.
- 9.9.39.2. A solução de análise de pacotes deve ser integrada à solução de visualização e também permitir operação autônoma.
- 9.9.39.3. A solução deve ser capaz de analisar os dados capturados pelo dispositivo de captura de pacotes sem a necessidade de transferir os pacotes capturados.
- 9.9.39.4. A solução deve ser capaz de exibir dados em intervalos mínimos de 1 segundo, com atraso de exibição de 1 segundo para métricas TCP/IP.
- 9.9.39.5. Deve ser possível configurar diversos parâmetros de rede (como interfaces de captura), usuários e protocolos, bem como tarefas de captura no dispositivo de captura fornecido.
- 9.9.39.6. Para tráfego de aplicação desconhecida, a solução deve suportar análise estatística de portas TOP, número de sessões, e suportar a visualização do host das portas ou reuniões selecionadas, pares de fluxo, e o número da porta usado por cada par de fluxo.
- 9.9.39.7. Deve possuir a capacidade de configurar gatilhos (thresholds) e alertas flexíveis para detectar comportamentos anômalos.
- 9.9.39.8. Deve permitir que “gatilhos” sejam configurados para alertar valores mínimos ou máximos. Esse evento deve gerar uma notificação para a equipe responsável via e-mail, SNMP trap ou syslog.
- 9.9.39.9. Disponibilizar a função de baseline, que possa calcular a linha de base para as métricas de desempenho. O baseline deve suportar o algoritmo de média, o algoritmo de pico etc., e deve suportar baseline de dados diários e semanais.
- 9.9.39.10. Suportar alerta por baseline, gerando alerta quando os dados atuais se desviarem de uma porcentagem da linha de base.
- 9.9.39.11. Simulação de alerta: simulação de alerta em tempo real e cálculo de teste do limiar de alerta configurado, combinado com dados históricos para verificar a efetividade da configuração do alerta.
- 9.9.39.12. Deve permitir a consulta de alertas de todos os tipos enviados pela ferramenta de monitoramento, em um determinado período (data/hora de início e fim) informado pelo usuário.
- 9.9.39.13. A solução oferecida deve permitir a criação de painéis personalizados com a definição dos parâmetros que o usuário deseja monitorar.
- 9.9.39.14. Os dashboards devem ser exibidos em intervalos personalizáveis pelo usuário e apresentar dados segmentados com resolução mínima de 1 minuto.
- 9.9.39.15. A solução deve permitir configurações individuais desses painéis.
- 9.9.39.16. Deve ser possível segmentar os dados exibidos nos dashboards por localizações, que podem ser definidas por diferentes sub-redes.
- 9.9.39.17. Em todos os painéis deve ser possível filtrar os dados exibidos por, no mínimo, os seguintes parâmetros: IP, sub-rede, porta TCP, vlan, aplicação e localização.
- 9.9.39.18. Ao criar um dashboard, espera-se que ele seja alimentado não apenas com os dados capturados a partir de sua criação, mas também com os dados já capturados e armazenados na memória da ferramenta.
- 9.9.39.19. A solução oferecida deve ser capaz de exibir métricas avançadas para cada comunicação. Essas métricas devem estar disponíveis em todas as aplicações e transações monitoradas. Parâmetros mínimos a serem exibidos:
 - 9.9.39.19.1. Tamanho do pacote;
 - 9.9.39.19.2. Taxas de transmissão por segundo;
 - 9.9.39.19.3. Total de bytes transmitidos e recebidos;
 - 9.9.39.19.4. Total de pacotes transmitidos e recebidos;

- 9.9.39.19.5. Número de conexões estabelecidas;
- 9.9.39.19.6. Número de conexões com falha;
- 9.9.39.19.7. Atraso de rede ou round trip time;
- 9.9.39.19.8. Retransmissões e pacotes fora de ordem;
- 9.9.39.19.9. Tempo de resposta.
- 9.9.39.20. A solução oferecida deve apresentar painéis personalizados no formato de tabela, gráfico de linha, indicador de status ou um conjunto desses.
- 9.9.39.21. Dashboards personalizados devem exibir valores em formato resumido ou individualizado no intervalo de tempo selecionado.
- 9.9.39.22. Painéis em formato gráfico devem permitir drill-down/zoom sobre o gráfico ao posicionar o ponteiro do mouse, detalhando as informações em cada ponto de medição.
- 9.9.39.23. A solução deve permitir no mínimo 20 (vinte) usuários simultâneos, cada um acessando a ferramenta com logins específicos.
- 9.9.39.24. As estatísticas coletadas por meio de captura de pacotes ou análise de fluxo devem ser acessadas por meio de uma interface gráfica única. Essa interface deve ser capaz de demonstrar métricas de análise de fluxo e de pacotes nos mesmos dashboards.
- 9.9.39.25. A solução deve exibir um relatório que demonstre quais endereços IP têm maior utilização em termos de throughput de rede, conexões abertas ou com falha, com maior tempo de resposta e com maior retransmissão.
- 9.9.39.26. Visualizar relatórios que demonstrem quais portas TCP/UDP ou aplicações geraram tráfego no momento da captura.
- 9.9.39.27. Exibir relatório com visualização das páginas web mais acessadas.
- 9.9.39.28. Exibir relatórios que demonstrem o volume de tráfego de dados por determinada porta TCP/UDP.
- 9.9.39.29. A solução deve gerar relatórios de forma automática e manual.
- 9.9.39.30. A solução deve ser capaz de gerar e encaminhar alarmes via e-mail, SNMP trap, syslog e na própria console.
- 9.9.39.31. Os relatórios devem incluir estatísticas com granularidade de 1 minuto / 5 minutos / 10 minutos / 1 hora.
- 9.9.39.32. A solução deve permitir a geração de relatórios sobre quaisquer métricas coletadas.
- 9.9.39.33. A arquitetura de armazenamento das métricas não deve apresentar limitações. Deve ser capaz de suportar análises aprofundadas a partir de diversas dimensões, tais como Ether Type, Mac, Mac session, VNI, IP, IP session, IP+Port, TCP session, UDP session etc., na mesma página. Qualquer dimensão pode ser usada como ponto de partida da mineração, e a análise pode ser conduzida entre quaisquer dimensões.
- 9.9.39.34. Capacidade de apresentar análise graficamente.
- 9.9.39.35. Deve suportar relatórios sobre todos os dados coletados ou qualquer outro filtro, e não apenas sobre os maiores ativos que geraram ou receberam tráfego de rede, critérios ou mecanismos que possam desconsiderar parte dos dados coletados.
- 9.9.39.36. Deve suportar relatórios em tempo real com dados históricos, sem perda de resolução dos dados por sumarização, amostragem, rolagem de dados de maior para menor resolução ou outras técnicas de redução.
- 9.9.39.37. Deve ser capaz de exportar todos os relatórios, no mínimo, em formato PDF.
- 9.9.39.38. Deve suportar filtragem e detalhamento para qualquer campo-chave em um relatório. Os filtros podem ser aplicados ao relatório analisado, ou podem invocar outro relatório associado ao relatório em análise. O detalhamento deve trazer mais informações de um relatório, para análise posterior até o nível de análise de pacotes de rede, de maneira ágil e simplificada sobre um campo-chave do relatório. Esse detalhamento pode ser exibido por meio de um novo relatório filtrado a partir do campo-chave selecionado.
- 9.9.39.39. Deve permitir o agendamento para geração automática de relatórios, bem como o armazenamento e/ou envio desses relatórios por e-mail.
- 9.9.39.40. Deve possibilitar a construção de relatórios para um período de tempo pré-determinado sobre, no mínimo, os seguintes elementos que geraram ou receberam mais tráfego de rede durante o período:
- 9.9.39.40.1. Hosts;
- 9.9.39.40.2. Pares de hosts;
- 9.9.39.40.3. Pares de hosts com portas TCP ou UDP;
- 9.9.39.40.4. Grupos de hosts;
- 9.9.39.40.5. Grupos de hosts com portas TCP ou UDP;
- 9.9.39.40.6. Aplicações;
- 9.9.39.40.7. Portas TCP ou UDP;
- 9.9.39.40.8. Protocolos;
- 9.9.39.40.9. Interfaces de rede;
- 9.9.39.40.10. Dispositivos de rede.
- 9.9.39.41. Suporte a busca global de tráfego para realizar funções de busca em todos os Probes gerenciados pela Plataforma. Por exemplo, buscar tráfego alvo incluindo pacotes brutos da rede com base em condições como IP de origem/destino, porta de origem/destino e aplicação.

9.10. Módulo de Visibilidade Modular e Inteligente de Tráfego (Network Packet Broker)

- 9.10.1.1. A CONTRATADA será responsável por fornecer, operar, monitorar e garantir a manutenção contínua de uma Plataforma de Visibilidade de Tráfego (Network Packet Broker) dentro do ambiente da PMESP, assegurando a alta disponibilidade da solução e sua integração com as demais ferramentas de segurança e monitoramento da rede. A solução deverá cumprir as exigências técnicas descritas neste documento e ser composta por ferramentas e infraestrutura compatíveis com os requisitos operacionais, podendo incluir appliances dedicados, software especializado, conforme necessidade.
- 9.10.1.2. É importante destacar que o licenciamento do NPB dimensionado para 2 (dois) TAPs e 1 (um) packet broker, conforme a necessidade e a estratégia de implantação. O custo do software será apurado mensalmente, de modo a permitir o correto dimensionamento dos pagamentos
- 9.10.1.3. Características técnicas
- 9.10.1.3.1. A Plataforma de Visibilidade de Tráfego é uma solução composta por hardware e software, voltada para a filtragem, agregação e distribuição de tráfego para ferramentas de análise e segurança, e deverá atender integralmente às exigências aqui descritas.
- 9.10.1.3.2. A solução poderá ser composta por equipamentos de diferentes fabricantes, desde que garantam total interoperabilidade e integração nativa, sem necessidade de adaptações ou conversões adicionais para o pleno funcionamento das funcionalidades exigidas neste documento.
- 9.10.1.3.3. O appliance deverá ser fornecido com suas devidas licenças, de funcionalidades ou de sistema operacional, que permitem a execução das técnicas previstas nesta especificação técnica.
- 9.10.1.3.4. A solução poderá incluir licenciamento de software na modalidade de subscrição ou perpétua, desde que garanta a continuidade operacional durante toda a vigência do contrato, sem necessidade de aquisição adicional pela PMESP.

- 9.10.1.3.5. Em qualquer modalidade escolhida, o software deverá garantir pleno funcionamento durante a vigência do contrato, sem restrições ou necessidade de renovação compulsória para manter a operação dos equipamentos adquiridos.
- 9.10.1.3.6. Deverá possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas de “rede”, “rede inline”, “ferramenta” e portas de “ferramenta inline”.
- 9.10.1.3.7. O sistema deverá permitir a configuração dinâmica de portas via software, permitindo a definição de diferentes tipos de portas, conforme suas funções específicas: Portas de rede: Responsáveis por receber a cópia do tráfego por meio de TAPs/SPANs, Portas de ferramenta: Utilizadas para encaminhar o tráfego, já filtrado e/ou modificado, para as ferramentas conectadas à solução de visibilidade de tráfego, Portas de rede inline: Conectadas diretamente entre os enlaces da rede de produção, atuando de forma inline, Portas de ferramenta inline: Destinadas ao encaminhamento do tráfego de produção, filtrado ou não, para as ferramentas inline conectadas à solução
- 9.10.1.3.8. A solução deverá ser composta por componentes modulares, compatíveis com racks de 19.
- 9.10.1.3.9. Os componentes físicos da solução deverão garantir operação contínua, com sistemas adequados de resfriamento e dissipação de calor.
- 9.10.1.3.10. A solução deverá garantir redundância elétrica e suporte a variações de tensão e frequência dentro do padrão 100V-240V, 50/60 Hz, incluindo fontes de alimentação redundantes quando aplicável.
- 9.10.1.3.11. A fonte de alimentação deverá ser fornecida com todos os cabos necessários para operação.
- 9.10.1.3.12. O equipamento deverá incluir todas as fontes de alimentação suportadas pelo modelo, garantindo redundância total. As fontes devem ser AC, internas ao chassi e hot-swappable.
- 9.10.1.3.13. Deverá suportar simultaneamente em sua memória Flash (ou semelhante), duas imagens do sistema operacional entregue com o equipamento.
- 9.10.1.4. Características de desempenho.
- 9.10.1.4.1. A solução deverá suportar um processamento mínimo inicial de 200 Gbps de tráfego agregado, com capacidade de expansão escalável para atender ao crescimento da demanda da PMESP, podendo atingir até 600 Gbps sem necessidade de substituição do hardware principal.
- 9.10.1.4.2. A solução deverá garantir um throughput exclusivo para tráfego criptografado de, no mínimo, 2,5 Gbps, com possibilidade de expansão conforme necessidade operacional.
- 9.10.1.4.3. A solução deverá suportar no mínimo 16.000 regras simultâneas por módulo, com capacidade de inspeção em múltiplas camadas (L2-L7), incluindo regras baseadas em aplicação e assinatura de tráfego (AppID).
- 9.10.1.4.4. A solução deverá implementar, no mínimo, 6 (seis) pares de interfaces by-pass em fibra para 1G/10G com conectores LC com proteção física. Não serão aceitas soluções com Bypass externo ao agregador. Não serão aceitas soluções que utilizarem baterias para manter o funcionamento do bypass.
- 9.10.1.4.5. Interfaces de comunicação.
- 9.10.1.4.6. A solução deverá garantir compatibilidade com os padrões de conectividade da PMESP, permitindo integração com a infraestrutura de rede existente.
- 9.10.1.4.7. A empresa contratada deverá fornecer todos os componentes necessários para a interconexão da solução, incluindo interfaces Ethernet compatíveis, transceivers ópticos e cabos de fibra óptica ou equivalentes, garantindo conectividade plena e desempenho adequado.
- 9.10.1.4.8. A solução deverá suportar conectividade mínima de 10 Gbps, podendo utilizar interfaces Ethernet 10Gbps SFP+ ou tecnologias equivalentes, conforme necessário para a operação eficiente do serviço.
- 9.10.1.4.9. A empresa contratada deverá garantir que a infraestrutura fornecida possa ser expandida, caso haja necessidade de aumento de capacidade ou interconexão com novos equipamentos no ambiente da PMESP.
- 9.10.1.5. Características de gerenciamento da solução.
- 9.10.1.5.1. A empresa contratada deverá fornecer e operar a Plataforma de Visibilidade de Tráfego com gerenciamento remoto centralizado e seguro, garantindo acesso contínuo para monitoramento e administração da solução.
- 9.10.1.5.2. O sistema deverá permitir configuração customizada baseada em perfis de acesso, implementando controle granular por função (RBAC – Role-Based Access Control).
- 9.10.1.5.3. A solução deverá oferecer suporte a protocolos padrão de gerenciamento de rede, incluindo SNMPv2c e SNMPv3, com capacidade de geração de traps e logs de eventos.
- 9.10.1.5.4. O serviço deverá incluir suporte a MIB II, além de MIBs privativas, garantindo monitoramento detalhado da operação da solução.
- 9.10.1.5.5. A solução deverá suportar SNMP traps sobre IPv6, garantindo compatibilidade com infraestruturas modernas.
- 9.10.1.5.6. A empresa contratada será responsável pela atualização remota da plataforma, incluindo manutenção do sistema operacional, configurações e segurança da solução, sem interrupção do serviço.
- 9.10.1.5.7. O serviço deverá garantir a gravação segura de logs (Syslog) e auditoria detalhada dos acessos e modificações realizadas na solução.
- 9.10.1.5.8. A solução deverá garantir persistência de configurações, permitindo recuperação automática após falhas elétricas, reinicializações ou atualizações programadas.
- 9.10.1.5.9. A empresa contratada deverá fornecer ferramentas de monitoramento e depuração, incluindo estatísticas de utilização, logs de eventos e análise de desempenho.
- 9.10.1.5.10. O gerenciamento deverá ser realizado via interface Web segura (HTTPS) e CLI (Command Line Interface), garantindo acesso autenticado e rastreável.
- 9.10.1.5.11. A solução deverá permitir sincronização de tempo via protocolo NTP (Network Time Protocol), garantindo consistência em registros de eventos e auditorias.
- 9.10.1.5.12. O serviço deverá incluir mecanismos de autenticação centralizada para acesso local e remoto, com suporte a TACACS+, RADIUS e LDAP.
- 9.10.1.5.13. A empresa contratada deverá garantir que a solução suporte IPv6 para TACACS+, garantindo compatibilidade futura com redes de próxima geração.
- 9.10.1.5.14. O acesso remoto à interface de gerenciamento deverá ser protegido por SSHv2, garantindo criptografia e segurança no controle da solução.
- 9.10.1.5.15. A interface de gerenciamento deverá possuir proteção contra acessos não autorizados, exigindo autenticação forte e controle de senha segura.
- 9.10.1.5.16. A solução deverá oferecer um gerenciador centralizado, permitindo a administração unificada de todos os elementos da Plataforma de Visibilidade de Tráfego, incluindo componentes físicos, virtuais, infraestrutura em nuvem e containers.

- 9.10.1.5.17. A solução deverá implementar mecanismos de agregação e encaminhamento de pacotes, garantindo a entrega otimizada dos dados de rede para as ferramentas de análise e segurança, tanto para fluxos Out-of-Band (Cópia de Tráfego) quanto para fluxos Inline, suportando os seguintes cenários:
- 9.10.1.5.18. Encaminhamento 1 para 1 (1:1) – Um fluxo de rede sendo entregue a uma única ferramenta de análise.
- 9.10.1.5.19. Encaminhamento 1 para vários (1:N) – Um fluxo de rede sendo distribuído para múltiplas ferramentas de análise, com suporte a balanceamento de carga.
- 9.10.1.5.20. Encaminhamento vários para 1 (N:1) – Múltiplos fluxos de rede sendo agregados em uma única ferramenta de análise.
- 9.10.1.5.21. Encaminhamento vários para vários (N:N) – Distribuição dinâmica e balanceada de múltiplos fluxos de rede para diferentes ferramentas de análise.
- 9.10.1.5.22. A solução deverá permitir a criação e aplicação dinâmica de filtros de tráfego, garantindo segmentação avançada e granularidade na entrega de pacotes. Os filtros deverão ser configuráveis com base nos seguintes critérios: Endereços MAC de origem e destino. Endereços IPv4 de origem e destino. Portas TCP e UDP de origem e destino. VLAN ID. Ethertype. Identificação de fragmentação de IP (IPFrag). Tempo de Vida do Pacote (TTL). Tipo de Serviço (TOS). Protocolo. Máscara de Controle TCP (TCP Control Mask/Bits). Differentiated Services Code Point (DSCP). Versão do protocolo IP (IPv4 e IPv6). Endereços IPv6 de origem e destino.
- 9.10.1.5.23. A solução deverá permitir modificação, inserção e remoção dinâmica de filtros (regras) em tempo real, sem necessidade de interrupção da operação ou impacto nos fluxos de tráfego analisados.
- 9.10.1.5.24. A solução deverá suportar sobreposição de filtros (overlapping), permitindo a aplicação simultânea de filtros de entrada (ingress) e saída (egress), garantindo maior flexibilidade no controle e roteamento do tráfego monitorado.
- 9.10.1.5.25. A solução deverá permitir operação em ambiente distribuído e integrado, incluindo suporte a tecnologias como Mesh/Cluster, garantindo balanceamento de carga e redundância
- 9.10.1.5.26. A solução deverá suportar a gerência centralizada de múltiplos equipamentos, permitindo sua operação como um único sistema lógico, sem exigir soluções proprietárias de empilhamento que comprometam a escalabilidade ou a interoperabilidade
- 9.10.1.5.27. A solução deverá suportar gestão centralizada de, no mínimo, 30 equipamentos distribuídos, garantindo operação integrada em modo Mesh /Cluster ou tecnologia equivalente que possibilite a administração eficiente de múltiplos dispositivos.
- 9.10.1.5.28. A solução deverá permitir a configuração unificada e gerenciamento centralizado de todos os dispositivos agregadores, utilizando interface Web segura (HTTPS) e CLI (Command Line Interface)
- 9.10.1.5.29. A solução deverá permitir a criação de filtros e regras de direcionamento de tráfego entre diferentes equipamentos físicos ou virtuais, garantindo encaminhamento otimizado de dados entre portas de rede e portas de ferramenta, independentemente da infraestrutura subjacente. Não serão aceitas soluções que comprometam a escalabilidade e a interoperabilidade, como empilhamento com dependência rígida entre equipamentos.
- 9.10.1.5.30. A solução deverá suportar arquitetura distribuída e escalável, como o modelo Spine/Leaf ou equivalente, garantindo balanceamento de tráfego eficiente, resiliência e redundância em caso de falha de um dos equipamentos.
- 9.10.1.5.31. A solução deverá permitir a distribuição inteligente de tráfego e regras de filtragem entre múltiplos equipamentos, garantindo integração fluida entre os dispositivos e possibilitando o uso de arquiteturas baseadas em tecnologias de Fabric Networking ou equivalentes.
- 9.10.1.5.32. A solução deverá permitir a interconexão entre múltiplos clusters ou domínios de processamento, possibilitando o encaminhamento eficiente do tráfego entre diferentes elementos da infraestrutura, conforme necessidade operacional.
- 9.10.1.6. Redundância e alta disponibilidade
- 9.10.1.6.1. A solução deve garantir alta disponibilidade, suportando redundância e operação distribuída em diferentes redes, conforme necessidade.
- 9.10.1.6.2. A solução deverá implementar mecanismos de alta disponibilidade e failover para evitar interrupções no tráfego de rede, garantindo continuidade operacional.
- 9.10.1.7. Funcionalidades para o tráfego interceptado em linha
- 9.10.1.7.1. A solução deverá permitir implantação no ambiente da PMESP sem necessidade de reconfiguração manual de roteadores e switches, quando operando no modo Inline (em linha).
- 9.10.1.7.2. A solução deverá suportar, de forma simultânea e em interfaces distintas, os seguintes modos operacionais:
- 9.10.1.7.2.1. TAP/SPAN (Cópia de Tráfego) – Captura passiva do tráfego para análise.
- 9.10.1.7.2.2. Inline (Tráfego de Produção) – Monitoramento e encaminhamento do tráfego diretamente na rede de produção.
- 9.10.1.7.3. A solução deverá permitir a configuração da sequência de ferramentas inline (serial), garantindo que os pacotes sejam processados sequencialmente em mais de uma ferramenta antes do reencaminhamento.
- 9.10.1.7.4. A solução deverá permitir a configuração de grupos de ferramentas inline (paralelo), garantindo o balanceamento de tráfego entre duas ou mais ferramentas conectadas ao sistema.
- 9.10.1.7.5. A solução deverá permitir a configuração combinada das funcionalidades serial e paralelo, possibilitando criar uma sequência serial de ferramentas que operam em paralelo.
- 9.10.1.7.6. A solução deverá garantir que ferramentas inline, operando em modos standalone, serial ou paralelo, possam receber apenas o tráfego de interesse, sem impactar outras ferramentas e sem necessidade de alterações físicas na infraestrutura;
- 9.10.1.7.7. Exemplos: uma ferramenta pode receber todo o tráfego da rede, outra ferramenta pode receber apenas tráfego HTTP/HTTPS, ambas operam simultaneamente sem interferência.
- 9.10.1.7.8. A solução deverá implementar monitoramento contínuo das ferramentas inline, utilizando heartbeat para detectar falhas e remover automaticamente qualquer ferramenta com erro, sem impactar o restante do tráfego.
- 9.10.1.7.9. A solução deverá suportar heartbeat negativo, onde pacotes de checagem são gerados e bloqueados antes de serem reenviados ao sistema. Caso um pacote de checagem retorne, a ferramenta inline deverá ser considerada falha e removida automaticamente, garantindo a continuidade do tráfego.
- 9.10.1.7.10. A solução deverá permitir a remoção dinâmica de ferramentas inline sem interrupção do tráfego da rede, garantindo que ferramentas possam ser retiradas para atualizações e troubleshooting sem gerar impactos operacionais.
- 9.10.2. Técnicas de segurança da informação
- 9.10.2.1. A solução deverá suportar encapsulamento seguro de tráfego (túnel), permitindo a transferência segura de pacotes entre diferentes elementos da infraestrutura da PMESP, através de redes L3 (roteadas).
- 9.10.2.2. O encapsulamento e desencapsulamento do tráfego deverá utilizar protocolos seguros, como L2GRE ou equivalente, permitindo transporte eficiente do tráfego encapsulado entre redes distintas.

9.10.2.3. A solução deverá implementar balanceamento de carga para pacotes encapsulados IPv6 L2GRE, garantindo distribuição eficiente e otimizada do tráfego entre os elementos da infraestrutura.

9.10.2.4. A solução deverá suportar balanceamento de carga entre múltiplos túneis, permitindo a utilização de duas ou mais ferramentas da plataforma para distribuir o tráfego de maneira equilibrada.

9.10.2.5. Deverá implementar capacidade de processamento agregado de, no mínimo, 23 (vinte e três) Gbps de throughput, específico para o processamento de geração de metadados, netflow, ipfix e cef.

9.10.2.6. Deve gerar, no mínimo, os seguintes metadados para prover informações superiores à da camada de rede, quando utilizando IPFIX/CEF, HTTP2, Response Code, Version, HTTP Host, User Agent, DNS Query Name, Query Type, Response Code, Response TIL, Response Name, RDP Encryption Level, SMB Filename, Filesize, Modbus events, fifo_count, Function_code, Mysql Error, Error_code, Query, Query_ID.

9.11. Ferramentas de Monitoramento e Gerenciamento – Cherwell e Zabbix/Grafana

9.11.1. Para garantir a continuidade operacional dos serviços de TI e a eficiência na gestão de incidentes, mudanças e monitoramento de infraestrutura, a CONTRATADA deverá fornecer e operar ferramentas adequadas para acompanhamento e gerenciamento dos serviços prestados.

9.11.2. As soluções adotadas devem permitir a visibilidade em tempo real da infraestrutura de TI, facilitar a identificação e resolução de problemas e assegurar a conformidade com os níveis de serviço estabelecidos.

9.11.3. As ferramentas devem ser compatíveis com os sistemas existentes e possibilitar integrações via API ou conectores compatíveis.

9.11.4. As seguintes ferramentas são exigidas:

9.11.4.1. ITSM (Ferramenta de Gestão de Serviços de TI): Plataforma para gestão de incidentes, requisições, mudanças, problemas e cumprimento de SLAs, assegurando a governança dos serviços de TI;

9.11.4.2. Ferramenta de Monitoramento Zabbix/Grafana: Solução para monitoramento contínuo da infraestrutura de TI e serviços críticos, garantindo a detecção precoce de falhas e degradações de desempenho.

9.11.5. Módulo de gerenciamento ITSM - Cherwell

9.11.5.1. A CONTRATADA deverá configurar, customizar e adequar a solução de ITSM alinhada as necessidades da CONTRATANTE, garantindo eficiência e disponibilidade contínua;

9.11.5.2. É importante destacar que o suporte Cherwell poderá chegar a até 180.000 (cento e oitenta mil) usuários e 1000 (mil) usuários concorrentes, conforme a necessidade e a estratégia de implantação. O custo do software será apurado mensalmente, de modo a permitir o correto dimensionamento dos pagamentos.

9.11.5.3. A CONTRATADA deverá fornecer toda documentação acerca das adequações e customizações realizadas na ferramenta de ITSM à CONTRATANTE;

9.11.5.4. A CONTRATADA deverá realizar a passagem de conhecimento para a equipe técnica da PMESP por 10 (dez) dias úteis após a conclusão da implementação de todas as funcionalidades solicitadas e realizar a entrega de documentação relacionada;

9.11.5.5. A implementação das funcionalidades da ferramenta deverá ser feita em até 06 (seis) meses a partir do início da vigência contratual;

9.11.5.6. A CONTRATANTE deverá ter acesso ao suporte homologado pelo fabricante, via e-mail ou telefone, onde a CONTRATADA fará a abertura de eventuais chamados, na modalidade 8x5 NBD (next business day) para a solução de problemas;

9.11.5.7. O tempo de resposta a incidentes deverá ser de 4 (quatro) horas a partir da abertura da solicitação junto ao fabricante;

9.11.5.8. Após a entrega da ferramenta customizada de acordo com o solicitado, será feita uma apresentação aos Gestores Contratuais do cumprimento do serviço e comprovar o conhecimento da equipe de ITSM na ferramenta para executar as demandas da CONTRATANTE, os recursos humanos deverão poder resolver problemas, criar customizações ou melhorias e implementar novas funcionalidades à ferramenta, bem como acionar o suporte homologado pelo fabricante quando necessário, sendo vedado a CONTRATADA não execução justificada por falta de conhecimento;

9.11.5.9. A solução deve possuir dashboards interativos (configuráveis), visando trazer informações importantes em um único ponto de exibição, fornecendo visibilidade em tempo real do desempenho dos serviços de TI, monitoramento de incidentes, cumprimento dos SLAs, com alertas automáticos em caso de não conformidade;

9.11.5.10. O sistema deve permitir o registro ágil de incidentes por meio de formulários e portais de autoatendimento, com campos para categorização, priorização e atribuição automática ou manual a equipes de suporte, com base em SLA e critérios personalizados;

9.11.5.11. Desenvolver melhoria na comunicação junto aos usuários, visando um melhor acompanhamento no fluxo de vida dos chamados, como por exemplo com notificações automatizadas sobre o status dos incidentes, via e-mail ou notificação no portal;

9.11.5.12. Deverão ser criadas automatização de tarefas repetitivas quando necessário, como aprovação de solicitações ou encaminhamento de incidentes para equipes específicas;

9.11.5.13. Automação de mudanças recorrentes por meio da criação de templates, simplificando processos repetitivos, oferecendo rastreabilidade e histórico completo de todas as mudanças, assegurando a conformidade com normas internas e externas;

9.11.5.14. Deverão ser criados grupos de Acordos de Nível de Serviço (SLAs) específicos para diferentes serviços e fornecedores, além de fornecer ferramentas para acompanhar, revisar e escalar SLAs de maneira eficiente, além de gerenciar e monitorar os Indicadores – chave de Desempenho (KPIs);

9.11.5.15. Deverão ser calculados automaticamente o SLA e extraídos em relatório, considerando o tempo por equipe, descontando o tempo que o chamado está com status de aguardando ou pendente, contabilizando todos os tickets, tarefas e tags. O sistema deve monitorar o cumprimento dos SLAs para cada grupo e acionar notificações ou escalonamentos automáticos caso os prazos estejam próximos de serem excedidos;

9.11.5.16. A CONTRATADA deve entregar as funcionalidades de “Tarefas”, “Campos Multivalorados ou Tags” em pleno funcionamento, levando em consideração que um ticket pode ter mais de uma equipe atuando e mais de uma categoria e/ou subcategoria sendo verificada e tratada, portanto, deverá ter todo o histórico do ticket, como tempo de atuação de cada equipe (SLA calculado da mesma forma que o ticket principal para cada tarefa), categoria e subcategoria, tags, nome do analista responsável, tempo total e por grupo de atuação;

9.11.5.17. Deverão ser criados relatórios padronizados, de acordo com o solicitado pela CONTRATANTE, para apresentação das informações de forma gráfica e de relatórios detalhados de fácil compreensão, para que sejam compartilhados, tais como, SLAs, KPIs, catálogos de serviços, incidentes, solicitações de serviço, mudanças, problemas, ativos de TI;

9.11.5.18. A CONTRATADA deverá configurar templates de tickets para casos recorrentes que envolvam múltiplas categorias, simplificando o processo de abertura e gerenciamento;

9.11.5.19. A CONTRATANTE deverá entregar a funcionalidade de Criação de Guias de Atendimento (Guided Workflows) em pleno funcionamento, permitindo desta forma que através do fluxo interativo o analista que estiver criando o ticket filtre melhor a demanda, reduzindo erros de abertura de ticket, padronização e melhor performance no atendimento, esta funcionalidade deve estar disponível no autoatendimento também;

- 9.11.5.20. A CONTRATADA deverá personalizar a ferramenta para que alguns campos sejam de preenchimento obrigatório de acordo com a classificação do ticket, de acordo com as definições da CONTRATANTE;
- 9.11.5.21. A CONTRATADA deverá personalizar os perfis de atendimento, permitindo a função (botão) encaminhar, apenas aos analistas com função de dispatcher ou similar, que façam o gerenciamento dos tickets e militares com aprovação do CONTRATANTE, desta forma o chamado só poderia ser enviado aos grupos de acordo com o previamente configurado, baseado no catálogo de serviços, considerando a classificação do ticket;
- 9.11.5.22. A CONTRATADA deverá entregar em formato de relatório e dashboard informações sobre as categorias e subcategorias com maior número de tickets por determinado período, permitindo que possam ser filtradas e extraídas de diferentes formas (por categoria de cada setor, por dia, por mês e /ou período personalizado), contabilizando inclusive as tarefas e/ou tags de acordo com sua classificação;
- 9.11.5.23. Criar relatórios para controle dos analistas com relação aos chamados onde existiu atuação, criação e chamados solucionados por ele, facilitando a autogestão de chamados;
- 9.11.5.24. A CONTRATADA deverá revisar e ajustar o fluxo de mudanças, revisar todos os nomes de grupos, revisão dos integrantes dos grupos de atendimento de tickets, grupo de aprovadores de mudanças, comitê de mudanças;
- 9.11.5.25. Revisão do portal de autoatendimento, tornando mais intuitivo, habilitando todos os recursos disponíveis, deixando igual ou o mais próximo do uso da ferramenta web e/ou cliente;
- 9.11.5.26. Portal de autoatendimento intuitivo, onde os usuários finais podem registrar incidentes, solicitar serviços, consultar artigos de conhecimento, acompanhar o status de seus tickets e que resolvam problemas de forma autônoma;
- 9.11.5.27. A CONTRATADA deverá realizar a análise e, se necessário, adequação da base de dados da ferramenta implementada para que o tamanho e desempenho sejam otimizados.
- 9.11.5.28. Deverão ser criados relatórios de forma agendada para automatização de rotinas de entrega de informações para o CONTRATANTE;
- 9.11.5.29. A contratada deverá realizar a criação de relatórios para identificação de problemas recorrentes com base na análise de incidentes e tendências.
- 9.11.5.30. Realizar estudo e implementar melhorias na automação de fluxos de trabalho, as tarefas, aprovações para solicitações de serviço e encaminhamentos para diferentes equipes de suporte com base em regras de negócios, reduzindo o trabalho manual e melhorando a eficiência, através de sua interface gráfica para desenhar e implementar fluxos de trabalho personalizados, sem a necessidade de programação;
- 9.11.5.31. Deverão ser implementadas integrações com ferramentas e sistemas que a CONTRATANTE já utiliza, fazer a integração dos mesmos (como Teams, e-mail, Zabbix, Grafana, entre outros).
- 9.11.5.32. A CONTRATADA deverá elaborar um treinamento para os militares e equipes técnicas onde serão expostas a formas mais adequadas para utilização da ferramenta em pontos como abertura de chamados, atendimento de chamados, encerramento de chamados, entre outros;
- 9.11.5.33. Eventuais problemas na adequação configuração e funcionamento da ferramenta decorrente da má implementação por parte da CONTRATADA deverá ser às expensas da CONTRATADA, não restando a CONTRATANTE a cobrança de horas técnicas e/ou horas de projeto por parte da CONTRATADA;
- 9.11.5.34. Os custos decorrentes desses serviços, deverão ser previstos pela CONTRATADA, não devendo ser usado horas técnicas ou horas de projeto para tanto, salvo quando após a implantação, seja demandado pela CONTRATADA, para expansão da solução ou implementação em novos dispositivos;
- 9.11.5.35. Assegurar, durante a vigência do contrato, a manutenção do funcionamento operacional da solução Cherwell, observadas as condições normais de uso e as políticas de suporte e ciclo de vida definidas pelo fabricante, promovendo a correção de falhas técnicas comprovadamente atribuíveis à CONTRATADA, sem ônus adicional ao CONTRATANTE.
- 9.11.5.36. Disponibilizar suporte técnico à solução Cherwell, prestado pelo fabricante ou por parceiro autorizado, sujeito à vigência e às condições do contrato de suporte do fabricante, com atendimento em língua portuguesa e/ou inglesa, incluindo, quando disponíveis, o registro e acompanhamento de chamados em portal especializado, aplicação de correções, patches e atualizações liberadas pelo fabricante e acesso a novas versões, desde que disponibilizadas pelo fabricante e cobertas pelo modelo de licenciamento vigente.
- 9.11.5.37. Os custos relativos ao suporte e manutenção corretiva da solução Cherwell, conforme escopo contratado e políticas vigentes do fabricante, deverão estar contemplados no valor da planilha de decomposição da proposta, excluídas evoluções tecnológicas ou mudanças de plataforma decorrentes de decisões de descontinuidade ou alteração comercial do fabricante.
- 9.11.5.38. No caso de a solução Cherwell vir a ser enquadrada em situação de End of Life (EoL) ou End of Support (EoS) pelo fabricante durante a vigência do contrato, a CONTRATADA deverá, comunicar formalmente o CONTRATANTE, em prazo razoável, sobre o evento de descontinuidade, apresentar plano de transição tecnológica, contemplando alternativas suportadas pelo mercado e compatíveis com o ambiente existente, atuar em regime de melhores esforços, visando garantir a continuidade operacional da gestão de serviços, enquanto perdurar o suporte oficialmente disponibilizado pelo fabricante, e eventual migração para nova solução, plataforma distinta ou alteração substancial do escopo original deverá ser objeto de negociação específica entre as partes, quanto a prazos, custos e condições técnicas.

9.11.6. Módulo de monitoramento Zabbix/Grafana:

- 9.11.6.1. A CONTRATADA deverá configurar e customizar a ferramenta ZABBIX para seguir com o padrão de softwares de monitoramento já na CONTRATANTE;
- 9.11.6.2. A CONTRATADA deverá alinhar previamente com a CONTRATANTE as necessidades a fim de realizar o sizing da ferramenta e necessidade de software e hardware para início da implantação;
- 9.11.6.3. A CONTRATADA deverá fornecer toda documentação sobre a instalação, configuração, suporte, customização eventuais licenças, em língua portuguesa a CONTRATANTE;
- 9.11.6.4. A implementação da solução deverá ser realizada utilizando as melhores práticas disponíveis e em Alta Disponibilidade, com os serviços instalados de forma redundante, para que em caso de queda do servidor primário o secundário possa atuar sem indisponibilidade dos serviços para o CONTRATANTE;
- 9.11.6.5. A CONTRATANTE disponibilizará o ambiente virtual para instalação, sendo de responsabilidade da CONTRATADA o preenchimento da documentação demandada pela CONTRATANTE;
- 9.11.6.6. A CONTRATADA deverá realizar a integração entre as múltiplas bases de dados já existentes na CONTRATANTE, assim como será responsável pela ampliação da ferramenta ZABBIX, garantindo que todas as configurações, históricos de monitoramento e relatórios previamente armazenados sejam consolidados e acessíveis na nova solução. A integração deverá manter a consistência dos dados e assegurar a continuidade das operações de monitoramento sem interrupções significativas;

- 9.11.6.7. A CONTRATADA deverá realizar a implementação e tuning de monitoramento na ferramenta ZABBIX inicialmente para 5500 (cinco mil e quinhentos) dispositivos;
- 9.11.6.8. A ferramenta deve ser capaz de realizar o envio de alarmes através de e-mail;
- 9.11.6.9. Os dispositivos a serem monitorados na ferramenta serão diversos, heterogêneos e de fabricantes diversos, em sua maioria roteadores, switches, firewalls, access points, servidores, geradores, PABX e enlaces de rádio, devendo ser capaz de monitorar todo e qualquer dispositivo demandado pela CONTRATANTE, além dos citados nesse item, independente de fabricante;
- 9.11.6.10. Deverão ser criados grupos de prioridade dos dispositivos, para classificação da urgência e alarmes de monitoramento;
- 9.11.6.11. Deverão ser elaboradas topologias que apresentem conexões físicas e localização dos equipamentos;
- 9.11.6.12. Deve ser implementados diferentes períodos para coleta de informação dos dispositivos, de forma a criar diferentes intervalos de acordo com a urgência e impacto do dispositivo;
- 9.11.6.13. O monitoramento deve ser feito preferencialmente através do protocolo SNMPv2 ou superior, porém quando os dispositivos não suportarem essa tecnologia o monitoramento pode ser feito através do ICMP;
- 9.11.6.14. Deverá ser previsto o monitoramento de até 5500 (cinco mil e quinhentos) interfaces de equipamentos, majoritariamente proveniente do Datacenter PMESP;
- 9.11.6.15. O monitoramento e alarme deverão ser feitos para identificação de falha ou indisponibilidade dos dispositivos, assim como em relação a performance, threshold;
- 9.11.6.16. Deverão ser criados relatórios padronizados, de acordo com o solicitado pela CONTRATANTE, para apresentação das informações de forma gráfica e de fácil compreensão, a fim de serem compartilhados, tais como, performance, estatísticas, análise de comportamento (Flow) e disponibilidade.
- 9.11.6.17. Para otimizar a criação e a qualidade dos relatórios, deverá ser utilizada uma ferramenta externa com interface intuitiva, que ofereça opções de personalização e permita a geração agendada e automatizada de relatórios, atendendo aos requisitos de apresentação definidos pela CONTRATANTE garantindo padronização e eficiência;
- 9.11.6.18. Deverá possuir dashboards e relatórios interativos, permitindo ao usuário expandir, filtrar e detalhar dados diretamente no relatório.
- 9.11.6.19. Deverá agendar a geração e distribuição automática de relatórios em vários formatos (PDF, Excel, HTML, Word), poderá enviar relatórios por e-mail ou integrá-los;
- 9.11.6.20. Deverão ser criados relatórios de forma agendada para automatização de rotinas de entrega de informações para o CONTRATANTE;
- 9.11.6.21. Deverão ser criados dashboards utilizando o software Grafana, visando trazer informações importantes para um único ponto de exibição;
- 9.11.6.22. Deverão ser implementados NetFlow/SFlow em até 150 (cento e cinquenta) equipamentos, visando a identificação de desvio de comportamento na rede;
- 9.11.6.23. A implementação das funcionalidades da ferramenta deverá ser feita em até 90 (noventa) dias a partir do início da vigência contratual e disponibilização das máquinas virtuais para implementação da ferramenta;
- 9.11.6.24. Após a implementação da ferramenta a CONTRATADA deverá apresentar relatório com as informações pertinentes a implementação de todos os itens da ferramenta de monitoramento, que constam nesse documento;
- 9.11.6.25. Todos os relatórios deverão ser entregues em língua portuguesa, mesmo aqueles desenvolvidos na ferramenta, restando a CONTRATADA a adaptação desses relatórios;
- 9.11.6.26. A CONTRATANTE deverá ter acesso ao suporte oficial do fabricante, via email ou telefone, onde a CONTRATADA fará a abertura de eventuais chamados, na modalidade 8x5 NBD (next business day) para a solução de problemas; O tempo de resposta a incidentes deverá ser de 4 (quatro) horas a partir da abertura da solicitação junto ao fabricante;
- 9.11.6.27. Após a implantação da ferramenta, as atividades de monitoramento e gerenciamento serão executadas pelos recursos humanos da equipe de gerenciamento e monitoramento, os quais deverão ter treinamento na ferramenta, com comprovado conhecimento para executar as demandas da CONTRATANTE, sendo vedado a CONTRATADA não execução justificada por falta de conhecimento;
- 9.11.6.28. Após a implantação da ferramenta, com a apresentação aos Gestores Contratuais do cumprimento do serviço e atestado conhecimento da equipe de monitoramento e gerenciamento na ferramenta, os recursos humanos deverão poder resolver problemas, criar customizações ou melhorias e implementar novas funcionalidades à ferramenta de monitoramento, bem como ter acesso ao suporte da fabricante;
- 9.11.6.29. A CONTRATADA deverá realizar a integração entre o Zabbix e o Grafana, garantindo a extração e transformação dos dados monitorados, para a criação de relatórios dinâmicos, interativos e personalizáveis. Essa integração deverá proporcionar uma visualização clara e intuitiva das métricas e indicadores de desempenho, permitindo análises detalhadas e suporte à tomada de decisão estratégica. A CONTRATADA será responsável pela configuração inicial, desenvolvimento de conexões seguras e automatizadas entre as ferramentas, bem como pela criação de dashboards no Grafana que atendam às necessidades operacionais e estratégicas da CONTRATANTE, assegurando a atualização contínua dos dados monitorados.
- 9.11.6.30. Eventuais problemas no tuning, implantação, configuração e funcionamento da ferramenta decorrente da má implementação por parte da CONTRATADA deverá ser às expensas da CONTRATADA, não restando a CONTRATANTE a cobrança de horas técnicas e/ou horas de projeto por parte da CONTRATADA;
- 9.11.6.31. Os custos decorrentes desses serviços, deverão ser previstos pela CONTRATADA, não devendo ser usado horas técnicas ou horas de projeto para tanto, salvo quando após a implantação, seja demandado pela CONTRATADA, para expansão da solução ou implementação em novos dispositivos.
- 9.11.6.32. Demais informações relacionadas às bases do Zabbix existentes na CONTRATANTE estão disponíveis no APÊNDICE A12 – Zabbix;

10. Análise comparativa de soluções

10.1. A presente análise comparativa tem como objetivo avaliar as alternativas disponíveis para a contratação de serviços técnicos especializados voltados ao suporte técnico em cibersegurança, data center, redes, governança, gerenciamento e monitoramento da infraestrutura de TIC, visando garantir a continuidade dos serviços de tecnologia da informação e comunicação. Foram consideradas três principais alternativas: a contratação de serviços gerenciados por integradores especializados, a execução interna por equipe própria e a adoção de infraestrutura híbrida com suporte técnico

especializado.

10.2. A primeira alternativa, baseada em serviços gerenciados, consiste na terceirização das atividades para empresas especializadas que oferecem suporte contínuo, monitoramento e gestão da infraestrutura de TIC. Essa opção apresenta como principais vantagens a alta especialização técnica, escalabilidade, flexibilidade contratual e a definição clara de níveis de serviço por meio de acordos de SLA. No entanto, implica em menor controle direto sobre a operação e maior dependência de fornecedores externos.

10.3. A segunda alternativa considera a execução das atividades por equipe técnica interna. Embora proporcione maior controle sobre os processos e integração com a cultura organizacional, essa abordagem demanda investimentos elevados em capacitação, manutenção de pessoal e infraestrutura, além de apresentar limitações técnicas e operacionais, especialmente em cenários de alta complexidade ou incidentes críticos.

10.4. A terceira alternativa envolve a utilização de infraestrutura híbrida em ambiente público, privada, associada a serviços especializados. Essa solução oferece alta escalabilidade, disponibilidade e acesso a tecnologias de ponta, com redução de custos relacionados à infraestrutura física. Contudo, exige uma gestão contratual financeira robusta e apresenta riscos relacionados à proteção de dados, que devem ser mitigados por meio de cláusulas contratuais e conformidade com a LGPD.

10.5. A avaliação das alternativas foi realizada com base em critérios como custo inicial, escalabilidade, especialização técnica, tempo de implantação, aderência à legislação de proteção de dados, flexibilidade contratual e capacidade de garantir a continuidade operacional. A análise demonstrou que a contratação de serviços gerenciados especializados, baseada em serviços gerenciados, consiste na terceirização das atividades para empresas especializadas que oferecem suporte contínuo, monitoramento e gestão da infraestrutura de TIC. Essa abordagem está alinhada às melhores práticas de governança e gestão de TIC, contribuindo para a mitigação de riscos operacionais e cibernéticos, além de assegurar a continuidade e a eficiência dos serviços prestados pela PMESP.

11. Registro de soluções consideradas inviáveis

11.1. Durante o estudo para definir a melhor solução de Tecnologia da Informação e Comunicação (TIC) para a Polícia Militar do Estado de São Paulo (PMESP), diversas alternativas foram analisadas. Algumas delas, no entanto, foram descartadas por apresentarem inviabilidades técnicas, operacionais, financeiras ou estratégicas. A seguir, são descritas as principais opções avaliadas e os motivos pelos quais não foram escolhidas:

11.2. A contratação baseada em entrega de serviços foi uma das opções consideradas, pois permitiria um ajuste mais flexível dos serviços conforme a demanda. No entanto, essa modalidade apresenta dificuldades para a quantificação/medição objetiva da entrega dos serviços, comprometendo a previsibilidade de custos e a utilidade operacional. Além disso, esse modelo não se alinha às diretrizes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), que recomenda a adoção de serviços gerenciados em vez da simples alocação de profissionais.

11.3. Outro modelo analisado foi a alocação fixa de profissionais dentro da PMESP. Embora garantisse a presença contínua da equipe, essa abordagem foi considerada rígida e pouco eficiente, dificultando ajustes conforme as variações da demanda. Além disso, o modelo não favorece metodologias ágeis e práticas modernas de automação, resultando em um custo operacional elevado.

11.4. A manutenção dos serviços atuais sem modificações também foi estudada, mas se mostrou inadequada devido à obsolescência tecnológica. A infraestrutura existente apresenta limitações que dificultam a modernização e a adoção de novas tecnologias. Além disso, a manutenção do cenário atual seria incompatível com o Plano Estratégico da PMESP 2024-2031, que prioriza a inovação e a digitalização dos serviços.

11.5. A adoção exclusiva de computação em nuvem pública foi considerada como uma possibilidade para modernizar a infraestrutura da PMESP. Contudo, essa alternativa foi descartada devido à dependência total de fornecedores externos, o que representaria riscos operacionais e estratégicos. Além disso, as exigências de segurança e sigilo das informações da corporação não poderiam ser plenamente garantidas nesse modelo, além das restrições regulatórias sobre o armazenamento de dados sensíveis em infraestruturas terceirizadas.

11.6. Foi avaliada a possibilidade de a própria PMESP desenvolver e operar internamente sua solução de TIC, eliminando a necessidade de contratação externa. No entanto, essa abordagem exigiria investimentos elevados em infraestrutura, tecnologia e capacitação de pessoal. Além disso, o tempo necessário para desenvolver e implantar uma solução própria seria incompatível com a necessidade imediata de modernização dos serviços. Outro desafio identificado seria a dificuldade na retenção de profissionais qualificados, dada a alta competitividade do mercado de tecnologia.

11.7. A terceirização parcial dos serviços foi outra alternativa analisada, com a proposta de manter algumas atividades sob gestão interna da PMESP. Como algumas especialidades técnicas dependem de fornecedores distintos, essa fragmentação pode dificultar a governança e a interoperabilidade entre prestadores de serviços e sistemas. No entanto, sob a perspectiva do conhecimento e da expertise técnica, essa abordagem permite a composição dos melhores perfis técnicos em cada área de atuação.

11.7.1. Diante dessas análises, concluiu-se que a melhor abordagem para atender às necessidades da PMESP é a contratação de serviços gerenciados, com um modelo de pagamento fixo mensal atrelado ao cumprimento de serviços exclusivos e dedicados, cumprindo SLA, em postos de trabalho. Esse formato proporciona previsibilidade nos custos, assegura a qualidade da prestação dos serviços, cumprimento dos níveis de serviços e permite que a PMESP conte com uma infraestrutura tecnológica moderna, segura e eficiente, garantindo governança e continuidade operacional.

12. Análise comparativa de custos (TCO)

12.1. Considerando o levantamento realizado no Relatório de Pesquisa de Preços, bem como as propostas recebidas das empresas, verifica-se que os valores apresentados contemplam não apenas os serviços de SOC e NOC, mas também licenciamento de softwares, módulos de monitoramento, observabilidade de sistemas e redes, gestão de vulnerabilidades, threat intelligence, testes de intrusão, além de custos operacionais e de suporte técnico especializado, refletindo assim o modelo de precificação adotado pelo mercado para serviços gerenciados de TIC.

12.2. Sob a ótica do TCO – Análise Comparativa de Custos, a análise não se restringe ao valor mensal estimado das propostas, mas considera a totalidade dos custos envolvidos no período contratual de 30 (trinta) meses. Isso inclui: custos diretos com a operação dos serviços, atualização tecnológica, manutenção de softwares e licenças, despesas com infraestrutura de apoio (como deslocamentos, hospedagens e insumos necessários à operação), governança e compliance, além de reserva técnica para atendimento a ordens de serviço sob demanda.

12.3. Cabe destacar que algumas empresas optaram por apresentar propostas em formato aglutinado, integrando serviços e licenciamento em pacotes unificados. Essa prática se mostra vantajosa sob a perspectiva do TCO, pois reduz riscos de incompatibilidade entre soluções de diferentes fornecedores, facilita a gestão contratual e permite maior previsibilidade de custos, eliminando despesas adicionais que poderiam ocorrer com integrações, retrabalho ou contratações complementares.

12.4. A comparação entre as propostas evidencia valores totais em patamares próximos, demonstrando consistência com os preços praticados no mercado para serviços de cibersegurança e gestão de infraestrutura de TIC em larga escala. Ressalta-se que, ainda que haja variação de preços unitários entre itens, a consolidação em pacotes integrados garante um custo total de propriedade mais eficiente e alinhado às necessidades da PMESP, sobretudo pela natureza crítica e contínua dos serviços a serem prestados.

13. Descrição da solução de TIC a ser contratada

13.1. A solução TIC a ser contratada visa garantir a continuidade, segurança, eficiência e modernização dos serviços críticos da Polícia Militar do Estado de São Paulo (PMESP), assegurando a alta disponibilidade da infraestrutura computacional e de telecomunicações.

13.2. A contratação será realizada por meio de serviços gerenciados, com pagamento fixo mensal vinculado ao atendimento de níveis mínimos de serviço (NMS) previamente estabelecidos.

13.3. A solução deve abranger suporte técnico especializado, monitoramento contínuo, prevenção de ameaças cibernéticas, resposta a incidentes, governança e gestão de infraestrutura de TIC.

13.4. A CONTRATADA deverá disponibilizar mão de obra qualificada com regime de dedicação exclusiva, alinhada às melhores práticas, padrões nacionais e internacionais, como ABNT NBR ISO/IEC 20000:2020 (Gestão de Serviços de TI), ISO/IEC 27001:2022 (Segurança da Informação), ITIL e ITSM.

13.5. Atribuições da Contratada:

13.5.1. A CONTRATADA, para a prestação do serviço deverá ainda atender aos requisitos mínimos de serviços especificados a seguir.

13.5.2. A CONTRATADA deve executar os serviços contratados, em conformidade com as especificações e condições discriminadas, dentro de elevados padrões de qualidade, observando as normas legais e regulamentares, cumprindo as responsabilidades resultantes do contrato;

13.5.3. Manter o sigilo e a inviolabilidade dos serviços, respeitadas as hipóteses e condições constitucionais e legais;

13.5.4. A guardar de sigilo inclui estudos, projetos, operações, instalações, documentos pertencentes ao Contratante qualificações pessoas, e qualquer outra informação tiver conhecimento para o cumprimento do objeto do contrato;

13.5.5. Implantar, de forma adequada, a supervisão permanente dos serviços, de modo a obter uma operação correta e eficaz;

13.5.6. As notas fiscais faturadas pela empresa deverão ser encaminhadas à contratante após validação pela PMESP dos relatórios de serviços prestados. A empresa deverá emitir a Nota Fiscal (NF) após a conferência dos serviços prestados, conforme prazos definidos em contrato;

13.5.7. Os pagamentos dos valores financeiros que a contratada fazer jus somente serão realizados após a emissão das NF, conferência e aprovação da contratante;

13.5.8. Comunicar ao representante da Contratante, qualquer anormalidade de caráter urgente e prestar os esclarecimentos julgados necessários;

13.5.9. Registrar eventuais falhas na área de cobertura dos serviços com indicação da data, horário, localização e tempo de duração;

13.5.10. Assumir inteira responsabilidade pela execução dos serviços que prestar, arcando com todos os ônus necessários à completa execução dos serviços;

13.5.11. Fornecer e utilizar, sob sua inteira responsabilidade, toda a competente e indispensável mão de obra habilitada adequadamente, atendidas sempre e regularmente todas as exigências legais pertinentes, como ônus trabalhistas, encargos sociais, tributos, indenizações e seguro contra acidentes;

13.5.12. Responsabilizar-se integralmente pelos serviços contratados, nos termos da legislação vigente, especialmente pelos encargos salariais, trabalhistas, fiscais e previdenciários, relativos a seus empregados envolvidos na execução dos serviços objeto do contrato;

13.5.13. Assegurar o acesso do gestor indicado pelo Contratante aos serviços em execução e à documentação pertinente, atendendo prontamente às solicitações e exigências por ele apresentadas;

13.5.14. Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato, não excluindo ou reduzindo essa responsabilidade à fiscalização ou ao acompanhamento pelo Contratante;

13.5.15. Assegurar que os funcionários de seu quadro, que estiverem à disposição da Contratante, tenham familiaridade com a ferramenta de abertura de chamados utilizada pela Instituição.

13.5.16. É dever ainda da Contratada, submeter solicitação e obter autorização prévia da PMESP para subcontratação de qualquer serviço técnico.

13.5.17. Os profissionais alocados deverão ter qualificação técnica, certificações e cursos nas áreas condizentes ao proposto em seu cargo/quadro técnico;

13.6. Substituição do Pessoal

13.6.1. Em caso de necessidade de substituição de algum técnico da empresa, deverá ser alocado novo técnico, mesmo que de forma temporária, em comum acordo com o Gestor do Contrato, de forma a não impactar a entrega do serviço em execução;

13.6.2. Os técnicos residentes da CONTRATADA deverão ser alocados no endereço indicado, conforme a solicitação de ocupação do quadro técnico.

13.7. Designação de gerente contratual

13.7.1. Designar, por escrito e no ato da assinatura deste Contrato e às expensas da Contratada, o preposto responsável pela fiel execução do objeto, outorgando-lhe poderes para a resolução de quaisquer ocorrências durante o período de vigência contratual, além do recebimento de notificações e para garantir o cumprimento do disposto em Contrato.

13.7.2. É vedado à Contratada, ou a seus representantes, ou parceiros comerciais manter relações, atender dúvidas, marcar reuniões, executar testes, treinamentos, palestras ou aulas, realizar acordos comerciais e enviar documentos com qualquer unidade da PMESP, sem prévio acordo entre o Gestor do Contrato e o preposto da Contratada, em pautas que possuam relações com a Solução Contratada.

13.8. Considerações Gerais de Execução

13.8.1. A CONTRATADA deverá assegurar o total sigilo das informações relativas ao ambiente computacional e de telecomunicações da Polícia Militar, principalmente no tocante às informações do ambiente de rede e segurança;

13.8.2. Todos os recursos humanos envolvidos deverão ser funcionários registrados da CONTRATADA, cumprindo o regime de serviços previsto pela

Legislação Trabalhista vigente de forma integral, sendo vedada a utilização de pessoas jurídicas ou prestadores de serviços autônomos, com exceção das horas de projeto no item de Serviços Técnicos Avançados;

13.8.3. A CONTRATADA deverá cumprir rigorosamente com as obrigações trabalhistas desde pagamento de horas de sobreaviso, adicional noturno, horas extras convencionais independentes se semana, fim de semana ou feriado, e qualquer obrigação, adicional, compensação e outros que seja obrigada por Legislação vigente, não restando obrigação por parte da CONTRATANTE;

13.8.4. A Polícia Militar poderá, a qualquer tempo, solicitar a substituição, reposição, remoção ou adição dos recursos humanos deste contrato, por meio de Notificação Contratual Numerada e assinada, devendo a CONTRATADA providenciar tal demanda em até 20 (vinte) dias úteis;

13.8.5. Os recursos humanos deverão, durante toda a vigência contratual, preencher todos os requisitos solicitados pela Polícia Militar e ofertados pela CONTRATADA durante o certame licitatório, sendo obrigada a comprovar o atendimento das especificações e certificações quando for demandada em até 10 (dez) dias úteis;

13.8.6. A comprovação de certificação profissional dar-se-á mediante a apresentação de certificado devidamente registrado pelo órgão, instituto ou fabricante mantenedor da certificação em questão, bem como pela disponibilização de URL oficial de verificação a respeito da sua validade;

13.8.7. Os registros em carteira de trabalho dos recursos humanos deverão ser iguais aos cargos exigidos neste edital ou equivalentes, sendo vedada a contratação e respectiva remuneração por cargo inferior ao aqui exigido;

13.8.8. A CONTRATADA deverá cumprir rigorosamente todas as determinações exaradas na legislação trabalhista, sob pena de responsabilização penal, administrativa, cível e trabalhista;

13.8.9. Todos os recursos humanos deverão ser alocados e faturados na posição referente a sua atividade, caso um analista de Nível 3 seja alocado para uma atividade inferior, este deverá ser faturado como tal;

13.8.10. Os recursos humanos deverão ser empregados exclusivamente no contrato em questão, sendo expressamente proibida a utilização dos mesmos em outros contratos ou para outras empresas de forma compartilhada, exceto Serviços Técnicos Avançados;

13.8.11. A CONTRATANTE poderá solicitar que os serviços dos recursos humanos sejam realizados nas dependências de outras unidades da Polícia Militar, outros órgãos governamentais e empresas privadas, majoritariamente no Estado de São Paulo, de acordo com os interesses da Polícia Militar;

13.8.12. Os membros da equipe poderão atuar em modelo híbrido, alternando entre trabalho remoto e presencial, conforme as escalas e cronogramas definidos pelo CONTRATANTE, de modo a garantir a eficiência das operações e o atendimento às necessidades do projeto. Exceção feita aos analistas de monitoramento, SOC e NOC, que devem obrigatoriamente exercer suas atividades de forma presencial, devido à natureza crítica de suas funções e à necessidade de supervisão direta e contínua da infraestrutura e serviços monitorados, bem como Gestão de TIC.

13.8.13. Os serviços do SOC, monitoramento Windows e monitoramento Linux deverão ser prestados em caráter de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;

13.8.14. A CONTRATANTE poderá solicitar, sem prévio aviso, que atividades sejam realizadas fora do horário de expediente, visando garantir a estabilidade do ambiente e atender aos interesses da Polícia Militar. Nessas circunstâncias, a CONTRATADA deverá remunerar os colaboradores envolvidos exclusivamente por meio de pagamento de horas extras, não sendo permitido o uso de banco de horas para compensação desse trabalho adicional. O uso de banco de horas poderá prejudicar a CONTRATANTE, pois a ausência do colaborador no momento da compensação inviabiliza a continuidade das operações e o atendimento imediato às demandas críticas, comprometendo os interesses da Polícia Militar e a estabilidade do ambiente operacional.

13.8.15. A CONTRATADA deverá, quando demandada pela Polícia Militar, providenciar toda a logística adequada para o deslocamento, hospedagem, alimentação, comunicação e demais necessidades, previsíveis ou não, para os recursos humanos empregados em local diverso ao DAS;

13.8.16. A CONTRATADA deverá buscar junto à Polícia Militar os contatos dos terceiros que devem ser acionados na detecção de problemas sob suas responsabilidades, cabendo à CONTRATADA a atualização e controle da referida informação;

13.8.17. Para melhor controle das horas trabalhadas presencialmente, deverá existir um sistema de controle de ponto digital, que deverá permitir registro do ponto em qualquer local, com o registro das horas e localização geográfica;

13.8.18. A CONTRATADA deverá providenciar no mínimo 05 (cinco) camisas ou camisetas com a identificação da empresa, além de 01(um) crachá com a identificação do funcionário;

13.8.19. O contrato será executado no regime de pagamento fixo mensal, atrelado ao nível mínimo de serviços do catálogo de serviços, cabendo a CONTRATADA custear todas as despesas decorrentes da contratação, inclusive com licenciamento de uso de softwares, salários, encargos e benefícios diretos ou indiretos (BDI) de funcionários, aquisição e manutenção de equipamentos e materiais, transportes, seguros e tributos de qualquer natureza. Não restando responsabilidade de horas extras, escalas de sobreaviso, adicionais noturnos entre outros a CONTRATANTE;

13.8.20. A CONTRATANTE deverá manter após término do contrato pelo tempo de armazenamento definido para 60 (sessenta) meses, as regras de SIEM (Hot) e Syslog (Cold) a consulta para a CONTRATADA;

13.9. Serviços Técnicos a serem contratados

13.9.1. Escopo dos Serviços

13.9.1.1. A solução desejada pela Polícia Militar do Estado de São Paulo contempla a contratação de serviços especializados de suporte técnico de cibersegurança, data center e redes, bem como de governança, gerenciamento e monitoramento, das demandas e mudanças de tecnologia da informação e comunicação e infraestrutura de data center e redes para ambiente computacional e de telecomunicações, de forma a garantir a continuidade dos serviços de TIC, que deverão atender as seguintes áreas de atuação:

13.9.1.2. Garantia de Continuidade e Qualidade dos Serviços: Assegurar a continuidade, a qualidade e a segurança das operações de TIC, com gestão integrada da infraestrutura de cibersegurança, datacenter, redes e sistemas de segurança da informação essenciais para o funcionamento das operações críticas da instituição.

13.9.1.3. Suporte Técnico Abrangente: O serviço deverá abranger desde a manutenção de rotina até a implementação de mudanças estruturais em TIC, sempre com o objetivo de melhorar o desempenho, reduzir riscos e minimizar impactos nas operações diárias.

13.9.1.4. Monitoramento e Resposta a Incidentes: A contratada deverá monitorar, gerenciar e responder proativamente a eventos e incidentes de segurança, implementando soluções que mitiguem riscos e garantam a integridade dos dados e a segurança de toda a infraestrutura de TIC.

13.9.1.5. Gestão Integrada e Melhorias Contínuas: Através do uso de ferramentas tecnológicas, a contratada deverá promover uma gestão eficiente e integrada, assegurando que todas as atividades cumpram as políticas e diretrizes da Polícia Militar e seus padrões de segurança. A solução deverá prever a implementação contínua de melhorias, tanto na infraestrutura técnica quanto na governança de processos, acompanhando a evolução das demandas e garantindo a adequação dos serviços prestados.

13.9.2. Serviços de Gestão de TIC

13.9.2.1. Descrição Geral

13.9.2.1.1. O Serviço de Gestão de TIC será responsável pela coordenação geral das operações relacionadas à gestão da infraestrutura de TIC do contrato, garantindo o alinhamento das equipes técnicas às metas estabelecidas pela CONTRATANTE. Suas atividades incluirão o planejamento, supervisão e validação das ações realizadas pelos analistas e técnicos alocados, assegurando que as práticas sigam os padrões técnicos, normativos e as melhores práticas.

13.9.2.2. Atribuições

- 13.9.2.2.1. Coordenar e gerenciar a atuação dos profissionais alocados no monitoramento, controle e operação da infraestrutura de TIC.
- 13.9.2.2.2. Supervisionar as equipes de suporte, produção, redes, segurança e sistemas, assegurando integração com outras áreas técnicas.
- 13.9.2.2.3. Participar de fóruns de discussão sobre novas tecnologias, promovendo inovação na operação da infraestrutura.
- 13.9.2.2.4. Planejar e coordenar implementações de infraestrutura para data center, redes e cibersegurança.
- 13.9.2.2.5. Desenvolver e manter documentações detalhadas da infraestrutura de TI.
- 13.9.2.2.6. Assegurar o alinhamento dos serviços prestados com as expectativas da CONTRATANTE.
- 13.9.2.2.7. Padronizar e racionalizar procedimentos de segurança e controle.

13.9.3. Serviço de Governança de TIC

13.9.3.1. Descrição Geral

13.9.3.1.1. O Serviço de Governança de TIC supervisiona e otimiza os processos de tecnologia da informação, garantindo alinhamento estratégico entre as operações de TI e as necessidades organizacionais da CONTRATANTE. A equipe será composta por analistas de projetos, analistas de processos e analistas de ITSM (Gerenciamento de Serviços de TI), assegurando conformidade com normas como a ABNT NBR ISO 20.000:2020.

13.9.3.2. Atribuições

- 13.9.3.2.1. Gerir as equipes alocadas para execução dos serviços, garantindo capacitação e alinhamento estratégico.
- 13.9.3.2.2. Utilizar software de gerenciamento de serviços para controle de incidentes, problemas e chamados.
- 13.9.3.2.3. Capacitar os recursos humanos no uso de ferramentas de service desk e ITSM.
- 13.9.3.2.4. Manter e atualizar documentação da infraestrutura de TI, redes, servidores e processos.
- 13.9.3.2.5. Implementar e auditar processos ITIL® V4 na gestão de configuração, incidentes e níveis de serviço.
- 13.9.3.2.6. Elaborar relatórios técnicos e gerenciais para análise de desempenho.
- 13.9.3.2.7. Avaliar impacto e riscos antes de qualquer alteração no ambiente do Data Center.

13.9.4. Suporte Técnico de Operação

13.9.4.1. Descrição Geral

13.9.4.1.1. A equipe de Suporte Técnico de Operação será responsável pelo monitoramento contínuo da infraestrutura de Datacenter, Redes e Segurança da CONTRATANTE, atuando também como NOC (Network Operations Center) e SOC (Security Operations Center), garantindo disponibilidade ininterrupta dos serviços essenciais.

13.9.4.2. Atribuições

- 13.9.4.2.1. Monitorar servidores Windows e Linux, bancos de dados, correio eletrônico, armazenamento e backups.
- 13.9.4.2.2. Atuar no monitoramento pró-ativo da segurança da infraestrutura.
- 13.9.4.2.3. Gerenciar e responder a incidentes de forma ágil e eficaz.
- 13.9.4.2.4. Realizar a configuração e manutenção da ferramenta de monitoramento Zabbix.
- 13.9.4.2.5. Monitorar e administrar a futura ferramenta de observabilidade definida pela CONTRATANTE.
- 13.9.4.2.6. Avaliar e priorizar chamados, garantindo respostas ágeis e eficazes.
- 13.9.4.2.7. Garantir disponibilidade 24x7 para tratamento de incidentes.

13.9.5. Suporte Técnico às Demandas e Mudanças de TIC

13.9.5.1. Descrição Geral

13.9.5.1.1. A equipe será responsável pela administração, monitoramento e otimização das redes, servidores e bancos de dados, além de implementar políticas de proteção cibernética e responder a incidentes.

13.9.5.2. Atribuições

- 13.9.5.2.1. Gerenciar ambientes Windows e Linux, garantindo sua alta disponibilidade.
- 13.9.5.2.2. Administrar a plataforma de virtualização ProxMox e a orquestração de containers com Rancher.
- 13.9.5.2.3. Monitorar e otimizar bancos de dados.
- 13.9.5.2.4. Suporte avançado ao Service Desk e Desenvolvimento.
- 13.9.5.2.5. Aplicação de atualizações e patches de segurança.
- 13.9.5.2.6. Realizar testes de invasão e auditorias para identificar vulnerabilidades.

13.9.6. Suporte Técnico às Demandas e Mudanças de TIC

13.9.6.1. Descrição Geral

13.9.6.1.1. A equipe será responsável pela administração, monitoramento e otimização das redes, servidores e bancos de dados, além de implementar políticas de proteção cibernética e responder a incidentes.

13.9.6.2. Atribuições

- 13.9.6.2.1. Gerenciar ambientes Windows e Linux, garantindo sua alta disponibilidade.
- 13.9.6.2.2. Administrar a plataforma de virtualização ProxMox e a orquestração de containers com Rancher.
- 13.9.6.2.3. Monitorar e otimizar bancos de dados.
- 13.9.6.2.4. Suporte avançado ao Service Desk e Desenvolvimento.
- 13.9.6.2.5. Aplicação de atualizações e patches de segurança.
- 13.9.6.2.6. Realizar testes de invasão e auditorias para identificar vulnerabilidades.
- 13.9.6.2.7. Gerenciamento de Patches e Vulnerabilidades de Endpoints
- 13.9.6.2.8. O serviço de Gerenciamento de Patches e Vulnerabilidades de Endpoints será responsável pela implementação e monitoramento contínuo da aplicação de patches em sistemas operacionais, softwares e endpoints da CONTRATANTE. Essa atividade visa mitigar vulnerabilidades e riscos de

segurança, garantindo um ambiente atualizado e protegido contra ameaças cibernéticas.

13.9.6.3. A CONTRATADA deverá utilizar ferramentas de CMDB (Configuration Management Database) e Patch Management, sendo responsável por propor, justificar e implementar soluções compatíveis que estejam alinhadas com as diretrizes e políticas da PMESP.

13.9.6.4. Configurar e gerenciar soluções de segurança de endpoint e de gerenciamento de identidade e acesso (IAM), incluindo o Active Directory (AD), antivírus (AV), proteção de endpoint (EPP) e resposta a ameaças em Endpoint (EDR), para assegurar o controle e a proteção dos dispositivos na rede.

13.9.6.5. A CONTRATADA poderá administrar e configurar além das soluções elencadas, propor a adoção de novas soluções de segurança desde que sejam OPEN SOURCE.

13.9.6.6. Monitoramento e Resposta a Ameaças nos Endpoints

13.9.6.7. Realizar a análise contínua de alertas e logs gerados pelas soluções de EPP (Endpoint Protection Platform) e

13.9.6.8. Responder de forma proativa a incidentes de segurança detectados nos endpoints, mitigando ameaças potenciais de maneira rápida e eficaz.

13.9.6.9. Estabelecer e revisar periodicamente as regras de acesso a sistemas e áreas da rede, garantindo a proteção e integridade dos dados.

13.9.6.10. Inventário e Gestão de Ativos Críticos

13.9.6.11. A CONTRATADA deverá realizar o mapeamento e a atualização contínua de sistemas e ativos, conforme as seguintes diretrizes:

13.9.6.11.1.1. Ativos críticos (servidores, firewalls, bancos de dados, sistemas essenciais): atualização trimestral.

13.9.6.11.1.2. Ativos de rede (switches, roteadores, access points, VPNs): atualização trimestral/semestral.

13.9.6.11.1.3. Endpoints (estações de trabalho, notebooks, dispositivos móveis, impressoras de rede): atualização semestral/anual.

13.9.6.11.1.4. Software e Licenciamento: atualização semestral/anual.

13.9.6.11.1.5. Equipamentos obsoletos ou desativados: atualização imediata no inventário após a baixa do ativo.

13.9.7. Gestão de Segurança e Conformidade

13.9.7.1. Trabalhar em conjunto com outros departamentos para priorizar iniciativas de segurança, de acordo com riscos pré-identificados, fundamentadas em uma gestão robusta de riscos.

13.9.7.2. Planejar e atuar proativamente em respostas a incidentes e investigações de violações, colaborando com medidas corretivas e auditorias de segurança.

13.9.7.3. Padronizar e racionalizar procedimentos de segurança e controle, com foco na implantação de sistemas eficientes e no processamento eletrônico de dados, assegurando acesso rápido e preciso às informações.

13.9.8. Suporte Técnico de Análise de Ameaças Cibernéticas

13.9.8.1. Descrição Geral

13.9.8.1.1. Este serviço será responsável por monitorar continuamente a infraestrutura de TI da CONTRATANTE para detectar, responder e mitigar ameaças de segurança.

13.9.8.2. Atribuições

13.9.8.2.1. Utilizar ferramentas de segurança para monitoramento contínuo de ameaças.

13.9.8.2.2. Analisar e investigar incidentes de segurança e coletar evidências.

13.9.8.2.3. Implementar processos de resposta a incidentes, contenção e recuperação.

13.9.8.2.4. Coletar dados de fontes internas e externas para identificar possíveis ameaças cibernéticas, utilizando técnicas de OSINT (Open Source Intelligence) para monitoramento de informações disponíveis em fontes abertas, como redes sociais, fóruns e deep/dark web, visando antecipar riscos e identificar vazamentos de dados sensíveis relacionados à CONTRATANTE

13.9.8.2.5. Realizar auditorias de segurança e propor medidas de mitigação, incluindo a execução de teste de penetração PENTEST (Penetration Testing) interno e externo para simular ataques cibernéticos e identificar vulnerabilidades em sistemas, redes e aplicações da CONTRATANTE.

13.9.8.2.6. Implementar práticas de WEBSEC (Web Security) para proteger aplicações web da CONTRATANTE contra ameaças como injeção de código, XSS (Cross-Site Scripting) e outras vulnerabilidades listadas no OWASP Top 10, assegurando a integridade e a confidencialidade dos serviços online;

13.9.8.2.7. Executar testes de DAST (Dynamic Application Security Testing) em aplicações em produção para identificar falhas de segurança em tempo real, complementando as auditorias estáticas e garantindo a robustez das soluções TIC frente a ataques dinâmicos;

13.9.9. Suporte Técnico de Infraestrutura de Banco de Dados

13.9.9.1. Descrição Geral

13.9.9.1.1. O serviço de Suporte Técnico de Infraestrutura de Banco de Dados será responsável por garantir a administração, segurança, desempenho e disponibilidade dos bancos de dados da CONTRATANTE. Esse serviço incluirá atividades de monitoramento contínuo, implementação de políticas de backup, controle de acessos, otimização de desempenho e suporte técnico avançado.

13.9.9.2. Atribuições

13.9.9.2.1. Gerenciamento de Banco de Dados

13.9.9.2.2. Administrar os bancos de dados utilizados pela CONTRATANTE, assegurando sua integridade, segurança e alta disponibilidade.

13.9.9.2.3. Monitorar continuamente a performance dos bancos de dados e identificar possíveis gargalos.

13.9.9.2.4. Implementar políticas de gerenciamento de acessos, garantindo conformidade com normas de segurança.

13.9.9.2.5. Políticas de Backup e Recuperação de Dados

13.9.9.2.6. Definir, atualizar e documentar as políticas de backup dos SGBDs (Sistemas de Gerenciamento de Banco de Dados).

13.9.9.2.7. Realizar testes periódicos de restauração para garantir a recuperação eficiente de dados.

13.9.9.2.8. Assegurar a proteção contra perda de dados, implementando estratégias de redundância.

13.9.9.2.9. Gestão de Permissões e Controle de Acesso

13.9.9.2.10. Controlar e gerenciar permissões de usuários e aplicações.

13.9.9.2.11. Criar e manter um registro detalhado dos acessos aos bancos de dados.

13.9.9.2.12. Garantir que todas as permissões estejam alinhadas às políticas de segurança.

13.9.9.3. Administração e Configuração de SGBD

- 13.9.9.3.1. Instalar e configurar sistemas de gerenciamento de banco de dados conforme padrões estabelecidos.
- 13.9.9.3.2. Ajustar parâmetros de rede e segurança para otimizar o funcionamento dos SGBDs.
- 13.9.9.3.3. Gerenciar o ciclo de vida dos bancos de dados, incluindo criação, manutenção e descontinuação.
- 13.9.9.3.4. Aplicação de Atualizações e Patches de Segurança
- 13.9.9.3.5. Implementar atualizações de software e patches de segurança nos SGBDs.
- 13.9.9.3.6. Monitorar vulnerabilidades e corrigir falhas identificadas.
- 13.9.9.3.7. Garantir que os sistemas estejam protegidos contra ameaças cibernéticas.
- 13.9.9.3.8. Suporte Técnico e Atendimento de Incidentes
- 13.9.9.3.9. Fornecer suporte de terceiro nível para equipes de Service Desk e Desenvolvimento.
- 13.9.9.3.10. Resolver problemas técnicos complexos relacionados ao ambiente de banco de dados.
- 13.9.9.3.11. Documentar soluções e boas práticas para referência futura.
- 13.9.9.4. Gestão de Desempenho e Otimização
 - 13.9.9.4.1. Monitorar e analisar métricas de desempenho dos bancos de dados.
 - 13.9.9.4.2. Implementar estratégias para otimizar consultas SQL e melhorar a eficiência dos sistemas.
 - 13.9.9.4.3. Ajustar índices e estrutura de tabelas para reduzir a latência e aumentar a performance.
- 13.9.9.5. Planejamento e Migração de Dados
 - 13.9.9.5.1. Executar processos de migração de bancos de dados com garantia de integridade e segurança.
 - 13.9.9.5.2. Planejar e coordenar projetos de atualização e migração tecnológica.
 - 13.9.9.5.3. Avaliar ferramentas de migração e definir as melhores abordagens para transições seguras.
- 13.9.9.6. Desenvolvimento e Execução de Scripts SQL
 - 13.9.9.6.1. Criar e manter scripts para automação de processos de banco de dados.
 - 13.9.9.6.2. Desenvolver e otimizar stored procedures, triggers e funções SQL.
 - 13.9.9.6.3. Executar auditorias para identificar melhorias e implementar correções em estruturas de dados.
- 13.9.9.7. Relatórios de Impacto e Análise de Riscos
 - 13.9.9.7.1. Elaborar relatórios técnicos sobre riscos e impactos de mudanças na infraestrutura de banco de dados.
 - 13.9.9.7.2. Garantir a documentação detalhada das alterações implementadas.
 - 13.9.9.7.3. Avaliar possíveis impactos de novas implementações no ambiente de produção.
- 13.9.9.8. Gestão de Consistência e Integridade dos Dados
 - 13.9.9.8.1. Implementar rotinas de verificação de integridade dos bancos de dados.
 - 13.9.9.8.2. Detectar e corrigir anomalias ou inconsistências nos registros armazenados.
 - 13.9.9.8.3. Monitorar continuamente a integridade lógica e física dos dados.
- 13.9.9.9. Segurança e Conformidade
 - 13.9.9.9.1. Trabalhar em conjunto com a equipe de segurança para mitigar riscos de vazamento ou perda de dados.
 - 13.9.9.9.2. Assegurar conformidade com regulamentações de segurança, incluindo a LGPD e outras normas aplicáveis.
 - 13.9.9.9.3. Implementar criptografia e outras técnicas de proteção de dados sensíveis.
- 13.9.9.10. Avaliação e Implementação de Novas Tecnologias
 - 13.9.9.10.1. Conduzir testes de novas tecnologias para aprimorar a eficiência e escalabilidade dos bancos de dados.
 - 13.9.9.10.2. Avaliar a viabilidade de implementação de novas ferramentas ou metodologias.
 - 13.9.9.10.3. Propor melhorias contínuas para manter a infraestrutura alinhada às melhores práticas do mercado.
- 13.9.9.11. Colaboração em Projetos de Infraestrutura
 - 13.9.9.11.1. Trabalhar em conjunto com equipes de TI na definição de requisitos para novos projetos.
 - 13.9.9.11.2. Fornecer suporte técnico para decisões estratégicas envolvendo bancos de dados.
 - 13.9.9.11.3. Integrar bancos de dados com outras plataformas de TI para otimizar processos internos.
- 13.9.10. Desenvolvimento Seguro de Software
 - 13.9.10.1. Descrição Geral
 - 13.9.10.1.1. O serviço de Desenvolvimento Seguro de Software será responsável por implementar princípios de segurança em todas as etapas do ciclo de desenvolvimento, garantindo a proteção contra vulnerabilidades e ameaças. Esse serviço engloba a análise de código, implementação de automação de segurança e auditoria de aplicações.
 - 13.9.10.2. Atribuições
 - 13.9.10.2.1. Implementar práticas de segurança em todas as fases do ciclo de desenvolvimento de software, incluindo automação de verificações em pipelines CI/CD.
 - 13.9.10.2.2. Identificar, monitorar e corrigir vulnerabilidades em código-fonte e infraestrutura de TI.
 - 13.9.10.2.3. Implementar ferramentas de monitoramento e resposta em tempo real para detecção e mitigação de ameaças.
 - 13.9.10.2.4. Desenvolver e manter scripts e automações para tarefas de segurança, como auditorias de acessos e análise de logs.
 - 13.9.10.2.5. Assegurar conformidade com normas e políticas de segurança da CONTRATANTE, realizando auditorias periódicas.
 - 13.9.10.2.6. Projetar e implementar APIs seguras, incluindo autenticação, autorização e proteção contra-ataques cibernéticos, utilizando práticas de WEBSEC (Web Security) para mitigar vulnerabilidades específicas de aplicações web e assegurar conformidade com padrões de segurança.
- 13.9.11. Teste de Penetração
 - 13.9.11.1. Conduzir testes de segurança manuais e automatizados, como testes de penetração PENTEST e análise de código dinâmico e estático, incorporando DAST (Dynamic Application Security Testing) para avaliar a segurança de aplicações em execução e identificar vulnerabilidades exploráveis em tempo real.
 - 13.9.11.2. Desenvolver documentação técnica contendo diretrizes de codificação segura e gestão de vulnerabilidades.
- 13.9.12. Arquitetura de Soluções de Inteligência Artificial
 - 13.9.12.1. Descrição Geral
 - 13.9.12.1.1. O serviço de Arquitetura de Soluções de Inteligência Artificial será responsável por projetar e implementar soluções baseadas em IA

garantindo escalabilidade, segurança e conformidade com regulamentos de privacidade e ética.

13.9.12.2. Atribuições

- 13.9.12.2.1. Projetar soluções de IA alinhadas aos objetivos da CONTRATANTE, garantindo escalabilidade e segurança.
- 13.9.12.2.2. Selecionar frameworks e plataformas apropriadas para IA, como TensorFlow, PyTorch e serviços de nuvem.
- 13.9.12.2.3. Identificar casos de uso onde a IA pode agregar valor, como automação, análise preditiva e visão computacional.
- 13.9.12.2.4. Criar e treinar modelos de aprendizado de máquina personalizados, otimizados para os desafios específicos da CONTRATANTE.
- 13.9.12.2.5. Desenvolver APIs e microsserviços para integração de modelos de IA em aplicações e sistemas corporativos.
- 13.9.12.2.6. Monitorar continuamente o desempenho dos modelos em produção, implementando estratégias de retreinamento e ajuste.
- 13.9.12.2.7. Garantir conformidade com a LGPD e outras regulamentações, assegurando a ética no uso de IA.
- 13.9.12.2.8. Estabelecer KPIs para medir o impacto das soluções de IA nos processos de negócio.

13.9.13. Segurança de Redes e Infraestrutura

13.9.13.1. Descrição Geral

13.9.13.1.1. O serviço de Segurança de Redes e Infraestrutura será responsável por gerenciar e proteger os dispositivos de rede, garantir a conformidade das configurações de segurança e monitorar continuamente vulnerabilidades e ameaças.

13.9.13.2. Atribuições

- 13.9.13.2.1. Gerenciar configurações de dispositivos de rede, garantindo segurança e alta disponibilidade.
- 13.9.13.2.2. Implementar configurações LAN, WAN e SAN conforme as necessidades da CONTRATANTE.
- 13.9.13.2.3. Aplicar patches e atualizações de segurança em dispositivos e sistemas de rede.
- 13.9.13.2.4. Monitorar logs de rede para identificar tráfegos anormais e ameaças potenciais.
- 13.9.13.2.5. Desenvolver regras no SIEM para aprimorar a detecção de anomalias de segurança.
- 13.9.13.2.6. Implementar processos de controle de acesso para áreas críticas da rede.
- 13.9.13.2.7. Executar testes de penetração internos e externos para avaliar vulnerabilidades em redes e infraestrutura críticas, propondo medidas de mitigação baseadas nos resultados.
- 13.9.13.2.8. Gerenciar e operar firewalls, VPNs, proxies e sistemas de filtragem de URL.
- 13.9.13.2.9. Desenvolver, documentar e atualizar as políticas de segurança de rede, alinhadas às diretrizes da CONTRATANTE.
- 13.9.13.2.10. Realizar auditorias de segurança para garantir conformidade com padrões e regulamentações do setor, utilizando dados coletados por meio do OSINT (Open Source Intelligence) para contextualizar ameaças externas e fortalecer a proteção contra adversários identificados em fontes abertas.

13.9.14. Serviços Técnicos Avançados

13.9.14.1. Descrição Geral

13.9.14.1.1. Os Serviços Técnicos Avançados fornecerão suporte especializado em diagnósticos críticos, projetos estratégicos e conformidade com normas de segurança.

13.9.14.2. Atribuições

- 13.9.14.2.1. Desenvolver projetos estratégicos de modernização de infraestrutura.
- 13.9.14.2.2. Implementar soluções de inteligência artificial, IoT e computação em nuvem.
- 13.9.14.2.3. Realizar avaliações de conformidade com normas como LGPD e ISO 27001.
- 13.9.14.2.4. Criar arquiteturas de segurança baseadas em "confiança zero".

13.9.15. Suporte Técnico de Infraestrutura Data Center e Redes

13.9.15.1. O Suporte Técnico de Infraestrutura Data Center e Redes será responsável pela gestão integrada da infraestrutura de redes e cabeamento estruturado que suporta o ambiente de tecnologia da informação e comunicação (TIC) da Polícia Militar do Estado de São Paulo (PMESP). Os analistas da CONTRATADA atuarão na instalação, organização e manutenção do cabeamento estruturado em conformidade com os padrões técnicos e normativos, incluindo suporte às operações de expansão e atualização em Data Centers e outros locais estratégicos, com referência a parte lógica, serão responsáveis pela administração, monitoramento e otimização das redes em unidades da CONTRATANTE, assegurando alta disponibilidade, desempenho e segurança conforme as melhores práticas da ITIL 4.

13.9.15.2. Atribuições Principais:

- 13.9.15.2.1. Realizar a instalação, organização e manutenção de cabos estruturados para redes de dados e sistemas relacionados, assegurando conformidade com padrões técnicos, como ANSI/TIA/EIA. O técnico será responsável pela identificação, roteamento, crimpagem e terminação de cabos, incluindo UTP e STP, conforme as necessidades do projeto.
- 13.9.15.2.2. Efetuar testes e diagnósticos em cabeamentos existentes utilizando ferramentas específicas, como testadores de cabos. Identificar falhas ou degradações no desempenho da rede causadas por cabeamentos, realizando reparos ou substituições para restabelecer a funcionalidade com o mínimo de interrupção.
- 13.9.15.2.3. A CONTRATADA deverá fornecer, conforme necessidade, materiais essenciais para manutenção e instalação, incluindo cabos de rede CAT6A ou superior, não superior a 2 caixas por mês, sob demanda, Patch Panels, Patch Cords, Keystones, organizadores de cabos, conectores RJ45, entre outros componentes essenciais, sob demanda.
- 13.9.15.2.4. Executar fusões de fibra óptica ao ano para garantir a integridade e estabilidade das conexões de rede, conforme demandas identificadas nas unidades da CONTRATANTE. O prazo máximo para a execução deste serviço será de três dias após a solicitação.
- 13.9.15.2.5. Assegurar a organização de racks, patch panels, bandejas e dutos, aplicando boas práticas de gerenciamento de cabos para garantir um ambiente limpo, acessível e de fácil manutenção. Isso inclui rotulagem, documentação precisa da infraestrutura e conformidade com padrões regulatórios.
- 13.9.15.2.6. Monitorar continuamente a infraestrutura de rede utilizando ferramentas de gerenciamento, identificando anomalias e pontos de falha, propondo ações corretivas sob supervisão para garantir o desempenho ideal dos serviços de rede, como conectividade, latência e disponibilidade.
- 13.9.15.2.7. Auxiliar na instalação, configuração e atualização de dispositivos de rede, incluindo switches, roteadores, access points e firewalls, garantindo a aplicação de configurações seguras e alinhadas às políticas internas da CONTRATANTE.
- 13.9.15.2.8. Executar rotinas de manutenção preventiva e corretiva, como inspeções físicas de cabos e dispositivos, atualização de firmware e limpeza de racks, documentando todas as ações realizadas.

13.9.15.2.9. Administrar o CMDB (Configuration Management Database), garantindo registro detalhado das configurações de todos os dispositivos de rede, histórico de alterações, monitoramento contínuo da conformidade das configurações e integração com ferramentas de ITSM (IT Service Management).

13.9.15.2.10. Atualizar e manter registros detalhados da infraestrutura de rede, incluindo mapas de topologia, configurações de dispositivos, políticas de roteamento e listas de inventário.

13.9.15.2.11. Participar ativamente de projetos de expansão ou atualização da infraestrutura, apoiando na configuração e implementação de novos dispositivos e tecnologias, como VLANs, redes de alta disponibilidade e integração com soluções em nuvem.

13.9.15.2.12. Realizar visitas técnicas para manutenções preventivas e vistorias em locais da CONTRATANTE, garantindo o funcionamento ideal dos sistemas e equipamentos.

13.9.15.2.13. Configurar dispositivos novos e existentes, garantindo conformidade com padrões estabelecidos e escalando incidentes mais complexos para níveis superiores quando necessário.

13.9.15.2.14. Implementar e manter a administração e configuração de soluções de segurança de rede, incluindo firewalls, VPNs, proxies e sistemas de filtragem de conteúdo, garantindo proteção contínua da infraestrutura.

13.9.15.2.15. Desenvolver, documentar e implementar políticas de segurança de rede, normas e procedimentos para fortalecer a proteção contra ameaças, assegurando um ambiente seguro.

13.9.15.2.16. Executar testes de segurança e varreduras em ativos de rede, realizando auditorias periódicas para identificar vulnerabilidades e implementar medidas corretivas.

13.9.15.2.17. Apoiar a configuração e operação de ferramentas de monitoramento e observabilidade, garantindo a visibilidade da infraestrutura de rede e segurança da CONTRATANTE.

13.9.15.2.18. Gerenciar chamados técnicos e monitorar soluções providas por terceiros, garantindo a rastreabilidade e controle adequado dos serviços prestados.

13.9.15.2.19. Criar relatórios detalhados e dashboards interativos que consolidem indicadores de desempenho, compliance e segurança da infraestrutura de rede, fornecendo informações estratégicas para tomada de decisão.

13.9.15.2.20. Garantir rastreabilidade completa no ITSM, com logs imutáveis, workflow de aprovação, e vínculo entre incidentes, problemas e mudanças da CONTRATANTE, mantendo um histórico claro e organizado de todas as operações realizadas

13.10. Modelos de Gestão e Operação

13.10.1. Fluxo de Atendimento

13.10.1.1. O Fluxo de Atendimento estabelece os procedimentos para o suporte eficaz às demandas da Polícia Militar do Estado de São Paulo - PMESP. Todas as solicitações devem ser registradas e tratadas exclusivamente na ferramenta de ITSM da CONTRATANTE, garantindo um acompanhamento sistemático e eficiente de cada demanda.

13.10.1.2. Este fluxo incluirá as etapas de registro, triagem, priorização e resolução das solicitações, assegurando que todas as interações sejam documentadas de forma clara. A equipe especializada da CONTRATADA será responsável por monitorar as solicitações em tempo real, promovendo uma comunicação transparente e atualizada com os usuários.

13.10.1.3. Início: Abertura de Requisições conforme categorização ITIL: Request, Incident, Change ou Problem;

13.10.1.4. Processo: Chamado registrado via portal de autoatendimento ou chatbot (quando aplicável), com campos obrigatórios definidos por tipo de requisição e vinculado ao catálogo de serviços.

13.10.1.5. Decisão: O chamado é analisado, classificado pela Central de Serviços e direcionado para a equipe de acordo com os scripts de atendimento e com o Catálogo de Serviços.

13.10.1.6. Validação das informações contidas no chamado:

13.10.1.7. Processo: O colaborador na posição de dispatcher fará a análise do chamado e a validação do correto preenchimento;

13.10.1.8. Decisão: O chamado é relacionado a:

13.10.1.9. Opção 1: Suporte Técnico de Operação

13.10.1.10. Problemas relacionados a operações, funcionamento diário, entre outros.

13.10.1.11. Opção 2: Suporte Técnico de Infraestrutura de Data Center e Redes

13.10.1.12. Problemas relacionados a infraestrutura, monitoramento, cabeamento, redes, entre outros.

13.10.1.13. Opção 3: Suporte Técnico às Demandas e Mudanças de TIC

13.10.1.14. Problemas relacionados a infraestrutura, servidores, redes, indisponibilidade de recursos, liberações de acesso, criação e configuração de ambiente e serviços, entre outros.

13.10.1.15. Opção 4: Suporte Técnico de Análise de Ameaças Cibernéticas

13.10.1.16. Problemas relacionados a infraestrutura, servidores, redes, entre outros.

13.10.1.17. Fluxo para Suporte Técnico de Operações, Suporte Técnico de Infraestrutura de Data Center e Redes, Suporte Técnico às Demandas e Mudanças de TIC ou Suporte Técnico de Análise de Ameaças Cibernéticas

13.10.1.18. Processo: Chamado encaminhado para analista responsável pelo atendimento, de acordo com o script de atendimento, disponibilidade e Catálogo de Serviços.

13.10.1.19. Decisão: O problema pode ser resolvido diretamente?

13.10.1.20. Sim: Realiza ação, registro e encerra o chamado com solução registrada.

13.10.1.21. Não: Escalar para analista/equipe especializada, com nível superior de conhecimento ou direcionamento para equipe competente visando a resolução adequada da requisição.

13.10.1.22. Escalamento (se necessário):

13.10.1.23. Processo: Caso não resolvido em primeira instância, o chamado é escalado para especialistas ou equipe competente.

13.10.1.24. Decisão: Problema resolvido com a escalada?

13.10.1.25. Sim: Encerrar chamado.

13.10.1.26. Não: Avaliar necessidade de escalar para Equipe Externa ou Outros Fornecedores.

13.10.1.27. Encerramento e Feedback:

13.10.1.28. Processo: Quando resolvido, o chamado é encerrado e documentado.

13.10.1.29. Processo: O usuário recebe feedback sobre a solução aplicada.

13.11. Serviços de SOC:

13.11.1. O Serviço de SOC (Security Operations Center) consiste em um conjunto de ferramentas e serviços de cibersegurança prestados para o ambiente da PMESP, com o objetivo de fornecer observabilidade contínua e respostas imediatas a ameaças, ataques cibernéticos e tentativas de invasão.

13.11.2. O SOC deverá dispor de capacidade técnica e ferramentas para a realização de análises forenses digitais, engenharia reversa de binários suspeitos e análise comportamental de arquivos maliciosos identificados nos endpoints. Para isso, recomenda-se a integração com ferramentas como Cuckoo Sandbox, REMnux, Velociraptor ou soluções equivalentes, permitindo análises automáticas e on-demand de arquivos coletados nos incidentes.

13.11.3. A prestação dos serviços deverá ocorrer de forma contínua e ininterrupta, sob regime 24x7x365, dentro das dependências da CONTRATADA, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018). A CONTRATADA deverá atuar presencialmente nas dependências do CONTRATANTE sempre que solicitado ou em casos de incidentes de segurança que exijam acompanhamento técnico especializado.

13.11.4. As respostas a incidentes deverão ocorrer nos tempos máximos informados no item que trata do nível de acordo de serviços (SLA).

13.11.5. O ambiente de administração dos serviços do SOC deverá atender aos seguintes requisitos mínimos:

Controle de Acesso e Segurança Física:

Implementação de sistemas de controle de acesso físico e monitoramento ambiental, com capacidade de rastreamento de pessoas e recuperação de registros e imagens.

Armazenamento de vídeos da área por, no mínimo, 90 dias.

Manutenção de registros de entrada e saída de pessoas e visitantes, com identificação única, por no mínimo 90 dias.

Controle de acesso físico com, no mínimo, dois fatores de autenticação.

13.11.6. Segurança e Continuidade Operacional:

Implementação de solução de monitoramento de disponibilidade e desempenho.

Proteção do perímetro contra intrusões e acessos indevidos.

Vigilância ininterrupta por segurança especializada, 24x7x365.

Configuração do ambiente para garantir que a falha de um único equipamento não interrompa os serviços.

13.11.7. Conformidade com Normas Técnicas:

O serviço de SOC deverá ser atendido observando a conformidade com as seguintes normas e boas práticas internacionais:

ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação.

ISO/IEC 20000 – Gestão de Qualidade de Serviços de TI

ISO 27017 – Controles de segurança para serviços em nuvem.

13.11.8. Gestão de Risco e Monitoramento Contínuo:

13.11.8.1. A CONTRATADA deverá realizar avaliações periódicas do nível de risco do ambiente computacional do CONTRATANTE, contemplando:

13.11.8.2. Identificação e análise dos indicadores de risco.

13.11.8.3. Realização de testes de vulnerabilidades ao menos trimestralmente e com ferramentas reconhecidas no mercado, tais como Nessus, Qualys, OpenVAS ou equivalentes.

13.11.8.4. Apresentação de recomendações de mitigação, incluindo aplicação de patches e correções.

13.11.8.5. O SOC deverá implementar processos contínuos de monitoramento em fontes abertas e na deep e dark web utilizando OSINT para identificar vazamentos de credenciais, dados sensíveis ou menções relacionadas à CONTRATANTE.

13.11.8.6. Utilizar ferramentas especializadas para rastrear possíveis exposições e gerar alertas proativos, complementando com PENTEST (Penetration Testing) periódico para validar a eficácia das defesas contra ameaças identificadas.

13.11.9. Dashboard e Indicadores de Risco:

13.11.9.1. O serviço de SOC deverá disponibilizar um dashboard centralizado, com os seguintes indicadores:

13.11.9.2. Top vulnerabilidades presentes no ambiente computacional do CONTRATANTE.

13.11.9.3. Top ativos com índice de risco elevado.

13.11.9.4. Top hosts afetados por detecção do XDR.

13.11.9.5. Top usuários com maior índice de risco.

13.11.9.6. Principais táticas e técnicas do MITRE ATT&CK detectadas no ambiente.

13.11.9.7. O SOC deverá desenvolver relatórios técnicos detalhados contendo análises de ameaças, tendências de ataques e perfis de adversários, além de criar e disseminar Indicadores de Comprometimento (IOCs) para auxiliar outras equipes na detecção e resposta a incidentes.

13.11.10. Índice de alertas avançados.

13.11.11. Métricas de severidade de riscos, classificadas de baixo a crítico.

13.11.12. Aplicação de Controles de Segurança:

13.11.12.1. A CONTRATADA será responsável pela aplicação de controles de segurança adequados, garantindo a confidencialidade das informações do CONTRATANTE. Para isso, deverá utilizar:

13.11.12.2. Algoritmos e chaves criptográficas robustos e reconhecidos pelo mercado.

13.11.12.3. Proteção contra vazamento de dados armazenados ou transmitidos.

13.11.12.4. Sempre que identificar falhas na implementação de serviços, que tornem o ambiente vulnerável, a CONTRATADA deverá comunicar formalmente o CONTRATANTE, propondo medidas corretivas.

13.11.12.5. O SOC deverá realizar periodicamente o mapeamento das regras de segurança da rede, incluindo a elaboração de relatórios técnicos, materiais de divulgação e suporte à gestão na criação de documentação oficial, como guias de melhores práticas e regras de segurança da informação.

13.11.13. Monitoramento e Resposta a Incidentes:

13.11.13.1. O serviço de SOC deverá garantir monitoramento contínuo e análise de logs, incluindo:

13.11.13.2. Coleta, correlação e análise de eventos de segurança.

13.11.13.3. Identificação de ataques cibernéticos em fases iniciais ou em andamento.

- 13.11.13.4. Acionamento imediato das equipes de resposta a incidentes para contenção e mitigação dos ataques.
 - 13.11.13.5. O monitoramento deverá ocorrer de forma proativa e contínua, utilizando:
 - 13.11.13.6. Plataformas de investigação avançadas, com machine learning e inteligência artificial.
 - 13.11.13.7. Modelos de inteligência do fabricante, permitindo análise aprofundada de incidentes.
 - 13.11.13.8. Interface web compatível com navegadores modernos, garantindo acesso a informações em tempo real.
 - 13.11.13.9. O monitoramento de ameaças será realizado por meio de uma solução SIEM integrada com uma plataforma de Threat Intelligence, permitindo a correlação de eventos e detecção proativa de atividades suspeitas.
 - 13.11.13.10. Incorporar técnicas de WEBSEC (Web Security) no monitoramento de aplicações web críticas, garantindo a detecção de ameaças específicas como ataques de injeção ou exploração de vulnerabilidades OWASP;
 - 13.11.13.11. Utilizar DAST (Dynamic Application Security Testing) como parte da estratégia de monitoramento contínuo, permitindo a identificação de vulnerabilidades em aplicações em tempo real e a resposta imediata a incidentes relacionados
- 13.11.14. Interface e Relatórios Gerenciais:
- 13.11.14.1. A solução deverá disponibilizar uma interface web, compatível com os navegadores mais recentes, para acompanhamento das atividades do SOC, incluindo:
 - 13.11.14.1.1. Métricas e gráficos de risco, permitindo a análise visual dos dados.
 - 13.11.14.1.2. Deve ser possível gerar relatórios detalhados sobre incidentes detectados, tratativas e recomendações de segurança.
 - 13.11.14.1.3. Geração de logs auditáveis, garantindo rastreabilidade das ações realizadas.
 - 13.11.14.2. O serviço deve contemplar um ou mais Centros de Operações de Segurança (SOC), operando em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano), tendo um grupo motor gerador e nobreak, ou 1 (um) Centro de Operações de Segurança (SOC) que garanta disponibilidade dos serviços com no mínimo dois links de internet, tendo um grupo motor gerador e nobreak, também operando em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano);
 - 13.11.14.3. A Contratada deverá realizar verificação da quantidade de pacotes baseada em EPS efetivamente consumida pela CONTRATANTE com utilização da ferramenta utilizada pelo contratante no levantamento inicial, de forma a apresentar consumo efetivo mensal, desde o faturamento inicial e mensalmente até o final do contrato, para fins de emissão de cada faturamento.
 - 13.11.14.4. A CONTRATADA deve prover níveis de segurança elevados, utilizando no SOC ferramentas para garantir a segurança dos dados manipulados, contemplando, no mínimo, os seguintes controles de segurança física e lógica:
 - 13.11.14.5. Solução de proteção de endpoints;
 - 13.11.14.6. Controle de acesso físico ao SOC, com a utilização de pelo menos 02 (dois) mecanismos de autenticação, sendo, no mínimo, um deles por biometria;
 - 13.11.14.7. Monitoramento por sistema interno de TV (CFTV), armazenando as imagens dos últimos 30 (trinta) dias;
 - 13.11.14.8. Todos os funcionários da CONTRATADA envolvidos na operação ou que possuam acesso às informações do CONTRATANTE devem assinar termo de responsabilidade e sigilo;
 - 13.11.14.9. A CONTRATADA deve disponibilizar toda a infraestrutura necessária para o monitoramento dos alertas de segurança realizado por seus analistas, em regime 24 X 7 (24 horas por dia, 7 dias da semana);
 - 13.11.14.10. O dimensionamento do ambiente foi realizado com base na metodologia que determina o quantitativo de eventos por segundo (EPS), para que analistas de segurança detectem, priorizem, investiguem e respondam rapidamente a ameaças em ambientes locais e baseados em nuvem. Os cálculos realizados consideraram o ambiente existente do CONTRATANTE, que engloba os diversos tipos de dispositivos de rede ativos, como servidores, roteadores, firewalls e etc.
 - 13.11.14.11. A CONTRATADA deve realizar as ações necessárias para identificação de incidentes de segurança por meio dos dados e alertas monitorados na Solução Integrada de SOC, que podem comprometer a segurança dos serviços e ativos do CONTRATANTE. A CONTRATADA deve analisar eventos detectados, classificar e categorizar conforme definição do CONTRATANTE. Identificar, registrar, escalar e notificar os incidentes de segurança ao CONTRATANTE para tratamento;
 - 13.11.14.12. A CONTRATADA é responsável pelas atividades de SOC, que para o modelo definido corresponde minimamente às atividades relacionadas abaixo:
 - 13.11.14.12.1. Definição de linha base (baseline) de forma a entender o comportamento normal do ambiente monitorado, ajustando métricas e limiares de detecção, com o objetivo de reduzir o número de falsos positivos e aumentar a precisão da detecção
 - 13.11.14.12.2. A ferramenta deve ser acompanhada de todos os itens necessários para operacionalização, tais como: softwares de apoio (sistema operacional, etc) e licenças de softwares;
 - 13.11.14.12.3. Os serviços prestados pelo SOC compreendem, entre outros, os seguintes procedimentos:
 - 13.11.14.12.4. Monitoramento proativo do ambiente de rede do CONTRATANTE;
 - 13.11.14.13. A CONTRATADA deverá agir de forma reativa para incidentes de segurança, restabelecimento do serviço o mais rápido possível minimizando o impacto, seja por meio de uma solução de contorno ou definitiva. Ainda caberá a CONTRATADA agir de forma proativa aplicando medidas para a boa manutenção a fim de garantir a regularidade da operação do serviço.
 - 13.11.14.14. A CONTRATADA deverá fornecer informações de monitoramento on-line, via dashboard que permita o acompanhamento em tempo real do estado dos ativos. Deverá ainda apresentar relatórios mensais, por meio digital (DOCX, XLSX ou PDF), com o diagnóstico e controle dos equipamentos monitorados (dados, informações, descrição, indicadores e métricas que permitam quantificar o desempenho e a disponibilidade da operação do serviço).
 - 13.11.14.15. A CONTRATADA deverá comunicar ao CONTRATANTE, os casos de eminente falha operacional dos equipamentos ou de qualquer outra ação que possa vir a colocar em risco a operação da rede dela, mesmo que a falha não tenha sido consumada, mas que tenha sido detectada a existência do risco.
 - 13.11.14.16. A CONTRATADA deverá respeitar os descritos no IMR e os tempos máximos de atendimentos e SLA (Nível de Acordo de Serviço) abaixo descritos, sob não cumprimento de contrato:
 - 13.11.14.16.1. Operação parada (incidente que gere parada total de algum serviço contemplado nesse contrato) o tempo de atendimento será de até 2 (duas) horas, incluindo o comparecimento de um profissional especializado ao local da sede da Contratante.
 - 13.11.14.16.2. Operação impactada (incidente que gere parada parcial de algum serviço contemplado nesse contrato) o tempo de atendimento será de

até 4 (quatro) horas, incluindo o comparecimento de um profissional especializado ao local da sede da Contratante;

13.11.14.16.3. Requisição de serviço (solicitações de mudanças nos equipamentos ou serviços do contrato) o tempo de atendimento será de até 8 (oito) horas.

13.11.14.16.4. Informações de contrato (solicitação de informação, parecer ou relatório de algum serviço contemplado no contrato) o tempo de atendimento será de até 24 (vinte e quatro) horas.

13.11.14.17. O CONTRATANTE é o responsável por definir o nível de criticidade do problema no momento da abertura do chamado técnico.

13.11.14.18. A abertura dos chamados para atendimento técnico deverá ser feita via telefone ou e-mail, além de sistema de Dispatcher via Internet com interface web. O sistema web de Dispatcher, deverá permitir o controle, por parte do CONTRATANTE, de todos os chamados e atendimentos realizados, em aberto ou fechados, além de permitir a emissão de relatórios estatísticos que mostrem o tipo de atendimento e quantidade de horas demandadas.

13.11.14.19. Após o atendimento técnico, a CONTRATADA só poderá dar por encerrado o chamado mediante a inspeção dos serviços e o respectivo aceite do CONTRATANTE.

13.11.14.20. Monitoração de alertas de segurança, onde o analista deve decidir se uma análise é necessária. A detecção consiste em avaliar os alertas de segurança dos sensores buscando indicadores de comportamentos maliciosos que ultrapassem os limiares estabelecidos no baseline. A lógica de detecção deve ser ajustada e desenvolvida, podendo passar a utilizar múltiplos eventos e diferentes fontes de dados. Os alertas devem indicar minimamente:

13.11.14.20.1. Ataques de força bruta com e sem sucesso;

13.11.14.20.2. Falhas de autenticação que indiquem suspeita de roubo de identidade;

13.11.14.20.3. Infecção de equipamentos por vírus;

13.11.14.20.4. Comprometimento de ativos da rede;

13.11.14.20.5. Realização de ações suspeitas por parte de usuários privilegiados;

13.11.14.20.6. Alertas de operação de serviços, como interrupções e falhas;

13.11.14.20.7. Ataques de negação de serviço;

13.11.14.20.8. Ataques comuns em aplicações WEB, como XSS e SQL injection;

13.11.14.20.9. Atividades de botnets;

13.11.14.20.10. Exploração de vulnerabilidades;

13.11.14.20.11. Detecção por análise de logs, onde o analista realiza pesquisas, revisões e análises estatísticas no histórico de log armazenado na Solução Integrada de SOC, com o objetivo de identificar comportamentos e evidências que indiquem atividades maliciosas ou novas ameaças.

13.11.14.21. Análise de eventos, onde o analista deve pesquisar informações adicionais que podem estar relacionadas ao evento em análise, que forneçam algum valor investigativo para identificar comportamentos anômalos ou maliciosos. A análise realizada nessa etapa é preliminar, tendo o objetivo de confirmar a ocorrência de um evento de segurança, eliminando falsos positivos confirmados. O resultado da análise pode ser uma das seguintes categorias:

13.11.14.21.1. Evento confirmado: os sensores detectaram corretamente uma ameaça válida. Os incidentes confirmados devem ser escalados para a etapa de mitigação da gestão de incidentes;

13.11.14.21.2. Falso positivo: ocorre quando o sistema detecta incorretamente uma ameaça ou não existe risco no evento detectado, sendo eventos alertados como maliciosos, mas não são;

13.11.14.21.3. Eventos autorizados: são ameaças detectadas corretamente, mas que são aprovadas pela política de segurança, como por exemplo, a análise de vulnerabilidades;

13.11.14.21.4. Indeterminado: quando não existe evidência suficiente para confirmar o evento de segurança;

13.11.14.22. Registro de análise, todo evento detectado que for selecionado para análise, deve ser registrado no Sistema de Ticket ofertado, incluindo as atividades de investigação. O resultado da análise pode ser a definição de um falso positivo, encerrando o tíquete, ou a confirmação de um incidente de segurança, escalando o tíquete para tratamento. O tíquete deve conter as seguintes informações:

13.11.14.22.1. Identificador do ticket;

13.11.14.22.2. Sensor que detectou o evento;

13.11.14.22.3. Identificador do evento gerado no sensor;

13.11.14.22.4. Limiar de detecção utilizado para enviar o evento para análise;

13.11.14.22.5. Log do evento detectado;

13.11.14.22.6. Origem e categoria do ataque;

13.11.14.22.7. Data e hora;

13.11.14.22.8. Triagem e Categorização de eventos;

13.11.14.23. Os tíquetes registrados devem ser priorizados por categorias, unificando os eventos potenciais de incidentes com as características em comum, que podem receber tratamento padronizado. Os eventos confirmados, classificados como incidente, devem ter seu tíquete escalado para os analistas do CONTRATANTE;

13.11.15. Elaboração de relatórios.

13.11.15.1. A CONTRATADA deverá disponibilizar relatórios em formato pdf, referentes aos indicadores monitorados com periodicidade mínima mensal, ou sob demanda, podendo incluir:

13.11.15.1.1. Classificação dos eventos de segurança;

13.11.15.1.2. Total de eventos avaliados;

13.11.15.1.3. Total de eventos escalados;

13.11.15.1.4. TOP aplicações mais impactadas, top origens dos eventos de segurança;

13.11.15.1.5. TOP endereços de destino das ameaças;

13.11.15.1.6. TOP URLs e suas categorias;

13.11.15.1.7. TOP atacantes, vulnerabilidades, ameaças, alarmes, violações de auditoria;

13.11.15.1.8. Principais tipos de ataques;

13.11.15.1.9. Descrição dos casos de uso utilizados para avaliar os alertas de segurança;

13.11.15.1.10. Novas informações de inteligência configuradas na ferramenta: como as novas regras de monitoramento, dashboards, assinaturas

instaladas, etc;

13.11.15.2. O Sistema de ticket ofertado deverá ser utilizado para registrar e escalar eventos de segurança, de modo a permitir o registro, envio de notificações e alertas entre as equipes do CONTRATANTE e da própria CONTRATADA;

13.11.15.3. O CONTRATANTE é responsável por avaliar os incidentes escalados após o processo de triagem inicial. Caso o incidente seja confirmado, o CONTRATANTE executará os seus processos e procedimentos internos para executar as medidas de contenção e correção, incluindo configurações nos sensores de segurança ou outros ativos. O CONTRATANTE registrará as ações realizadas no tíquete correspondente ao incidente, permitindo que a CONTRATADA esteja ciente do fechamento do mesmo;

13.11.15.4. Os analistas do CONTRATANTE responsáveis pelos tíquetes escalados devem possuir acesso total as informações do incidente relacionado;

13.11.15.5. Os analistas do CONTRATANTE devem poder contatar os analistas da CONTRATADA, por telefone ou via Sistema de Ticket, para consulta de informações em caso de qualquer dúvida sobre os eventos escalados e demais procedimentos para tratamento dos incidentes. As solicitações e respostas de informações adicionais sobre os incidentes, como logs e evidências, devem ser anexadas ao tíquete registrado na ferramenta;

13.11.15.6. O CONTRATANTE é responsável por fornecer informações de negócio adequadas, seguindo a regra do privilégio mínimo e necessidade de conhecer, para melhoria da atividade de monitoramento da CONTRATADA;

13.11.15.7. O CONTRATANTE pode solicitar, a qualquer momento, a customização dos indicadores e informações sobre incidentes e eventos apresentados nos relatórios. A CONTRATADA deve avaliar os requisitos técnicos necessários e operacionalizar. As solicitações devem ser registradas e realizadas por meio dos canais de suporte da CONTRATADA;

13.11.15.8. A CONTRATADA deverá demonstrar e apresentar relatórios de conformidade com as boas práticas e normas de segurança da informação, com no mínimo uma das certificações a seguir:

13.11.15.8.1. Certificação ISO 27.001;

13.11.15.8.2. Certificação ISO 20.000;

13.11.15.9. Por padrão, a CONTRATADA não deve possuir nenhum tipo de acesso aos ativos, sensores e ferramentas de proteção do CONTRATANTE. Em casos específicos e por tempo determinado, caso autorizado pela área de segurança do CONTRATANTE, pode ser fornecido acesso de leitura de registros do IPS, dados de sessão de rede (flow) e outras ferramentas de segurança para auxiliar em pesquisas pontuais de eventos de segurança. Não será fornecido nenhum tipo de acesso a dados ou sistemas do CONTRATANTE, além dos estritamente necessários para o serviço de monitoramento que serão armazenados na ferramenta de inteligência;

13.11.15.10. Caso a CONTRATANTE identifique necessidade de intervenção na solução ofertada, a CONTRATADA deverá realizar acesso remoto aos equipamentos para operação e ajustes necessários.

13.11.15.11. A CONTRATADA deverá definir pessoas do seu quadro de funcionários que terão acesso de administração nos equipamentos disponibilizados.

13.11.15.12. Após o acesso remoto, a CONTRATADA deverá comunicar ao CONTRATANTE qualquer alteração de configuração realizada nos equipamentos fornecidos nessa contratação e nessa situação respondendo por sua conta e risco pelas intervenções que possam ter efetuado.

13.11.15.13. A CONTRATADA deve prover informação específica sobre ameaças, gerada através de um processo (com coleta, validação, correlação, avaliação e interpretação de conhecimento baseado em evidências), que colocam em perigo ativos de informação ou de tecnologia do CONTRATANTE. Tal inteligência pode ser usada para embasar decisões sobre a resposta a tal ameaça ou risco, permitindo melhorar as táticas de detecção de ataques e configuração dos sensores de segurança. O processo deve resultar ainda em conhecimento utilizado para criação de novos indicadores e auxiliar na detecção de ataques futuros, possibilitando a identificação de ameaças específicas ao ambiente do CONTRATANTE;

13.11.15.14. O serviço de suporte técnico engloba as atividades de fornecer aconselhamento técnico e direcionamento para questões não cobertas pela GARANTIA, bem como atender a solicitações para questões de projeto, desenvolvimento e implantação de novas soluções envolvendo os equipamentos objeto dessa extensão;

13.11.15.15. Apoio técnico para tarefas de auditoria e análise de logs. O atendimento e suporte técnico especializado de 1º (primeiro nível) será

13.11.15.16. Sempre telefônico e remoto em regime 24x7 e assim, responsável pelo acompanhamento e gestão dos chamados, controle dos Indicadores de monitoramento, atuando como ponto único de contato entre a CONTRATANTE e profissionais da equipe da CONTRATADA.

13.11.15.17. O atendimento e suporte técnico especializado de 2º (segundo nível) poderão ser presenciais ou remotos em regime 24x7 caso o suporte remoto não seja suficiente para resolução do problema. Também é responsável pela prevenção e resolução de incidentes, problemas e requisições, identificando a causa raiz de eventual problema e buscando sua solução e execução de atividades remotas e/ou presenciais em incidentes e solicitações de maior complexidade.

13.11.15.18. O CONTRATANTE deverá ser notificado com uma estimativa do tempo de solução do chamado dentro da primeira hora de atendimento.

13.11.15.19. Para todo atendimento deverá ser disponibilizado ao CONTRATANTE um relatório detalhado, no qual conste no mínimo as seguintes informações:

13.11.15.19.1. Data e hora do atendimento.

13.11.15.19.2. Nomes dos responsáveis pelo chamado, pelo atendimento e pela comprovação do restabelecimento de funcionamento, com assinaturas dos dois últimos.

13.11.15.19.3. Descrição do(s) equipamento(s) envolvido(s), inclusive modelo, número de série e outros códigos identificadores.

13.11.15.19.4. Descrição da(s) anormalidade(s) observada(s).

13.11.15.19.5. Providências tomadas que dirimiram o problema observado. Sempre que for solicitado, a CONTRATADA deverá fornecer uma relação dos chamados técnicos gerados pelo CONTRATANTE, nos quais constarão, pelo menos: status do chamado, descrição do problema, datas e prazos de atendimento, descrição da solução e responsável técnico.

13.11.15.19.6. Acesso direto ao time de Engenharia: Acesso que permita comunicação disponível 24 horas por dia, 7 dias por semana, 365 dias por ano ao time de engenharia do fabricante, sem necessidade de escalonamento. O canal de comunicação deve ser seguro e permitir a troca de logs e binários de software certificados, todos os dados deverão permanecer armazenados para que possam ser referenciados posteriormente.

13.11.16. MONITORAMENTO DOS ATIVOS DE SEGURANÇA

13.11.16.1. É de responsabilidade da CONTRATADA o monitoramento contínuo dos ativos de segurança (Firewalls, IPSs, Balanceadores, WAF, EPM, ANTI- MALWARE, SASE, etc), a fim de sejam identificados e notificados problemas relacionados a:

13.11.16.1.1. Capacidade

13.11.16.1.2. Disponibilidade

- 13.11.16.1.3. Versão
- 13.11.16.1.4. Funcionalidades

13.11.17. COLETA E ANÁLISE DE EVENTOS DE DIVERSAS FONTES E SENSORES

- 13.11.17.1. A CONTRATADA deverá atuar proativamente e reativamente na análise de eventos de segurança, de forma a identificar possíveis incidentes e evitar possíveis impactos nos serviços;
- 13.11.17.2. A CONTRATADA deverá reagir aos eventos de Segurança da Informação que possam afetar a disponibilidade, integridade ou confidencialidade das informações existentes nos sistemas ou serviços de TI do CONTRATANTE;
- 13.11.17.3. A contratada deverá ser capaz de coletar eventos das fontes de dados especificadas, de modo a correlacionar eventos e identificar possíveis incidentes de segurança;
- 13.11.17.4. As informações fornecidas na etapa de identificação deverão ser utilizadas no processo de detecção, a fim de que se reflitam comportamentos do ambiente do CONTRATANTE;
 - 13.11.17.4.1. A CONTRATADA deve sempre manter assinaturas ativas de pelo menos 8 (oito) serviços de inteligência de ameaças, devendo conter ao menos 2 (dois) dos seguintes:
 - 13.11.17.4.2. Anomali ThreatStream
 - 13.11.17.4.3. CrowdStrike
 - 13.11.17.4.4. Cybersixgill Darkfeed
 - 13.11.17.4.5. IBM X-Force Exchange
 - 13.11.17.4.6. Mandiant Advantage Palo Alto AutoFocus
 - 13.11.17.4.7. DigitalShadows
 - 13.11.17.4.8. Canadian Cyber Threat Exchange (CCTX)
 - 13.11.17.4.9. RecordedFuture.
 - 13.11.17.4.10. Alien Vault
 - 13.11.17.4.11. FortiGuard
 - 13.11.17.4.12. Dragos
 - 13.11.17.4.13. ThreadConnect
 - 13.11.17.4.14. MISP (Malware Information Sharing Platform & Threat Sharing)
 - 13.11.17.4.15. OpenCTI
 - 13.11.17.4.16. Apura
 - 13.11.17.4.17. Penlink
 - 13.11.17.5. Coletar e investigar eventos de segurança e alertas dos componentes de segurança cobertos, aproveitando a inteligência de ameaças das bases utilizadas;
 - 13.11.17.6. Utilizar os recursos dos componentes de segurança cobertos, em alinhamento com a configuração e as políticas recomendadas. Isso inclui controles de segurança, ações de resposta e técnicas de detecção; como por exemplo, mas não limitado a assinaturas de IPS recomendadas, categorias de filtro Web, etc;
 - 13.11.17.7. Utilizar a inteligência das bases de Threat Intel e a análise segura de malware para ajudar a identificar as ameaças mais recentes e relevantes, indicadores de ataque ou comprometimento e práticas recomendadas de mitigação, usando padrões/frameworks abertos como MITRE Att&ck, NIST NVD, etc;
 - 13.11.17.8. Aproveitar as ferramentas de inteligência, bases de Threat Intel, indicadores compartilhados, assim como todos os recursos disponíveis para enriquecer alertas com informações que subsidiem os processos de investigação e mitigação;
 - 13.11.17.9. Relatar todas as ameaças potenciais detectadas em tempo hábil ao CONTRATANTE por meio de notificações detalhadas disponíveis no portal de serviços, incluindo notificações para todas novas detecções por meio de telefone, e-mail e Telegram;
 - 13.11.17.10. Possuir monitoramento nas dependências da CONTRATADA em regime 24x7x365, com ambiente monitorado por CFTV e controle biométrico de acesso;
 - 13.11.17.11. Acompanhar os alertas de segurança em tratamento à medida que evoluem ao longo do tempo, adicionando contexto ou detecções adicionais, conforme necessário e sempre que possível;
 - 13.11.17.12. Responder a consultas do CONTRATANTE relacionadas a eventos/alertas de segurança ativos e informações contextuais relacionadas, como inteligência de ameaças ou impacto geral no ambiente ou nas operações do CONTRATANTE;
 - 13.11.17.13. Notificar o CONTRATANTE sobre quaisquer interrupções planejadas ou não planejadas relacionadas a: portal de serviços, os recursos de monitoramento ou funcionalidades relacionadas à capacidade da contratada de monitorar eventos provenientes dos componentes de segurança cobertos.
 - 13.11.17.14. A CONTRATADA deverá utilizar as informações de risco e relevância para o negócio, fornecidas durante o processo de identificação, para oferecer uma visão objetiva a respeito de detecções e ações necessárias, priorizando aqueles cujo risco e valor operacional sejam mais expressivos
 - 13.11.17.15. O plano de comunicações deverá refletir as prioridades relacionadas aos ativos mais expressivos, encaminhando ao CONTRATANTE os eventos a eles relacionados de forma mais urgente.
- 13.11.18. MONITORAMENTO CONTÍNUO DE SEGURANÇA
 - 13.11.18.1. A CONTRATADA deverá construir de forma personalizada, casos de uso e regras de detecção que permitam monitorar continuamente o comportamento do ambiente, de forma a identificar possíveis ameaças de segurança. Devendo cobrir pelo menos os seguintes itens:
 - 13.11.18.1.1. Atividades de login
 - 13.11.18.1.2. Consultas DNS
 - 13.11.18.1.3. Comportamentos de tráfego
 - 13.11.18.1.4. Comunicações suspeitas
 - 13.11.18.1.5. Tentativas de intrusão
 - 13.11.18.1.6. Movimentações laterais
 - 13.11.18.1.7. Desvios de uso
 - 13.11.18.1.8. Atividades suspeitas no endpoint
 - 13.11.18.1.9. Exfiltração de dados

- 13.11.18.1.10. Atividades suspeitas de geolocalização
- 13.11.18.1.11. Novos serviços publicados
- 13.11.18.1.12. Atividades de acesso privilegiado
- 13.11.18.1.13. Serviços vulneráveis publicados na Internet
- 13.11.18.1.14. Garantir que todas as fontes de dados esperadas estejam enviando dados conforme esperado e em prazos aceitáveis, considerando a configuração e a integração, gerando alertas em casos de falha.
- 13.11.18.1.15. Investigar certas categorias de eventos anômalos onde não há uma causa conhecida, onde esses eventos possam, na opinião da CONTRATADA ou sob demanda da CONTRATANTE, representar uma ameaça
- 13.11.18.1.16. Usar inteligência de ameaças para pesquisar indicadores de comprometimento (IOCs) e/ou ataque (IOAs) para confirmar ameaças, ataques, comprometimentos ou explorações;
- 13.11.18.2. A CONTRATADA deverá manter em suas dependências uma equipe de "engenharia de detecção", responsável por:
 - 13.11.18.2.1. Implementar um ambiente de simulação de ataques para criação de novas detecções e testar de forma contínua a capacidade do SIEM em detectar comportamentos suspeitos;
 - 13.11.18.2.2. Utilizar o framework Mitre Att&CK para desenvolver cenários de ataque no ambiente de simulação, implementando técnicas e procedimentos comumente utilizadas por usuários mal-intencionados;
- 13.11.18.3. As simulações devem implementar variações de procedimentos para uma mesma técnica, de forma que a execução de uma técnica possa ser detectada mesmo que ela seja realizada de diferentes formas;
- 13.11.18.4. Analisar os logs e eventos produzidos no SIEM durante a simulação de ataques, para:
 - 13.11.18.4.1. Identificar se o SIEM recebeu das fontes de dados os logs e eventos referentes ao ataque simulado e realizar os devidos ajustes em conjunto com a CONTRATANTE para que os eventos cheguem até o SIEM;
 - 13.11.18.4.2. Validar se o SIEM possui uma regra de detecção capaz de identificar e alertar o comportamento simulado;
 - 13.11.18.4.3. Realizar a criação de novas regras de detecção, que serão utilizadas para alertar a ocorrência destes comportamentos no ambiente da CONTRATANTE;
 - 13.11.18.4.4. Implementar regras de detecção que atendam as necessidades do ambiente, sob demanda da CONTRATANTE, com o objetivo de identificar possíveis incidentes de segurança;
 - 13.11.18.4.5. Produzir relatórios e dashboards contendo as principais detecções e eventos de segurança.
- 13.11.19. RESPOSTA A INCIDENTES DE SEGURANÇA
 - 13.11.19.1. Atuar por meio de orientações quando ocorrer a falha dos controles de segurança ou situação previamente desconhecida e que tenha probabilidade de comprometer os sistemas e serviços de TI.
 - 13.11.19.2. Envolver-se com o CONTRATANTE em caso de incidente de segurança de alto risco (alerta positivo verdadeiro verificado). O CONTRATANTE fornecerá contexto sobre a gravidade da(s) ameaça(s), devendo a CONTRATADA fornecer insumos e recomendações ao CONTRATANTE para que o mesmo conclua a correção final e a resolução do Incidente de Segurança;
 - 13.11.19.3. Fornecer orientações sobre como mitigar, interromper ou prevenir um Incidente de segurança com base na inteligência e nos avisos fornecidos, conforme relevante para o ambiente do cliente. A resposta recomendada a um evento/incidente de segurança pode ser uma ou mais das seguintes:
 - 13.11.19.3.1. Com a permissão do CONTRATANTE, realizar alterações de política ou configuração aprovadas nos componentes de segurança cobertos para ajudar a mitigar ou responder a incidentes de segurança
 - 13.11.19.3.2. Quando o incidente de segurança for um ataque conhecido, recomendar ações de resposta para ajudar a mitigar o ataque e fornecer orientação sobre como ajudar a remediar ainda mais o Incidente de segurança, aproveitando os componentes de segurança cobertos;
 - 13.11.19.3.3. Onde for necessária uma validação adicional da ameaça, a CONTRATADA fornecerá recomendações sobre áreas de foco para investigação do cliente;
 - 13.11.19.3.4. Onde as ações de resposta estiverem fora dos componentes de segurança cobertos, a CONTRATADA fornecerá ao cliente recomendações para investigação e correção adicionais;
 - 13.11.19.4. A CONTRATADA poderá, sempre que necessário, solicitar maior riqueza de informações que possam contribuir para a resposta a uma investigação de segurança, tais como saídas de comandos, logs adicionais, acesso ao ativo, etc
 - 13.11.19.5. Sempre que houver viabilidade técnica e operacional para a automação, desde que o escopo seja definido previamente levando em consideração possíveis impactos e desdobramentos da ação tomada, a contratada poderá sugerir ações que reduzam o esforço operacional e implementem medidas preventivas, como por exemplo:
 - 13.11.19.5.1. Isolamento de endpoint (isolar um computador do resto da rede, deixando apenas as conexões necessárias para acesso ao seu sensor pelo servidor de gerenciamento);
 - 13.11.19.5.2. Bloquear automaticamente endereços IPs incluídos em listas de reputação públicas, ou de fontes de threat intel ou oriundos de IOCs ou IOAs próprios da contratada, extraídos à partir de eventos e incidentes de segurança de outros clientes, desde que aferidos e definidos como maliciosos;
 - 13.11.19.5.3. Liberar avisos à medida que novas informações são obtidas sobre ameaças novas ou inovadoras. Tais avisos não precisam ser especificamente focados no ambiente do CONTRATANTE, podendo ser de natureza ampla e genérica;
 - 13.11.19.5.4. Investigar ameaças bloqueadas de alta prioridade para determinar quaisquer informações e recomendações contextuais adicionais conforme necessário;
 - 13.11.19.5.5. Fornecer um relatório semanal sobre ameaças bloqueadas de baixa a média prioridade com recomendações conforme necessário;
 - 13.11.19.5.6. Investigar quaisquer ameaças não bloqueadas de média e alta prioridade e fornecer recomendações ao CONTRATANTE em termos de alterações de política sugeridas ou ações de resposta;
 - 13.11.19.5.7. Revisar periodicamente as ameaças não bloqueadas de baixa prioridade e fazer recomendações conforme necessário;
 - 13.11.19.5.8. Notificar o contato do CONTRATANTE sobre eventos de segurança usando um ou mais dos seguintes meios: eletronicamente pelo portal de serviços, e-mail, telefone, chat.
 - 13.11.19.5.9. Fazer recomendações ao CONTRATANTE quanto a quaisquer ações de resposta a serem executadas nos terminais em resposta a uma ameaça identificada;
 - 13.11.19.5.10. Fornecer pontos de verificação trimestrais de briefing (até uma (1) hora via teleconferência) para revisar relatórios, quaisquer alterações nos procedimentos de relatório, telemetria, processos, fluxos de trabalho e tecnologias.

- 13.11.19.6. A CONTRATADA, através do seu responsável técnico pelo contrato, deverá realizar, a cada 06 (seis) meses, visitas presenciais à sede da CONTRATANTE, para levantamento de informações técnicas, apresentações de relatórios e planos de melhoria contínuos;
- 13.12. Serviços de NOC:
- 13.12.1. Definição do Serviço
- 13.12.1.1. O Serviço de NOC (Network Operations Center) consiste em um conjunto de ferramentas e serviços de monitoramento, gerenciamento e otimização da infraestrutura de redes do ambiente da PMESP, garantindo alta disponibilidade, desempenho e segurança da comunicação.
- 13.12.1.2. A prestação dos serviços deverá ocorrer de forma contínua e ininterrupta, sob regime 24x7x365, dentro das dependências da CONTRATADA, garantindo proatividade na detecção e mitigação de falhas.
- 13.12.1.3. A resposta a incidentes deverá ocorrer nos tempos máximos informados no item que trata do Nível de Acordo de Serviços (SLA).
- 13.12.1.4. Requisitos do Ambiente de Administração dos Serviços do NOC
- 13.12.1.5. Controle de Acesso e Segurança Física
- 13.12.1.5.1. Implementação de sistemas de controle de acesso físico e monitoramento ambiental, com capacidade de rastreamento de pessoas e recuperação de registros e imagens.
- 13.12.1.5.2. Armazenamento de vídeos da área do NOC por, no mínimo, 90 dias.
- 13.12.1.5.3. Manutenção de registros de entrada e saída de pessoas e visitantes, com identificação única, por no mínimo 90 dias.
- 13.12.1.5.4. Controle de acesso físico com, no mínimo, dois fatores de autenticação.
- 13.12.1.5.5. Segurança e Continuidade Operacional
- 13.12.1.5.6. Implementação de solução de monitoramento de disponibilidade e desempenho de redes.
- 13.12.1.5.7. Proteção do perímetro contra intrusões e acessos indevidos.
- 13.12.1.5.8. Vigilância ininterrupta por segurança especializada, 24x7x365.
- 13.12.1.5.9. Configuração do ambiente para garantir que a falha de um único equipamento não interrompa os serviços.
- 13.12.1.6. Conformidade com Normas Técnicas
- 13.12.1.6.1. O serviço de NOC deverá estar em conformidade com as seguintes normas e boas práticas internacionais:
- 13.12.1.6.1.1. ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação.
- 13.12.1.6.1.2. ISO/IEC 20000 – Gestão de Qualidade de Serviços de TI.
- 13.12.1.6.1.3. ISO/IEC 27017 – Controles de segurança para serviços em nuvem.
- 13.12.1.6.1.4. ITIL v4 – Melhores práticas para gerenciamento de serviços de TI.
- 13.12.1.6.1.5. Gestão de Rede e Monitoramento Contínuo
- 13.12.1.7. A CONTRATADA deverá realizar avaliações periódicas do estado da rede do CONTRATANTE, contemplando:
- 13.12.1.7.1. Monitoramento proativo de disponibilidade, desempenho e latência da rede.
- 13.12.1.7.2. Análise de tráfego e uso da banda disponível, garantindo eficiência na comunicação.
- 13.12.1.7.3. Realização de testes de vulnerabilidades ao menos trimestralmente, com ferramentas reconhecidas no mercado.
- 13.12.1.7.4. Implementação e manutenção do Packet Broker, garantindo otimização e distribuição inteligente do tráfego de rede para ferramentas de análise.
- 13.12.1.7.5. Monitoramento de tráfego via sFlow, garantindo visibilidade granular da infraestrutura de rede.
- 13.12.1.8. Dashboard e Indicadores de Rede
- 13.12.1.8.1. O serviço de NOC deverá disponibilizar um dashboard centralizado, com os seguintes indicadores:
- 13.12.1.8.1.1. Top aplicações e serviços consumindo maior largura de banda.
- 13.12.1.8.1.2. Top ativos com tráfego anômalo ou comportamento suspeito.
- 13.12.1.8.1.3. Top interfaces de rede com maior uso e latência.
- 13.12.1.8.1.4. Principais ataques detectados e bloqueados na infraestrutura de rede.
- 13.12.1.8.1.5. Índice de disponibilidade da rede, métricas de SLA e desempenho.
- 13.12.1.8.1.6. Métricas de severidade de incidentes, classificadas de baixo a crítico.
- 13.12.1.9. Aplicação de Controles de Segurança na Rede
- 13.12.1.9.1. A CONTRATADA será responsável pela aplicação de controles de segurança adequados, garantindo a confidencialidade e integridade do tráfego de rede do CONTRATANTE. Para isso, deverá utilizar:
- 13.12.1.9.1.1. Criptografia robusta e reconhecida pelo mercado para proteção do tráfego de dados críticos.
- 13.12.1.9.1.2. Segmentação de rede baseada em políticas de segurança, evitando acessos indevidos.
- 13.12.1.9.1.3. Sempre que identificar falhas na implementação de serviços que tornem a infraestrutura vulnerável, a CONTRATADA deverá comunicar formalmente o CONTRATANTE e propor medidas corretivas.
- 13.12.1.10. Monitoramento e Resposta a Incidentes na Rede
- 13.12.1.10.1. O serviço de NOC deverá garantir monitoramento contínuo e análise de logs de rede, incluindo:
- 13.12.1.10.1.1. Coleta, correlação e análise de eventos de desempenho e falhas de rede.
- 13.12.1.10.1.2. Identificação de anomalias de tráfego, possíveis ataques DDoS e falhas críticas.
- 13.12.1.10.1.3. Acionamento imediato das equipes de resposta a incidentes para contenção e mitigação de falhas de rede.
- 13.12.1.10.1.4. O monitoramento deverá ocorrer de forma proativa e contínua, utilizando:
- 13.12.1.10.1.5. Plataformas de investigação avançadas, com machine learning e inteligência artificial.
- 13.12.1.10.1.6. Modelos de inteligência do fabricante, permitindo análise aprofundada de incidentes.
- 13.12.1.10.1.7. Interface web compatível com navegadores modernos, garantindo acesso a informações em tempo real.
- 13.12.1.11. Interface e Relatórios Gerenciais
- 13.12.1.11.1. A solução deverá disponibilizar uma interface web, compatível com os navegadores mais recentes, para acompanhamento das atividades do NOC, incluindo:
- 13.12.1.11.1.1. Métricas e gráficos de desempenho da rede, permitindo análise visual dos dados.
- 13.12.1.11.1.2. Possibilidade de gerar relatórios detalhados sobre incidentes detectados, tratativas e recomendações de otimização.
- 13.12.1.11.1.3. Geração de logs auditáveis, garantindo rastreabilidade das ações realizadas.
- 13.12.1.11.1.4. Entrega de relatórios gerenciais mensais, contendo uma visão geral dos eventos da rede, ações tomadas e melhorias sugeridas.

13.13. Procedimentos de transição e finalização do contrato

13.13.1. Ainda o presente ETP tem por finalidade disciplinar o procedimento de transição e de encerramento contratual relativo à contratação de serviços especializados de suporte técnico em cibersegurança, data center, redes, governança, gerenciamento e monitoramento contínuo das demandas e mudanças de tecnologia da informação e comunicação, envolvendo infraestrutura crítica de ambientes computacionais e de telecomunicações. Considerando que o escopo contratual abrange serviços de natureza estratégica, essenciais à continuidade operacional da PMESP e diretamente relacionados à salvaguarda, disponibilidade e integridade dos ativos informacionais, impõe-se a elaboração de artefatos formais para assegurar a adequada transferência de responsabilidades ao término da vigência contratual.

13.13.2. A conclusão de um contrato de missão crítica exige planejamento técnico e governança adequada, dado que a ausência de procedimentos estruturados de transição pode resultar em riscos materialmente relevantes, tais como indisponibilidade de serviços essenciais, perda ou comprometimento de informações sensíveis, exposição indevida de credenciais administrativas, degradação de níveis de segurança cibernética, prejuízo à rastreabilidade de ações executadas durante a vigência contratual e dificuldades operacionais na assunção das atividades por nova equipe ou novo prestador de serviços. Assim, estes itens consolidam as medidas necessárias para mitigar tais riscos e garantir a continuidade plena dos serviços de TIC.

13.13.3. A contratada deverá apresentar, com antecedência mínima de 30 (trinta) dias do término da vigência, um Plano de Transição de Encerramento contendo, no mínimo, a descrição detalhada das atividades a serem executadas, o cronograma proposto, a designação de responsáveis técnicos, o inventário inicial dos serviços, ativos e configurações sob sua gestão, além da identificação de riscos operacionais e das estratégias de mitigação correspondentes. O plano também deverá contemplar matriz de comunicação e mecanismos de reporte entre as partes. A contratante procederá à análise do artefato e poderá solicitar ajustes, devendo formalizar sua aprovação no prazo máximo de 10 (dez) dias úteis.

13.13.4. Durante o processo de transição, a contratada deverá promover a entrega integral, atualizada e validada de toda a documentação técnica produzida e utilizada ao longo da execução contratual, incluindo inventários de equipamentos e sistemas, arquiteturas físicas e lógicas, diagramas de rede, registros de configuração, regras e políticas de segurança cibernética, perfis de acesso e credenciais administrativas, relatórios de incidentes, de capacidade, de desempenho e de monitoramento contínuo, bem como scripts, rotinas operacionais e demais artefatos essenciais à governança do ambiente. A contratada será responsável pela acurácia, completude e integridade das informações entregues.

13.13.5. Complementarmente, deverá ser executado processo formal de transferência de conhecimento técnico, por meio de sessões estruturadas de capacitação, reuniões técnicas e apresentações direcionadas à equipe indicada pela contratante ou ao futuro contratado. Essas ações deverão abordar, de forma minuciosa, os procedimentos operacionais padrão, as particularidades de configuração dos ambientes, as rotinas críticas, as integrações sistêmicas existentes, os protocolos de segurança implementados e os fluxos de trabalho utilizados no gerenciamento e na operação dos ambientes de data center, redes e cibersegurança.

13.13.6. A contratada deverá assegurar a manutenção integral dos serviços e dos níveis de desempenho estabelecidos em contrato durante todo o período de transição, atuando de forma cooperativa e garantindo que não haja degradação dos ambientes ou interrupção de serviços críticos. Após a conclusão das atividades previstas no plano de transição, será executado o processo de desmobilização, compreendendo a revogação, transferência ou readequação de todas as credenciais e acessos, a remoção de ferramentas, softwares, agentes e componentes instalados exclusivamente para atendimento contratual, bem como a devolução de quaisquer ativos físicos ou lógicos pertencentes à contratante.

13.13.7. Ao término do processo, a contratada deverá apresentar Relatório Final de Encerramento de Contrato, contendo a comprovação documentada das entregas realizadas, o registro de eventuais pendências e recomendações técnicas, além da demonstração de conformidade com as normas aplicáveis de segurança da informação e governança de TIC. A contratante avaliará a conformidade das informações entregues e emitirá o correspondente termo de aceite ou relatório de inconformidades, que deverá ser atendido pela contratada no prazo estipulado (10 dias úteis).

13.13.7.1. Em resumo, este ETP evidencia a necessidade de um procedimento formal, técnico e estruturado de transição e de finalização contratual, imprescindível para assegurar a continuidade operacional, preservar o conhecimento institucional, manter a resiliência dos ambientes de TIC e garantir padrões adequados de segurança, disponibilidade e governança. O procedimento nestes itens busca mitigar riscos, assegurar a transferência ordenada de responsabilidades e proporcionar o encerramento seguro e transparente da relação contratual.

14. Estimativa de custo total da contratação

[Conteúdo Sigiloso | Justificativa: A justificativa para manter o sigilo da estimativa de custo total da contratação no ETP está prevista no art. 24 da Lei nº 14.133/2021, que permite o sigilo do orçamento estimado quando houver fundamentação técnica. O objetivo é preservar a competitividade e evitar que os licitantes ajustem suas propostas ao valor previamente divulgado, o que poderia comprometer a obtenção da proposta mais vantajosa para a PMESP.]

15. Justificativa técnica da escolha da solução

15.1 A presente análise comparativa tem como objetivo avaliar as alternativas disponíveis para a contratação de serviços técnicos especializados voltados ao suporte técnico em cibersegurança, data center, redes, governança, gerenciamento e monitoramento da infraestrutura de TIC, visando garantir a continuidade dos serviços de tecnologia da informação e comunicação. Foi considerada a contratação de serviços gerenciados por integradores especializados.

15.2 A alternativa, baseada em serviços gerenciados, consiste na terceirização das atividades para empresas especializadas que oferecem suporte contínuo, monitoramento e gestão da infraestrutura de TIC. Essa opção apresenta como principais vantagens a alta especialização técnica, escalabilidade, flexibilidade contratual e a definição clara de níveis de serviço por meio de acordos de SLA. No entanto, implica em menor controle direto sobre a operação e maior dependência de fornecedores externos.

15.3 A avaliação das alternativas foi realizada com base em critérios como custo inicial, escalabilidade, especialização técnica, tempo de implantação, aderência à legislação de proteção de dados, flexibilidade contratual e capacidade de garantir a continuidade operacional. A análise demonstrou que a contratação de serviços gerenciados especializados, baseada em serviços gerenciados, consiste na terceirização das atividades para empresas

especializadas que oferecem suporte contínuo, monitoramento e gestão da infraestrutura de TIC. Essa abordagem está alinhada às melhores práticas de governança e gestão de TIC, contribuindo para a mitigação de riscos operacionais e cibernéticos, além de assegurar a continuidade e a eficiência dos serviços prestados pela PMESP.

16. Justificativa econômica da escolha da solução

16.1 A escolha pela contratação de serviços especializados terceirizados, apresenta justificativa econômica sólida na área pública, conforme previsto no art. 18, §1º, inciso V da Lei nº 14.133/2021, que exige a demonstração da viabilidade técnica e econômica da solução adotada. A contratação de empresa especializada proporciona maior eficiência na alocação dos recursos públicos, ao reduzir custos operacionais, eliminar despesas com capacitação e manutenção de equipe interna, e mitigar riscos de falhas operacionais e cibernéticas. Além disso, essa abordagem permite a implantação mais ágil da solução, com menor impacto sobre os recursos humanos e financeiros da PMESP. A contratação de serviços gerenciados também favorece a obtenção de propostas mais vantajosas, ao estimular a competitividade entre empresas especializadas, alinhando-se às melhores práticas de governança e gestão de TIC. Dessa forma, a solução escolhida representa a alternativa mais econômica e eficaz para garantir a continuidade e a segurança dos serviços de tecnologia da informação e comunicação da Polícia Militar do Estado de São Paulo.

17. Benefícios a serem alcançados com a contratação

17.1. Esta contratação visa substituir os serviços atualmente em execução na Polícia Militar do Estado de São Paulo (PMESP), cujos contratos vigentes expiram em breve. A nova contratação garantirá a continuidade operacional, com o aprimoramento da segurança da informação e modernização da infraestrutura de TIC da corporação. Os resultados esperados incluem:

17.1.1. Garantir a disponibilidade dos recursos de TIC por meio da realização de atividades técnicas necessárias para o suporte, manutenção, segurança e melhoria contínua do hardware, software e sistemas que compõem o ambiente tecnológico da PMESP;

17.1.2. Monitoramento contínuo e medidas preventivas para assegurar a disponibilidade de todo o parque computacional e de telecomunicações da PMESP;

17.1.3. Cumprir os acordos de nível de serviço estabelecidos para o processamento ininterrupto dos programas que suportam os sistemas corporativos da Polícia Militar, garantindo o cumprimento de sua missão institucional;

17.1.4. Redução de tempos de indisponibilidade e otimização da performance de aplicações e infraestrutura, garantindo resiliência e escalabilidade dos serviços de TIC;

17.1.5. Conduzir adequadamente projetos relacionados à implantação de novas soluções, evolução das existentes, adequação do ambiente a novos requisitos de negócio, controle das ameaças cibernéticas e até migração de serviços para a nuvem.

17.1.6. Melhorar a experiência do usuário quando ocorrer a unificação dos serviços de operação de infraestrutura de TIC da PMESP.

17.1.7. Em resumo os benefícios serão:

17.1.7.1. Maior disponibilidade e confiabilidade dos serviços de TIC;

17.1.7.2. Melhoria na gestão de segurança da informação, com resposta rápida a incidentes;

17.1.7.3. Na automação de processos e otimização do suporte técnico, reduzindo tempo de resposta;

17.1.7.4. Na redução de custos operacionais com a adoção de práticas de eficiência energética e otimização de infraestrutura;

17.2. Adoção de um modelo de contratação moderno, alinhado às melhores práticas do setor público.

18. Providências a serem Adotadas

18.1. Previamente à contratação, a Administração deverá seguir o rito da licitação, de acordo com a Lei 14.133 de 1 de abril de 2021, através da plataforma Compras, provendo transparência e isonomia dos licitantes.

18.2. A Administração deverá nomear Gestores e Fiscais do contrato para acompanhar e supervisionar a execução dos contratos, para a celebração do contrato.

18.3. Fazem parte deste Estudo Técnico Preliminar – ETP, os seguintes documentos:

18.3.1. ANEXO A - INSTRUMENTO DE MEDIÇÃO DE RESULTADO – IMR;

18.3.2. ANEXO B - PLANILHA SIMPLIFICADA PARA ESTIMATIVA DO VALOR MENSAL DO SERVIÇO;

18.3.3. ANEXO C - PLANILHA DE CUSTOS E FORMAÇÃO DE PREÇOS;

18.3.4. ANEXO D - CATEGORIAS DE SERVIÇOS;

18.3.5. ANEXO E - Roteiro para fiscalização administrativa;

18.3.6. ANEXO F - MODELO DE RELATÓRIO DE FISCALIZAÇÃO TÉCNICA;

18.3.7. APÊNDICE A01 – TERMO DE CONFIDENCIALIDADE E SIGILO;

18.3.8. APÊNDICE A02 – ATESTADO DE VISITA TÉCNICA;

18.3.9. APÊNDICE A03 – LOCAIS DE ATENDIMENTO DE DEMANDAS;

18.3.10. APÊNDICE A04 – PLANILHA PONTO-A-PONTO;

18.3.11. APÊNDICE A05 - QUADRO RESUMO DE EXECUÇÃO;

18.3.12. APÊNDICE A06 - DESCRIÇÃO DO AMBIENTE ATUAL E DOS SERVIÇOS (CONFIDENCIAL E PESSOAL);

18.3.13. APÊNDICE A07 - INVENTÁRIO DOS ATIVOS LEGADOS DE REDE E SEGURANÇA (CONFIDENCIAL E PESSOAL);

- 18.3.14. APÊNDICE A08 – CATALOGO DE SERVIÇOS (CONFIDENCIAL E PESSOAL);
- 18.3.15. APÊNDICE A09 – HISTÓRICO DE REQUISIÇÃO DE DEMANDA (CONFIDENCIAL E PESSOAL);
- 18.3.16. APÊNDICE A10 – ATESTADO DE CAPACIDADE TÉCNICA;
- 18.3.17. APÊNDICE A11 – ZABBIX (CONFIDENCIAL E PESSOAL).
- 18.4. Em relação aos anexos classificados como confidencial e pessoal, recomenda-se que a licitante compreenda a pertinência e a conexão desses documentos com o objeto do processo. Ressalta-se que tais anexos poderão ser acessados durante a vistoria técnica, com a finalidade de subsidiar a elaboração de proposta consistente e adequada.

19. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

19.1. Justificativa da Viabilidade

19.1 A presente contratação foi precedida de análise detalhada quanto à viabilidade técnica e econômica, conforme exigido pelo §1º do art. 18 da Lei nº 14.133/2021. A solução proposta atende diretamente à necessidade identificada pela PMESP, considerando o interesse público envolvido e os objetivos estratégicos institucionais. Foram avaliadas alternativas disponíveis no mercado, por meio de levantamento técnico e mercadológico, que permitiram identificar a opção mais eficiente, segura e economicamente sustentável.

19.2 A viabilidade técnica está evidenciada pela capacidade da solução em atender aos requisitos funcionais e operacionais exigidos, com garantia de desempenho, escalabilidade e conformidade com normas legais, incluindo a Lei Geral de Proteção de Dados - LGPD. Já a viabilidade econômica foi demonstrada por meio da análise comparativa de custos, que indicou que a contratação proposta representa a melhor relação custo-benefício, com potencial de economia de escala, redução de riscos operacionais e otimização dos recursos humanos e financeiros disponíveis.

19.3 Dessa forma, a contratação é considerada viável e vantajosa, estando alinhada ao planejamento da PMESP e às diretrizes da Nova Lei de Licitações, garantindo a legalidade, a eficiência e a transparência do processo.

20. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

Despacho: Maj PM - DivCiber/DPC/DTIC

MARCELO FUMIO TAMASHIRO

Equipe de apoio



Assinou eletronicamente em 11/03/2026 às 18:13:30.

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - ANEXO A - INSTRUMENTO DE MEDIÇÃO DE RESULTADO – IMR v4.pdf (571.77 KB)
- Anexo II - ANEXO B - PLANILHA SIMPLIFICADA PARA ESTIMATIVA DO VALOR MENSAL DO SERVIÇO v4.pdf (245.19 KB)
- Anexo III - ANEXO C - PLANILHA DE CUSTOS E FORMAÇÃO DE PREÇOS v3.pdf (487.33 KB)
- Anexo IV - ANEXO D - CATEGORIAS DE SERVIÇOS.pdf (253.48 KB)
- Anexo V - ANEXO E - Roteiro para fiscalização administrativa.pdf (238.98 KB)
- Anexo VI - ANEXO F - MODELO DE RELATÓRIO DE FISCALIZAÇÃO TÉCNICA.pdf (231.07 KB)
- Anexo VII - APÊNDICE A01 – TERMO DE CONFIDENCIALIDADE E SIGILO.pdf (199.02 KB)
- Anexo VIII - APÊNDICE A02 – ATESTADO DE VISITA TÉCNICA.pdf (298.01 KB)
- Anexo IX (sigiloso)
- Anexo X - APÊNDICE A04 – PLANILHA PONTO-A-PONTO.pdf (599.01 KB)
- Anexo XI - APÊNDICE A05 - QUADRO RESUMO DE EXECUÇÃO V2.pdf (415.61 KB)
- Anexo XII (sigiloso)
- Anexo XIII (sigiloso)
- Anexo XIV (sigiloso)
- Anexo XV (sigiloso)
- Anexo XVI - APÊNDICE A10 – Atestado de Capacidade Técnica v2.pdf (364.05 KB)
- Anexo XVII (sigiloso)

SECRETARIA DA SEGURANÇA PÚBLICA

POLICIA MILITAR DO ESTADO DE SÃO PAULO

ANEXO A – INSTRUMENTO DE MEDIÇÃO DE RESULTADO – IMR

1. O objetivo do Instrumento de Medição de Resultado – IMR é aferir a qualidade e pontualidade da contratação para pagamento mensal dos serviços especializados de suporte técnico de cibersegurança, data center e redes, bem como de governança, gerenciamento e monitoramento, das demandas e mudanças de tecnologia da informação e comunicação e infraestrutura de data center e redes para ambiente computacional e de telecomunicações, de forma a garantir a continuidade dos serviços de TIC da PMESP, conforme especificações do ETP e Termo de Referência.

2. CRITÉRIOS DE CLASSIFICAÇÃO

2.1. Prioridade de Atendimento

2.1.1. A urgência e o impacto deverão ser classificados em alto (1), médio (2) e baixo (3);

2.1.2. A prioridade será definida por um agrupamento realizado sobre o resultado da multiplicação entre a urgência e o impacto;

2.1.3. A Tabela 1, apresentada a seguir, descreve o resultado da multiplicação entre urgência e impacto, de maneira a se obter a prioridade associada:

Tabela 1

Impacto x Urgência				
		Impacto		
		Baixo – 1	Médio - 2	Alto – 3
Urgência	Alta – 3	3	6	9
	Média – 2	2	4	6
	Baixa – 1	1	2	3

2.1.4. A Tabela 2 a seguir apresenta a prioridade derivada de um agrupamento realizado sobre o resultado da multiplicação entre urgência e impacto, bem como exemplos de tempo máximo para resolução, relativos a cada um dos níveis de prioridade descritos:

Tabela 2

Prioridade	
9	CRÍTICA

Prioridade	
6	Alta
3-4	Média
2	Baixa
1	Agendada

2.2. Tempo de Solução

2.2.1. O CONTRATANTE definiu 5 níveis de prioridade demonstrados nos quadros acima e 5 níveis de atendimento, desta forma, o Tempo de Solução para o atendimento é obtido por meio da combinação destes vetores e está demonstrado nos itens a seguir:

2.2.2. *Priorização de Incidentes para todos os Serviços Governança, Cibersegurança, SPD e SER*

2.2.2.1. Deverá ser utilizada a tabela de impacto conforme a Tabela 3, a seguir:

Tabela 3

Impacto	Descrição
Alto	Quando atinge a 70% ou mais da organização, 100% de uma localidade ou a IC classificados como críticos.
Médio	Quando atinge a mais de 40% e menos de 70% da organização, afeta a dois ou mais serviços de uma localidade ou a IC classificados como relevantes (de produção e não críticos).
Baixo	Quando atinge a 40% ou menos da organização, a somente 1 (um) serviço de uma localidade ou a IC que não sejam de produção.

2.2.2.2. Também deverá ser utilizada a Tabela 4 para a classificação de urgência:

Tabela 4

Urgência	Descrição
Alta	Quando os IC ou Serviços (de Negócios) atingidos são classificados como críticos.
Média	Quando os IC ou Serviços (de Negócios) atingidos são classificados como relevantes (de produção e não críticos).
Baixa	Quando os IC ou Serviços (de Negócios) atingidos não são de produção (desenvolvimento, testes, etc.).

2.2.2.3. Finalmente, a Tabela 5 apresenta a priorização que deverá ser adotada:

Tabela 5

Prioridade	Observação	Tempo de Solução
CRÍTICA (S1)	Devem ser inclusos nessa categoria de priorização todos IC que sustentem os serviços (de Negócio) definidos pelo CONTRATANTE como estratégicos. Dá-se quando o recurso computacional, equipamento ou softwares (programas aplicativos, módulos de sistemas, sistemas aplicativos e suas derivações) está parado (indisponível) em razão de pane, falha ou não-conformidade técnica.	2 horas

Prioridade	Observação	Tempo de Solução
Alta (S2)	Devem ser inclusos nessa categoria os incidentes de prioridade média que afetem 70% ou mais das localidades remotas. Dá-se quando o recurso computacional, equipamento ou softwares (programas aplicativos, módulos de sistemas, sistemas aplicativos e suas derivações) apresenta pane, falha ou não-conformidade técnica que prejudica o uso de uma função básica.	4 horas
Média (S3)	Devem ser inclusos nessa categoria os incidentes de prioridade baixa que afetem mais de 40% e menos de 70% das localidades remotas. Dá-se quando o recurso computacional, equipamento ou softwares (programas aplicativos, módulos de sistemas, sistemas aplicativos e suas derivações) apresenta pane, falha ou não-conformidade técnica que provoca restrições ao uso de algumas funções acessórias.	12 horas
Baixa (S4)	Devem ser inclusas nessa categoria mudanças de médio porte (criação de estruturas de rede, reset de servidor de testes, etc.), liberação de acesso, criação de usuário no ambiente AD, etc. Demanda de assistência técnica para a instalação, configuração, customização, otimização ou migração do recurso computacional ou do equipamento de conectividade de rede.	24 horas úteis
Agendada (S5)	Devem ser inclusas nessa categoria mudanças de pequeno porte (movimentação de dados, criação de novo ambiente de desenvolvimento padrão, etc.). Inclui também demanda sazonal de serviços para a instalação, configuração, customização, otimização ou migração simultânea de novos recursos computacionais (hardware e software) ou de equipamentos de conectividade de rede em várias Organizações Policiais Militares (OPM).	Agendada

2.2.2.4. Incidentes de segurança sempre deverão ser atendidos com prioridade CRÍTICA. (e.g.: Infecção de Vírus, atualização de segurança de roteadores e firewalls);

2.2.2.5. Nos casos de impossibilidade da solução de problemas, a contratada deverá demonstrar evidências, **por meio de informações diretamente dos fabricantes dos recursos suportados;**

2.2.2.6. Para os casos em que a solução dos incidentes/problemas não for possível pelos técnicos da CONTRATADA, há necessidade que a contate o fabricante, mesmo que a Polícia Militar não possua contrato de manutenção.

2.2.3. *Priorização de Solicitação de Serviços*

2.2.3.1. Além dos Incidentes, a CONTRATADA deverá também atender às solicitações de serviços como criação de usuário, execução de backup, instalação de aplicativos, etc., assim como mudanças pequenas e médias e para isso deverá considerar a Tabela 6, a seguir:

Tabela 6

Prioridade	Observação	Tempo de Solução
CRÍTICA (S1)	Ambientes (estações de trabalho) de usuários VIP. Mudanças emergenciais essenciais para manter IC e serviços (de negócios) classificados como críticos.	2 horas

Prioridade	Observação	Tempo de Solução
Alta (S2)	Mudanças emergenciais que sejam essenciais para manter IC de produção não críticos ou de 70% ou mais das localidades remotas.	8 horas
Média (S3)	Instalação de aplicativos pré-aprovados. Mudanças que sejam essenciais para manter mais de 40% e menos de 70% das localidades remotas.	24 horas úteis
Baixa (S4)	Mudanças não emergenciais. Manutenção preventiva de ambiente (estações de trabalho) de usuários.	48 horas úteis
Agendada (S5)	Instalação de aplicativos não homologados (onde seja necessário todo o processo de aprovação da aquisição e homologação do mesmo no ambiente do CONTRATANTE). Também devem ser incluídas nessa categoria mudanças de médio porte (movimentação de dados, criação de novo ambiente de desenvolvimento padrão, etc.).	Agendada

2.2.4. A CONTRATADA deverá garantir a disponibilidade do Ambiente Computacional, por meio do desempenho dos serviços prestados, dimensionados com base nos seguintes padrões mínimos de desempenho:

2.2.4.1. **Índice de Atendimento de Chamados Técnicos:** todos os chamados técnicos encaminhados ao atendimento de terceiro nível devem ser atendidos;

2.2.4.2. **Taxa de Resolução de Chamados Técnicos e de Ocorrências:** o limite mínimo de resolução de chamados técnicos no atendimento de terceiro nível, dentro dos limites de tempo (SLA) dos níveis de severidade, é de 85% (oitenta e cinco por cento) do total mensal;

3. CRITÉRIOS DE MEDIÇÃO DOS SERVIÇOS

3.1. Os serviços serão aferidos mensalmente pelo critério da efetiva prestação de serviços, com base na somatória do número de horas técnicas por recurso (Σ htf) dedicadas ao objeto contratado, conforme segue:

HTM_{gov} = (Σ htr), onde:

HTM_{gov} = Horas Técnicas Mensais de Governança de TIC demandadas

hts = horas técnicas prestadas por serviço

HTM_{ciber} = (Σ htr), onde:

HTM_{ciber} = Horas Técnicas Mensais de Cibersegurança demandadas

hts = horas técnicas prestadas por serviço

HTM_{spd} = (Σ htr), onde:

HTM_{spd} = Horas Técnicas Mensais de Seção de Data Center demandadas

hts = horas técnicas prestadas por serviço

HTM_{ser} = (Σ htr) , onde:

HTM_{ser} = Horas Técnicas Mensais da Seção de Engenharia de Redes demandadas

htr = horas técnicas prestadas por recurso

3.2. A CONTRATADA apresentará um relatório de controle diário dos serviços executados, computando as horas técnicas prestadas em planilha de controle própria, a qual será cotejada com o Relatório de Serviços e apresentada para aval da equipe da CONTRATANTE apresentada pela contratada de acordo com o cronograma estabelecido em Contrato;

3.3. Sem prejuízo das penalidades previstas em Contrato, a CONTRATADA arcará com todos os custos gerados pelo excesso de horas técnicas demandadas para atendimento de Chamados Técnicos (mudanças e solicitações de serviço), Ocorrências (incidentes) e Acionamentos na execução dos serviços contratados:

3.3.1. Nos casos de acionamento para atendimento de incidentes com níveis de Severidade S1 e S2 (nesse caso, todos os chamados e ocorrências fora do horário do expediente contratual não terão cômputo de Horas Técnicas extras, podendo ser compensado do total de horas do recurso, mediante autorização da CONTRATANTE, sendo considerado como garantia de disponibilidade do Ambiente Computacional, conforme tabela de priorização de incidentes);

3.3.2. Para os acionamentos fora dos dias e horários estabelecidos, a fim de atender demandas específicas, nos casos em que não seja possível a sua execução em horário normal de trabalho pela complexidade ou disponibilidade do recurso, software ou aplicativo, ou ainda pelo nível de criticidade que o recurso computacional representa, ou nos casos de atendimento VIP fora do horário normal de trabalho, a CONTRATADA poderá compensar a hora total não sendo adicionado ao total mensal;

3.3.3. Acionamentos com nível de Severidade S3, em que for autorizado seu acionamento/deslocamento, deverá ser formalizada, em termo próprio e no primeiro dia útil após o acionamento, a quantidade de horas utilizadas para a resolução;

3.3.4. Nos casos dos acionamentos com níveis de Severidade S4 e S5, o acionamento estará condicionado à um planejamento prévio aprovado pelo Gestor;

3.3.5. Poderão ocorrer casos de necessidade de prestar serviços em horários ou locais diversos do estabelecido, nas seguintes condições:

3.3.5.1. Para atender demanda de intervenção técnica nos recursos computacionais (hardware e software) instalados no DAS, aos sábados, domingos e feriados ou no horário noturno/madrugada;

3.3.5.2. Para atender demanda de intervenção técnica em órgãos da Polícia Militar com alto grau de concentração de recursos computacionais (hardware e software) e/ou responsáveis pela operação de sistemas críticos;

3.3.5.3. Para atendimento de usuários VIP, diretamente em suas OPM, até o limite da região metropolitana de São Paulo, fora do horário normal de trabalho.

4. PAGAMENTOS

4.1. O IMR tem por finalidade estabelecer critérios objetivos para mensurar o desempenho da CONTRATADA, garantindo a qualidade do serviço e vinculando o pagamento ao cumprimento dos requisitos contratuais.

4.2. Os valores referentes aos pagamentos devidos à CONTRATADA serão aferidos mensalmente de acordo com a prestação de Serviços, item 2.1, baseado no número de horas técnicas mensais (HTM) dedicadas ao objeto contratado, conforme segue:

$$VM = \%SLA_{cumprido} * ((HTM_{gov} * VHT_{gov}) + (HTM_{ciber} * VHT_{ciber}) + (HTM_{spd} * VHT_{spd}) + (HTM_{ser} * VHT_{ser}))$$

Onde:

VM = valor mensal

% SLA_{cumprido} = percentual do Acordo de Nível de Serviço executado apurado mensalmente

HTM = Horas Técnicas Mensais demandadas

VHT = valor da hora técnica

Exemplificando: caso a empresa tenha uma taxa de resolução dos Chamados (Requisições de Serviços, Incidentes, Problemas, Mudanças etc.), que chamaremos

de acordo de Nível de Serviço – SLA de 90% e tenha prestado 3.000 (três mil) horas de Serviço de Seção de Data Center a R\$60,00/hora, 1.300 (mil e trezentas) horas de Serviço de Seção de Engenharia de Redes a R\$80,00/hora, 700 (setecentas) horas de Serviço de Cibersegurança a R\$90,00/hora e 1.000 (mil) horas de Governança de TIC a R\$100,00/hora em um determinado mês temos:

$$\text{Valor Mensal} = 0,9 * ((3000*60)+(1300*80)+(700*90)+ (1000*100))$$

$$\text{Valor Mensal} = 0,9*447000 = R\$402.300,00$$

4.3. A CONTRATADA deverá apresentar mensalmente relatório extraído da ferramenta de ITSM em uso na PMESP, de maneira a demonstrar o atendimento de no mínimo 85% dos chamados dentro dos níveis estabelecidos nos níveis acordados de severidade, justificando os casos que fugiram à sua capacidade de resolução, os quais serão alvo de apreciação pela CONTRATANTE;

4.4. Para os casos de ser apurado IMR inferior ao mínimo estabelecido, ou seja, não atingir a 85% dos chamados atendidos dentro dos tempos estabelecidos nos níveis de severidade, a contratada incorrerá, além do desconto previsto acima, em quebra de cláusula contratual e suas sanções previstas neste Edital.

5. ACOMPANHAMENTO POR MEIO DE INDICADORES - KPI

5.1. Os serviços devem ser acompanhados por indicadores de desempenho (KPIs) definidos em alinhamento aos SLAs, abrangendo métricas como disponibilidade, tempo de resposta, tempo de resolução e taxa de incidentes recorrentes. Para serviços contínuos de alta criticidade, os KPIs devem ser calibrados para garantir monitoramento efetivo, apoiar auditorias e permitir evolução da prestação de serviço em caso de não conformidade. Os indicadores servirão de base para avaliação de desempenho, revisão de níveis de serviço, escalonamento e garantia da qualidade dos serviços prestados. Serão consideradas os seguintes indicadores para o cálculo do desempenho da CONTRATADA:

5.1.1. Quantidade de chamados (requisição e incidentes) atendidos dentro do prazo

5.1.1.1. Finalidade: Apurar a quantidade de chamados atendidos dentro do prazo estabelecido

5.1.1.2. Meta a cumprir: 85%

5.1.1.3. Instrumento de medição: Base ITSM

5.1.1.4. Forma de acompanhamento: Base ITSM e Status Report

- 5.1.1.5. Periodicidade: Mensal
- 5.1.1.6. Mecanismo de cálculo (%): $(\text{Total de chamados atendidos dentro do prazo} / \text{Total de chamados abertos no período}) \times 100$
- 5.1.1.7. Início da vigência: início do contrato
- 5.1.1.8. Faixa no ajuste no pagamento: Glosa
- 5.1.1.9. Sanções: Processo
- 5.1.1.10. Observações: Nenhuma

5.1.2. Disponibilidade da operação de TIC

- 5.1.2.1. Finalidade: Apurar a disponibilidade do ambiente durante o período especificado
- 5.1.2.2. Meta a cumprir: 99,97% (Representa nenhum downtime no ano, ou seja, o data center não esteve nem um minuto sequer indisponível)
- 5.1.2.3. Instrumento de medição: ITSM
- 5.1.2.4. Forma de acompanhamento: Base do ITSM
- 5.1.2.5. Periodicidade: Mensal
- 5.1.2.6. Mecanismo de cálculo (%): $(\text{Horas Totais de Funcionamento no Período} - \text{Horas de Manutenção Preventiva} - \text{Horas Indisponíveis Justificadas}) / (\text{Horas Totais no Período} - \text{Horas de Manutenção Preventiva} - \text{Horas Indisponíveis Justificadas}) \times 100$.
- 5.1.2.7. Início da vigência: início do contrato
- 5.1.2.8. Faixa no ajuste no pagamento: Glosa
- 5.1.2.9. Sanções: processo
- 5.1.2.10. Observações: nenhuma

5.1.3. Eficácia no tratamento de chamados (requisições, incidentes e incidentes de segurança)

- 5.1.3.1. Finalidade: Apurar a eficácia do contratado na resolução de chamados
- 5.1.3.2. Meta a cumprir: 85%
- 5.1.3.3. Instrumento de medição: ITSM
- 5.1.3.4. Forma de acompanhamento: Base do ITSM
- 5.1.3.5. Periodicidade: Mensal
- 5.1.3.6. Mecanismo de cálculo (%): $(\text{Total de chamados atendidos} - \text{Total de chamados reaberto}) / (\text{Total de chamados atendidos}) \times 100$
- 5.1.3.7. Início da vigência: início do contrato
- 5.1.3.8. Faixa no ajuste no pagamento: Glosa
- 5.1.3.9. Sanções: processo

5.1.3.10. Observações: nenhuma

5.1.4. Satisfação dos usuários

5.1.4.1. Finalidade: Aferir o grau de satisfação dos usuários sobre o serviço prestado

5.1.4.2. Meta a cumprir: 70%

5.1.4.3. Instrumento de medição: ITSM em conjunto com a SAL/DAS/DTIC/PMESP

5.1.4.4. Forma de acompanhamento: Base do ITSM

5.1.4.5. Periodicidade: Mensal

5.1.4.6. Mecanismo de cálculo (%): (Média das notas obtidas) / (Nota máxima da avaliação)

5.1.4.7. Início da vigência: início do contrato

5.1.4.8. Faixa no ajuste no pagamento: Glosa

5.1.4.9. Sanções: processo

5.1.4.10. Observações: nenhuma

5.1.5. Índice de vinculação da resolução de requisições de serviço à base de conhecimento

5.1.5.1. Finalidade: Aferir a cobertura dos padrões de atendimento registrados na base de conhecimento

5.1.5.2. Meta a cumprir: 85%

5.1.5.3. Instrumento de medição: ITSM

5.1.5.4. Forma de acompanhamento: ITSM

5.1.5.5. Periodicidade: Mensal

5.1.5.6. Mecanismo de cálculo (%): (Total de requisições com resolução vinculada à base de conhecimento / Total de requisições resolvidas) x 100

5.1.5.7. Início da vigência: início do contrato

5.1.5.8. Faixa no ajuste no pagamento: Glosa

5.1.5.9. Sanções: processo

5.1.5.10. Observações: nenhuma

5.1.6. Para a PMESP que já adota o conceito de DevOps, ou ainda que possuem razoável grau de automação em sua infraestrutura, será adotado níveis de serviços complementares com vistas a assegurar mais agilidade e qualidade nas operações, a exemplo:

5.1.7. Tempo de deployment

- 5.1.7.1. Finalidade: Aferir o tempo de conclusão do deployment após a aprovação
- 5.1.7.2. Meta a cumprir: 85%
- 5.1.7.3. Instrumento de medição: Pipeline do DAS/DTIC
- 5.1.7.4. Forma de acompanhamento: em conjunto com a fábrica de software do DAS/DTIC
- 5.1.7.5. Periodicidade: Mensal
- 5.1.7.6. Mecanismo de cálculo (%): $(\text{Total de deployments executados no tempo mínimo exigido} / \text{Total de deployments executados}) \times 100$
- 5.1.7.7. Início da vigência: Após 3 meses da assinatura do contrato
- 5.1.7.8. Faixa no ajuste no pagamento: Glosa
- 5.1.7.9. Sanções: processo
- 5.1.7.10. Observações: nenhuma

5.1.8. Taxa de falhas de deployments

- 5.1.8.1. Finalidade: Aferir a quantidade de deployments malsucedidos
- 5.1.8.2. Meta a cumprir: < 30%
- 5.1.8.3. Instrumento de medição: Pipeline do DAS/DTIC
- 5.1.8.4. Forma de acompanhamento: em conjunto com a fábrica de software do DAS/DTIC
- 5.1.8.5. Periodicidade: Mensal
- 5.1.8.6. Mecanismo de cálculo (%): $(\text{Total de deployments que apresentaram falha} / \text{Total de deployments executados}) \times 100$
- 5.1.8.7. Início da vigência: Após 3 meses da assinatura do contrato
- 5.1.8.8. Faixa no ajuste no pagamento: Glosa
- 5.1.8.9. Sanções: processos
- 5.1.8.10. Observações: nenhuma

5.1.9. Taxa de deployments realizados por meio de Deployment Pipeline - DP definidos

- 5.1.9.1. Finalidade: Aferir a quantidade de deployments realizados por meio de processo automatizado de implantação
- 5.1.9.2. Meta a cumprir: 70%
- 5.1.9.3. Instrumento de medição: Pipeline do DAS/DTIC
- 5.1.9.4. Forma de acompanhamento: em conjunto com a fábrica de software do DAS/DTIC
- 5.1.9.5. Periodicidade: Mensal

5.1.9.6. Mecanismo de cálculo (%): $(\text{Total de deployments em DP} / \text{Total de deployments executados}) \times 100$

5.1.9.7. Início da vigência: Após 3 meses da assinatura do contrato

5.1.9.8. Faixa no ajuste no pagamento: Glosa

5.1.9.9. Sanções: processo

5.1.9.10. Observações: nenhuma

5.1.10. Tempo de recuperação de deployment

5.1.10.1. Finalidade: Aferir o tempo de retorno às condições anteriores após detectado um deployment danificado

5.1.10.2. Meta a cumprir: 85%

5.1.10.3. Instrumento de medição: Pipeline do DAS/DTIC

5.1.10.4. Forma de acompanhamento: em conjunto com a fábrica de software do DAS/DTIC

5.1.10.5. Periodicidade: Mensal

5.1.10.6. Mecanismo de cálculo (%): $(\text{Total de deployments recuperados dentro do tempo máximo definido} / \text{Total de deployments recuperados}) \times 100$

5.1.10.7. Início da vigência: Após 3 meses da assinatura do contrato

5.1.10.8. Faixa no ajuste no pagamento: Glosa

5.1.10.9. Sanções: processo

5.1.10.10. Observações: nenhuma

5.1.11. Tempo médio de implementação de uma mudança

5.1.11.1. Finalidade: Aferir o tempo necessário para se implementar uma mudança no ambiente

5.1.11.2. Meta a cumprir: 85%

5.1.11.3. Instrumento de medição: Pipeline do DAS/DTIC

5.1.11.4. Forma de acompanhamento: em conjunto com a fábrica de software do DAS/DTIC

5.1.11.5. Periodicidade: Mensal

5.1.11.6. Mecanismo de cálculo (%): $(\text{Total de requisições de mudanças atendidas dentro do tempo máximo definido} / \text{Total de requisições de mudanças}) \times 100$

5.1.11.7. Início da vigência: Após 3 meses da assinatura do contrato

5.1.11.8. Faixa no ajuste no pagamento: Glosa

5.1.11.9. Sanções: processo

5.1.11.10. Observações: nenhuma

5.1.12. Taxa de implantação de controles de segurança

5.1.12.1. Finalidade: Aferir a quantidade de controles de segurança implantados diante dos controles de segurança recomendados pelos frameworks

5.1.12.2. Meta a cumprir: 70%

5.1.12.3. Instrumento de medição: Ferramentas e soluções de segurança

5.1.12.4. Forma de acompanhamento: em conjunto com a cibersegurança

5.1.12.5. Periodicidade: Mensal

5.1.12.6. Mecanismo de cálculo (%): $(\text{Total de controles de segurança implantados} / \text{Total controles recomendados e estabelecidos pelo Contratante}) \times 100$

5.1.12.7. Início da vigência: Após 3 meses da assinatura do contrato

5.1.12.8. Faixa no ajuste no pagamento: Glosa

5.1.12.9. Sanções: processo

5.1.12.10. Observações: nenhuma

5.1.13. Para serviços de atendimento ao usuário deve-se observar indicadores de qualidade adicionais, a exemplo:

5.1.14. Índice de chamados atendidos no Nível I

5.1.14.1. Finalidade: Apurar a percentagem de chamados que são atendidos diretamente pelo nível I

5.1.14.2. Meta a cumprir: 70%

5.1.14.3. Instrumento de medição: ITSM

5.1.14.4. Forma de acompanhamento: ITSM

5.1.14.5. Periodicidade: Mensal

5.1.14.6. Mecanismo de cálculo (%): $(\text{Total de chamados atendidos pelo Nível I} / \text{Total de chamados registrados}) \times 100$

5.1.14.7. Início da vigência: Após 3 meses da assinatura do contrato

5.1.14.8. Faixa no ajuste no pagamento: Glosa

5.1.14.9. Sanções: processo

5.1.14.10. Observações: nenhuma

5.1.15. Indicadores de Nível de Serviço II:**5.1.16. Índice de chamados com severidade 1 (alto impacto) resolvidos dentro do prazo**

5.1.16.1. Finalidade: Apurar a eficácia na resolução de chamados com severidade 1

5.1.16.2. Meta a cumprir: 90%

5.1.16.3. Instrumento de medição: ITSM

- 5.1.16.4. Forma de acompanhamento: Base ITSM
- 5.1.16.5. Periodicidade: Mensal
- 5.1.16.6. Mecanismo de cálculo (%): $(\text{Total de chamados com severidade 1} / \text{Total de chamados recebidos com severidade 1}) \times 100$
- 5.1.16.7. Início da vigência: Após 3 meses da assinatura do contrato
- 5.1.16.8. Faixa no ajuste no pagamento: Glosa
- 5.1.16.9. Sanções: processo
- 5.1.16.10. Observações: nenhuma
- 5.1.17. Índice de chamados com severidade 2 (médio impacto) resolvidos dentro do prazo**
 - 5.1.17.1. Finalidade: Apurar a eficácia na resolução de chamados com severidade 2 ou critério equivalente definido pela PMESP
 - 5.1.17.2. Meta a cumprir: 70%
 - 5.1.17.3. Instrumento de medição: ITSM
 - 5.1.17.4. Forma de acompanhamento: Base ITSM
 - 5.1.17.5. Periodicidade: Mensal
 - 5.1.17.6. Mecanismo de cálculo (%): $(\text{Total de chamados com severidade 2} / \text{Total de chamados recebidos com severidade 2}) \times 100$
 - 5.1.17.7. Início da vigência: Após 3 meses da assinatura do contrato
 - 5.1.17.8. Faixa no ajuste no pagamento: Glosa
 - 5.1.17.9. Sanções: processo
 - 5.1.17.10. Observações: nenhuma
- 5.1.18. Índice de chamados com severidade 3 (baixo impacto) resolvidos dentro do prazo**
 - 5.1.18.1. Finalidade: Apurar a eficácia na resolução de chamados com severidade 3 ou critério equivalente definido pela PMESP
 - 5.1.18.2. Meta a cumprir: 50%
 - 5.1.18.3. Instrumento de medição: ITSM
 - 5.1.18.4. Forma de acompanhamento: Base ITSM
 - 5.1.18.5. Periodicidade: Mensal
 - 5.1.18.6. Mecanismo de cálculo (%): $(\text{Total de chamados com severidade 3} / \text{Total de chamados recebidos com severidade 3}) \times 100$
 - 5.1.18.7. Início da vigência: Após 3 meses da assinatura do contrato
 - 5.1.18.8. Faixa no ajuste no pagamento: Glosa

5.1.18.9. Sanções: processo

5.1.18.10. Observações: nenhuma

5.2. No cálculo de indicadores que possuam principal fator a disponibilidade, a apuração dos resultados deverá desconsiderar períodos de indisponibilidades justificados, tais como:

5.2.1. Períodos de interrupção previamente acordados com o contratante;

5.2.2. Interrupção de serviços públicos essenciais à plena execução dos serviços (exemplo: suprimento de energia elétrica);

5.2.3. Indisponibilidade de acesso ao ambiente e/ou aos sistemas da rede, motivada por razões incontroláveis ou de força maior (exemplo: desastres naturais, enchentes, terremotos ou calamidade pública);

5.2.4. Falhas da infraestrutura que não aquela sob a responsabilidade do contratado;

5.2.5. Falhas em serviços ou ativos de TIC que tenham sido causadas pela ação de servidores ou colaboradores do contratante não relacionados ao contratado;

5.3. Outras eventualidades ocorridas durante a execução contratual mediante justificativa devidamente fundamentada do contratado

6. METODOLOGIA DE MEDIÇÃO

6.1. A fiscalização registrará todas as demandas (Requisições de Serviços, Incidentes, Problemas, Mudanças etc) e auditará os acordos de nível de serviços correspondentes ao catalogo de serviço, durante o período de medição mensal, cálculo do % SLA_{cumprido}.

7. COMUNICAÇÃO DE RESULTADOS

7.1. O resultado da apuração da pontuação do acordo de nível de serviços do respectivo IMR será comunicado pelo fiscal do contrato, por meio de notificação formal, à CONTRATADA, que terá 5 (cinco) dias úteis, a partir do recebimento da comunicação, para contestar o cálculo do SLA.

8. JUSTIFICATIVAS E EXCEPCIONALIDADES

8.1. A CONTRATADA poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pela CONTRATANTE, desde que comprovada a excepcionalidade da ocorrência, resultante de fatores imprevisíveis e alheios ao controle do prestador (por motivo de caso fortuito ou força maior).

8.2. Caso a justificativa não seja aceita, o fiscal do contrato realizará a medição conforme o valor apurado para o IMR e poderá aplicar as glosas e/ou penalidades previstas no contrato.

9. FATURAS AJUSTADAS

9.1. A CONTRATADA deverá apresentar ao fiscal/gestor do contrato a fatura referente ao período de medição com o valor ajustado pela aplicação do IMR. Caso a fatura apresentada não esteja ajustada ao valor apurado pelo IMR, esta será devolvida para a CONTRATADA ajustá-la ao valor correto medido pelo SLA.

10. DISPOSIÇÕES GERAIS

10.1. O IMR será recalculado a cada período de medição, sem considerar os valores apurados em medições anteriores, deste modo o IMR não é acumulativo para as medições, sendo realizado novo cálculo a cada período de medição dos serviços.

10.2. A não execução dos serviços previstos em contrato, além de impactar no cálculo do IMR, poderá resultar na aplicação de penalidades previstas no contrato, inclusive a rescisão unilateral sem ônus financeiro para a CONTRATANTE.

11. APROVAÇÃO

11.1. Este IMR entra em vigor na data de assinatura do contrato e servirá como referência para todas as medições realizadas durante a execução dos serviços.

SECRETARIA DA SEGURANÇA PÚBLICA

POLICIA MILITAR DO ESTADO DE SÃO PAULO

ANEXO A - PLANILHA SIMPLIFICADA PARA ESTIMATIVA DO VALOR MENSAL DO SERVIÇO

Departamento/ Divisão/Seção	Descrição – Categoria de Serviço	Perfil de Trabalho	Atribuição	Qtd	HTS	HTM	Custo Mensal (R\$)	Custo 30 Meses (R\$)
DAS/DOI DPC/DIVCIBER	Gerente de infraestrutura de tecnologia da informação	Serviço de Gestão de TIC	Coordenador/Governança /Gestão	1	176	176		
	Gerente de suporte técnico de tecnologia da informação	Serviço de Governança de TIC	Projetos/Processos	1	176	176		
	Analista de sistemas de automação - Júnior	Serviço de Suporte Técnico de Operação SO/NOC/SOC	SOC/NOC/SO	8	180	1440		
	Técnico de suporte ao usuário de tecnologia da informação Júnior	Serviço de Infraestrutura Data Center e Redes	N1/Dispatcher	2	176	352		
	Técnico de Rede (Telecomunicações) - Júnior	Serviço de Infraestrutura Data Center e Redes	Cabista	1	176	176		
DAS/DOI/SPD	Gerente de suporte técnico de tecnologia da informação	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	Líder	1	176	176		
	Analista de suporte computacional Pleno	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	Windows, Linux - Pleno	4	176	704		
	Administrador de sistemas operacionais Sênior	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	Windows, Linux - Senior	4	176	704		

	Administrador de sistemas operacionais Sênior	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	Notes - Senior	3	176	528		
	Administrador de banco de dados - Sênior	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	DBA SQL e (Oracle) - Senior	1	176	176		
	Administrador de banco de dados - Pleno	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	DBA SQL - Pleno	2	176	352		
	Especialista em Cloud Sênior	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	IA - Arquiteto de Solução - Senior	1	176	176		
DAS/DOI/SER	Gerente de segurança da informação	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	Lider de Segurança	1	176	176		
	Gerente de segurança da informação	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	Líder de Infraestrutura	1	176	176		
	Analista de redes e de comunicação de dados Sênior	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	N3	4	176	704		
	Analista de redes e de comunicação de dados Pleno	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	N2	7	176	1232		
DPC/DIVCIBER	Administrador em segurança da informação - Sênior	Serviço de Suporte Técnico de Análise de Threat Hunting	Senior	1	176	176		
	Analista de sistemas de automação - Pleno	Serviço de Suporte Técnico de Análise Threat Intelligence	Pleno	1	176	176		

	Desenvolvedor de sistemas de tecnologia da informação Sênior	Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center	Full Stack - DevSecOps - Senior	1	176	176		
Total				45		7952		

HTR – Hora Técnica por Serviço

HTM – Hora Técnica Mensal

SECRETARIA DA SEGURANÇA PÚBLICA

POLICIA MILITAR DO ESTADO DE SÃO PAULO

ANEXO C - PLANILHA DE CUSTOS E FORMAÇÃO DE PREÇOS

1. Orientações gerais sobre a planilha de custos e formação de preços

1.1. A Planilha de Custos e Formação de Preços é uma importante ferramenta que contribui para a análise crítica da composição dos preços unitários e total, com vistas a mitigar a assimetria de informações e auxiliar na eventual realização de diligência destinada a esclarecer ou a complementar a instrução do processo.

1.1.2. A Planilha de Custos e Formação de Preços deve ser entregue pelo licitante durante a fase de recebimento de propostas e não se vincula à estimativa apresentada pela PMESP na fase de planejamento da contratação.

1.1.3. Por se tratar de contratação por pagamento fixo mensal com mão de obra com dedicação exclusiva, vinculada ao atendimento de níveis mínimos de serviços:

a) O contratado deverá alocar os profissionais mínimos exigidos para cada perfil em cada demanda, além respeitar o limite mínimo da base salarial dos profissionais e demais encargos e custos previstos na planilha de custos e formação de preços constante da proposta vencedora da licitação;

b) A fiscalização do contrato verificará o alcance do objetivo da demanda, a efetiva disponibilização dos profissionais mínimos previstos para cada perfil, a qualidade dos produtos/resultados entregues e o prazo de atendimento conforme critérios de aceitação e níveis mínimos de serviço estabelecidos;

c) O contratado possui gestão sobre a equipe alocada no contrato, podendo realizar alterações na quantidade dos profissionais envolvidos na prestação do serviço, desde que alocue a quantidade mínima de profissionais prevista na respectiva demanda, observando a senioridade e qualificação profissional mínima requerida.

2. Planilha de custos e formação de preços

2.1. A Planilha de Custos e Formação de Preços deverá ser elaborada para cada item previsto no objeto da contratação, conforme estrutura mínima a seguir:

Identificação do Perfil Profissional	Salário (S)	Custo total por perfil (CT=S)	Qtde. profissionais por perfil (Q)	Custo Mensal por Perfil (CM=CTxQ)
1				
2				
3				
4				
5				
6				
7				
8				
9				
...				
n				

Descrição	Memória de Cálculo / Justificativa
Custos com software	
Custos com recursos de computação	
Custos com equipamentos	
Custos com serviços de informações	

Outros custos (especificar)	
Subtotal Demais componentes de custo	
Componentes de Preço	

Descrição	Valor Mensal
Elementos Comerciais (Fatores/Ajustes Comerciais)	
Cobertura Tributária	
Outros componentes (especificar)	
Subtotal componentes de preço	
Total Mensal:	
Valor Total: [Valor mensal x 30 meses]	

3. Os componentes de custos que integram a planilha são:

a) Custo de Pessoal: Consolida todos os custos incorridos com a utilização de serviços de profissionais, que mantém vínculo celetista com a empresa contratada. Deverá ser computado o somatório de todos os custos acrescidos dos encargos aprovionados que afetem a composição do preço final ofertado, a exemplo da remuneração, encargos sociais, auxílios e benefícios dos recursos humanos relacionados à prestação do serviço.

b) Custos com software: Equivale ao somatório de todos os custos de disponibilização e utilização de recursos de software que integrarão a prestação dos serviços e que afetem a composição do preço final ofertado, a exemplo de ferramentas de EDR, XDR, OSINT, SIEM, SYSLOG, APM, NPM, NPB, ZABBIX, ITSM, dentre outras. Na coluna "Memória de Cálculo / Justificativa", os custos devem ser apresentados com as justificativas que demonstrem a memória de cálculo, evidenciando o tipo, identificação (nome do produto e código único de identificação), forma de licenciamento ou aquisição e o valor total do software adquirido, além do período previsto de amortização desses custos e outras informações que permitam descrever os critérios de rateio desses custos que resultam no valor declarado.

c) Custos com recursos de computação: Equivale ao somatório de todos os custos de disponibilização e utilização de recursos físicos ou virtuais de computação que integrarão a prestação dos serviços e que afetem a composição do preço final ofertado, a exemplo de instâncias de computação, plataformas, middlewares, centrais de processamento de dados, entre outros recursos de computação. Na coluna "Memória de Cálculo / Justificativa", os custos devem ser apresentados com as justificativas que demonstrem a memória de cálculo, evidenciando o tipo, identificação (nome do produto), forma de aquisição e o valor total dos recursos adquiridos, além do período previsto de amortização desses custos e outras informações que permitam descrever os critérios de rateio desses custos que resultam no valor declarado.

d) Custos com equipamentos: Equivale ao somatório de todos os custos de disponibilização e utilização de equipamentos, utilitários e dispositivos diversos que serão utilizados diretamente na prestação dos serviços e que afetem a composição do preço final ofertado, a exemplo de equipamentos de comunicação, ferramentas de medição eletrônica, tokens, mídias, gerador de sinal, dentre outros. Na coluna "Memória de Cálculo / Justificativa", os custos devem ser apresentados com as justificativas que demonstrem a memória de cálculo, evidenciando o tipo, identificação (nome do produto), forma de aquisição e o valor total dos equipamentos adquiridos, além do período previsto de amortização desses custos e outras informações que permitam descrever os critérios de rateio desses custos que resultam no valor declarado.

e) Custos com serviços de informações: Equivale ao somatório de todos os custos de fornecimento de informações técnicas especializadas às equipes que prestam os serviços e que afetem a composição do preço final ofertado, a exemplo de plataformas digitais de fornecimento de conteúdo técnico especializado, serviços de mentoring, plataformas de suporte especializado, entre outras soluções de fornecimento de informações técnicas especializadas. Na coluna "Memória de Cálculo / Justificativa", os custos devem ser apresentados com as justificativas que demonstrem a memória de cálculo, evidenciando o tipo, identificação (nome do serviço e código único de identificação), forma de licenciamento e o valor total do serviço adquirido, além do período previsto de amortização desses custos e outras informações que permitam descrever os critérios de rateio desses custos que resultam no valor declarado.

4. Os componentes de formação do preço que integram a planilha são:

a) Elementos Comerciais (Fatores/Ajustes Comerciais): Fator de preço que pode ser aplicado, tendo como base estratégias de negócio, elementos mercadológicos e estratégias de precificação da empresa, a exemplo de margem operacional, margem de risco, lucro, dentre outros fatores internos e externos considerados na precificação.

b) Cobertura Tributária: Fator de preço que inclui os custos tributários associados à prestação dos serviços que variam de acordo com o planejamento tributário de cada empresa.

5. Para cada Perfil Profissional deverá ser apresentada a planilha complementar a seguir:

Nº PROCESSO

LICITAÇÃO Nº

CNPJ

NOME DA EMPRESA

LOTE

ITEM

PERFIL PROFISSIONAL

Discriminação dos Serviços (dados referentes à contratação)	
A Data da Apresentação da Proposta (dia/mês/ano)	
B Município/UF	
C Ano acordo, convenção ou Sentença Normativa em Dissídio Coletivo	
D Número de Meses de Execução do Contrato	
E Numero de registro da convenção coletiva de trabalho	
F Regime Tributário da Empresa:	

Dados complementares para composição dos custos referentes ao profissional alocado	
1 Tipo de Serviço (mesmo serviço com características distintas)	
2 Remuneração do profissional	
3 Categoria Profissional (vinculada à execução contratual) :	
4 Data Base da Categoria (dia/mês/ano)	

MÓDULO 1: COMPOSIÇÃO DA REMUNERAÇÃO		
1 Composição da Remuneração	Valor	(R\$)
A Salário Base		R\$
B Adicional de Periculosidade	%	R\$

C Adicional de Insalubridade	%	R\$
D Adicional Noturno		R\$
E Hora Noturna Adicional		R\$
F Adicional de Hora Extra no feriado trabalhado		R\$
G Outros (especificar)		R\$
TOTAL DO MÓDULO 1		R\$

MÓDULO 2: ENCARGOS E BENEFÍCIOS ANUAIS, MENSAIS E DIÁRIOS		
2.1 Submódulo 2.1 - 13º (décimo terceiro) Salário, Férias e Adicional de Férias	Valor	(R\$)
A 13º Salário	%	R\$
B Férias e Adicional de Férias	%	R\$
	Subtotal	R\$
Incidência do Submódulo 2.2	%	R\$
	Total R\$	R\$

2.2 Submódulo 2.2 - Encargos Previdenciários (GPS), FGTS e Outras Contribuições	Valor	(R\$)
A INSS	%	R\$
B Salário Educação	%	R\$
C Seguro Acidente de Trabalho RAT FAP	%	R\$
D SESI ou SESC	%	R\$
E SENAI ou SENAC	%	R\$
F SEBRAE	%	R\$
G INCRA	%	R\$
H FGTS	%	R\$
I Outras Contribuições (especificar)	%	R\$
	Total	R\$

2.3 Submódulo 2.3 - Benefícios Mensais e Diários	Valor	(R\$)
--------------------------------------------------	-------	-------

A Transporte: Nº Vales Valor do Vale Nº dias úteis Desc. Empregado	%	R\$
B Auxílio Alimentação (Vales, cestas básicas, etc.): Valor do Vale Nº dias úteis Desc. Empregado	%	R\$
C Assistência Médica e Familiar/Odontológica	%	R\$
D Auxílio Creche	%	R\$
E Seguro de vida, invalidez e funeral	%	R\$
F Auxílio cesta básica	%	R\$
I Outros (especificar)	%	R\$
Total	%	R\$

MÓDULO 2: RESUMO		
2.1 13º (décimo terceiro) Salário, Férias e Adicional de Férias		R\$
2.2 GPS, FGTS e outras contribuições		R\$
2.3 Benefícios Mensais e Diários		R\$
TOTAL DO MÓDULO 2		R\$

MÓDULO 3: PROVISÃO PARA RESCISÃO		
3.1 Provisão para Rescisão Valor		R\$
A Aviso Prévio Indenizado	%	R\$
B Incidência do FGTS sobre o Aviso Prévio Indenizado	%	R\$
C Aviso Prévio Trabalhado	%	R\$
D Incidência do Submódulo 2.2 sobre o Aviso Prévio Trabalhado	%	R\$
E Multa sobre o FGTS sobre o Aviso Prévio Indenizado e Trabalhado	%	R\$
TOTAL DO MÓDULO 3	%	R\$

MÓDULO 4: CUSTO DE REPOSIÇÃO DO PROFISSIONAL AUSENTE		
4.1 Submódulo 4.1 - Ausências Legais	Valor	(R\$)
A Férias e Terço Constitucional de Férias		R\$

B Ausências Legais	%	R\$
C Licença Paternidade Licenças/ano:	%	R\$
Incidência:		
D Ausência por Acidente de Trabalho Licenças/ano:	%	R\$
Incidência:		
E Afastamento Maternidade Licenças/ano:	%	R\$
Incidência:		
F Outros (especificar)	%	R\$
Total		R\$

4.2 Submódulo 4.2 - Intra jornada	Valor	R\$
A Substituto no Intervalo para repouso ou alimentação	%	R\$
Total		R\$

MÓDULO 4: RESUMO		
4.1 Substituto nas Ausências Legais		R\$
4.2 Substituto na Intra jornada		R\$
Subtotal do Módulo 4		R\$
Incidência do submódulo 2.2	%	R\$
TOTAL DO MÓDULO 4		R\$

MÓDULO 5: INSUMOS DIVERSOS		
5 Insumos Diversos (valores mensais por empregado)	Valor	(R\$)
A Uniformes (valor em parte não renovável)		R\$
B Materiais		R\$
C Microcomputador utilizado por profissional		R\$
D Outros (especificar)		R\$

TOTAL DO MÓDULO 5	R\$
-------------------	-----

MÓDULO 6: CUSTOS INDIRETOS, TRIBUTOS E LUCRO		
6 Custos Indiretos, Tributos e Lucro Base	Valor	(R\$)
A Custos Indiretos	%	R\$
B Lucro	%	R\$
Subtotal - Base de Cálculo de Tributos		R\$
Subtotal B - Base de Cálculo de Tributos por dentro ou racional		R\$

C.1 Tributos federais (COFINS)	%	R\$
C.2 Tributos Federais (PIS)	%	R\$
C.3 INSS (Desoneração)	%	R\$
D Tributos Estaduais (especificar)	%	R\$
E.1 Tributos Municipais (ISS)	%	R\$
E.2 Outros Tributos Municipais (especificar)	%	R\$
F Total dos Tributos	%	R\$

MÓDULO 6: RESUMO	
6.A Custos Indiretos	R\$
6.B Lucro	R\$
6.F Tributos	R\$
TOTAL DO MÓDULO 6	R\$

QUADRO RESUMO DO CUSTO DO PERFIL PROFISSIONAL		
Mão-de-Obra vinculada à execução contratual (valor por empregado)	Valor	(R\$)
A MÓDULO 1: COMPOSIÇÃO DA REMUNERAÇÃO		R\$
B MÓDULO 2: ENCARGOS E BENEFÍCIOS ANUAIS, MENSAIS E DIÁRIOS		R\$
C MÓDULO 3: PROVISÃO PARA RESCISÃO		R\$

D MÓDULO 4: CUSTO DE REPOSIÇÃO DO PROFISSIONAL AUSENTE	R\$
E MÓDULO 5: INSUMOS DIVERSOS	R\$
Subtotal (A + B + C + D + E)	R\$
F MÓDULO 6: CUSTOS INDIRETOS, TRIBUTOS E LUCRO	R\$

VALOR TOTAL DO PERFIL PROFISSIONAL	R\$
QUANTIDADE DE PROFISSIONAIS	
CUSTO TOTAL MENSAL DO PERFIL PROFISSIONAL	R\$
TOTAL ANUAL DO PERFIL PROFISSIONAL	R\$
TOTAL GLOBAL DO PERFIL PROFISSIONAL	

SECRETARIA DA SEGURANÇA PÚBLICA

POLICIA MILITAR DO ESTADO DE SÃO PAULO

ANEXO D - CATEGORIAS DE SERVIÇOS

1. A operação de infraestrutura de serviços de TIC abrange serviços continuados para monitoramento e sustentação do ambiente computacional que podem ser subdivididos nas seguintes categorias:

1.1. Gerenciamento de Serviços de TIC

a) Principais atividades:

Implantar e manter os processos de Gerenciamento de Serviços de TIC definidos pelo contratante, baseado nas melhores práticas, utilizando ferramenta(s) especializada(s);

Operar, manter, atualizar e criar fluxos de processos na ferramenta de Gerenciamento de Serviços de TIC;

Adaptar os fluxos básicos de incidentes, requisição, mudanças, problemas e configuração, com o desenho de formulários e criação de regras e validações;

Criar e adaptar outros fluxos de trabalho, ancorados nos processos básicos de gerenciamento de serviços de TI, o que inclui desenho de formulários e criação de regras e validações;

Discutir os requisitos dos fluxos de trabalho, para propor a sua adequação às boas práticas de Gerenciamento de Serviços de TI - GSTI;

Identificar melhorias nos processos básicos de gerenciamento de serviços de TIC sob a ótica das melhores práticas de GSTI preconizadas pelo ITIL;

Utilizar os indicadores chave de desempenho para apoiar a atividade de evolução dos processos;

Difundir o conhecimento de melhores práticas para as equipes de TIC;

Realizar as integrações das ferramentas necessárias para o correto funcionamento dos processos;

Resolver falhas relativas aos fluxos e à ferramenta de suporte ao gerenciamento de serviços de TIC;

Elaborar, manter e atualizar os relatórios de acompanhamento dos processos e indicadores de níveis de serviço;

Elaborar relatórios gerenciais e técnicos quando solicitados;

Realizar a interface de comunicação entre as demais categorias de serviços e o contratante.

b) Abordagem adotada no ambiente de TIC

Essa categoria é indicada para ambientes de TIC que possuem tanto abordagem tradicional quanto baseada em DevOps ou DevSecOps.

1.2. Sustentação de Infraestrutura para Aplicações

a) Principais atividades:

Projetar, operar, administrar e manter o conjunto de soluções, ferramentas, softwares e hardwares que compõe a camada de sustentação de serviços e aplicações do contratante;

Operar, administrar e manter os servidores físicos e virtuais do contratante;

Tratar incidentes, problemas, requisições e mudanças relacionados à camada de sustentação de serviços e aplicações do contratante;

Realizar configurações, alterações e otimizações no ambiente de sustentação de serviços e aplicações do contratante;

Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;

Acompanhar fornecedores caso necessário;

Elaborar e manter atualizada a documentação de todo o ambiente.

b) Abordagem adotada no ambiente de TIC

Essa categoria é indicada para ambientes de TIC que possuem abordagem baseada em DevOps ou DevSecOps.

1.3. Armazenamento e Backup

a) Principais atividades:

Projetar, operar, administrar e manter o conjunto de soluções, ferramentas, softwares e hardwares que compõe o ambiente de backup e armazenamento do contratante;

Executar, manter, atualizar, implantar e apoiar na criação das políticas de backup do contratante;

Tratar incidentes, problemas, requisições e mudanças relacionados ao ambiente de backup e armazenamento do contratante;

Realizar configurações, alterações e otimizações no ambiente de backup e armazenamento do contratante;

Realizar testes de restore com definição de frequência, a critério do contratante;

Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;

Acompanhar fornecedores caso necessário;

Elaborar e manter atualizada a documentação de todo o ambiente.

b) Abordagem adotada no ambiente de TIC

Essa categoria é indicada para ambientes de TIC que possuem tanto abordagem tradicional quanto baseada em DevOps ou DevSecOps.

1.4. Sustentação de Banco de Dados

a) Principais atividades:

Projetar, instalar, implantar, operar, administrar e manter o conjunto de ferramentas, softwares e hardwares que compõem recursos e soluções relacionadas a bancos de dados do contratante;

Tratar incidentes, problemas, requisições e mudanças relacionados ao ambiente de banco de dados do contratante;

Realizar configurações, alterações e otimizações no ambiente de banco de dados do contratante;

Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;

Acompanhar fornecedores caso necessário;

Registrar chamados para fornecedores das soluções;

Elaborar e manter atualizada a documentação de todo o ambiente.

b) Abordagem adotada no ambiente de TIC

Essa categoria é indicada para ambientes de TIC que possuem tanto abordagem tradicional quanto baseada em DevOps ou DevSecOps.

1.5. Administração de Dados

a) Principais atividades:

Apoiar na auditoria, análise, revisão de documentação relativas à modelagem de dados;

Construção de queries;

Apoiar na manutenção de repositório de metadados;
Manter esquemas de banco de dados;
Elaborar e manter modelo de dados;
Apoio na elaboração e definição de política de segurança do banco de dados;
Realizar apuração especial;
Confecção e manutenção de documentação e de procedimentos técnicos;
Validação de modelos de dados quanto às melhores práticas de modelagem;
Desenvolvimento, execução, teste e documentação de rotinas de Extração, Transformação e Carga - ETL;
Instalar, configurar, otimizar, parametrizar ferramenta ETL;
Sugerir automatização das rotinas.

b) Abordagem adotada no ambiente de TIC

Essa categoria é indicada para ambientes de TIC que possuem tanto abordagem tradicional quanto baseada em DevOps ou DevSecOps.

1.6. Conectividade e Comunicação

a) Principais atividades:

Projetar, operar, administrar e manter o conjunto de soluções, ferramentas, softwares e hardwares que compõe o ambiente de conectividade e comunicação do contratante;
Tratar incidentes, problemas, requisições e mudanças relacionados ao ambiente de conectividade e comunicação do contratante;
Realizar configurações, alterações e otimizações no ambiente de conectividade e comunicação do contratante;
Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;
Acompanhar fornecedores caso necessário;
Elaborar e manter atualizada a documentação de todo o ambiente.

b) Abordagem adotada no ambiente de TIC

Essa categoria é indicada para ambientes de TIC que possuem tanto abordagem tradicional quanto baseada em DevOps ou DevSecOps.

1.7. Segurança de TIC

a) Principais atividades:

Projetar, operar, administrar e manter o conjunto de soluções, ferramentas, softwares e hardwares que compõe o ambiente de segurança de TIC do contratante;
Tratar incidentes, problemas, requisições e mudanças relacionados ao ambiente de segurança de TIC do contratante;
Realizar configurações, alterações e otimizações no ambiente de segurança de TIC do contratante;
Realizar testes de vulnerabilidades dos sistemas e serviços de TIC do contratante, identificando os riscos e sugerindo ações para o devido tratamento;
Apoiar na elaboração e manutenção da política de segurança do contratante;
Apoiar na elaboração e manutenção do plano de continuidade de negócio do contratante;
Apoiar na elaboração e manutenção do plano de gerenciamento de risco do contratante;
Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;
Acompanhar fornecedores caso necessário;
Elaborar e manter atualizada a documentação de todo o ambiente.

b) Abordagem adotada no ambiente de TIC

Essa categoria é indicada para ambientes de TIC que possuem tanto abordagem tradicional quanto baseada em DevOps ou DevSecOps.

1.8. Monitoramento de Serviços de TIC

a) Principais atividades:

Realizar o monitoramento dos sistemas, aplicações, serviços e infraestrutura de TIC do contratante através de ferramenta (as) especializada (as);

Executar o plano de comunicação realizando os acionamentos dos responsáveis pela resolução dos incidentes, bem como manter informadas as partes interessadas;

Operar, administrar e manter o conjunto de ferramentas e softwares que compõe a solução de monitoramento de TIC do contratante;

Realizar configurações, alterações e otimizações na solução de monitoramento de TIC do contratante;

Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;

Acompanhar fornecedores caso necessário;

Elaborar e manter atualizada a documentação de toda a solução.

b) Abordagem adotada no ambiente de TIC

Essa categoria é indicada para ambientes de TIC que possuem tanto abordagem tradicional quanto baseada em DevOps ou DevSecOps.

1.9. Suporte ao Usuário

a) Principais atividades:

Administrar e manter o conjunto de softwares e hardwares que compõe o ambiente de dispositivos de usuários do contratante;

Tratar incidentes, problemas, requisições e mudanças relacionados ao ambiente de dispositivos de usuários do contratante;

Manter o registro de requisições de serviços solicitados e de reclamações efetuadas pelos usuários;

Realizar a instalação, configuração e atualização de softwares homologados pelo contratante;

Realizar a instalação, configuração e atualização de hardwares homologados pelo contratante;

Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;

Acompanhar fornecedores caso necessário;

Elaborar e manter atualizada a documentação de todo o ambiente;

Identificar, mapear e atualizar o inventário de ativos de TIC.

b) Abordagem adotada no ambiente de TIC

Essa categoria é indicada para ambientes de TIC que possuem central de serviços ou service desk implantado.

Os perfis profissionais que atuarão nas diferentes categorias são padronizados com vistas a possibilitar publicação periódica de pesquisa salarial pela SGD.

Cada perfil profissional possui uma característica e um propósito de atuação, conforme descrito a seguir:

2.1. Gerente de infraestrutura de tecnologia da informação

Profissional com responsabilidade de coordenar e gerenciar a atuação dos demais profissionais alocados no monitoramento, controle e operação da infraestrutura de TIC, garantindo a adequada prestação dos serviços, bem como controlando e planejando operacionalmente as ações dessa equipe. Presta também apoio à tomada de decisão do órgão auxiliando na prospecção de soluções de infraestrutura de TIC, fornecimento de informações táticas e operacionais, e proposição de ações de aprimoramento dos serviços de operações na infraestrutura de TIC.

2.2. Gerente de suporte técnico de tecnologia da informação

Profissional com responsabilidade de coordenar e gerenciar a atuação dos demais técnicos de suporte e de manutenção, garantindo a adequada prestação dos serviços, bem como controlando e planejando operacionalmente as ações da equipe. Presta também apoio à tomada de decisão do órgão auxiliando na prospecção de soluções de suporte ao usuário, fornecimento de informações táticas e operacionais e proposição de ações de aprimoramento dos serviços de suporte ao usuário.

2.3. Analista de sistemas de automação - (Júnior, Pleno e Sênior)

Profissional responsável por assegurar a utilização adequada de soluções de integração - CI ou de entrega contínua - CD. Pode atuar como arquiteto de soluções e propor, projetar, executar e aprimorar arquiteturas de soluções necessárias à manutenção e melhoria das operações na infraestrutura de TIC. Pode atuar também como arquiteto de computação em nuvem, ou ainda como arquiteto de soluções híbridas.

2.4. Técnico de suporte ao usuário de tecnologia da informação (Júnior, Pleno e Sênior)

Profissional atuante em centrais de atendimento de TIC (em nível 1) prestando suporte ao usuário, orientando-os na utilização de hardwares e softwares. Pode atuar no monitoramento de aplicações, recursos de rede, banco de dados, servidores entre outros componentes de serviço de TIC.

2.5. Técnico de Rede (Telecomunicações) (Júnior, Pleno e Sênior)

Profissional atuante no monitoramento, configuração, manutenção e otimização de recursos de telecomunicações de dados, áudio e vídeo. Atua também na integração e garantia do desempenho de redes de telecomunicações, centrais de comutação e integração a serviços de telefonia digital.

2.6. Analista de suporte computacional (Júnior, Pleno e Sênior)

Profissional atuante em nível 3 em uma central de atendimento ou associado ao centro de dados. Presta serviços de gerenciamento físico e lógico de equipamentos, servidores, storages, entre outros equipamentos do centro de dados ou no ambiente virtualizado. Atua também no gerenciamento de backups, configuração de procedimentos de recuperação de desastres computacionais, gerenciamento de recursos computacionais avançados (a exemplo de servidores de arquivos, de impressão e de comunicação institucional) que demandam alocação, configuração ou instalação de softwares ou construção e execução de scripts para o controle, monitoramento e gerenciamento desses recursos.

2.7. Administrador de sistemas operacionais (Júnior, Pleno e Sênior)

Profissional que atua na camada de virtualização e orquestração de sistemas operacionais de servidores de dados. Presta serviços de configuração, instalação e ampliação de ambientes de

containers. Responsável pela adequada operação, desempenho e uso racional de recursos utilizados pelos softwares básicos, orquestradores de containers e virtualizadores.

2.8. Administrador de banco de dados - (Júnior, Pleno e Sênior)

Profissional responsável pela administração, operação, gerenciamento, otimização e monitoramento dos recursos de banco de dados. Presta serviços de gerenciamento dos esquemas de banco de dados, alocação e administração de recursos físicos e lógicos, realiza dimensionamentos e prospecções de uso, monitora incidentes e promove adequações, aprimoramentos e expansão dos recursos. Pode atuar na análise de dados propondo padrões e assegurando a normalização e melhor uso dos recursos para armazenamento e utilização de dados corporativos.

2.9. Desenvolvedor de sistemas de tecnologia da Informação

Profissional com a responsabilidade de assegurar a implantação adequada dos entregáveis de softwares. Pode atuar como analista de teste de aplicações executando testes automatizados e assegurando a cobertura mínima de testes nas soluções entregues. Pode atuar como analista de qualidade dos produtos a serem implantados.

2.10. Especialista em Computação em Nuvem – Cloud (Pleno e Sênior)

Profissional responsável pela infraestrutura de nuvem, envolvendo a arquitetura, estruturação, operação, monitoramento, otimização, sustentação e migração de ambientes em nuvem.

2.11. Gerente de segurança da informação

Profissional com responsabilidade de coordenar e gerenciar a atuação dos demais profissionais de segurança da informação, garantindo a adequada prestação dos serviços, bem como controlando e planejando operacionalmente as ações dessa equipe. Presta também apoio à tomada de decisão do órgão auxiliando na prospecção de soluções de segurança da informação, fornecimento de informações táticas e operacionais, e proposição de ações de aprimoramento dos serviços de segurança da informação seja preventiva ou reativa.

2.12. Analista de redes e de comunicação de dados (Júnior, Pleno e Sênior)

Profissional que atua na intercomunicação de redes locais e de longa distância, com ou sem fio, assegurando a operação, desempenho e qualidade dos serviços de rede e comunicação de dados, bem como no aprimoramento e funcionamento adequados dos ativos de redes. Presta serviços de execução, aprimoramento e manutenção dos projetos de redes, além da configuração e otimização de recursos de interconexão de dados.

2.13. Administrador em segurança da informação - (Júnior, Pleno e Sênior)

Profissional responsável por assegurar a prestação de serviços de segurança da informação, incluindo o monitoramento e tratamento de incidentes, ações preventivas, implantação e monitoramento de controles de segurança, realização dos diferentes testes e inspeções de segurança. presta serviços de controle de segurança preventivo e reativo relacionados aos diferentes ativos da infraestrutura, bem como apoia na implementação das ações técnicas previstas na política de segurança.

SECRETARIA DA SEGURANÇA PÚBLICA

POLICIA MILITAR DO ESTADO DE SÃO PAULO

ANEXO E – Roteiro para fiscalização administrativa do cumprimento das obrigações trabalhistas, sociais e previdenciárias

1. A fiscalização administrativa deve ser realizada pelo Fiscal Administrativo do Contrato (servidor representante da Área Administrativa, indicado pela autoridade competente) e consiste no acompanhamento dos aspectos administrativos contratuais quanto às obrigações previdenciárias, fiscais e trabalhistas e quanto ao controle do contrato administrativo no que se refere a revisões, a reajustes, a repactuações e a providências tempestivas nas hipóteses de inadimplemento.

2. A fiscalização das obrigações trabalhistas, previdenciárias e com o FGTS realizada nos contratos de prestação de serviços de operação de infraestrutura e atendimento ao usuário poderá ser realizada por amostragem, de modo que a documentação de todos os empregados alocados em ordens de serviços seja avaliada ao final de um ano, sem prejuízo de a análise ser realizada mais de uma vez para um mesmo empregado.

2.1 A extensão da amostra mensal não deve ser inferior a 10% do total de funcionários alocados em ordens de serviços e poderá ser majorada caso a equipe de fiscalização julgue necessário, em razão da avaliação do risco de descumprimento pela contratada das obrigações trabalhistas e previdenciárias com os empregados.

3. O fiscal Administrativo deve:

- a) Prestar apoio técnico e operacional ao gestor do contrato, com a realização das tarefas relacionadas ao controle dos prazos relacionados ao contrato e à formalização de apostilamentos e de termos aditivos, ao acompanhamento do empenho e do pagamento e ao acompanhamento de garantias e glosas;
- b) Verificar a manutenção das condições de habilitação da contratada, com a solicitação dos documentos comprobatórios pertinentes, caso necessário;
- c) Examinar a regularidade no recolhimento das contribuições fiscais, trabalhistas e previdenciárias e na hipótese de descumprimento;
- d) Atuar tempestivamente na solução de eventuais problemas relacionados ao descumprimento das obrigações contratuais e reportar ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência;
- e) Auxiliar o gestor do contrato com as informações necessárias, na elaboração do documento comprobatório da avaliação realizada na fiscalização do cumprimento de obrigações assumidas pelo contratado;
- f) Verificar a aderência aos termos contratuais e atuação tempestiva na solução de eventuais problemas relacionados ao descumprimento das obrigações contratuais e reportar ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência;
- g) Verificar as regularidades fiscais, trabalhistas e previdenciárias para fins de pagamento;

- h) Apoiar o Fiscal Requisitante do Contrato na verificação da manutenção da necessidade, economicidade e oportunidade da contratação;
 - i) Apoiar o Gestor do Contrato na manutenção do Histórico de Gestão do Contrato;
 - j) Elaborar relatório de acompanhamento mensal do contrato, com o cálculo de desconto de horas ou dias não trabalhados pelos profissionais e as retenções/glosas aplicadas à contratada nos termos do contrato;
 - k) Analisar, juntamente com o fiscal técnico, os documentos apresentados para pagamento juntamente com a nota fiscal, conferi-los com as condições estabelecidas no contrato e submeter ao gestor para ateste ou para notificação da contratada de impropriedade constatada;
 - l) Solicitar à contratada, periodicamente e por amostragem, comprovantes dos registros de recolhimento das contribuições previdenciárias e do FGTS dos profissionais alocados nas ordens de serviço. A consulta poderá ser solicitada mais de uma vez para o mesmo empregado, contudo o objetivo é que todos os empregados tenham seus extratos avaliados ao final de um ano. As pendências constatadas deverão ser comunicadas imediatamente ao gestor do contrato para as providências devidas;
 - m) Instruir e submeter ao gestor do contrato o pedido de prorrogação contratual, mediante a juntada da documentação que habilitou a contratada devidamente atualizada, bem como da pesquisa de mercado e avaliação dos resultados obtidos que comprovem a necessidade e a vantagem econômica da contratação;
 - n) Informar ao gestor do contrato a execução dos saldos empenhados e as questões previdenciárias, trabalhistas e fiscais, quando necessário;
 - o) Solicitar à contratada a documentação necessária para a análise relativa à observância da legislação referente à concessão de férias e licenças, bem como do respeito à estabilidade provisória de seus empregados (estabilidade gestante e acidentária) para avaliação da unidade competente.
4. No caso de substituição ou inclusão de empregados da contratada, o Fiscal Administrativo do Contrato deve exigir ao preposto os Termos de Ciência e de Responsabilidade assinados pelos novos empregados envolvidos na execução dos serviços contratados, além da documentação comprobatória de vínculo trabalhista com a empresa contratada e outros documentos exigidos no Termo de Referência.
5. O Fiscal Administrativo deverá mensalmente verificar se foram realizados, dentro do prazo, os pagamentos salariais e dos benefícios aos prestadores de serviço conforme estabelecido em contrato.
6. O exame da regularidade no recolhimento das contribuições fiscais, trabalhistas e previdenciárias abrange conferir os documentos comprobatórios do adimplemento das obrigações trabalhistas, previdenciárias e fiscais, exigidos em contrato para a realização do pagamento, especialmente:
- a) Pagamento do salário dos empregados;
 - b) Repasse dos valores referentes a vale-transporte e auxílio alimentação;
 - c) Recolhimento do Fundo de Garantia por Tempo de Serviço;

- d) Recolhimento da Previdência Social;
- e) Certidões negativas da empresa (CNDT, CRF e certidões negativas ou positivas com efeito de negativa relativas aos créditos tributários federais, municipais ou distritais, conforme o caso);
- f) Concessão de férias e licenças aos empregados; e
- g) Pagamento de verbas rescisórias.

7. O fiscal administrativo poderá exigir da contratada, por amostragem, a entrega do extrato da conta do INSS e do FGTS de qualquer empregado, bem como de outros documentos previstos em contrato ou instrumento coletivo da categoria, que deverão ser entregues no prazo máximo de quinze dias corridos.

8. Os direitos não previstos em contrato, mas previstos no instrumento coletivo da categoria, deverão ser fiscalizados pelo fiscal administrativo no máximo a cada três meses.

9. Cabe esclarecer e informar que as cláusulas do contrato são os atos formais para do Gestor Contratual e este Anexo segue como roteiro complementar para fiscalização administrativa.

SECRETARIA DA SEGURANÇA PÚBLICA

POLICIA MILITAR DO ESTADO DE SÃO PAULO

ANEXO F - MODELO DE RELATÓRIO DE FISCALIZAÇÃO TÉCNICA

1 - INTRODUÇÃO

1.1. O contrato nº <xx/aaaa>, processo <nº do processo>, objeto deste relatório, é relativo à prestação de serviços de <descrição do objeto>. Os serviços são prestados pela empresa <Nome da Contratado>, CNPJ: <número do CNPJ>, iniciado em <dd/mm/aaaa> (Pregão Eletrônico nº XX/AAAA). A fiscalização técnica executada pelo(s) servidor(es) <Nome do(s) Servidor(es)>, iniciou-se em <dd/mm/aaaa>, após a publicação da Portaria Nº <número da portaria>, de <dd/mm/aaaa>.

2 - REGISTRO DE OCORRÊNCIAS

2.1. Conforme § 1º do art. 117 da Lei nº 14.133, de 2021, a execução do contrato deverá ser acompanhada e fiscalizada por representantes da Administração, que deverão anotar em registro próprio todas as ocorrências relacionadas com a execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados.

Dessa forma, a partir da nomeação do fiscal técnico, mantém-se registro em planilha eletrônica sobre todas as ocorrências relacionadas à execução deste contrato (tabela a seguir):

ID	Data	Tipo de Ocorrência	Descrição da Ocorrência	Sistema Afetado
1	01/12/2025			
2				
...				
n				

3 - AFERIÇÃO DOS NÍVEIS DE SERVIÇO

3.1. A verificação da adequação da prestação do serviço é realizada com base em Níveis de Serviço definidos nesta seção.

3.2. A aferição dos níveis mínimos de serviço das Ordens de Serviço entregues no mês de <mm/aaaa> evidenciou:

Indicadores:

Identificação da Ordem de Serviço relacionada:

Valor Aferido do indicador:

Valor total das Ordens de Serviços:

Situação:

(atendido/Não atendido)

Glosas/faixas de ajuste aplicadas:

Valor da Glosa apurada:

Indicação de sanção:

Observações complementares:

4 - Dessa forma, encaminhamos este Relatório de Fiscalização para análise do(a) Gestor(a) do Contrato e providências cabíveis.

Este é o relatório.

(Documento assinado eletronicamente)

<NOME DO FISCAL TECNICO>

Fiscal Técnico

SECRETARIA DA SEGURANÇA PÚBLICA

POLICIA MILITAR DO ESTADO DE SÃO PAULO

APÊNDICE A1 – TERMO DE CONFIDENCIALIDADE E SIGILO

1. Comprometo-me a cumprir rigorosamente as normas regulamentares sobre a utilização dos meios e infraestrutura e as diretrizes estipuladas pela Polícia Militar do Estado de São Paulo (PMESP).

2. Comprometo-me a manter a confidencialidade com relação a toda a documentação, toda a informação, ou acesso predial obtido nas atividades exercidas, envolvidas e vinculadas à Polícia Militar do Estado de São Paulo (PMESP), oriunda de qualquer pessoa física, jurídica, de terceiros vinculados de alguma, concordando em:

2.1. não divulgar a qualquer pessoa, que não esteja expressamente autorizada pela PMESP, o conteúdo de documentação, informação, ou dos acessos prediais;

2.2. não permitir a nenhuma pessoa o manuseio de qualquer documentação física ou eletrônica que componha ou tenha resultado de atividades, sem a devida autorização da PMESP;

2.3. não explorar, em benefício próprio ou de terceiros, informações e documentos adquiridos pela participação em atividades da aquisição e implantação da solução.

3. Estou ciente também de que a PMESP se reserva ao direito de monitorar e auditar quaisquer atividades que envolvam estas informações.

4. Estou ciente de que os termos contidos neste TERMO DE MANUTENÇÃO DO SIGILO se estendem por tempo indeterminado, independente da quebra do vínculo profissional com a PMESP.

São Paulo, de _____ de _____ 20_____.

Empresa:

Nome:

Função na Empresa:

RG:

CPF:

Fone/Ramal:

E-mail:

SECRETARIA DA SEGURANÇA PÚBLICA

POLICIA MILITAR DO ESTADO DE SÃO PAULO

APÊNDICE A2 – ATESTADO DE VISITA TÉCNICA

ATESTAMOS, para fins de participação na licitação referente à *contratação de serviços especializados de suporte técnico de cibersegurança, data center e redes, bem como de governança, gerenciamento e monitoramento, das demandas e mudanças de tecnologia da informação e comunicação e infraestrutura de data center e redes para ambiente computacional e de telecomunicações, de forma a garantir a continuidade dos serviços de TIC.*, que a empresa abaixo, por intermédio de seu representante infra-assinado, realizou a visita técnica, nesta data, no Departamento de Aplicações e Sistemas da Polícia Militar do Estado de São Paulo, localizado na Rua Ribeiro de Lima, nº 140 – Bom Retiro, São Paulo/SP e demais locais, tomando conhecimento dos detalhes e condições inerentes à referida licitação, para adequar a elaboração das propostas às peculiaridades do objeto pretendido, dirimir dúvidas e dar pleno conhecimento das instalações e necessidades.

São Paulo, de de .20....

Nome do integrante da PMESP

Posto/Graduação – Função

EMPRESA INTERESSADA: *Nome da empresa*

CNPJ:

Declaro que, nesta oportunidade, assinei o Termo de Manutenção de Sigilo, pois tive acesso às informações da Polícia Militar, necessárias à elaboração da proposta para participação no certame, e fui informado de que demais esclarecimentos serão prestados em publicação no Diário Oficial do Estado.

..... (assinatura).....

NOME COMPLETO:

RG:

FUNÇÃO NA EMPRESA:.....

SECRETARIA DA SEGURANÇA PÚBLICA
POLÍCIA MILITAR DO ESTADO DE SÃO PAULO
APÊNDICE A4 – PLANILHA PONTO-A-PONTO

Empresa: _____

Exigência Técnica		Documento de Comprovação	Página(s)	Observação
9.	Levantamento de Soluções:			
9.1.	Ferramentas e Tecnologias Aplicadas			
9.1.1.	Para otimizar o processo de operação e reduzir a necessidade de efetivo técnico, a contratada deverá aplicar ferramentas e softwares especializados que monitorarão e munirão os analistas com informações detalhadas e em tempo real. Essas ferramentas permitirão análises automatizadas e precisas, facilitando a tomada de decisão, maximizando a eficiência dos serviços.			
9.1.2.	As ferramentas utilizadas para a prestação dos serviços deverão ser plenamente compatíveis com o ambiente tecnológico da CONTRATANTE, assegurando integração, escalabilidade, desempenho e conformidade com os requisitos de segurança da informação. A CONTRATADA deverá utilizar exclusivamente ferramentas licenciadas, onde a Contratada possuir também ferramentas licenciadas, a exemplo EDR, devidamente licenciadas e reconhecidas pelo mercado, garantindo níveis adequados de suporte, atualização contínua, confiabilidade, auditoria e segurança, bem como ferramentas open onde a Contratada utiliza ferramenta open, a exemplo Zabbix,. Não haverá imposição de fabricante, marca ou modelo específico; contudo, todas as licenças, assinaturas, renovações e demais custos associados às ferramentas utilizadas deverão estar integralmente incluídos na proposta comercial da CONTRATADA e mantidos durante todo o período contratual.			
9.1.3.	As ferramentas devem ser tecnicamente reconhecidas pelo mercado e amplamente adotadas por organizações de grande porte, garantindo suporte e atualizações regulares das ferramentas.			
9.1.4.	Todas as ferramentas utilizadas deverão possuir suporte técnico e manutenção garantidos pela CONTRATADA, incluindo correções de segurança, patches e atualizações durante toda a vigência do contrato.			
9.1.5.	As soluções devem oferecer capacidade de integração via APIs abertas ou conectores seguros, permitindo interoperabilidade com os sistemas e infraestruturas já existentes da CONTRATANTE, principalmente o ITSM, sistema que irá proporcionar padrão no atendimento dos SLAs.			
9.1.6.	As ferramentas escolhidas devem atender requisitos normativos e boas práticas.			
9.1.7.	A CONTRATANTE não exigirá métricas de desempenho ou KPIs específicos das ferramentas, mas o desempenho final dos serviços prestados deverá atender aos SLA e níveis de serviço estabelecidos no contrato principal.			
9.1.8.	A CONTRATADA será responsável por dimensionar corretamente as ferramentas, garantindo que possuam capacidade suficiente para suportar o ambiente da CONTRATANTE, conforme o escopo dos serviços contratados.			
9.1.9.	A CONTRATADA deverá executar Testes de Penetração da rede (Pentest) internos e externos para identificação de vulnerabilidades;			
9.1.10.	Executar testes de penetração em sistemas, redes e aplicações: para identificar vulnerabilidades exploráveis e avaliar a postura de segurança da infraestrutura da CONTRATANTE.			

9.2.	Ferramentas para o SOC (Security Operations Center)			
9.2.1.	A operação do SOC deverá ser sustentada por uma suíte de ferramentas integradas para detecção, análise e resposta a incidentes, correlação em tempo real, e integração com feeds de Threat Intelligence externos e internos.			
9.2.2.	A CONTRATADA poderá adotar outras ferramentas adicionais, conforme necessário, desde que respeitem as diretrizes e políticas de segurança da PMESP e que sejam compatíveis com os serviços prestados.			
9.2.3.	Para garantir um nível mínimo de segurança e capacidade operacional, as seguintes ferramentas são exigidas:			
9.2.3.1.	Módulo de Gestão e Correlação de Eventos (SIEM);			
9.2.3.2.	Modulo de Sistema de Logs (SysLog);			
9.2.3.3.	Modulo de Detecção em Endpoint (EDR);			
9.2.3.4.	Módulo Avançado de Detecção e Resposta (XDR);			
9.2.3.5.	Módulo de Teste de Penetração (PENTEST);			
9.2.3.6.	Modulo de Threat Intelligence (OSINT);			
9.3.	Modulo de Gestão e Correlação de Eventos (SIEM) e Modulo de Sistema de Logs (SysLog):			
9.3.1.	A CONTRATADA deverá fornecer o serviço de Security Information and Event Management (SIEM), contemplando a coleta, armazenamento, análise, classificação e correlação de logs de segurança provenientes de diversas fontes, garantindo auditoria, compliance e detecção de incidentes.			
9.3.2.	A ferramenta de SIEM deverá ser uma solução utilizada no âmbito público, adotada em serviços de SOC, e capaz de atender a requisitos de segurança da informação. A solução deverá oferecer funcionalidades de monitoramento, detecção de ameaças e resposta a incidentes, suportando, no mínimo, 3.000 (três mil) eventos por segundo e ou 133GB/DIA, com garantia de escalabilidade e desempenho adequados às demandas do CONTRATANTE.			
9.3.3.	A ferramenta de SIEM, como elemento central para processamento e armazenamento de logs e eventos, com histórico comprovado em ambientes governamentais, e capacidade de ingestão superior a 1.000 EPS (Eventos por Segundo).			
9.3.4.	É importante destacar que o licenciamento deverá suportar até 3.000 (três mil) EPS com 30 dias de retenção. E quanto ao Syslog 5 (cinco) anos de retenção. E o custo do software será apurado mensalmente, de modo a permitir o correto dimensionamento dos pagamentos.			
9.3.5.	O serviço deverá ser contínuo e ininterrupto (24x7x365), garantindo a ingestão e o tratamento adequado dos eventos de segurança do ambiente computacional do CONTRATANTE.			
9.3.6.	A prestação do serviço deve incluir, no mínimo:			
9.3.6.1.	Administração e operação da solução de SIEM.			
9.3.6.2.	Monitoramento contínuo e análise de eventos de segurança.			
9.3.6.3.	Suporte técnico e manutenção evolutiva e corretiva da solução.			
9.3.6.4.	Implementação de processos para avaliação e otimização da ingestão de logs.			
9.3.6.5.	Atualizações regulares, garantindo segurança, patches e melhorias contínuas.			
9.3.6.6.	A ferramenta de SIEM deverá incorporar tecnologias, alinhadas às melhores práticas do mercado, para identificar eventos de segurança e comportamentos anômalos com maior assertividade, superando limitações de tecnologias tradicionais, aprimorando a detecção de ameaças com alta precisão, reduzindo falsos positivos.			
9.3.7.	Integração e Compatibilidade			

9.3.7.1.	A ferramenta de SIEM deverá possuir integração nativa com as demais ferramentas da SOLUÇÃO, ou via APIs seguras, garantindo a interoperabilidade e a cobertura completa das funcionalidades necessárias.			
9.3.7.2.	Deve ser capaz de coletar, normalizar e correlacionar logs de diversas fontes, incluindo sistemas operacionais, aplicações, dispositivos de rede, firewalls, sistemas de autenticação e demais sistemas de segurança.			
9.3.7.3.	A solução deverá permitir a ingestão de eventos utilizando padrões como:			
9.3.7.3.1.	Syslog RFC 3164 e RFC 5424			
9.3.7.3.2.	CEF (Common Event Format)			
9.3.7.3.3.	JSON, XML, CSV e logs estruturados			
9.3.7.3.4.	Microsoft Windows Event Logs			
9.3.7.3.5.	ODBC/JDBC para bancos de dados			
9.3.7.3.6.	NetFlow/IPFIX para análise de tráfego de rede			
9.3.7.4.	Deverá possuir painéis de análise, com dashboards interativos e personalizáveis, classificação de incidentes por criticidade, apresentação das evidências associadas e possibilidade de integração com ferramentas externas para implementação de workflow de tratamento e escalonamento.			
9.3.7.5.	Deve permitir a criação e personalização de regras de correlação de eventos, permitindo ajustes conforme o ambiente do CONTRATANTE, incluindo:			
9.3.7.6.	Definição de alertas customizados.			
9.3.7.7.	Aplicação de regras para detectar padrões de ataques e ameaças persistentes.			
9.3.7.8.	Filtragem e categorização de eventos de segurança.			
9.3.8.	Infraestrutura e Segurança			
9.3.8.1.	A ferramenta de SIEM deverá ser disponibilizada em infraestrutura própria da CONTRATADA ou em ambiente de nuvem, podendo ser ofertada na modalidade SaaS (Software as a Service), PaaS (Platform as a Service) ou hospedagem dedicada, desde que atenda aos requisitos de segurança e desempenho estabelecidos.			
9.3.8.2.	O ambiente utilizado pela CONTRATADA para hospedagem da solução deverá atender aos seguintes requisitos mínimos:			
9.3.8.3.	Infraestrutura de alta disponibilidade e resiliência, garantindo continuidade dos serviços e recuperação de desastres.			
9.3.8.4.	Armazenamento e processamento dos dados do CONTRATANTE em conformidade com regulamentações de proteção de dados aplicáveis.			
9.3.8.5.	Isolamento adequado dos dados do CONTRATANTE para evitar concorrência de recursos críticos com outros clientes.			
9.3.8.6.	A CONTRATADA deverá garantir que a comunicação entre os elementos locais do CONTRATANTE e o SIEM seja realizada por meio de conexões seguras, utilizando TLS 1.2 ou superior, com protocolos criptográficos robustos que assegurem a integridade e a confidencialidade dos dados.			
9.3.9.	Gestão de Eventos e Resposta a Incidentes			
9.3.9.1.	A ferramenta de SIEM deverá permitir:			
9.3.9.1.1.	Deteção e categorização automática de ameaças.			
9.3.9.1.2.	Geração de alertas e notificações em tempo real sobre eventos suspeitos.			
9.3.9.1.3.	A solução deverá permitir o encaminhamento automático de alertas para plataformas externas de orquestração de resposta, possibilitando a execução de playbooks automatizados, enriquecimento com fontes de Threat Intelligence e acionamento escalonado por severidade, com suporte a integrações que permitam gestão baseada em SLA.			

9.3.9.2.	A solução deverá possuir interface gráfica para análise forense, permitindo:			
9.3.9.2.1.	Busca avançada com suporte a expressões regulares (regex) e filtros adaptativos, utilizando sintaxe de consulta compatível com ferramentas de mercado, e possibilidade de integração com mecanismos externos para execução de consultas YARA, quando aplicável.			
9.3.9.2.2.	Visualização centralizada dos eventos e alertas de segurança.			
9.3.9.2.3.	Geração de relatórios detalhados e gráficos interativos para auditoria e investigação.			
9.3.9.2.4.	Retenção de dados configurável, com possibilidade de exportação segura e integridade garantida por mecanismos de criptografia e/ou assinatura digital, incluindo integração com ferramentas externas quando necessário para atender à cadeia de custódia.			
9.3.9.3.	A ferramenta de SIEM deverá permitir a configuração de políticas de retenção de logs, suportando pelo menos dois níveis de armazenamento:			
9.3.9.3.1.	SIEM: Retenção de logs ativos por até 30 dias.			
9.3.9.3.2.	SISLOG: Arquivamento de logs de longo prazo por pelo menos 60 meses.			
9.3.9.4.	Deve suportar a exportação de logs e incidentes, permitindo que o CONTRATANTE migre os dados para outro prestador de serviço, sem custo adicional e sem perda de integridade.			
9.3.10.	Responsabilidades da CONTRATADA			
9.3.10.1.	A CONTRATADA será integralmente responsável pelo fornecimento, suporte e manutenção da solução.			
9.3.10.2.	Licenciamento oficial e vigente da ferramenta durante toda a vigência do contrato.			
9.3.10.3.	Monitoramento contínuo e atualizações regulares de segurança.			
9.3.10.4.	Treinamento operacional para os responsáveis pelo uso da solução.			
9.3.10.5.	A CONTRATADA deve promover a automação de processos e fluxos de trabalho, que por sua vez, deverá ser capaz de criá-los por meio de interface low-code/no-code com biblioteca de conectores prontos (REST/SOAP) e integração a ferramentas como EDR, Firewall, DLP e antivírus.			
9.3.10.6.	Possuir recursos gráficos de workflow interativos para criação e processos e rotinas operacionais, que permita operações como arrastar-e-soltar para o desenho dos fluxos de trabalho;			
9.3.10.7.	Apresentar componente próprio para a modelagem gráfica e a automação de processos e fluxos de trabalho da solução;			
9.3.10.8.	Permitir a automação de fluxos de automação de forma gráfica, incluindo estágios, tarefas paralelas ou sequenciais, regras de decisão e aprovação, sem a necessidade de programação ou alteração de código fonte;			
9.3.10.9.	Possuir ferramenta de criação de formulários com campos específicos de cada processo e fluxo de trabalho, a fim de personalizar a inserção de informações e controles de acordo com a necessidade, sem a necessidade de programação ou alteração do código-fonte;			
9.3.10.10.	Dispensar a necessidade da criação de tabelas, colunas e campos de banco de dados na solução, ou a necessidade de programação ou alteração do código-fonte, tornando estas alterações, quando necessárias, transparentes aos operadores e administradores que implementam os fluxos de trabalho;			
9.3.10.11.	Permitir a criação de campos compartilhados que possam ser utilizados em quaisquer outras entidades da solução, sem a necessidade de programação ou alteração do código-fonte;			
9.3.10.12.	Disponibilizar recursos tecnológicos de catálogo de serviços que possibilitem a automação de processos de gestão de TI;			

9.3.10.13.	Permitir a customização de menus, formulários, labels, automatizações de fluxos de trabalho e processos de TI, desenvolvidos na solução, permitindo a adequação às necessidades de uso de cada usuário, sem a necessidade de programação ou alteração do código-fonte;			
9.3.10.14.	Permitir a criação e automação de processos e fluxos de trabalho de forma segregada e independente a fim de permitir a personalização para cada departamento;			
9.3.10.15.	Permitir a automação de processos e fluxos de trabalho;			
9.3.10.16.	Permitir a criação de painéis e dashboards com gráficos de gestão, de forma ágil e intuitiva, sem a necessidade de programação e alteração do código-fonte;			
9.3.10.17.	Permitir a criação de painéis e dashboards com gráficos do tipo pizza, linha, colunas, barras e tabelas dinâmicas, sem a necessidade de programação e alteração do código-fonte. E que contemple as diversas necessidades de visão gerencial com agilidade e flexibilidade de ajustes necessários;			
9.3.10.18.	Permitir alterações de atributos de forma dinâmica em gráficos de gestão, contidos em painéis e dashboards da solução, possibilitando a alteração de eixos, título do gráfico, legenda, escala, rótulos de dados, tamanho do gráfico, de forma gráfica na solução e sem a necessidade de alterações do código-fonte;			
9.3.10.19.	Permitir aos atendentes e solucionadores de chamados criarem seus próprios painéis e gráficos dentro da solução e compartilharem com grupos ou usuários específicos da solução, permitindo gerenciar as permissões de compartilhamento de acordo com os perfis de usuários da solução;			
9.3.10.20.	Permitir a criação de gráficos com informações de diferentes entidades da solução, permitindo a sobreposição e cruzamento de informações e delimitação de linhas de tendência;			
9.3.10.21.	Permitir geração de relatórios com metadados, trilha de auditoria, hash de integridade, e exportação nos formatos .csv, .html, .pdf, .xml, .json e integração com ferramentas BI;			
9.3.10.22.	Prover informação em “real-time” de maneira gráfica por meio de dashboards;			
9.3.10.23.	Permitir configurar o envio automático e agendado de relatórios e gráficos gerenciais para grupos de usuários ou usuários específicos.			
9.3.10.24.	A CONTRATADA é responsável por desenvolver, implementar e aprimorar continuamente fluxos de trabalho automatizados para detecção, investigação e resposta a incidentes de segurança. Isso inclui a identificação de processos que podem ser automatizados, a criação de scripts e integrações necessárias, e a validação da eficácia desses fluxos de trabalho.			
9.3.10.25.	A CONTRATADA deve manter uma biblioteca de playbooks e scripts atualizados, os quais são essenciais para automatizar a resposta a incidentes, incluindo o desenvolvimento de novos playbooks conforme necessário, bem como a revisão e atualização periódica dos existentes para garantir sua eficácia e relevância.			
9.3.10.26.	A CONTRATADA deve designar o grupo técnico responsável pela gestão, definição de fluxos de trabalho, análise de processos de segurança, automação, otimização de processos para garantir a eficácia na detecção e resposta a incidentes.			
9.3.11.	Características gerais:			
9.3.11.1.	Deve utilizar de inteligência artificial e algoritmos de aprendizado de máquina para fornecer detecção aprimorada de ameaças, resposta a incidentes de segurança, análise de comportamentos anômalos para tomada de decisão de forma automatizada, reduzindo o tempo de resposta;			

9.3.11.2.	A orquestração deverá permitir a criação de scripts, playbooks, e fluxos de trabalho para execução de tarefas corretivas, ou escalção para equipes especializadas, com objetivo de atender a diversos tipos de incidentes;			
9.3.11.3.	Deve possuir processos, scripts e automações baseados em casos de uso em sua base de orquestração com capacidade de adaptação ao ambiente da PMESP, permitindo maior agilidade na implantação;			
9.4.	Modulo de Detecção em Endpoint (EDR):			
9.4.1.	A proteção de terminais e a prevenção contra vazamento de informações são componentes essenciais para a segurança cibernética da PMESP. Para isso, a CONTRATADA deverá adotar soluções eficazes para monitoramento de ameaças e controle de dados sensíveis.			
9.4.2.	É importante destacar que o licenciamento dos EDR poderá chegar a até 20.000 (vinte mil) unidades, conforme a necessidade e a estratégia de implantação. O custo do software será apurado mensalmente, de modo a permitir o correto dimensionamento dos pagamentos.			
9.4.3.	As ferramentas implementadas devem ser compatíveis com os demais sistemas de segurança e permitir integração com a estrutura do SOC, garantindo uma visão centralizada dos eventos de segurança.			
9.4.4.	Deverá preencher os seguintes requisitos:			
9.4.4.1.	O Servidor de Administração e Console Administrativa.			
9.4.4.1.1.	Compatibilidade: Microsoft Windows Server 2012 (Todas edições x64); Microsoft Windows Server 2012 R2 (Todas edições x64); Microsoft Windows Server 2016 x64; Windows Server 2022 Core Standard/ Datacenter; Windows Server 2022 Core Standard/ Datacenter; Microsoft Windows 10 (Todas edições x32); Microsoft Windows 10 (Todas edições x64);			
9.4.4.2.	Suporta as seguintes plataformas virtuais:			
9.4.4.2.1.	Vmware: Workstation 14.x Pro, vSphere 6. vSphere 6.5; Microsoft Hyper-V: 2008, 2008 R2, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 e 2022; Citrix;			
9.4.4.3.	Estações Windows			
9.4.4.3.1.	Compatibilidade: Microsoft Windows 10 Pro / Enterprise x86 / x64; Microsoft Windows Server 2012 R2 Standard x64; Microsoft Windows Server 2012 Foundation x64; Microsoft Windows Server 2012 Standard x64; Microsoft Windows Server 2008 R2 Standard/Enterprise x64 SP1; Microsoft Windows Server 2016 x64; Windows Server 2019 Core Standard/ Datacenter; Windows Server 2022 Core Standard/ Datacenter; Estações Mac OS X; Mac OS macOS 13.X Ventura e posteriores; Ubuntu 18.04; Ubuntu 20.04 LTS; CentOS-6.9; CentOS-7.4; CentOS-8; CentOS-9 stream; Debian GNU/Linux 9.4; OracleLinux 7.4;			
9.4.4.4.	Servidores Windows			
9.4.4.4.1.	Compatibilidade: Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter; Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter; Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter; Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter; Windows Server 2016 Essentials/Standard/Datacenter/MultiPoint Premium Server; Windows Server 2016 Core Standard / Datacenter; Windows Server 2019 Core Standard/ Datacenter; Windows Server 2022 Core Standard/ Datacenter.			
9.4.4.5.	Servidores Linux:			

9.4.4.5.1.	Compatibilidade: Plataforma 64-bits: Red Hat® Enterprise Linux® 6.9 Server; Red Hat® Enterprise Linux® 7.4 Server; Red Hat® Enterprise Linux® 7.5 Server; CentOS-6.9; CentOS-7.4; CentOS-7.5; CentOS-8; CentOS-9; Ubuntu 18.04; Ubuntu 24; Ubuntu Server 20.04.1 LTS.			
9.4.5.	Deve prover as seguintes proteções:			
9.4.5.1.	Varredura de arquivos residente que verifique qualquer arquivo criado, copiado (de fonte interna ou externa), acessado ou modificado, sendo realizado em tempo real, e também agendada ou solicitada;			
9.4.5.2.	Autoproteção contra-ataques aos serviços/processos do antivírus;			
9.4.5.3.	Capacidades de detecção e priorização de vulnerabilidades do Windows e de aplicativos instalados, fornecendo visibilidade detalhada para ação imediata de correção ou mitigação;			
9.4.5.4.	Deteção e bloqueio de tentativas de exploração no endpoint, utilizando análise comportamental, inteligência de ameaças e prevenção de execução de código malicioso;			
9.4.6.	Deve ter as seguintes capacidades:			
9.4.6.1.	As atualizações de conteúdo e assinaturas devem ser disponibilizadas e aplicadas automaticamente pelo fabricante, diariamente.			
9.4.6.2.	Ter a capacidade para importação e distribuição automática e manual de atualizações a partir da console do produto;			
9.4.6.3.	Não deve haver a necessidade de reinicialização do computador ou serviço e sem a necessidade de instalação de ou módulos adicionais à solução de antivírus ofertada;			
9.4.6.4.	Notificar automaticamente por meio de mensagem na tela a detecção de vírus ou de falha no processo de “limpeza”/” exclusão” dos arquivos infectados, com exibição da ação tomada. Esta mensagem deverá ser configurável permitindo a inserção de textos personalizados pela PMESP e/ou uma mensagem de notificação enviada por e-mail;			
9.4.6.5.	Disponibilizar ao menos um console central de gerenciamento hospedado em ambiente cloud, na modalidade SaaS, sem limitação de processadores ou quantidade de dispositivos gerenciados;			
9.4.6.6.	Permitir administração descentralizada com base em perfis e permissões configuráveis, integrados ao Active Directory da PMESP quando aplicável;			
9.4.6.7.	Possuir capacidade para configurar como serão distribuídas as atualizações de conteúdo, produto e configurações, de forma centralizada via console de gerenciamento;			
9.4.6.8.	Permitir definir grupos de endpoints para aplicação de políticas e atualizações conforme critérios da contratante;			
9.4.6.9.	Permitir acesso a console de gerenciamento por meio da tecnologia MMC (Microsoft Management Console) ou da tecnologia Web com acesso seguro (HTTPS);			
9.4.6.10.	Capacidade para configurar manualmente e/ou automaticamente repositórios distribuídos principais e secundários, de forma para que no caso de o repositório principal ficar indisponível, o computador de ponta irá buscar atualizações em repositórios secundários;			
9.4.6.11.	Ter a capacidade de implementação de senha em todos os softwares (agentes) adquiridos, de forma que operações que resultam na desinstalação, alteração de parâmetros de configuração ou desativação do software, sejam restritas pelo uso de senha;			

9.4.6.12.	Permitir o agrupamento dos computadores (que estiverem com o software (agente) instalado) em grupos lógicos e independentes da estrutura de domínio de rede, conforme política e critérios de definição fixados pela Contratada na console de gerenciamento;			
9.4.6.13.	Ter a capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:			
9.4.6.14.	Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);			
9.4.6.15.	Gerenciamento de tarefa (criar ou excluir tarefas de verificação);			
9.4.6.16.	Leitura de configurações;			
9.4.6.17.	Modificação de configurações;			
9.4.6.18.	Gerenciamento de Backup;			
9.4.6.19.	Visualização de relatórios;			
9.4.6.20.	Gerenciamento de relatórios;			
9.4.6.21.	Gerenciamento de chaves de licença;			
9.4.6.22.	Gerenciamento de permissões (adicionar/excluir permissões acima);			
9.4.6.23.	Possuir capacidade de monitorar e inspecionar continuamente todos os processos em execução no endpoint, aplicando análise comportamental e baseada em machine learning para detectar e prevenir atividades maliciosas em tempo real, sem impacto perceptível ao usuário final;			
9.4.6.24.	Bloquear malwares tais como ransomwares mesmo quando o ataque vier de um computador sem antivírus na rede;			
9.4.6.25.	Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa;			
9.4.6.26.	Garantir continuidade da proteção mesmo após interrupções inesperadas, retomando automaticamente os processos de monitoramento em tempo real e análise comportamental assim que o sistema estiver operacional;			
9.4.6.27.	Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (Uninterruptible Power supply – UPS);			
9.4.6.28.	Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;			
9.4.6.29.	Ter capacidade de configurar políticas de verificação diferentes para grupos de dispositivos permitindo ainda exceções e exclusões de pastas e arquivos;			
9.4.6.30.	Ter capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;			
9.4.6.31.	Ter capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan. banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;			
9.4.6.32.	Ter capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;			
9.4.6.33.	Ter capacidade de verificar somente arquivos novos e alterados;			
9.4.6.34.	Ter capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .pst, arquivos compactados por compactadores binários, etc.);			
9.4.6.35.	Ter capacidade de verificar objetos usando heurística;			

9.4.6.36.	Ter capacidade de configurar diferentes ações para diferentes tipos de ameaças;			
9.4.7.	O antivírus, ao encontrar um arquivo potencialmente perigoso, deve:			
9.4.7.1.	Bloquear acesso ao objeto;			
9.4.7.2.	Quarentenar ou excluir automaticamente o arquivo, conforme política previamente definida pelo administrador;			
9.4.7.3.	A solução deve ser projetada para funcionar no modo off-line.			
9.4.7.4.	A comunicação entre agente e console de gerenciamento deve ser criptografada.			
9.4.8.	Manutenção / Subscrição de Software			
9.4.8.1.	Manutenção para Atualizações e Correções dos Softwares			
9.4.8.2.	A subscrição terá prazo de vigência do contrato.			
9.4.8.3.	Consiste no fornecimento das atualizações da solução (engine), perfis de comportamento, assinaturas de ameaças, bem como, das correções, atualizações, novas versões, qualquer alteração do software ou de suas bases complementares (listas, assinaturas, métodos de funcionamento, etc.) e novos releases de todos os softwares que compõe a solução fornecida e que forem lançadas no mercado pelo fabricante do produto, devendo ser prestada na seguinte conformidade:			
9.4.8.4.	Durante toda vigência do contrato, por vinte e quatro horas/dia para todos os dias da semana, deverá;			
9.4.8.5.	Fornecer as novas versões, novos releases, correções, alterações, bases acessórias do software (qualquer lista ou base de dados que seja necessária para o perfeito funcionamento do software ou para mantê-lo em níveis recentes de atualização) e atualizações desenvolvidas para todos os softwares que compõe a solução fornecida e que forem lançadas no mercado pelo fabricante do produto;			
9.4.8.6.	Fornecer a correção de erros e defeitos de todos os softwares que compõe a solução fornecida sempre que forem identificados erros ou defeitos de programação prejudiciais ao seu perfeito uso, funcionamento e administração no ambiente da PMESP;			
9.4.8.7.	Fornecimento contínuo de novas assinaturas, regras de detecção e indicadores de ameaças assim que liberados pelo fabricante, garantindo que a solução permaneça atualizada frente a novas técnicas de ataque;			
9.4.8.8.	A retirada de circulação comercial ou a exclusão da lista de produtos suportados pelo fabricante não excluirá as obrigações da contratada sobre os softwares fornecidos;			
9.4.8.9.	Caso o software seja descontinuado durante a vigência do Contrato, sendo entendido que software descontinuado é aquele que tenha sido excluído da lista de produtos suportados e que o seu desenvolvimento, aperfeiçoamento e manutenção foi encerrado pelo fabricante, as obrigações da contratada serão mantidas até a data final de vigência do contrato.			
9.4.9.	Suporte Técnico dos Softwares			
9.4.9.1.	A CONTRATADA deverá possuir de forma permanente durante 24h em todos os dias da semana, setor de suporte para atendimento da Contratante, sendo que:			
9.4.9.2.	Consiste no atendimento dos chamados técnicos da Contratante, na resolução de dúvidas, panes, falhas e não conformidades técnicas prejudiciais ao uso, instalação, administração, funcionamento, desempenho e à performance dos softwares fornecidos, sendo prestada em duas modalidades:			

9.4.9.3.	Remoto (telefônico, em língua portuguesa): Atendimento feito por meio de Central de Serviços (Service Desk), com posições de atendimento (PAs) suficientes para o atendimento, registro, resolução e/ou direcionamento dos chamados técnicos do Contratante.			
9.4.9.4.	Local (on site): Atendimento feito por meio de analistas de campo devidamente habilitados e capacitados, que atuarão diretamente no local de instalação do software fornecido.			
9.4.9.5.	O Suporte Técnico dos Softwares, remoto e local, deve ser prestada na seguinte conformidade:			
9.4.9.6.	Durante toda vigência do contrato, por vinte e quatro horas/dia para todos os dias da semana, deverá:			
9.4.9.7.	Diagnosticar erros e defeitos dos softwares fornecidos;			
9.4.9.8.	Identificar as correções necessárias para a resolução de problemas gerados pelos erros e defeitos diagnosticados;			
9.4.9.9.	Identificar as soluções de contorno para a resolução de problemas gerados por erros e defeitos apresentados no software fornecido;			
9.4.9.10.	Efetuar a solicitação de correções para erros e defeitos do software;			
9.4.9.11.	Efetuar a solução de dúvidas, panes, falhas e não-conformidades técnicas relacionadas com a execução de todas as operações e intervenções técnicas necessárias à instalação, configuração, teste, otimização, operacionalização, aplicação de atualizações, correção de erros, operacionalização, uso e administração da solução contratada;			
9.4.9.12.	Prover a infraestrutura presencial ou de Help Desk em língua portuguesa necessária para o atendimento dos chamados técnicos;			
9.4.9.13.	As atividades relativas serão executadas nos locais de instalação dos softwares, limitando-se somente ao município de São Paulo e sua região metropolitana.			
9.4.10.	Condições de Atendimento			
9.4.10.1.	Define as principais metas e responsabilidades da Contratada para o atendimento das Obrigações da Contratada – Subscrição de Software. O atendimento será feito pela contratante por meio da abertura de chamados técnicos pela contratada, que serão classificados por grau de severidade, devendo ser prestados dentro dos padrões mínimos de atendimento abaixo:			
9.4.10.1.1.	Severidade 1 (S1): software apresenta pane, falha ou não-conformidade técnica que o torna total ou parcialmente inoperante. O primeiro retorno telefônico da Contratada deve ser realizado em no máximo 02 (duas) horas e a solução técnica, definitiva ou de contorno, não poderá exceder a 8 (oito) horas, contadas do chamado técnico;			
9.4.10.1.2.	Severidade 2 (S2): software apresenta pane, falha ou não-conformidade técnica que prejudica a operação, uso ou acesso de função(s) básica(s). O primeiro retorno telefônico da Contratada deve ser realizado em no máximo 02 (duas) horas e a solução técnica, definitiva ou de contorno, não poderá exceder a 24 (vinte e quatro) horas, contadas do chamado técnico;			
9.4.10.1.3.	Severidade 3 (S3): software apresenta pane, falha ou não-conformidade técnica que causa restrições de operação de funções acessórias. O primeiro retorno telefônico da Contratada deve ser realizado em no máximo 02 (duas) horas e a solução técnica, definitiva ou de contorno, não poderá exceder a 48 (quarenta e oito) horas, contadas do chamado técnico;			
9.4.11.	Condições Gerais			
9.4.11.1.	A contratada deverá fornecer todo e qualquer software necessário ao perfeito funcionamento, uso e administração da solução proposta.			

9.4.11.2.	Todos os softwares fornecidos deverão ter as funcionalidades já disponíveis em mercado, não sendo permitida a adequação destes softwares para atender requisitos específicos exigidos neste projeto básico, não será admitido o desenvolvimento de software para atender as demandas específicas definidas neste projeto básico;			
9.4.11.3.	O licenciamento dos softwares deverá ser feito sem limites quanto ao número de processadores existentes no microcomputador onde estiver sendo processado o módulo;			
9.4.11.4.	Compatibilidade para a instalação, funcionamento e utilização plena de todos os recursos em microcomputadores do tipo servidores, estações de trabalho, notebooks e netbooks;			
9.4.12.	Instalação:			
9.4.12.1.	A instalação compreende as atividades de preparação da infraestrutura, instalação lógica do software e testes;			
9.4.12.2.	Incluem-se na instalação as atividades de: Levantamento de dados; Adequação da solução à infraestrutura apresentada; Execução dos testes dos testes de funcionamento do software; A contratada deverá prover todos os materiais necessários à instalação da solução fornecida;			
9.4.12.3.	Durante a fase preparatória e de execução da instalação, a CONTRATADA deverá observar as indicações técnicas do Fabricante, as normas de segurança aplicáveis à espécie.			
9.4.12.4.	Os serviços de instalação compreendem a execução direta, pelos técnicos da contratada, das operações e intervenções necessárias à instalação da solução de Endpoint Protection, visando o seu perfeito funcionamento, uso, administração e a sua total interligação, integração e compatibilidade com o ambiente computacional da Contratada, observadas as seguintes condições:			
9.4.12.5.	Integrar e compatibilizar a solução com os demais ativos do ambiente computacional da Contratada.			
9.4.12.6.	Integrar com a solução de SIEM, atual ou ofertada na estrutura de SOC.			
9.5.	Módulo Avançado de Detecção e Resposta - XDR:			
9.5.1.	A plataforma deve ser entregue na modalidade Software-as-a-Service com alta disponibilidade;			
9.5.2.	É importante destacar que o licenciamento dos XDR poderá chegar a até 200 (duzentas) unidades, conforme a necessidade e a estratégia de implantação. O custo do software será apurado mensalmente, de modo a permitir o correto dimensionamento dos pagamentos.			
9.5.3.	O acesso a plataforma deve ser realizado via browser, ao menos: Google Chrome, Mozilla Firefox e Microsoft Edge;			
9.5.4.	Deve receber telemetria dos demais sensores existentes, de forma centralizar a visão de logs, alertas e incidentes;			
9.5.5.	Deve permitir que as detecções vindas dos sensores sejam correlacionadas, permitindo investigação multicamadas.			
9.5.6.	A plataforma deve ser entregue em nuvem como um serviço (SaaS), sendo o fabricante responsável por todas as manutenções, atualizações e garantia de disponibilidade;			
9.5.7.	Deve possuir capacidade centralizar a visibilidade dos logs coletados, criando uma relação de objetos que apresente as ações envolvidas no alerta de fim a fim;			
9.5.8.	A plataforma deve possuir os seguintes módulos de forma:			
9.5.8.1.	Módulo de investigação de incidentes;			
9.5.8.2.	Módulo de análise forense de ameaças digitais;			
9.5.8.3.	Módulo de inteligência de ameaças;			
9.5.8.4.	Modulo de gestão de vulnerabilidades;			
9.5.9.	Serviço de monitoramento avançado especializado da plataforma 24x7;			

9.5.9.1.	Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias e suportar extensão deste prazo para até 60 meses totais;			
9.5.9.2.	A plataforma de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;			
9.5.9.3.	A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;			
9.5.9.4.	Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total, permissão para realizar investigações e permissão de apenas leitura;			
9.5.9.5.	Deve permitir a criação de perfis de acesso customizados, sendo possível vincular a visão de menus da plataforma de acordo com grupos de dispositivos e contas de usuários;			
9.5.9.6.	Deve permitir que o administrador atribua acesso ao grupo de funcionalidades da console para cada usuário;			
9.5.9.7.	A console deve suportar limitação de sessões concorrentes de acesso via navegador;			
9.5.9.8.	A console deve restringir acesso por meio de endereço de IP e range de IP;			
9.5.9.9.	Deve listar os logs de auditoria da console dos últimos 30 dias;			
9.5.9.10.	Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;			
9.5.9.11.	Deve possibilitar adição de MFA para acesso a plataforma, da Contratante;			
9.5.9.12.	Deve permitir o envio de notificações para os administradores através de e-mail, API e integrações com sistemas de ITSM;			
9.5.10.	Módulo de investigação de incidentes;			
9.5.10.1.	Deve gerar visibilidade de todos os alertas vindos dos demais sensores de telemetria da plataforma, a saber: Rede, Endpoint, Cloud e Identidade;			
9.5.10.2.	Deve correlacionar tais alertas de forma a indicar por meio de relação de objetos quais são os dispositivos, IPs, usuários e servidores envolvidos no contexto do alerta gerado;			
9.5.10.3.	Deve apresentar arquivos, caminhos de pastas, comandos, URLs e Hashs envolvidos nos alertas;			
9.5.10.4.	Deve associar a técnica identificada com base na matriz do framework MITRE ATT&CK;			
9.5.10.5.	Deve ser possível assignar um usuário responsável para tratar e analisar o alerta gerado;			
9.5.10.6.	Deve ser possível categorizar os alertas de acordo as análises realizadas, de forma a ser possível apontar que o alerta se trata de um:			
9.5.10.6.1.	Verdadeiro positivo;			
9.5.10.6.2.	Falso positivo;			
9.5.10.6.3.	Incidente notável;			
9.5.10.7.	Deve ser possível inserir informações a respeito do alerta analisado;			
9.5.10.8.	Cada alerta gerado deve apresentar um nível de severidade de risco ao ambiente da CONTRATANTE, segundo categorização:			
9.5.10.8.1.	Risco Baixo;			
9.5.10.8.1.	Risco Médio;			
9.5.10.8.1.	Risco Alto;			
9.5.10.8.1.	Risco Crítico.			
9.5.10.9.	Dentro da tela de visibilidade dos alertas, deve ser possível tomar ações de resposta imediata perante o contexto do possível ataque:			
9.5.10.9.1.	Acesso remoto a máquina sessão da própria solução;			

9.5.10.9.2.	Isolamento de máquina – Essa ação deve restringir completamente a comunicação da máquina com dispositivos da rede local e endereços da internet, permitindo apenas a conexão com a plataforma XDR;			
9.5.10.9.3.	Reset senha do usuário;			
9.5.10.9.4.	Bloqueio de conta do usuário;			
9.5.10.9.5.	Envio de script customizado;			
9.5.10.10.	Deve prover visualização em linha do tempo com informações dos eventos monitorados;			
9.5.10.11.	Deve possuir funcionalidade de busca inteligente aos dados coletados advindos dos sensores da plataforma, suportando buscas via operadores lógicos;			
9.5.10.12.	Deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque;			
9.5.10.13.	Deve permitir a visualização entre usuários, máquinas, processos, comandos, arquivos e demais componentes correlacionados em determinado ataque;			
9.5.10.14.	O módulo de investigação de incidentes deve atuar baseado em modelos de detecção de ataques avançados e furtivos;			
9.5.10.15.	Deve implementar e organizar os ataques baseados no framework MITRE ATT&CK, identificando técnicas e táticas dos ataques;			
9.5.10.16.	Deve possuir capacidades de criação de modelos de detecção customizados;			
9.5.10.17.	Deve informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;			
9.5.10.18.	Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscas específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.			
9.5.10.19.	A partir da identificação de uma exploração de vulnerabilidade em determinadas máquinas, a solução deve ser capaz de fornecer recomendações de mitigação, permitindo aplicar políticas de proteção diretamente ou via integrações;			
9.5.10.20.	Com base na telemetria gerada, deve apresentar de forma gráfica fases de um possível ataque, por meio das correlações aplicadas;			
9.5.10.21.	Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;			
9.5.10.22.	Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;			
9.5.10.23.	Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;			
9.5.10.24.	Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;			
9.5.10.25.	Possuir capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;			
9.5.10.26.	Capacidade de construir sequências de buscas para localizar os dados ou objetos no ambiente que será feita a análise;			
9.5.10.27.	Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta para identificar, categorizar e recuperar os resultados da pesquisa;			
9.5.10.28.	Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais;			
9.5.10.29.	Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;			

9.5.10.30.	Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;			
9.5.10.31.	Deve exibir os eventos de forma a priorizar os alertas mais críticos para otimizar o tempo de investigação, como pontuações ou níveis de prioridade;			
9.5.10.32.	Atuar com ações planejadas, por meio de roteiros customizáveis, quando da detecção de alto risco de máquinas presentes no ambiente da CONTRATANTE;			
9.5.10.33.	Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;			
9.5.10.34.	Deve prover visualização em linha do tempo com informações dos eventos monitorados em dispositivo;			
9.5.10.35.	Deve associar cada alerta gerado a um incidente macro, a fim de correlacionar os alertas gerando visão de impacto e criticidade;			
9.5.10.36.	Deve ser possível assignar um alerta a um incidente;			
9.5.10.37.	Deve ser possível correlacionar um alerta a um caso no ITSM;			
9.5.11.	Módulo de análise forense de ameaças digitais;			
9.5.11.1.	Deve possuir módulo de análise forense de ameaças digitais, sendo possível a investigação em tempo real nas máquinas por meio de queries avançadas;			
9.5.11.2.	Deve ser possível a criação de espaços de investigação dentro da plataforma, para que informações de máquinas e evidências sejam coletadas;			
9.5.11.3.	Deve possuir capacidades de coleta de arquivos conforme alvos detectados;			
9.5.11.4.	Deve possuir suporte à coleta de grandes volumes de evidências digitais, permitindo a extração e transferência eficiente de artefatos para análise forense;			
9.5.11.5.	A coleta de arquivos e evidências devem ser de forma remota via ações automáticas e manuais, quando necessário;			
9.5.11.6.	Deve suportar a coleta de evidências com base em informações de sistema das máquinas, linha do tempo de arquivos, dispositivos externos conectados, informações de serviço, processos e tarefas agendas.			
9.5.11.7.	Deve possuir ambiente isolado para análise de artefatos, tal ambiente de estar hospedado na própria nuvem do fabricante e integrado a plataforma, suportando a execução de URLs e arquivos suspeitos;			
9.5.11.8.	Tais objetos advindos das análises devem ser adicionados automaticamente na lista de objetos suspeitos;			
9.5.11.9.	Deve suportar no mínimo a análise de 50 artefatos por dia;			
9.5.12.	Módulo de Inteligência de Ameaças			
9.5.12.1.	A solução deve contar com módulo dedicado a inteligência de ameaças;			
9.5.12.2.	Deve gerar alertas de indicadores de comprometimento (IOCs) presentes no ambiente da CONTRATANTE e que possam estar correlacionados a companhias globais de ameaças;			
9.5.12.3.	Deve gerar relatórios com base nas fontes de inteligência do fabricante e de terceiros, a fim de identificar possíveis IOCs no ambiente;			
9.5.12.4.	Deve ter suporte a customização das buscas por IOCs no ambiente;			
9.5.12.5.	Deve possuir lista customizável de indicadores de comprometimento e objetos suspeitos;			
9.5.12.6.	Deve permitir adicionar arquivos SHA-1, SHA-256, URLs, IPs, domínios e endereços de e-mail a lista de objetos suspeitos;			
9.5.12.7.	Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de objetos suspeitos.			
9.5.12.8.	Deve ser possível determinar o tempo de vida da existência de um IOC;			
9.5.12.9.	Deve ser capaz de configurar o nível de risco de cada IOC;			

9.5.12.10.	Deve ter suporte ao consumo de fontes externas de IOCs, por meio de integração nativa ou via API;			
9.5.12.11.	Quando um IOC é inserido na lista de objetos, o módulo deve enviar tal informação a todos os agentes que compõem a solução, unificando a informação;			
9.5.13.	Módulo de Gestão de Vulnerabilidade			
9.5.13.1.	A solução deve ser entregue como um serviço Software-as-a-Service (SaaS) em uma nuvem proprietária do fabricante para todos os seus serviços e aplicativos exigidos neste documento. Serviços fornecidos por nuvens de terceiros não são aceitos;			
9.5.13.2.	A gestão de todos os módulos considerados neste termo deve ser feita através de uma console única;			
9.5.13.3.	A solução deverá possuir no mínimo, duas das seguintes certificações de privacidade e segurança: EU-U.S. Privacy Shield Framework, Swiss-U.S. Privacy Shield Framework, Cloud Security Alliance e (CSA) STAR.			
9.5.13.4.	Todos os serviços da plataforma devem estar disponíveis sob o mesmo padrão de qualidade de serviço 24x7x365 e garantir 99% de disponibilidade;			
9.5.13.5.	O ofertante deve oferecer manutenção e atualização constante da plataforma durante todo o período de vigência do contrato de serviço;			
9.5.13.6.	As atualizações de serviço devem ser transparentes para o administrador da solução, sem afetar nenhum dos dados armazenados - serviços fornecidos;			
9.5.13.7.	Todas as comunicações entre componentes, transferência de dados e sincronização da solução devem ser criptografadas de ponta a ponta, fazendo uso de no mínimo TLS 1.2, certificados assinados com RSA 2048 bits e algoritmo de assinatura SHA256;			
9.5.13.8.	A solução deve permitir criação de usuários distintos;			
9.5.13.9.	Deve permitir separação de funções e permissões na console;			
9.5.13.10.	Deve permitir integração através de SSO com, pelo menos, Active Directory;			
9.5.13.11.	A console deve ser acessível a partir de, pelo menos, um dos navegadores comerciais dentre Google Chrome, Microsoft Edge e Firefox;			
9.5.13.12.	A solução proposta deve oferecer um agente de baixo impacto nos sistemas operacionais onde está instalado e no consumo de largura de banda que utilizará na rede;			
9.5.13.13.	A solução deve ser instalada em servidores, estações de trabalho, e máquinas virtuais, suportando sua implantação em rede local, em rede doméstica e na nuvem;			
9.5.13.14.	A solução deve oferecer suporte para sua implantação em pelo menos os seguintes sistemas operacionais: Windows 7/Windows Server 2003 SP2 e posterior (x86, x64), Red Hat Enterprise Linux/CentOS 6.5+, 7.x (x64), 8.x (x64), Ubuntu 14, 16,18,19,20 (x64), Oracle Enterprise Linux 8, Oracle Enterprise Linux (OEL) 7 até 7.5, Oracle Enterprise Linux (OEL) 6, Amazon Linux 2, Amazon Linux 2018.03, Amazon Linux 2017.09, Amazon Linux 2017.03, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 11.			
9.5.13.15.	O agente da solução deve se atualizar automaticamente e gerir as suas atualizações automaticamente;			
9.5.13.16.	A solução deve suportar plataformas de nuvem AWS, GCP, Azure;			
9.5.13.17.	A solução deve ser capaz de coletar informações sobre o inventário de ativos;			
9.5.13.18.	As funcionalidades de gestão de ativos, gestão de vulnerabilidade e detecção de patches devem ser fornecidas pelo mesmo agente de gerenciamento, não serão aceitas soluções com múltiplos agentes;			

9.5.13.19.	O agente de gerenciamento deve suportar o uso de proxy;			
9.5.13.20.	Deve ser possível definir o intervalo de comunicação entre o agente e a console de gerenciamento;			
9.5.13.21.	Deve ser possível limitar o consumo de CPU ou memória do agente;			
9.5.13.22.	Deve permitir a definição de um período global de inatividade dos agentes;			
9.5.13.23.	A solução deve permitir o uso de scanners capazes de identificar vulnerabilidades através de varreduras em ranges de IP definidos pelo administrador;			
9.5.13.24.	Não deverá haver restrições para instalação de scanners virtuais no ambiente;			
9.5.13.25.	Deve ser permitido o uso de scanners externos, sem necessidade de instalação, em nuvem própria do fabricante para varreduras de ativos publicados na internet;			
9.5.13.26.	Os scanners virtuais devem suportar pelo menos um dos hypervisors: Hyper-V, ProxMox.			
9.5.13.27.	Os Scanners devem suportar a varredura de ambientes em nuvem para pelo menos dois dos seguintes provedores: Azure; AWS; Google Cloud Platform; Oracle;			
9.5.13.28.	Os scanners devem reportar vulnerabilidades para console em nuvem, permitindo uma visão consolidada de vulnerabilidades;			
9.5.13.29.	Deve ser permitido a configuração de varreduras periódicas (com intervalo mínimo de 4 horas) para máquinas identificadas manualmente por meio de perfil de configuração ou tags associadas a uma versão específica de banco de dados em execução;			
9.5.13.30.	Deve ser permitido a varredura sob demanda para um ou mais ativos de rede;			
9.5.13.31.	O mesmo scanner deve ser capaz de varrer por falhas de conformidade e também por vulnerabilidades;			
9.5.13.32.	O scanner deverá consolidar vulnerabilidades encontradas em um ativo que possua agente instalado;			
9.5.13.33.	A solução deve permitir a configuração do tipo de varredura a ser realizada, permitindo pelo menos definir as seguintes configurações ao defini-la:			
9.5.13.33.1.	Configuração de quantidades de portas TCP/UDP a serem validadas;			
9.5.13.33.2.	Consumo de largura de banda e recursos (alto, médio, baixo);			
9.5.13.33.3.	Digitalize para dispositivos que não suportam ping - traceroute;			
9.5.13.33.4.	Deteção de balanceadores de carga;			
9.5.13.33.5.	Configuração de força bruta para usar em senhas;			
9.5.13.33.6.	Uso de um cabeçalho HTTP personalizado;			
9.5.13.33.7.	Ignorar pacotes;			
9.5.13.33.8.	Instalação de agente temporário para validação de registro local;			
9.5.13.34.	A solução proposta deve permitir a coleta de informações detalhadas sobre o ativo gerenciado, deve detalhar pelo menos os seguintes dados para cada ativo: Serviços em execução; Software instalado; Usuários; Portas abertas; Nome do host; FQDN; IP v4 / v6; Endereço MAC; Processador; Memória; Volumes de disco; BIOS;			
9.5.13.35.	A solução deve classificar automaticamente os ativos por famílias de tecnologia, tipo de dispositivo, tipo de plataforma e fabricante;			
9.5.13.36.	A solução deve normalizar automaticamente os nomes dos fabricantes de HW e SW com seus dados relevantes, como o nome dos aplicativos e versões, para facilitar sua posterior busca na solução;			

9.5.13.37.	A solução deve possuir a habilidade de etiquetagem (Tags) de ativos para facilitar a identificação, deve permitir a geração de Tags, pelo menos, usando os seguintes parâmetros: Palavras-chaves; Endereço IP e intervalos de IP; Segmento de rede; Portas abertas;			
9.5.13.38.	Informações de inventário considerando, no mínimo: Sistema operacional; Presença ou ausência de determinado software instalado ou serviço em execução;			
9.5.13.39.	A solução deve permitir agrupamento manual a critério do administrador da solução;			
9.5.13.40.	A solução deve permitir atribuir criticidade ao ativo para priorizá-lo durante o processo de gerenciamento.;			
9.5.13.41.	Deve permitir criação de Dashboards personalizados que sejam capazes de trazer as seguintes informações sobre os ativos: Categorias de softwares instalados nos ativos; Hosts que executam máquinas virtuais; Sistemas operacionais utilizados; Serviços e portas TCP ou UDP abertas; Softwares de segurança instalados;			
9.5.13.42.	A solução deve permitir uma interface de busca de ativos que utilize uma sintaxe lógica baseados, no mínimo, nos critérios abaixo: Fabricante de hardware; Último usuário logado; Categoria de software instalado;			
9.5.13.43.	A solução deve permitir a visualização de quantidade de máquinas com um determinado software instalado;			
9.5.13.44.	Deve permitir visualização de recursos em nuvem AWS ou Azure tais como VPCs, Virtual Networks, Security Group, S3 buckets, RDS, SQL Server, através de conectores ou via agente;			
9.5.13.45.	Deve permitir visibilidade a respeito de hosts que executam containers e containers em execução;			
9.5.13.46.	A solução deve permitir descobrir, avaliar, priorizar e auxiliar na correção de vulnerabilidades/ configurações em toda a infraestrutura de rede, incluindo estações de trabalho, servidores, dispositivos de rede, dispositivos de telecomunicações e dispositivos de segurança, hypervisors, máquinas virtuais, orquestradores de contêineres, contêineres e nuvens (Azure, GCP, AWS), proporcionando através de única interface para o administrador via um portal web para gerenciamento de todos os ativos, permitindo o gerenciamento centralizado de todos os componentes da solução a partir de um único ponto, sem a necessidade de incorrer em consoles - componentes adicionais fora dele para a administração dos serviços oferecidos			
9.5.13.47.	A solução deve ser oferecida na modalidade SaaS em nuvem própria do fabricante, sem necessidade de instalação de componentes locais para a gerência;			
9.5.13.48.	A solução deve ser licenciada por Asset (IP - HOST) para ativos de infraestrutura;			
9.5.13.49.	A solução deve ser licenciada com foco em servidores, de acordo com as quantidades especificadas na tabela de quantitativos;			
9.5.13.50.	A CONTRATANTE poderá solicitar a cobertura de desktops considerados críticos, a serem acionados sob demanda;			
9.5.13.51.	A solução deve permitir varreduras de vulnerabilidade com base em: Sistemas Operacionais; Portas TCP e UDP; Serviços; Bancos de dados; Dispositivos de rede como switches, roteadores e balanceadores de carga;			
9.5.13.52.	No mínimo, a ferramenta deve abranger os seguintes sistemas operacionais, bancos de dados aplicativos: Microsoft Windows, UNIX, LINUX, MacOS e VMware.			
9.5.13.53.	Detectar e analisar vulnerabilidades nas principais versões de Bancos de Dados, pelo menos: Microsoft SQL Server, MySQL e Oracle.			

9.5.13.54.	Detectar e analisar vulnerabilidades em plataformas WEB, pelo menos: IIS, Apache Tomcat, Detectar e analisar vulnerabilidades em porta e serviços TCP e UDP.			
9.5.13.55.	Detectar vulnerabilidades em pelo menos os seguintes aplicativos ou plataformas: Adobe, Apple, Microsoft (Office, IIS, Exchange), Oracle e Java.			
9.5.13.56.	Permitir a descoberta de vulnerabilidades na rede, oferecendo as seguintes alternativas de varredura: Varredura ativa de rede não autenticada, Varredura ativa de rede autenticada, Agente, Varreduras externas e O mecanismo de varredura deve ter uma taxa de precisão de detecção de vulnerabilidade de 99,99966% (seis sigma) durante os últimos 10 anos.			
9.5.13.57.	A base de conhecimento de vulnerabilidade deve ser atualizada semanalmente, garantindo a incorporação de pelo menos 20 CVEs a ela e deve ter pelo menos uma base de conhecimento de 35.000 CVEs relacionados incluindo tecnologias legadas e atuais;			
9.5.13.58.	A solução deve oferecer suporte ao padrão da indústria para pontuação de vulnerabilidade do Common Vulnerability Scoring System (CVSS);			
9.5.13.59.	A solução deve oferecer suporte ao padrão da indústria para adicionar detecções personalizadas usando Open Vulnerability Assessment Language (OVAL);			
9.5.13.60.	A solução deve permitir vincular as vulnerabilidades detectadas e indicar sua relação com ameaças como Vírus, Trojan e Malware;			
9.5.13.61.	A solução deve ser capaz de indicar explorações disponíveis e códigos disponíveis para uma vulnerabilidade, quando aplicável;			
9.5.13.62.	O banco de dados deve relacionar a maioria das vulnerabilidades ao CVE e Bugtraq;			
9.5.13.63.	A solução deve oferecer suporte à integração para autenticação por ferramentas de cofres de senha;			
9.5.13.64.	A solução deve permitir buscas interativas de vulnerabilidade utilizando filtros como severidade, categoria, sistema operacional, status, classificação do CVSS, CVE ou KB;			
9.5.13.65.	A solução deve permitir a utilização de operadores lógicos na busca de vulnerabilidades para que seja possível encontrar, no mínimo, as seguintes informações: Vulnerabilidades associadas a ransomware e que possuem patches disponíveis, Vulnerabilidades detectadas em um segmento de rede, Vulnerabilidades detectadas em serviços específicos, Vulnerabilidades detectadas por um usuário específico, Vulnerabilidades detectadas em hardware específico e Vulnerabilidades detectadas por tag AWS ou Azure específicas.			
9.5.13.66.	Na busca de vulnerabilidades deve permitir agrupamento para mostrar, no mínimo, as seguintes visualizações: Quantidade de ocorrências de uma mesma vulnerabilidade, Quantidade de vulnerabilidades por sistema operacional, Quantidade de vulnerabilidades por host, Quantidade de vulnerabilidades por Exploit disponível e Quantidade de vulnerabilidades por produto/software vulnerável.			
9.5.13.67.	A solução deve permitir exportar buscas e filtros criados para um dashboard;			
9.5.13.68.	A solução deve permitir salvar filtros criados em buscas para reutilização;			
9.5.13.69.	Deve mostrar dashboards que consigam mostrar variação histórica de vulnerabilidades novas, corrigidas, reabertas;			
9.5.13.70.	Deve permitir mostrar dashboards que contenham quantidades de vulnerabilidades associadas a ramsonware, que contém exploits públicos e que permitem exploração sem autenticação;			
9.5.13.71.	Deve mostrar dashboards que mostrem o racional de vulnerabilidades que podem ser corrigidas através de patches;			

9.5.13.72.	Deve mostrar patches faltantes em sistemas operacionais independente da relação com uma vulnerabilidade existente;			
9.5.13.73.	A solução deve oferecer a possibilidade de monitorar dispositivos móveis Android, iOS;			
9.5.13.74.	A solução deve permitir a avaliação, o relatório e o relatório de problemas de configuração, com base nas referências do padrão da indústria do Centro de Segurança da Internet (CIS);			
9.5.13.75.	O fabricante deve ser oficialmente certificado pelo CIS para fornecer este nível de controles;			
9.5.13.76.	A solução deve oferecer avaliação de configuração com base no benchmark CIS padrão da indústria, cobrindo esta funcionalidade nas seguintes categorias: Sistemas operacionais, Software de servidor, Provedores de nuvem, Dispositivos de rede e Software de desktop.			
9.5.13.77.	A solução deve suportar detecção de falhas de conformidades através de varreduras autenticadas ou através de agente instalado diretamente no ativo monitorado;			
9.5.13.78.	A solução deve permitir que os administradores recebam informação de conformidade de sistemas operacionais Windows e Linux, mesmo que não estejam conectados a rede corporativa;			
9.5.13.79.	A solução deve permitir a avaliação de certificados digitais (internos e externos) e configurações de TLS em busca de problemas e vulnerabilidades de certificados, resultando em diferentes graus de conformidade de acordo com os resultados da avaliação de seu emissor, prazo de validade, tipo de certificado, robustez do o algoritmo e o conjunto de criptografia usados;			
9.5.13.80.	A solução proposta deve permitir enviar alertas em tempo real sobre irregularidades na rede, identificar ameaças e monitorar mudanças inesperadas que ocorram na mesma;			
9.5.13.81.	A solução deve permitir enviar notificações para usuários específicos e grupos de usuários para o perfil de monitoramento - perfis de monitoramento múltiplos;			
9.5.13.82.	A solução deve permitir a personalização do perfil de monitoramento associado a uma lista específica de critérios;			
9.5.13.83.	A solução deve permitir que os alertas sejam personalizados para uma ampla variedade de condições que afetam sistemas, certificados, vulnerabilidades, portas, serviços e software. Cada regra deve permitir que seja configurada para detectar mudanças gerais comuns - para se ajustar a circunstâncias muito específicas;			
9.5.13.84.	A solução deve permitir a atribuição de destinatários diferentes para cada alerta;			
9.5.13.85.	A solução deve enviar alertas de monitoramento sobre vulnerabilidades, configurações incorretas e outros parâmetros definidos pelo administrador da solução:			
9.5.13.85.	Ativos com sistemas operacionais não aprovados;			
9.5.13.85.	Certificados expirados - expirando;			
9.5.13.85.	Portas abertas;			
9.5.13.85.	Vulnerabilidades graves;			
9.5.13.85.	Tickets de correção abertos, resolvidos e fechados;			
9.5.13.85.	Software não aprovado;			
9.5.13.86.	A solução proposta deve fornecer fontes de inteligência de ameaças em tempo real e técnicas de aprendizado de máquina para fornecer controle de administrador sobre a evolução das ameaças relacionadas a vulnerabilidades encontradas nos ativos da organização e identificar quais corrigir primeiro;			

9.5.13.87.	A solução deve permitir consultas ad-hoc com múltiplas variáveis e critérios, como classe de ativo, tipo de vulnerabilidade, indicadores de ameaça em tempo real, etiqueta de ativo e o sistema operacional, de modo que, por exemplo, seja possível pesquisar todas as vulnerabilidades que tenham uma alta classificação de gravidade, são fáceis de explorar e foram lançados na semana passada;			
9.5.13.88.	A solução deve permitir que se faça uma correlação em tempo real das ameaças ativas contra as vulnerabilidades detectadas nos ativos corporativos;			
9.5.13.89.	A solução deve incluir indicadores de ameaças em tempo real que ajudam a avaliar e priorizar vulnerabilidades detectadas, categorizados da seguinte forma:			
9.5.13.89.	Dia Zero: vulnerabilidades para as quais não há patch disponível e para as quais um ataque ativo foi observado;			
9.5.13.89.	Exploração pública: Vulnerabilidades cujo mecanismo de exploração é conhecido, para o qual existe um código de exploração e está disponível publicamente;			
9.5.13.89.	Ataques ativos: vulnerabilidades que estão sendo atacadas ativamente;			
9.5.13.89.	Movimento lateral: vulnerabilidades que permitem ao invasor espalhar o ataque amplamente pela rede violada;			
9.5.13.89.	Fácil exploração: vulnerabilidades que podem ser facilmente exploradas, exigindo poucas habilidades e pouco conhecimento;			
9.5.13.89.	Perda de dados: vulnerabilidades cuja exploração causará perda massiva de dados;			
9.5.13.89.	Negação de serviço: vulnerabilidades cuja carga útil pode sobrecarregar - impedir que sistemas comprometidos estejam permanentemente - temporariamente disponíveis;			
9.5.13.89.	No Patch: Vulnerabilidades para as quais não há solução do provedor;			
9.5.13.89.	Malware: vulnerabilidades associadas a infecções por malware;			
9.5.13.89.	Kit de exploração: vulnerabilidades para as quais um kit de exploração está disponível;			
9.5.13.90.	A solução deve atribuir uma pontuação a cada vulnerabilidade de forma contextual de forma a quantificar o risco associado a esta vulnerabilidade;			
9.5.13.91.	Os fatores de risco devem considerar, pelo menos 3 dos fatores abaixo:			
9.5.13.91.	Malwares associados;			
9.5.13.91.	Atores maliciosos associados;			
9.5.13.91.	Possibilidade de remediação;			
9.5.13.92.	A solução proposta deve fornecer um workflow de correção baseado em políticas de criação e atribuição, atribuindo tickets de acordo com as condições definidas pelo administrador da solução através de políticas ou manualmente;			
9.5.13.93.	A solução deve permitir a criação de tickets com status aberto, fechado, ignorado, com base nos seguintes critérios:			
9.5.13.93.	Host(s) a quem a regra se aplica;			
9.5.13.93.	Vulnerabilidade (s) a que a regra se aplica;			
9.5.13.93.	Usuário atribuído;			
9.5.13.93.	Data de criação - expiração;			
9.5.13.93.	Mudança de estado;			
9.5.13.94.	A solução deve permitir a criação de tickets de correção automaticamente a partir do resultado de uma varredura de vulnerabilidade - com base nas informações de um host específico e também manualmente por um administrador de solução;			
9.5.13.95.	A solução proposta deve correlacionar vulnerabilidades e patches automaticamente para os hosts da sua organização;			

9.5.13.96.	A solução deve mapear automaticamente os patches com CVEs associados às vulnerabilidades detectadas;			
9.5.13.97.	Deve mostrar patches faltantes mesmo que não exista correlação com uma vulnerabilidade existente;			
9.5.13.98.	Deve mostrar patches faltantes para no mínimo as seguintes categorias: Navegadores, Ferramentas de compressão de arquivos, Visualizadores de PDF e Sistemas operacionais.			
9.5.13.99.	A solução proposta deve permitir administração centralizada via interface gráfica WEB usando HTTPS;			
9.5.13.100	A solução deve possibilitar o acesso a console de todos os componentes do serviço a partir de um único ponto;			
9.5.13.101	A solução deve permitir a definição de diferentes perfis de usuários e funções para administração;			
9.5.13.102	A solução deve fornecer controles de acesso de usuário hierárquicos e baseados em funções que permitem a delegação de responsabilidades para refletir a estrutura organizacional;			
9.5.13.103	A solução deve permitir o acesso de um usuário autorizado de qualquer local;			
9.5.13.104	A solução deve suportar integração com uma biblioteca API XML extensível;			
9.5.13.105	A solução deve suportar autenticação de dois fatores para usuários e login;			
9.5.13.106	A solução deve suportar configurações de segurança de senha;			
9.5.13.107	A solução deve suportar personalizar a política de segurança para configurações de gerenciamento de senha, por:			
9.5.13.107	Idade e expiração da senha;			
9.5.13.107	Conta do usuário bloqueada após uma série de logins com falha;			
9.5.13.107	Comprimento mínimo da senha;			
9.5.13.107	Complexidade da senha, caracteres alfanuméricos e numéricos a serem usados;			
9.5.13.107	Forçar mudança de senha no login inicial			
9.5.13.107	Notificação de senha expirada antes de vários dias;			
9.5.13.108	A solução deve suportar a capacidade de restringir o acesso apenas de rede interna da empresa;			
9.5.13.109	A solução deve suportar a capacidade de rastrear a atividade do usuário por nome da conta do usuário, data, ação e informações sobre a ação;			
9.5.13.110	A solução deve suportar acesso por SSO (Single Sign-on) usando SAML 2.0;			
9.5.13.111	A solução proposta deve gerar relatórios por IPs, Grupo e Tags			
9.5.13.112	A solução deve permitir a geração de relatórios de qualquer IP - Host previamente verificado;			
9.5.13.113	A solução deve permitir agendar relatórios diários, semanais, mensais e sob demanda;			
9.5.13.114	A solução deve permitir o envio de notificações por email sempre que um relatório estiver disponível para o administrador da solução, usuários específicos e perfis diferentes criados na ferramenta;			
9.5.13.115	A Solução deve permitir pelo menos os seguintes tipos de relatórios: Relatório de correção; Relatório de vulnerabilidades altamente críticas; Relatório Executivo; Relatório de autenticação; Relatório de conformidade normativa e regulatória; e Relatório de remediação.			
9.5.13.116	A solução deve fornecer relatórios de correção por grupo de ativos, usuário e vulnerabilidade;			
9.5.13.117	A solução deve permitir a criação de relatórios baseados em IPv4, endereços IPv6, nome do host, grupo de ativos e rótulos personalizados pelo administrador;			
9.5.13.118	A solução deve permitir relatórios com cálculo de risco de segurança, permitindo um cálculo de risco global para todos os ativos incluídos no relatório;			

9.5.13.119	A solução deve permitir relatórios que possibilitem o cálculo do risco do negócio, utilizando como base para o cálculo do risco de impacto ao negócio e do risco de segurança dos ativos incluídos no relatório;			
9.5.13.120	A solução deve permitir relatar as descobertas com base no status das vulnerabilidades detectadas e seu status, conforme lista abaixo: Novo, Resolvido, Reaberto e Ativo.			
9.5.13.121	A solução deve permitir relatórios que incluam vulnerabilidades com base na data de publicação;			
9.5.13.122	A solução deve permitir excluir vulnerabilidades que não são exploráveis devido à configuração do sistema / plataforma onde foi detectada;			
9.5.13.123	A solução deve permitir a exclusão de patches da Microsoft que foram substituídos por um novo patch ou um patch cumulativo do mesmo fabricante;			
9.5.13.124	A solução deve fornecer relatórios automatizados de tendências e diferenciais;			
9.5.13.125	A solução deve fornecer várias opções de distribuição de relatórios, incluindo PDF criptografado;			
9.5.13.126	A solução deve dar suporte à personalização do modelo de relatório conforme necessário;			
9.5.13.127	A solução deve permitir a exportação de relatórios para dois dos formatos HTML, MHT, PDF, DOC, CSV e XML;			
9.5.13.128	A solução deve permitir que relatórios sejam apresentados em tabelas e gráficos com as ocorrências ocorridas, permitindo a customização detalhada de cada relatório;			
9.5.13.129	A solução deve possuir um painel (dashboard) que, por padrão, permite que você veja as tendências de vulnerabilidades por gravidade, plataforma, idade e status de remediação;			
9.5.13.130	A solução deve permitir a customização dos painéis fazendo uso de qualquer um dos dados disponíveis associados aos ativos varridos para selecionar diferentes tipos de gráficos, tabelas e visualizações sobre a priorização de vulnerabilidades;			
9.5.13.131	A solução deve fornecer painéis executivos personalizáveis com uma visão unificada de todos os componentes da solução;			
9.5.13.132	Deve ser possível criar dashboards que mostrem a pontuação de risco global de ativos e sua variação ao longo do tempo;			
9.6.	Modulo de Teste de Penetração - Pentest:			
9.6.1.	Objetivo dos Testes:			
9.6.2.	Executar testes de penetração em sistemas, redes e aplicações da CONTRATANTE, com o objetivo de identificar vulnerabilidades exploráveis, avaliar a postura de segurança da infraestrutura e fornecer recomendações práticas para mitigar riscos identificados.			
9.6.3.	Os testes devem ser realizados com ferramentas desenvolvidas pelo próprio analista ou ferramentas reconhecidas no mercado: Nmap, Metasploit, Cobalt Strike, Kali Linux, BloodHound, CrackMapExec, além de técnicas personalizadas em Python/Bash entre outras linguagens;			
9.6.4.	Os testes devem ser realizados sem comprometer a confidencialidade disponibilidade ou integridade dos sistemas, salvo acordo prévio, e culminar na entrega de um relatório final detalhado com os resultados, impactos e sugestões de correção.			
9.6.5.	É importante destacar que o PENTEST poderá ser realizado 3 (três) vezes durante a execução do contrato e custo do teste será apurado mensalmente, de modo a permitir o correto dimensionamento dos pagamentos.			
9.6.6.	Escopo dos Testes:			
9.6.6.1.	Ambientes a Serem Testados			

9.6.6.1.1.	Definir os ambientes a serem testados, incluindo, mas não se limitando a: redes internas e externas, serviços expostos, aplicações web, APIs, dispositivos IoT, sistemas legados, bancos de dados, serviços em nuvem (ex.: AWS, Azure) e aplicações móveis.			
9.6.6.1.2.	O escopo deve ser detalhado em conjunto com a CONTRATANTE, com base em uma lista de ativos ou diagrama de infraestrutura previamente fornecidos.			
9.6.6.2.	Simulações de Ataque			
9.6.6.2.1.	O testes devem incluir simulações de ataques internos e externos, explorando diferentes vetores de ameaça, como phishing, escalonamento de privilégios, injeção de código e exploração de configurações incorretas. Os testes podem ser realizados nos formatos black-box (sem informações prévias) ou gray-box (informações parciais), conforme definido no escopo acordado com a CONTRATANTE.			
9.6.6.3.	Frequência e Agendamento			
9.6.6.4.	Periodicidade dos Testes			
9.6.6.4.1.	Determinar a periodicidade dos testes (trimestral, semestral, anual ou conforme demanda específica), considerando a criticidade dos sistemas testados, requisitos regulatórios ou políticas internas da CONTRATANTE.			
9.6.6.5.	Testes Adicionais			
9.6.6.5.1.	Estabelecer critérios para a execução de testes adicionais em caso de grandes mudanças na infraestrutura (como implementação de novos sistemas, atualizações críticas ou expansões significativas) ou incidentes relevantes, com prazo de execução definido em até 7 (sete) dias após o evento, conforme acordado com a CONTRATANTE.			
9.6.7.	Metodologias e Padrões de Segurança			
9.6.7.1.	Metodologias Reconhecidas			
9.6.7.1.1.	Indicar metodologias reconhecidas para a realização dos testes, como OWASP (Open Web Application Security Project) para aplicações web e APIs, NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment) para diretrizes de avaliação técnica, MITRE ATT&CK para simulações de Red Team, PTES (Penetration Testing Execution Standard) para testes abrangentes, OSSTMM (Open Source Security Testing Methodology Manual) e, quando aplicável, alinhamento com a ISO/IEC 27001. As metodologias podem ser combinadas ou adaptadas ao contexto da CONTRATANTE, utilizando ferramentas reconhecidas, conforme especificado no plano de teste.			
9.6.7.2.	Os testes devem ser conduzidos por equipe técnica qualificada, com experiência comprovada e, preferencialmente, certificações reconhecidas na área de segurança da informação, como CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional) ou CISSP (Certified Information Systems Security Professional).			
9.6.7.3.	Exploração de Vulnerabilidades:			
9.6.7.4.	A ferramenta deve permitir a exploração controlada de vulnerabilidades identificadas, com as seguintes capacidades:			
9.6.7.5.	O analista deverá utilizar ferramentas que permitam a exploração controlada das vulnerabilidades identificadas, sem colocar em risco a integridade ou disponibilidade do ambiente, atendendo algumas premissas básicas de pentest, como por exemplo:			
9.6.7.6.	Execução de Exploits: Suporte à execução segura e documentada de exploits para validar a explotabilidade de falhas.			

9.6.7.7.	Criação de Payloads Personalizados: Funcionalidade para gerar sessões reversas, shells e payloads customizados (ex.: reverse shell para acesso remoto).			
9.6.7.8.	Integração com Bases de Exploits: Conexão com repositórios atualizados, como Exploit-DB, para acesso a exploits relevantes e recentes.			
9.6.7.9.	Testes em Diferentes Perspectivas: Capacidade de realizar testes de intrusão em redes internas e externas, simulando cenários de ataque realistas.			
9.6.7.10.	As vulnerabilidades identificadas devem ser classificadas conforme o sistema CVSS (Common Vulnerability Scoring System), acompanhadas de recomendações detalhadas e prazos sugeridos para mitigação. Deve ser oferecida a opção de retestes para validação das correções implementadas pela CONTRATANTE.			
9.6.8.	Conformidade Legal e Ética			
9.6.8.1.	Os testes devem ser realizados em conformidade com a legislação aplicável, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, e mediante autorização formal da CONTRATANTE, garantindo que todas as ações sejam éticas e legais.			
9.6.8.2.	Comunicação e Notificação, vulnerabilidades críticas devem ser comunicadas à CONTRATANTE em até 24 horas após a identificação, com relatórios preliminares, se necessário. Relatórios detalhados, contendo todas as descobertas, análises e recomendações, devem ser entregues ao final dos testes, em formato acordado com a CONTRATANTE			
9.6.9.	Suporte a Criptografia e Força Bruta:			
9.6.9.1.	A ferramenta deve oferecer recursos para testar a robustez de sistemas de autenticação e criptografia, incluindo:			
9.6.9.2.	Ataques a Senhas: Capacidade de quebrar senhas por meio de ataques de dicionário, força bruta ou métodos híbridos.			
9.6.9.3.	Compatibilidade com Protocolos: Suporte a testes em serviços como SSH, FTP, HTTP Auth, SMB, entre outros.			
9.6.10.	Para avaliação da segurança de ativos computacionais, redes, aplicações e serviços, com capacidade de identificar, explorar e relatar vulnerabilidades, conforme boas práticas reconhecidas internacionalmente, a CONTRATADA deverá em seu ambiente de SOC utilizar ferramenta com a capacidade mínimas para estes objetivos:			
9.6.11.	Coleta de Informações (Reconhecimento Passivo e Ativo)			
9.6.11.1.	A ferramenta deve oferecer capacidades robustas de reconhecimento, incluindo:			
9.6.11.2.	Varredura de Portas e Serviços: Capacidade de escanear portas e identificar serviços ativos em protocolos TCP, UDP e ICMP, detectando pontos de entrada em hosts-alvo.			
9.6.11.3.	Deve realizar a identificação de sistemas e serviços, com a Detecção automática de sistemas operacionais (ex.: Windows, Linux) e versões de serviços (ex.: Apache, SSH) em execução nos alvos.			
9.6.11.4.	Coleta de Informações Públicas (OSINT): Suporte à obtenção de metadados e dados públicos a partir de fontes abertas, como WHOIS, registros DNS e plataformas OSINT, sem interação direta com o alvo.			
9.6.11.5.	Descoberta de Subdomínios e DNS: Funcionalidade para identificar subdomínios e servidores DNS associados ao domínio-alvo;			

9.6.11.6.	Todas as ferramentas utilizadas pelo time técnico deverão ser fornecidas pela CONTRATADA, como exemplo cito ferramentas para realização de pentest web, máquinas para quebra de senha e ferramentas para engenharia reversa, variando de acordo com o escopo do teste definido pelo CONTRATANTE.			
9.6.12.	Análise de Vulnerabilidades:			
9.6.12.1.	A ferramenta deve possuir recursos avançados para identificação e classificação de vulnerabilidades, incluindo:			
9.6.12.2.	Detecção de Vulnerabilidades Conhecidas: Capacidade de detectar falhas catalogadas no banco CVE, com classificação baseada no CVSS (ex.: crítico, alto, médio).			
9.6.12.3.	Suporte a Múltiplos Alvos: Análise de vulnerabilidades em aplicações web, APIs, infraestrutura de rede e sistemas tradicionais.			
9.6.12.4.	Filtros de Severidade: Opções para filtrar resultados por nível de criticidade e severidade, facilitando a priorização de correções.			
9.6.12.5.	Exportação de Resultados: Geração de relatórios exportáveis em formatos abertos, como XML, JSON, CSV e PDF, para integração com outros sistemas ou entrega à CONTRATANTE;			
9.6.13.	Armazenamento e descarte de Relatórios e Evidências			
9.6.13.1.	Com base no NIST e OWASP todas as evidências técnicas, relatórios preliminares, finais e demais artefatos gerados durante a execução do serviço de teste de intrusão (pentest) deverão ser, obrigatoriamente, armazenados exclusivamente na infraestrutura da CONTRATANTE, seja em ambiente local ou em seus serviços próprios de nuvem.			
9.6.13.2.	É vedado ao contratado manter cópias desses documentos ou evidências em qualquer outro meio físico ou digital após a conclusão do projeto, salvo autorização expressa e formal da CONTRATANTE.			
9.6.13.3.	Após a conclusão da atividade as evidências coletadas nos computadores, dispositivo utilizado no pentest deverão ser apagados mantendo apenas as copias na infraestrutura da CONTRATANTE.			
9.6.14.	Escopo de pentest			
9.6.14.1.	O escopo do pentest será definido pelo CONTRATANTE e será dividido em 3 diferentes fases:			
9.6.14.1.1.	Pentest Blackbox/Graybox na(s) aplicações, infraestrutura ou serviços definidos pelo cliente. Com base de 160 horas de execução seguindo as melhores práticas de mercado: 1. Reconhecimento, 2. Escaneamento e Exploração, 3. Movimentação Lateral, 4. Manutenção de Acesso, 5. Exfiltração de Dados.			
9.6.14.1.2.	Pentest Blackbox/Graybox na(s) aplicações, infraestrutura ou serviços definidos pelo cliente. Com base de 80 horas de execução seguindo as melhores práticas de mercado: 1. Reconhecimento, 2. Escaneamento e Exploração, 3. Movimentação Lateral, 4. Manutenção de Acesso, 5. Exfiltração de Dados.			
9.6.14.1.3.	Pentest Blackbox/Graybox na(s) aplicações, infraestrutura ou serviços definidos pelo cliente. Com base de 80 horas de execução seguindo as melhores práticas de mercado: 1. Reconhecimento, 2. Escaneamento e Exploração, 3. Movimentação Lateral, 4. Manutenção de Acesso, 5. Exfiltração de Dados.			
9.7.	Modulo de Threat Intelligence (OSINT):			
9.7.1.	Deverá ser fornecido o serviço de Inteligência em Ameaças Cibernéticas (Threat Intelligence), com foco em coleta, correlação e análise de dados públicos e fontes abertas (OSINT), através de uma solução que atenda aos requisitos abaixo:			

9.7.1.1.	Capacidade para operação simultânea de, no mínimo, 03 usuários autenticados,			
9.7.1.2.	A operação da ferramenta será realizada pelo time de SOC da empresa CONTRATADA em regime 24x7.			
9.7.1.3.	O funcionamento da plataforma deverá ser em nuvem, acessível via web no modelo SaaS (Software-as-a-Service), com disponibilidade mínima de 99,9%.			
9.7.1.4.	A solução deverá operar em cloud pública, com arquitetura redundante e escalável.			
9.7.1.5.	Compatibilidade com navegadores modernos (Firefox 60+, Chrome 65+), incluindo suporte a autenticação multifator.			
9.7.2.	Integração e API:			
9.7.2.1.	Integração por API RESTful e/ou SDK, com respostas em formato JSON e documentação acessível.			
9.7.2.2.	Suporte a webhooks e integração com plataformas de SIEM, SOAR, e Threat Intelligence Platform (TIP).			
9.7.2.3.	Controle granular de acesso por usuário, times e perfis de operação.			
9.7.2.4.	Integração com MISP (Malware Information Sharing Platform), com importação/exportação de IOCs.			
9.7.3.	Armazenamento e Logs:			
9.7.3.1.	Retenção ilimitada de eventos OSINT, mesmo após exclusão da fonte original.			
9.7.3.2.	Armazenamento mínimo de 5 bilhões de eventos e 25 milhões de entidades maliciosas (atores, domínios, IPs, etc.).			
9.7.3.3.	Logs de acesso detalhados (usuário, atividade, IP, data/hora, user-agent), armazenados por no mínimo 1 ano.			
9.7.4.	Processamento, Enriquecimento e Inteligência Artificial:			
9.7.4.1.	Capacidade de enriquecimento automático de dados coletados com IA/ML.			
9.7.4.2.	Detecção com IA de cartões de crédito expostos, credenciais vazadas, perfis falsos de executivos, menções a VIPs.			
9.7.4.3.	Correlação automática entre dados coletados (rede social, domínio, e-mail, telefone, endereço IP).			
9.7.4.4.	Apoio a técnicas de fingerprinting e clusterização de entidades maliciosas.			
9.7.4.5.	Identificação de links de phishing, typosquatting e infraestruturas de comando e controle (C2).			
9.7.5.	Metadados dos Eventos:			
9.7.5.1.	Cada evento OSINT deverá conter:			
9.7.5.1.1.	Data da coleta e data de indexação			
9.7.5.1.2.	Hash do conteúdo (SHA-256)			
9.7.5.1.3.	Fonte original (URL, domínio, plataforma)			
9.7.5.1.4.	Nome do robô/coletor			
9.7.5.1.5.	Classificação por tipo e severidade			
9.7.6.	Mecanismos de Busca e Visualização OSINT			
9.7.6.1.	Busca avançada por data, metadados, fontes, palavras-chave, atores, campanhas, hashtags e IOC.			
9.7.6.2.	Suporte a filtros avançados: proximidade, fuzzy search, lógica binária, regex, operadores lógicos, wildcard.			
9.7.6.3.	Capacidade de drill-down exploratório com filtros dinâmicos (inclusão/exclusão).			
9.7.6.4.	Identificação automática de campanhas de phishing, perfis falsos, vulnerabilidades exploradas (zeroday), defacements, malspam, scam e fraude.			
9.7.6.5.	Monitoramento e análise de domínios, certificados SSL, URLs, arquivos suspeitos e infraestrutura relacionada.			
9.7.7.	Dashboards e Visualização Analítica			
9.7.7.1.	Painéis interativos com gráficos de tendências, volume de ameaças, fontes monitoradas e perfis observados.			

9.7.7.2.	Busca de perfis e entidades por nome, apelido, e-mail, telefone, CPF/CNPJ, usernames e handles.			
9.7.7.3.	Visualização de pesquisas salvas com filtros organizacionais e exportação em diversos formatos (XLSX, JSON, CSV, DOCX, PDF).			
9.7.8.	Gerenciamento de Ocorrências e Casos de Investigação:			
9.7.8.1.	Associação de eventos OSINT a ocorrências específicas ou incidentes internos.			
9.7.8.2.	Campos com suporte a imagens embutidas, anexos, histórico de alterações e adição de comentários colaborativos.			
9.7.8.3.	Notificações configuráveis por e-mail e WebHook com base em palavras-chave, nível de risco e origem.			
9.7.8.4.	Ferramentas de triagem por criticidade, categoria, período, responsável e organização.			
9.7.8.5.	Inclusão de IOCs, marcadores e histórico de modificações em cada ocorrência.			
9.7.9.	Relatórios de Inteligência:			
9.7.9.1.	Mínimo de relatórios desenvolvidos por analistas humanos e IA, com foco em, sob demanda:			
9.7.9.1.1.	Ameaças emergentes			
9.7.9.1.2.	Infraestruturas maliciosas			
9.7.9.1.3.	Hacktivismo, geopoliticamente motivado			
9.7.9.1.4.	Deep e Dark Web			
9.7.9.1.5.	Deteção de novos TTPs e ferramentas ofensivas			
9.7.9.2.	Base histórica de 3.000 relatórios com pesquisa por palavras-chave, categoria, autor e data.			
9.7.9.3.	Relatórios exportáveis em PDF criptografado para casos confidenciais.			
9.7.10.	Fontes Monitoradas e Coleta OSINT:			
9.7.10.1.	Coleta automatizada de:			
9.7.10.1.1.	Mídias sociais (Facebook, Twitter, LinkedIn, Instagram, TikTok, Reddit)			
9.7.10.1.2.	Deep Web (fóruns, pastebins, marketplaces)			
9.7.10.1.3.	Dark Web (Tor, I2P, ZeroNet)			
9.7.10.1.4.	Blogs, sites de notícias, grupos públicos de Telegram e Discord			
9.7.10.2.	Suporte a crawlers personalizados, scraping de páginas públicas, monitoramento de canais fechados com autorização.			
9.7.10.3.	Web beacon para rastreamento de acessos a sites da CONTRATANTE.			
9.7.10.4.	Scripts para detecção de clonagem de sites, redirecionamentos maliciosos e alterações de DNS.			
9.7.11.	Solicitação e Gestão de Takedowns			
9.7.11.1.	Serviço integrado de takedown, com opção para remoção automatizada de conteúdos maliciosos.			
9.7.11.2.	Mínimo de 10 remoções/mês durante a vigência contratual.			
9.7.11.3.	Tela dedicada para solicitação de takedowns com os campos:			
9.7.11.3.1.	URL			
9.7.11.3.2.	Empresa			
9.7.11.3.3.	Prioridade			
9.7.11.3.4.	Categoria			
9.7.11.4.	Possibilidade de feedback para cada ocorrência encerrada.			
9.7.11.5.	Painel com visualização por data, prioridade, status e número de ocorrências.			
9.7.11.6.	Filtros por empresa, período, categoria, responsável e status.			
9.7.12.	Takedown Automatizado e Dashboard			
9.7.12.1.	Recurso de takedown automatizado para perfis e páginas em:			
9.7.12.1.1.	Instagram, Facebook, TikTok			
9.7.12.1.2.	Hospedagens como Hostgator, GoDaddy			
9.7.12.1.3.	Compartilhadores de arquivos (ex: Scribd, MediaFire).			
9.7.12.2.	Dashboard com:			
9.7.12.2.1.	Volume de takedowns solicitados			
9.7.12.2.2.	Status atual por categoria			

9.7.12.2.3.	Tempo médio de resposta			
9.7.12.2.4.	Lista com filtros avançados por empresa, período e responsável.			
9.8.	Ferramentas para o NOC (Network Operations Center) e SO (Setor Operacional)			
9.8.1.	O NOC e SO deverá dispor de soluções de observabilidade de rede e sistemas, análise de fluxo, análise de pacotes e correlacionadores de performance com alertas baseados em políticas e IA.			
9.8.2.	As soluções adotadas devem proporcionar visibilidade detalhada do tráfego de rede, permitir a análise avançada de pacotes e facilitar a identificação de problemas de desempenho e segurança.			
9.8.3.	A CONTRATADA poderá utilizar outras ferramentas adicionais, conforme necessário, desde que respeitem as diretrizes acordadas com a contratante e sejam compatíveis com os serviços prestados.			
9.8.4.	Para garantir um nível mínimo de capacidade operacional e eficiência na ações de rede, o NOC e SO deve contar com as seguintes ferramentas modulares:			
9.8.4.1.	Módulo de observabilidade de rede e sistemas - APM (Application Performance Monitoring) e NPM (Network Performance Monitoring);			
9.8.4.2.	Módulo de visibilidade de tráfego - NPB (Network Packet Broker) agregação e distribuição de tráfego;			
9.8.4.3.	Modulo de gerenciamento e monitoramento – ITSM (Cherwell) e Zabbix/ Grafana.			
9.8.4.4.	Módulo de observabilidade de rede e sistemas - APM (Application Performance Monitoring) e NPM (Network Performance Monitoring)			
9.8.5.	Monitormaneto por APM (Application Performance Monitoring)			
9.8.5.1.	A CONTRATADA deverá disponibilizar, configurar e customizar uma solução de Observabilidade baseada em padrões como OpenTelemetry, Prometheus e Grafana, capaz de coletar logs, métricas e traces distribuídos. A solução deverá contemplar integração com ambientes críticos de segurança pública e permitir a geração de alertas correlacionados por AI/ML para antecipação de falhas e incidentes. O sistema deverá possibilitar o monitoramento contínuo do tempo de resposta de chamadas de API, uso de recursos por diferentes componentes de aplicações e detecção de anomalias, garantindo eficiência operacional e alta disponibilidade dos sistemas da CONTRATANTE.			
9.8.5.2.	O monitoramento contínuo da infraestrutura e das aplicações da CONTRATANTE deverá contar com ferramentas especializadas para identificar gargalos de desempenho, falhas, impactos na experiência do usuário e incidentes de segurança.			
9.8.5.3.	A solução adotada deverá garantir visibilidade completa do ciclo de vida das aplicações e serviços, permitindo análise detalhada dos tempos de resposta, consumo de recursos, comportamento transacional e correlação de eventos em tempo real.			
9.8.5.4.	O monitoramento deverá abranger todas as aplicações críticas da CONTRATANTE, incluindo aquelas hospedadas no Datacenter, bem como serviços distribuídos em ambientes híbridos ou na nuvem.			
9.8.5.5.	A solução deverá oferecer recursos avançados para detecção de anomalias, diagnóstico proativo e resposta automatizada a incidentes de TI, garantindo resiliência operacional.			
9.8.5.6.	A CONTRATADA poderá adotar outras ferramentas adicionais, conforme necessário, desde que respeitem as diretrizes da contratante e que sejam compatíveis com os serviços prestados.			

	A CONTRATADA será responsável pela hospedagem, operação e gerenciamento da solução de monitoramento e observabilidade, garantindo que os serviços sejam prestados de forma contínua e segura, com alta disponibilidade e redundância. A CONTRATANTE deverá ter acesso remoto, contínuo e seguro às informações estratégicas, dashboards, relatórios e alertas, sem a necessidade de operação direta do sistema. A CONTRATADA deverá garantir a exportação e consulta dos dados históricos, conforme prazos e formatos definidos pela CONTRATANTE, incluindo a possibilidade de solicitações eventuais de extração de dados pela CONTRATANTE para auditoria ou análise detalhada.			
9.8.5.7.				
9.8.5.8.	Requisitos Gerais da Solução			
	A solução deverá ser disponibilizada e operada pela CONTRATADA, garantindo conformidade com normas de proteção de dados, incluindo a Lei Geral de Proteção de Dados (LGPD) e regulamentações internacionais compatíveis.			
9.8.5.9.				
	A CONTRATADA deverá assegurar que a CONTRATANTE tenha acesso seguro e contínuo aos dashboards, relatórios e métricas necessárias para acompanhamento dos serviços, incluindo dados históricos e exportáveis.			
9.8.5.10.				
	A CONTRATADA deverá fornecer mecanismos para contingência e continuidade operacional, incluindo arquitetura ativa-ativa ou ativa-passiva com failover automático, RTO inferior a 15 minutos e RPO de no máximo 5 minutos, replicação geográfica de dados críticos, e testes mensais de resiliência com relatórios auditáveis.			
9.8.5.11.				
	A ferramenta deverá fornecer integração ampla com soluções de terceiros por meio de APIs abertas e suporte a padrões de mercado, como REST, Webhooks e OpenTelemetry.			
9.8.5.12.				
	A solução deverá ser compatível com ambientes híbridos e multicloud, permitindo o monitoramento de aplicações distribuídas e infraestrutura localizada no Datacenter da CONTRATANTE.			
9.8.5.13.				
	A plataforma deverá utilizar inteligência artificial e aprendizado de máquina para detecção de anomalias, com capacidade de construir perfis comportamentais baseados em séries temporais, identificar padrões de degradação e recomendar ações proativas com base em modelos supervisionados e não supervisionados.			
9.8.5.14.				
	A ferramenta deverá oferecer suporte a análise preditiva de falhas utilizando modelos supervisionados e não supervisionados, com detecção de comportamento anômalo, predição de picos de uso e sugestão de remediações preventivas baseadas em incidentes históricos.			
9.8.5.15.				
	A solução deverá permitir a criação de métricas de negócio personalizáveis, incluindo volume de transações e tempo médio de processamento, garantindo flexibilidade para monitoramento de desempenho operacional.			
9.8.5.16.				
9.8.5.17.	Requisitos Técnicos e Funcionalidades Mínimas			
	A plataforma deverá integrar logs, métricas e rastreamentos (traces) de forma nativa, seguindo a especificação do Three Pillars of Observability, e permitir correlação contextual em tempo real. Deverá suportar ingestão via agentes leves e coleta via API para ambientes híbridos, com disponibilidade mínima de 99,9%, replicação de dados e escalabilidade horizontal, permitindo correlação automática entre eventos de diferentes fontes.			
9.8.5.17.1.				

9.8.5.17.2.	A solução deverá prover visibilidade detalhada do uso de CPU, consumo de memória, rede e armazenamento, com série temporal de métricas, coleta via agentes leves e exportação em dashboards de análise comparativa por componente, host e serviço, além de permitir criação de alertas threshold e análise preditiva de capacidade, permitindo diagnóstico preciso de degradação de performance.			
9.8.5.17.3.	O sistema deve permitir a criação de alertas automatizados com base em limiares configuráveis, anomalias detectadas e tendências históricas.			
9.8.5.17.4.	A ferramenta deverá fornecer dashboards interativos e personalizáveis, permitindo filtragem de dados e visualizações detalhadas em tempo real.			
9.8.5.17.5.	A solução deverá fornecer suporte ao monitoramento de banco de dados, incluindo tempo de resposta de queries, taxa de acertos em cache, consumo de CPU por sessão e detecção de anomalias em acessos concorrentes.			
9.8.5.17.6.	A solução deverá permitir a análise detalhada do desempenho de aplicações, garantindo visibilidade fim a fim por meio da coleta, processamento e correlação de eventos.			
9.8.5.17.7.	A ferramenta deverá fornecer integração com soluções de ITSM, facilitando a abertura e acompanhamento de incidentes.			
9.8.5.17.8.	A solução deverá suportar armazenamento de logs e métricas históricos para análise forense e auditorias de segurança.			
9.8.5.17.9.	A solução deverá incluir mecanismos para detecção proativa de falhas de segurança em aplicações monitoradas, integrando-se com bases públicas de vulnerabilidades e permitindo alertas automatizados para atividades suspeitas.			
9.8.5.18.	Requisitos de Implantação e Suporte			
9.8.5.19.	A solução deverá garantir conformidade com a Lei Geral de Proteção de Dados (LGPD), assegurando a privacidade e integridade das informações monitoradas.			
9.8.5.20.	A solução deverá permitir integração segura com sistemas externos, utilizando protocolos de comunicação criptografados.			
9.8.5.21.	A CONTRATADA deverá garantir a alta disponibilidade da solução, assegurando que incidentes internos da sua infraestrutura não impactem a continuidade do monitoramento da CONTRATANTE. Deverão ser implementados mecanismos de redundância e contingência para evitar interrupções nos serviços prestados. Caso ocorra falha de comunicação entre os agentes e a plataforma da CONTRATADA, os dados coletados localmente deverão ser armazenados e sincronizados assim que a conectividade for restabelecida, garantindo integridade e continuidade do monitoramento. Em casos de falhas prolongadas na infraestrutura da CONTRATADA, a mesma deverá disponibilizar à CONTRATANTE um plano de contingência que permita acesso emergencial aos dados críticos e relatórios previamente coletados.			
9.8.5.22.	A CONTRATADA deverá fornecer documentação técnica sobre a operação e utilização da plataforma, incluindo a definição dos fluxos de monitoramento e análise.			
9.8.5.23.	A CONTRATADA deverá fornecer capacitação para usuários da CONTRATANTE, abordando a navegação em dashboards, geração de relatórios e interpretação de métricas relevantes ao acompanhamento dos serviços prestados.			
9.8.5.24.	A CONTRATANTE poderá solicitar capacitação adicional para novos usuários ou atualizações da ferramenta, sempre que forem implementados novos recursos ou alterações significativas na plataforma.			

9.8.5.25.	A CONTRATADA deverá fornecer documentação técnica e de usuário, contendo instruções detalhadas sobre a utilização dos recursos disponíveis para a CONTRATANTE.			
9.8.5.26.	O suporte da ferramenta deverá ser prestado na modalidade 8x5 NBD (Next Business Day), garantindo tempo de resposta de até 4 horas para incidentes críticos.			
9.8.5.27.	A contratada deverá realizar a implementação e tuning do monitoramento para os seguintes sistemas críticos da CONTRATANTE: COPOM Online; SIOPM Web; SIOPM Corp/V; Citrix App and Desktop Virtualization; Microsoft SQL Server.			
9.8.5.28.	Além desses sistemas, a CONTRATANTE poderá solicitar a inclusão de outras aplicações e infraestruturas críticas, devendo a solução ofertada ser capaz de monitorar qualquer ativo demandado, independentemente do fabricante e da arquitetura.			
9.8.5.29.	Ao final da implementação a CONTRATADA deverá entregar um documento técnico detalhado (LLD - Low-Level Design), contendo: Topologia dos sistemas monitorados, Relação dos componentes monitorados, incluindo endereços IP e hostnames, Passo a passo de cada configuração realizada e Capturas de tela e logs de configuração e dashboards principais.			
9.8.5.30.	O LLD deverá ser entregue de forma faseada, acompanhando a implementação da solução, garantindo visibilidade à CONTRATANTE sobre as configurações realizadas ao longo do projeto.			
9.8.5.31.	A Plataforma de Observabilidade deverá permitir a correlação automatizada de eventos em aplicações, infraestrutura e serviços, fornecendo uma visão fim a fim do ambiente monitorado.			
9.8.5.32.	A solução deverá integrar logs, métricas e rastreamentos (traces) de forma nativa, permitindo análise unificada e identificação de falhas em tempo real.			
9.8.5.33.	A A ferramenta deverá suportar descoberta automática e remota de componentes de TI, incluindo servidores, bancos de dados, aplicações, APIs e microsserviços, gerando um mapa dinâmico das dependências. A solução deverá ser compatível com arquiteturas distribuídas, garantindo que componentes monitorados na infraestrutura da CONTRATANTE sejam corretamente identificados e correlacionados dentro da plataforma da CONTRATADA.			
9.8.5.34.	A solução deverá incluir análise preditiva baseada em inteligência artificial e aprendizado de máquina para identificar padrões, prever falhas e recomendar ações corretivas.			
9.8.5.35.	O sistema deverá ser compatível com ambientes on-premises, híbridos e multicloud, permitindo o monitoramento centralizado de infraestruturas distribuídas.			
9.8.5.36.	A plataforma deverá incluir detecção automática de anomalias e alertas inteligentes, ajustando-se dinamicamente ao comportamento esperado dos sistemas.			
9.8.5.37.	O sistema deverá fornecer dashboards interativos e personalizáveis, com suporte à criação de painéis customizados para diferentes equipes e necessidades.			
9.8.5.38.	A solução deverá oferecer integração com ferramentas de ITSM e SIEM, facilitando a resposta a incidentes e a rastreabilidade de eventos críticos.			
9.8.5.39.	A plataforma deverá possuir APIs abertas e documentadas, permitindo integração com sistemas existentes da CONTRATANTE e soluções de terceiros.			
9.8.5.40.	A ferramenta deverá fornecer suporte a consulta histórica de dados, permitindo auditoria e análise forense de eventos passados.			

9.8.5.41.	A plataforma deverá contar com mecanismos de alta disponibilidade e escalabilidade, garantindo desempenho adequado para grandes volumes de dados e comunicação eficiente com ambientes distribuídos e remotos. A infraestrutura da CONTRATADA deverá ser dimensionada para suportar picos de demanda, garantindo que o monitoramento da CONTRATANTE ocorra sem degradação de desempenho ou perda de eventos críticos. A solução deverá assegurar baixa latência na comunicação entre os agentes de monitoramento da CONTRATANTE e a plataforma hospedada na infraestrutura da CONTRATADA, garantindo a entrega de eventos em tempo real para serviços críticos.			
9.8.5.42.	A Plataforma deverá ser capaz de monitorar qualquer aplicação ou infraestrutura crítica que venha a ser adicionada no ambiente da CONTRATANTE, garantindo escalabilidade e compatibilidade com múltiplos fabricantes.			
9.8.5.43.	O APM deverá fornecer monitoramento contínuo do desempenho das aplicações, identificando gargalos e falhas em tempo real.			
9.8.5.44.	A ferramenta deverá medir e analisar tempo de resposta de chamadas de API, execução de queries em banco de dados, consumo de CPU/memória e latência de serviços.			
9.8.5.45.	O sistema deverá ser capaz de mapear automaticamente dependências entre aplicações, serviços e infraestrutura, fornecendo visão fim a fim do ambiente, incluindo a comunicação entre os agentes remotos e a plataforma da CONTRATADA.			
9.8.5.46.	A solução deverá incluir rastreamento distribuído de transações, permitindo identificar onde ocorre degradação de desempenho em arquiteturas baseadas em microserviços.			
9.8.5.47.	A ferramenta deverá oferecer baselines dinâmicos, ajustando automaticamente os limiares de alerta com base no comportamento normal da aplicação.			
9.8.5.48.	O sistema deverá permitir análise detalhada de código, identificando métodos e consultas SQL com maior impacto no tempo de resposta.			
9.8.5.49.	A solução deverá gerar alertas proativos, notificando automaticamente equipes responsáveis quando ocorrerem degradações de desempenho.			
9.8.5.50.	A ferramenta deverá suportar testes sintéticos, permitindo simular interações de usuários para detectar falhas antes que impactem o ambiente produtivo.			
9.8.5.51.	O APM deverá ser compatível com diversas tecnologias e linguagens de desenvolvimento, incluindo Java, .NET, Python, Node.js, PHP, entre outras.			
9.8.5.52.	A Solução deverá ser integrada à Plataforma de Observabilidade, permitindo correlação de eventos e análise conjunta de métricas, logs e traces.			
9.8.5.53.	A solução deve ser capaz de monitorar a experiência de usuários finais da aplicação, através de um código JavaScript injetado no front-end da aplicação de maneira automática. A coleta de dados não deve requerer alteração de arquivos da aplicação ou alteração de código da aplicação. Novas configurações na UI devem ser propagadas automaticamente para o agente, sem requerer alterações ao código JavaScript. Não deve requerer alterações no ambiente/navegador do usuário final e também não serão permitidas alterações nos servidores HTTP assim como inserções manuais de URL via interface.			

9.8.5.54.	Deverá permitir a configuração de capturas de informações a partir de pelo menos Meta Tag, componentes CSS e JavaScript Variables, na página executada no navegador do usuário. O objetivo identificar o usuário logado ou enriquecer as transações de negócio. Não será permitido a alteração de código para captura de informações			
9.8.5.55.	A solução deverá permitir a consulta (queries) de informações capturadas no monitoramento da experiência do usuário, podendo ser visualizadas em dashboards e utilizá-las como métricas de negócio.			
9.8.5.56.	Deverá realizar a monitoração fim-a-fim das aplicações hospedadas no DataCenter, registrando e avaliando, no mínimo: 9.8.5.56.1. A requisição feita pelo usuário no navegador (click e carregamento de páginas ou ação do usuário na aplicação, gerando tráfego no servidor). 9.8.5.56.2. A execução do código nos servidores de aplicação. 9.8.5.56.3. As consultas aos servidores de banco de dados. 9.8.5.56.4. O retorno do resultado ao navegador do usuário. 9.8.5.56.5. Tempo de execução total da sessão/visita; 9.8.5.56.6. Tempo gasto em rede; 9.8.5.56.7. Tempo de servidor (execução transacional da aplicação) 9.8.5.56.8. Tempo de download do HTML e outros recursos da página; 9.8.5.56.9. Tempo de renderização do browser (DOM Build); 9.8.5.56.10. Tempo de pós-load; 9.8.5.56.11. Identificar webservices e chamadas a serviços externos das transações de uma aplicação.			
9.8.5.57.	O módulo de experiência de usuário deve permitir, nativamente, a configuração de capturas de dados na página executada no navegador do usuário de forma anonimizada, com objetivo de reproduzir a sessão do usuário a partir da captura de eventos do navegador que permitam a visualização em formato de vídeo do ponto de vista do usuário a navegação realizada. Estas visualizações devem estar disponíveis para reprodução por, no mínimo, 30 dias após a sua realização;			
9.8.5.58.	A solução de reprodução de sessão do usuário deve vir com mascaramento de informações sensíveis do usuário por padrão e também permitir a configuração customizada deste mecanismo de privacidade de dados., permitindo, a nível de permissões de perfis de analistas, visualizar ou não as informações sensíveis.			
9.9.	Modulo de Network Performance Monitoring - NPM			
9.9.1.	A solução deve ser composta por equipamentos físicos e virtuais independentes de um único fabricante.			
9.9.2.	É importante destacar que o licenciamento dos NPM poderá chegar a 100 (cem) unidades, conforme a necessidade e a estratégia de implantação. O custo do software será apurado mensalmente, de modo a permitir o correto dimensionamento dos pagamentos.			
9.9.3.	Os equipamentos ofertados devem possuir memória e capacidade de processamento suficientes para garantir o atendimento a todos os requisitos desta especificação, mesmo sob uso máximo.			
9.9.4.	A solução deve suportar alta disponibilidade, adotando mecanismos de clusterização ou similares, ou permitir balanceamento de tráfego por meio de solução Network Packet Broker.			
9.9.5.	Não será aceita administração por meio de aplicação cliente ou solução executada em JVM (Java Virtual Machine).			

9.9.6.	Todos os equipamentos fornecidos devem ser novos, sem uso anterior, e compatíveis com a linha de produção atual do fabricante na data de entrega.			
9.9.7.	Os equipamentos devem implementar mecanismos nativos de monitoramento e detecção de falhas internas.			
9.9.8.	Todos os ativos gerenciáveis devem possuir pelo menos uma interface dedicada 1GbE RJ45 para gerenciamento.			
9.9.9.	Os discos rígidos devem suportar tecnologia hot swappable e RAID para proteção contra perda de dados.			
9.9.10.	A administração remota deve ser realizada por meio de interface gráfica (GUI) via canal seguro.			
9.9.11.	Deve haver suporte à interface de gerenciamento Web (HTTPS) e CLI.			
9.9.12.	Devem ser implementados os protocolos de gerenciamento SNMPv2c, SNMPv3, incluindo geração de traps.			
9.9.13.	Deve ser implementado o protocolo NTP (Network Time Protocol).			
9.9.14.	Deve permitir acesso via SSHv2, com proteção por senha.			
9.9.15.	Deve permitir autenticação com base em servidores RADIUS ou LDAP.			
9.9.16.	Deve permitir envio de logs para servidores externos (syslog).			
9.9.17.	Deve permitir auditoria de alterações de configuração por meio de logs.			
9.9.18.	Deve permitir atualização remota do sistema operacional e arquivos de configuração via interface de gerenciamento.			
9.9.19.	Deve implementar controle de acesso baseado em funções (RBAC) com perfis de acesso configuráveis.			
9.9.20.	A solução deve coletar dados em tempo real da solução Network Packet Broker, sem impactar o desempenho da rede ou das aplicações.			
9.9.21.	A solução deve fornecer métricas de desempenho na camada de rede, incluindo: Taxa de Bits, Largura de Banda, Conexões Simultâneas, Atraso de Rede, Atraso no Servidor, Tempo de Transmissão de Dados, Perda de Pacotes, Retransmissão, Janela TCP Zero, Desconexão Anormal TCP, etc.			
9.9.22.	Deve haver suporte à personalização de aplicações agrupadas por portas TCP/UDP, URLs, endereços IPv4/IPv6 e marcações DSCP.			
9.9.23.	Deve ser capaz de identificar e eliminar instâncias duplicadas de pacotes durante a coleta.			
9.9.24.	Deve permitir gravação e exportação de arquivos capturados em formato .pcap.			
9.9.25.	Deve fornecer visualizações personalizadas por login de usuário.			
9.9.26.	Deve permitir renomear aplicações inspecionadas com base no número da porta TCP/UDP e/ou endereço IP.			
9.9.27.	Deve fornecer análise de comportamento de rede com alertas de baseline para anomalias nas métricas selecionadas.			
9.9.28.	Deve suportar integração de alertas via SNMP Trap, SNMP GET, API ou outros meios de integração.			
9.9.29.	Deve montar um mapeamento dinâmico da rede com base nos pacotes capturados da rede.			
9.9.30.	Este mapeamento deve ter como referência os endereços IP dos servidores e apresentar as condições dos segmentos de rede, das aplicações e a causa raiz de falhas, permitindo uma análise aprofundada da comunicação.			
9.9.31.	Deve emitir alertas para desvios de desempenho da rede e aplicações, bem como variações sazonais, com base em análise detalhada de cada aplicação existente.			
9.9.32.	Deve permitir inventariar sub-redes e VLANs, visualizando cada uma como localidade distinta.			

9.9.33.	Todas as licenças de software necessárias devem ser fornecidas para cumprimento integral desta especificação, incluindo atualizações durante o período contratual.			
9.9.34.	Deve permitir acesso simultâneo de múltiplos usuários à interface gráfica (GUI) da solução, por navegadores populares ou aplicação proprietária.			
9.9.35.	Todas as funcionalidades de gráficos, relatórios, buscas e gerenciamento devem estar acessíveis em formato de página web.			
9.9.36.	Deve permitir integração com outras plataformas por meio de APIs para consultas automatizadas.			
9.9.37.	A solução deve suportar, no mínimo, os seguintes tipos de contas de usuário:			
9.9.37.1.	Administrador: configuração de hardware, criação de contas de usuário, monitoramento de dispositivos, backup, acesso completo às funcionalidades, gerenciamento de contas, etc.			
9.9.37.2.	Operador: gerenciamento de grupos, alertas, relatórios de tráfego/eventos e configuração de detecção de eventos.			
9.9.37.3.	Monitor: consultas a relatórios e acompanhamento do status de eventos.			
9.9.38.	Probe de Captura de Dados de Rede:			
9.9.38.1.	A solução ofertada deve ser estruturada em hardware próprio e dedicado, visando garantir a disponibilidade e o desempenho do serviço.			
9.9.38.2.	Deve ser completamente passiva na rede existente, garantindo que qualquer interrupção na solução não leve à indisponibilidade dos serviços.			
9.9.38.3.	Toda nova aplicação configurada na rede deve ser capaz de ser capturada e inspecionada sem a necessidade de desenvolvimento da ferramenta.			
9.9.38.4.	Os pacotes capturados devem ser armazenados por um determinado período de tempo, conforme solicitado no Período de Retenção, e deve ser permitido extrair esses pacotes, no mínimo, nos formatos PCAP.			
9.9.38.5.	Os ativos utilizados para captura de pacotes devem possuir alta velocidade de processamento e placas de captura de ultra-baixa latência com, no mínimo, 2 interfaces 40/100 Gbps QSFP/QSFP28.			
9.9.38.6.	Para atender ao período de retenção com armazenamento de dados brutos e metadados, a solução deve possuir, no mínimo, 240 TB de armazenamento sem expansão, operando em RAID 5 ou superior, que forneça desempenho e proteção contra perda de dados.			
9.9.38.7.	Deve suportar o armazenamento de dados brutos da rede por, no mínimo, 3 dias.			
9.9.38.8.	A solução de captura de pacotes deve armazenar e ser capaz de sobrescrever/excluir automaticamente dados antigos.			
9.9.38.9.	Deve ser capaz de capturar dados brutos automaticamente, de forma contínua, 24 horas por dia, 7 dias por semana, sobrescrevendo dados antigos quando atingir 100% de utilização do disco.			
9.9.38.10.	Os pacotes brutos da rede capturados podem ser armazenados em tempo real em formato comprimido, reduzindo a utilização do espaço em disco.			
9.9.38.11.	Deve possuir, no mínimo, 256 GB de RAM.			
9.9.38.12.	A solução deve coletar pacotes em fluxo constante com, no mínimo, 40 Gbps de throughput em um único appliance.			
9.9.38.13.	A solução deve possuir capacidade de gravação em disco de, no mínimo, 40 Gbps, de forma constante e sem perdas e/ou interrupções.			

9.9.38.14.	A solução pode identificar inteligentemente o comprimento do cabeçalho de diferentes tipos de pacotes (como VLAN, VXLAN, VXLAN over VXLAN) e remover com precisão as informações de carga útil, garantindo a segurança dos dados sem perder informações da camada de rede.			
9.9.38.15.	Deve operar de forma independente da console central fornecida, no que diz respeito à captura de pacotes de rede.			
9.9.38.16.	Capacidade de apresentar análises graficamente.			
9.9.38.17.	Deve então enviar esses dados e métricas para a console central fornecida, para compilar estatísticas e gerar relatórios.			
9.9.38.18.	Deve capturar pacotes em múltiplas interfaces de rede em modo ininterrupto, com a opção de gravação em disco rígido por meio de capture jobs ou filtros.			
9.9.38.19.	Deve ser capaz de armazenar os pacotes de forma indexada, permitindo examiná-los no próprio dispositivo, sem necessidade de transferência para analisador externo.			
9.9.38.20.	Deve permitir a implementação da função de agregação de suas diversas interfaces de rede ou link aggregation.			
9.9.38.21.	Deve permitir a criação de arquivos de captura para porções definidas dos capture jobs ou filtros. Esses arquivos devem ser definidos por horário de início e término. Além disso, deve permitir que esses arquivos sejam exportados para estudo através de analisadores de protocolo no formato de dados "pcap".			
9.9.38.22.	Deve permitir a nomeação de portas e protocolos nos casos em que o dispositivo não os classifique automaticamente.			
9.9.38.23.	Deve permitir o agrupamento de portas em grupos lógicos, a fim de criar categorias e enriquecer relatórios.			
9.9.38.24.	A solução ofertada pode ser baseada em appliance dedicado (hardware) ou por software via virtual appliance. Caso seja ofertada por software, o proponente deve fornecer o hardware (servidor), bem como o sistema operacional e as licenças necessárias para executar a máquina virtual.			
9.9.38.25.	Os servidores utilizados para captura de fluxo devem possuir, no mínimo, 1 interface de gerenciamento Gigabit Ethernet e armazenamento interno com arranjo RAID 5 ou superior, que garanta proteção contra perda de dados, com área compatível com o volume de dados desta solução.			
9.9.38.26.	Deve ser fornecida uma licença que permita o processamento, no mínimo, da taxa de 200.000 (duzentos mil) registros de fluxo por minuto.			
9.9.38.27.	Deve suportar o recebimento de informações via fluxos de, no mínimo, 2.000 fontes.			
9.9.38.28.	A solução ofertada deve permitir a coleta de dados por NetFlow v5, v9 e IPFIX.			
9.9.38.29.	A solução ofertada deve apresentar os fluxos. Parâmetros mínimos a serem exibidos:			
9.9.38.29.	IP de origem e destino;			
9.9.38.29.	Porta e aplicações de rede utilizadas;			
9.9.38.29.	Número de pacotes e total de bytes.			
9.9.39.	Plataforma de Gerenciamento de Análise de Desempenho de Rede			
9.9.39.1.	A solução oferecida pode ser baseada em appliance dedicado (hardware) ou por software por meio de máquina virtual (virtual appliance). Caso seja oferecida por software, o proponente deve fornecer o hardware, bem como o sistema operacional e as licenças necessárias para execução da máquina virtual.			
9.9.39.2.	A solução de análise de pacotes deve ser integrada à solução de visualização e também permitir operação autônoma.			

9.9.39.3.	A solução deve ser capaz de analisar os dados capturados pelo dispositivo de captura de pacotes sem a necessidade de transferir os pacotes capturados.			
9.9.39.4.	A solução deve ser capaz de exibir dados em intervalos mínimos de 1 segundo, com atraso de exibição de 1 segundo para métricas TCP/IP.			
9.9.39.5.	Deve ser possível configurar diversos parâmetros de rede (como interfaces de captura), usuários e protocolos, bem como tarefas de captura no dispositivo de captura fornecido.			
9.9.39.6.	Para tráfego de aplicação desconhecida, a solução deve suportar análise estatística de portas TOP, número de sessões, e suportar a visualização do host das portas ou reuniões selecionadas, pares de fluxo, e o número da porta usado por cada par de fluxo.			
9.9.39.7.	Deve possuir a capacidade de configurar gatilhos (thresholds) e alertas flexíveis para detectar comportamentos anômalos.			
9.9.39.8.	Deve permitir que “gatilhos” sejam configurados para alertar valores mínimos ou máximos. Esse evento deve gerar uma notificação para a equipe responsável via e-mail, SNMP trap ou syslog.			
9.9.39.9.	Disponibilizar a função de baseline, que possa calcular a linha de base para as métricas de desempenho. O baseline deve suportar o algoritmo de média, o algoritmo de pico etc., e deve suportar baseline de dados diários e semanais.			
9.9.39.10.	Suportar alerta por baseline, gerando alerta quando os dados atuais se desviarem de uma porcentagem da linha de base.			
9.9.39.11.	Simulação de alerta: simulação de alerta em tempo real e cálculo de teste do limiar de alerta configurado, combinado com dados históricos para verificar a efetividade da configuração do alerta.			
9.9.39.12.	Deve permitir a consulta de alertas de todos os tipos enviados pela ferramenta de monitoramento, em um determinado período (data/hora de início e fim) informado pelo usuário.			
9.9.39.13.	A solução oferecida deve permitir a criação de painéis personalizados com a definição dos parâmetros que o usuário deseja monitorar.			
9.9.39.14.	Os dashboards devem ser exibidos em intervalos personalizáveis pelo usuário e apresentar dados segmentados com resolução mínima de 1 minuto.			
9.9.39.15.	A solução deve permitir configurações individuais desses painéis.			
9.9.39.16.	Deve ser possível segmentar os dados exibidos nos dashboards por localizações, que podem ser definidas por diferentes sub-redes.			
9.9.39.17.	Em todos os painéis deve ser possível filtrar os dados exibidos por, no mínimo, os seguintes parâmetros: IP, sub-rede, porta TCP, vlan, aplicação e localização.			
9.9.39.18.	Ao criar um dashboard, espera-se que ele seja alimentado não apenas com os dados capturados a partir de sua criação, mas também com os dados já capturados e armazenados na memória da ferramenta.			
9.9.39.19.	A solução oferecida deve ser capaz de exibir métricas avançadas para cada comunicação. Essas métricas devem estar disponíveis em todas as aplicações e transações monitoradas. Parâmetros mínimos a serem exibidos:			
9.9.39.19.	Tamanho do pacote;			
9.9.39.19.	Taxas de transmissão por segundo;			
9.9.39.19.	Total de bytes transmitidos e recebidos;			
9.9.39.19.	Total de pacotes transmitidos e recebidos;			
9.9.39.19.	Número de conexões estabelecidas;			
9.9.39.19.	Número de conexões com falha;			
9.9.39.19.	Atraso de rede ou round trip time;			

9.9.39.19.	Retransmissões e pacotes fora de ordem;			
9.9.39.19.	Tempo de resposta.			
9.9.39.20.	A solução oferecida deve apresentar painéis personalizados no formato de tabela, gráfico de linha, indicador de status ou um conjunto desses.			
9.9.39.21.	Dashboards personalizados devem exibir valores em formato resumido ou individualizado no intervalo de tempo selecionado.			
9.9.39.22.	Painéis em formato gráfico devem permitir drill-down/zoom sobre o gráfico ao posicionar o ponteiro do mouse, detalhando as informações em cada ponto de medição.			
9.9.39.23.	A solução deve permitir no mínimo 20 (vinte) usuários simultâneos, cada um acessando a ferramenta com logins específicos.			
9.9.39.24.	As estatísticas coletadas por meio de captura de pacotes ou análise de fluxo devem ser acessadas por meio de uma interface gráfica única. Essa interface deve ser capaz de demonstrar métricas de análise de fluxo e de pacotes nos mesmos dashboards.			
9.9.39.25.	A solução deve exibir um relatório que demonstre quais endereços IP têm maior utilização em termos de throughput de rede, conexões abertas ou com falha, com maior tempo de resposta e com maior retransmissão.			
9.9.39.26.	Visualizar relatórios que demonstrem quais portas TCP/UDP ou aplicações geraram tráfego no momento da captura.			
9.9.39.27.	Exibir relatório com visualização das páginas web mais acessadas.			
9.9.39.28.	Exibir relatórios que demonstrem o volume de tráfego de dados por determinada porta TCP/UDP.			
9.9.39.29.	A solução deve gerar relatórios de forma automática e manual.			
9.9.39.30.	A solução deve ser capaz de gerar e encaminhar alarmes via e-mail, SNMP trap, syslog e na própria console.			
9.9.39.31.	Os relatórios devem incluir estatísticas com granularidade de 1 minuto / 5 minutos / 10 minutos / 1 hora.			
9.9.39.32.	A solução deve permitir a geração de relatórios sobre quaisquer métricas coletadas.			
9.9.39.33.	A arquitetura de armazenamento das métricas não deve apresentar limitações. Deve ser capaz de suportar análises aprofundadas a partir de diversas dimensões, tais como Ether Type, Mac, Mac session, VNI, IP, IP session, IP+Port, TCP session, UDP session etc., na mesma página. Qualquer dimensão pode ser usada como ponto de partida da mineração, e a análise pode ser conduzida entre quaisquer dimensões.			
9.9.39.34.	Capacidade de apresentar análise graficamente.			
9.9.39.35.	Deve suportar relatórios sobre todos os dados coletados ou qualquer outro filtro, e não apenas sobre os maiores ativos que geraram ou receberam tráfego de rede, critérios ou mecanismos que possam desconsiderar parte dos dados coletados.			
9.9.39.36.	Deve suportar relatórios em tempo real com dados históricos, sem perda de resolução dos dados por sumarização, amostragem, rolagem de dados de maior para menor resolução ou outras técnicas de redução.			
9.9.39.37.	Deve ser capaz de exportar todos os relatórios, no mínimo, em formato PDF.			

9.9.39.38.	Deve suportar filtragem e detalhamento para qualquer campo-chave em um relatório. Os filtros podem ser aplicados ao relatório analisado, ou podem invocar outro relatório associado ao relatório em análise. O detalhamento deve trazer mais informações de um relatório, para análise posterior até o nível de análise de pacotes de rede, de maneira ágil e simplificada sobre um campo-chave do relatório. Esse detalhamento pode ser exibido por meio de um novo relatório filtrado a partir do campo-chave selecionado.			
9.9.39.39.	Deve permitir o agendamento para geração automática de relatórios, bem como o armazenamento e/ou envio desses relatórios por e-mail.			
9.9.39.40.	Deve possibilitar a construção de relatórios para um período de tempo pré-determinado sobre, no mínimo, os seguintes elementos que geraram ou receberam mais tráfego de rede durante o período:			
9.9.39.40.1	Hosts;			
9.9.39.40.2	Pares de hosts;			
9.9.39.40.3	Pares de hosts com portas TCP ou UDP;			
9.9.39.40.4	Grupos de hosts;			
9.9.39.40.5	Grupos de hosts com portas TCP ou UDP;			
9.9.39.40.6	Aplicações;			
9.9.39.40.7	Portas TCP ou UDP;			
9.9.39.40.8	Protocolos;			
9.9.39.40.9	Interfaces de rede;			
9.9.39.40.10	Dispositivos de rede.			
9.9.39.41.	Suporte a busca global de tráfego para realizar funções de busca em todos os Probes gerenciados pela Plataforma. Por exemplo, buscar tráfego alvo incluindo pacotes brutos da rede com base em condições como IP de origem/destino, porta de origem/destino e aplicação.			
9.10.	Módulo de Visibilidade Modular e Inteligente de Tráfego (Network Packet Broker)			
9.10.1.1.	A CONTRATADA será responsável por fornecer, operar, monitorar e garantir a manutenção contínua de uma Plataforma de Visibilidade de Tráfego (Network Packet Broker) dentro do ambiente da PMESP, assegurando a alta disponibilidade da solução e sua integração com as demais ferramentas de segurança e monitoramento da rede. A solução deverá cumprir as exigências técnicas descritas neste documento e ser composta por ferramentas e infraestrutura compatíveis com os requisitos operacionais, podendo incluir appliances dedicados, software especializado, conforme necessidade.			
9.10.1.2.	É importante destacar que o licenciamento do NPB dimensionado para 2 (dois) TAPs e 1 (um) packet broker, conforme a necessidade e a estratégia de implantação. O custo do software será apurado mensalmente, de modo a permitir o correto dimensionamento dos pagamentos			
9.10.1.3.	Características técnicas			
9.10.1.3.1.	A Plataforma de Visibilidade de Tráfego é uma solução composta por hardware e software, voltada para a filtragem, agregação e distribuição de tráfego para ferramentas de análise e segurança, e deverá atender integralmente às exigências aqui descritas.			
9.10.1.3.2.	A solução poderá ser composta por equipamentos de diferentes fabricantes, desde que garantam total interoperabilidade e integração nativa, sem necessidade de adaptações ou conversões adicionais para o pleno funcionamento das funcionalidades exigidas neste documento.			
9.10.1.3.3.	O appliance deverá ser fornecido com suas devidas licenças, de funcionalidades ou de sistema operacional, que permitam a execução das técnicas previstas nesta especificação técnica.			

9.10.1.3.4.	A solução poderá incluir licenciamento de software na modalidade de subscrição ou perpétua, desde que garanta a continuidade operacional durante toda a vigência do contrato, sem necessidade de aquisição adicional pela PMESP.			
9.10.1.3.5.	Em qualquer modalidade escolhida, o software deverá garantir pleno funcionamento durante a vigência do contrato, sem restrições ou necessidade de renovação compulsória para manter a operação dos equipamentos adquiridos.			
9.10.1.3.6.	Deverá possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas de “rede”, “rede inline”, “ferramenta” e portas de “ferramenta inline”.			
9.10.1.3.7.	O sistema deverá permitir a configuração dinâmica de portas via software, permitindo a definição de diferentes tipos de portas, conforme suas funções específicas: Portas de rede: Responsáveis por receber a cópia do tráfego por meio de TAPs/SPANs, Portas de ferramenta: Utilizadas para encaminhar o tráfego, já filtrado e/ou modificado, para as ferramentas conectadas à solução de visibilidade de tráfego, Portas de rede inline: Conectadas diretamente entre os enlaces da rede de produção, atuando de forma inline, Portas de ferramenta inline: Destinadas ao encaminhamento do tráfego de produção, filtrado ou não, para as ferramentas inline conectadas à solução			
9.10.1.3.8.	A solução deverá ser composta por componentes modulares, compatíveis com racks de 19.			
9.10.1.3.9.	Os componentes físicos da solução deverão garantir operação contínua, com sistemas adequados de resfriamento e dissipação de calor.			
9.10.1.3.10.	A solução deverá garantir redundância elétrica e suporte a variações de tensão e frequência dentro do padrão 100V-240V, 50/60 Hz, incluindo fontes de alimentação redundantes quando aplicável.			
9.10.1.3.11.	A fonte de alimentação deverá ser fornecida com todos os cabos necessários para operação.			
9.10.1.3.12.	O equipamento deverá incluir todas as fontes de alimentação suportadas pelo modelo, garantindo redundância total. As fontes devem ser AC, internas ao chassi e hot-swappable.			
9.10.1.3.13.	Deverá suportar simultaneamente em sua memória Flash (ou semelhante), duas imagens do sistema operacional entregue com o equipamento.			
9.10.1.4.	Características de desempenho.			
9.10.1.4.1.	A solução deverá suportar um processamento mínimo inicial de 200 Gbps de tráfego agregado, com capacidade de expansão escalável para atender ao crescimento da demanda da PMESP, podendo atingir até 600 Gbps sem necessidade de substituição do hardware principal.			
9.10.1.4.2.	A solução deverá garantir um throughput exclusivo para tráfego criptografado de, no mínimo, 2,5 Gbps, com possibilidade de expansão conforme necessidade operacional.			
9.10.1.4.3.	A solução deverá suportar no mínimo 16.000 regras simultâneas por módulo, com capacidade de inspeção em múltiplas camadas (L2-L7), incluindo regras baseadas em aplicação e assinatura de tráfego (AppID).			
9.10.1.4.4.	A solução deverá implementar, no mínimo, 6 (seis) pares de interfaces by-pass em fibra para 1G/10G com conectores LC com proteção física. Não serão aceitas soluções com Bypass externo ao agregador. Não serão aceitas soluções que utilizarem baterias para manter o funcionamento do bypass.			
9.10.1.4.5.	Interfaces de comunicação.			
9.10.1.4.6.	A solução deverá garantir compatibilidade com os padrões de conectividade da PMESP, permitindo integração com a infraestrutura de rede existente.			

9.10.1.4.7	A empresa contratada deverá fornecer todos os componentes necessários para a interconexão da solução, incluindo interfaces Ethernet compatíveis, transceivers ópticos e cabos de fibra óptica ou equivalentes, garantindo conectividade plena e desempenho adequado.			
9.10.1.4.8	A solução deverá suportar conectividade mínima de 10 Gbps, podendo utilizar interfaces Ethernet 10Gbps SFP+ ou tecnologias equivalentes, conforme necessário para a operação eficiente do serviço.			
9.10.1.4.9	A empresa contratada deverá garantir que a infraestrutura fornecida possa ser expandida, caso haja necessidade de aumento de capacidade ou interconexão com novos equipamentos no ambiente da PMESP.			
9.10.1.5.	Características de gerenciamento da solução.			
9.10.1.5.1	A empresa contratada deverá fornecer e operar a Plataforma de Visibilidade de Tráfego com gerenciamento remoto centralizado e seguro, garantindo acesso contínuo para monitoramento e administração da solução.			
9.10.1.5.2	O sistema deverá permitir configuração customizada baseada em perfis de acesso, implementando controle granular por função (RBAC – Role-Based Access Control).			
9.10.1.5.3	A solução deverá oferecer suporte a protocolos padrão de gerenciamento de rede, incluindo SNMPv2c e SNMPv3, com capacidade de geração de traps e logs de eventos.			
9.10.1.5.4	O serviço deverá incluir suporte a MIB II, além de MIBs privativas, garantindo monitoramento detalhado da operação da solução.			
9.10.1.5.5	A solução deverá suportar SNMP traps sobre IPv6, garantindo compatibilidade com infraestruturas modernas.			
9.10.1.5.6	A empresa contratada será responsável pela atualização remota da plataforma, incluindo manutenção do sistema operacional, configurações e segurança da solução, sem interrupção do serviço.			
9.10.1.5.7	O serviço deverá garantir a gravação segura de logs (Syslog) e auditoria detalhada dos acessos e modificações realizadas na solução.			
9.10.1.5.8	A solução deverá garantir persistência de configurações, permitindo recuperação automática após falhas elétricas, reinicializações ou atualizações programadas.			
9.10.1.5.9	A empresa contratada deverá fornecer ferramentas de monitoramento e depuração, incluindo estatísticas de utilização, logs de eventos e análise de desempenho.			
9.10.1.5.1	O gerenciamento deverá ser realizado via interface Web segura (HTTPS) e CLI (Command Line Interface), garantindo acesso autenticado e rastreável.			
9.10.1.5.1	A solução deverá permitir sincronização de tempo via protocolo NTP (Network Time Protocol), garantindo consistência em registros de eventos e auditorias.			
9.10.1.5.1	O serviço deverá incluir mecanismos de autenticação centralizada para acesso local e remoto, com suporte a TACACS+, RADIUS e LDAP.			
9.10.1.5.1	A empresa contratada deverá garantir que a solução suporte IPv6 para TACACS+, garantindo compatibilidade futura com redes de próxima geração.			
9.10.1.5.1	O acesso remoto à interface de gerenciamento deverá ser protegido por SSHv2, garantindo criptografia e segurança no controle da solução.			
9.10.1.5.1	A interface de gerenciamento deverá possuir proteção contra acessos não autorizados, exigindo autenticação forte e controle de senha segura.			

9.10.1.5.1	A solução deverá oferecer um gerenciador centralizado, permitindo a administração unificada de todos os elementos da Plataforma de Visibilidade de Tráfego, incluindo componentes físicos, virtuais, infraestrutura em nuvem e containers.			
9.10.1.5.1	A solução deverá implementar mecanismos de agregação e encaminhamento de pacotes, garantindo a entrega otimizada dos dados de rede para as ferramentas de análise e segurança, tanto para fluxos Out-of-Band (Cópia de Tráfego) quanto para fluxos Inline, suportando os seguintes cenários:			
9.10.1.5.1	Encaminhamento 1 para 1 (1:1) – Um fluxo de rede sendo entregue a uma única ferramenta de análise.			
9.10.1.5.1	Encaminhamento 1 para vários (1:N) – Um fluxo de rede sendo distribuído para múltiplas ferramentas de análise, com suporte a balanceamento de carga.			
9.10.1.5.2	Encaminhamento vários para 1 (N:1) – Múltiplos fluxos de rede sendo agregados em uma única ferramenta de análise.			
9.10.1.5.2	Encaminhamento vários para vários (N:N) – Distribuição dinâmica e balanceada de múltiplos fluxos de rede para diferentes ferramentas de análise.			
9.10.1.5.2	A solução deverá permitir a criação e aplicação dinâmica de filtros de tráfego, garantindo segmentação avançada e granularidade na entrega de pacotes. Os filtros deverão ser configuráveis com base nos seguintes critérios: Endereços MAC de origem e destino. Endereços IPv4 de origem e destino. Portas TCP e UDP de origem e destino. VLAN ID. Ethertype. Identificação de fragmentação de IP (IPFrag). Tempo de Vida do Pacote (TTL). Tipo de Serviço (TOS). Protocolo. Máscara de Controle TCP (TCP Control Mask/Bits). Differentiated Services Code Point (DSCP). Versão do protocolo IP (IPv4 e IPv6). Endereços IPv6 de origem e destino.			
9.10.1.5.2	A solução deverá permitir modificação, inserção e remoção dinâmica de filtros (regras) em tempo real, sem necessidade de interrupção da operação ou impacto nos fluxos de tráfego analisados.			
9.10.1.5.2	A solução deverá suportar sobreposição de filtros (overlapping), permitindo a aplicação simultânea de filtros de entrada (ingress) e saída (egress), garantindo maior flexibilidade no controle e roteamento do tráfego monitorado.			
9.10.1.5.2	A solução deverá permitir operação em ambiente distribuído e integrado, incluindo suporte a tecnologias como Mesh/Cluster, garantindo balanceamento de carga e redundância			
9.10.1.5.2	A solução deverá suportar a gerência centralizada de múltiplos equipamentos, permitindo sua operação como um único sistema lógico, sem exigir soluções proprietárias de empilhamento que comprometam a escalabilidade ou a interoperabilidade			
9.10.1.5.2	A solução deverá suportar gestão centralizada de, no mínimo, 30 equipamentos distribuídos, garantindo operação integrada em modo Mesh/Cluster ou tecnologia equivalente que possibilite a administração eficiente de múltiplos dispositivos.			
9.10.1.5.2	A solução deverá permitir a configuração unificada e gerenciamento centralizado de todos os dispositivos agregadores, utilizando interface Web segura (HTTPS) e CLI (Command Line Interface)			

9.10.1.5.2	A solução deverá permitir a criação de filtros e regras de direcionamento de tráfego entre diferentes equipamentos físicos ou virtuais, garantindo encaminhamento otimizado de dados entre portas de rede e portas de ferramenta, independentemente da infraestrutura subjacente. Não serão aceitas soluções que comprometam a escalabilidade e a interoperabilidade, como empilhamento com dependência rígida entre equipamentos.			
9.10.1.5.3	A solução deverá suportar arquitetura distribuída e escalável, como o modelo Spine/Leaf ou equivalente, garantindo balanceamento de tráfego eficiente, resiliência e redundância em caso de falha de um dos equipamentos.			
9.10.1.5.3	A solução deverá permitir a distribuição inteligente de tráfego e regras de filtragem entre múltiplos equipamentos, garantindo integração fluida entre os dispositivos e possibilitando o uso de arquiteturas baseadas em tecnologias de Fabric Networking ou equivalentes.			
9.10.1.5.3	A solução deverá permitir a interconexão entre múltiplos clusters ou domínios de processamento, possibilitando o encaminhamento eficiente do tráfego entre diferentes elementos da infraestrutura, conforme necessidade operacional.			
9.10.1.6.	Redundância e alta disponibilidade			
9.10.1.6.1	A solução deve garantir alta disponibilidade, suportando redundância e operação distribuída em diferentes redes, conforme necessidade.			
9.10.1.6.2	A solução deverá implementar mecanismos de alta disponibilidade e failover para evitar interrupções no tráfego de rede, garantindo continuidade operacional.			
9.10.1.7.	Funcionalidades para o tráfego interceptado em linha			
9.10.1.7.1	A solução deverá permitir implantação no ambiente da PMESP sem necessidade de reconfiguração manual de roteadores e switches, quando operando no modo Inline (em linha).			
9.10.1.7.2	A solução deverá suportar, de forma simultânea e em interfaces distintas, os seguintes modos operacionais:			
9.10.1.7.2	TAP/SPAN (Cópia de Tráfego) – Captura passiva do tráfego para análise.			
9.10.1.7.2	Inline (Tráfego de Produção) – Monitoramento e encaminhamento do tráfego diretamente na rede de produção.			
9.10.1.7.3	A solução deverá permitir a configuração da sequência de ferramentas inline (serial), garantindo que os pacotes sejam processados sequencialmente em mais de uma ferramenta antes do reencaminhamento.			
9.10.1.7.4	A solução deverá permitir a configuração de grupos de ferramentas inline (paralelo), garantindo o balanceamento de tráfego entre duas ou mais ferramentas conectadas ao sistema.			
9.10.1.7.5	A solução deverá permitir a configuração combinada das funcionalidades serial e paralelo, possibilitando criar uma sequência serial de ferramentas que operam em paralelo.			
9.10.1.7.6	A solução deverá garantir que ferramentas inline, operando em modos standalone, serial ou paralelo, possam receber apenas o tráfego de interesse, sem impactar outras ferramentas e sem necessidade de alterações físicas na infraestrutura;			
9.10.1.7.7	Exemplos: uma ferramenta pode receber todo o tráfego da rede, outra ferramenta pode receber apenas tráfego HTTP/HTTPS, ambas operam simultaneamente sem interferência.			
9.10.1.7.8	A solução deverá implementar monitoramento contínuo das ferramentas inline, utilizando heartbeat para detectar falhas e remover automaticamente qualquer ferramenta com erro, sem impactar o restante do tráfego.			

9.10.1.7.9.	A solução deverá suportar heartbeat negativo, onde pacotes de checagem são gerados e bloqueados antes de serem reenviados ao sistema. Caso um pacote de checagem retorne, a ferramenta inline deverá ser considerada falha e removida automaticamente, garantindo a continuidade do tráfego.			
9.10.1.7.10.	A solução deverá permitir a remoção dinâmica de ferramentas inline sem interrupção do tráfego da rede, garantindo que ferramentas possam ser retiradas para atualizações e troubleshooting sem gerar impactos operacionais.			
9.10.2.	Técnicas de segurança da informação			
9.10.2.1.	A solução deverá suportar encapsulamento seguro de tráfego (túnel), permitindo a transferência segura de pacotes entre diferentes elementos da infraestrutura da PMESP, através de redes L3 (roteadas).			
9.10.2.2.	O encapsulamento e desencapsulamento do tráfego deverá utilizar protocolos seguros, como L2GRE ou equivalente, permitindo transporte eficiente do tráfego encapsulado entre redes distintas.			
9.10.2.3.	A solução deverá implementar balanceamento de carga para pacotes encapsulados IPv6 L2GRE, garantindo distribuição eficiente e otimizada do tráfego entre os elementos da infraestrutura.			
9.10.2.4.	A solução deverá suportar balanceamento de carga entre múltiplos túneis, permitindo a utilização de duas ou mais ferramentas da plataforma para distribuir o tráfego de maneira equilibrada.			
9.10.2.5.	Deverá implementar capacidade de processamento agregado de, no mínimo, 23 (vinte e três) Gbps de throughput, específico para o processamento de geração de metadados, netflow, ipfix e cef.			
9.10.2.6.	Deve gerar, no mínimo, os seguintes metadados para prover informações superiores à da camada de rede, quando utilizando IPFIX/CEF, HTTP2, Response Code, Version, HTTP Host, User Agent, DNS Query Name, Query Type, Response Code, Response TIL, Response Name, RDP Encryption Level, SMB Filename, Filesize, Modbus events, fifo_count, Function_code, Mysql Error, Error_code, Query, Query_ID.			
9.11.	Ferramentas de Monitoramento e Gerenciamento – Cherwell e Zabbix/Grafana			
9.11.1.	Para garantir a continuidade operacional dos serviços de TI e a eficiência na gestão de incidentes, mudanças e monitoramento de infraestrutura, a CONTRATADA deverá fornecer e operar ferramentas adequadas para acompanhamento e gerenciamento dos serviços prestados.			
9.11.2.	As soluções adotadas devem permitir a visibilidade em tempo real da infraestrutura de TI, facilitar a identificação e resolução de problemas e assegurar a conformidade com os níveis de serviço estabelecidos.			
9.11.3.	As ferramentas devem ser compatíveis com os sistemas existentes e possibilitar integrações via API ou conectores compatíveis.			
9.11.4.	As seguintes ferramentas são exigidas:			
9.11.4.1.	ITSM (Ferramenta de Gestão de Serviços de TI): Plataforma para gestão de incidentes, requisições, mudanças, problemas e cumprimento de SLAs, assegurando a governança dos serviços de TI;			
9.11.4.2.	Ferramenta de Monitoramento Zabbix/Grafana: Solução para monitoramento contínuo da infraestrutura de TI e serviços críticos, garantindo a detecção precoce de falhas e degradações de desempenho.			
9.11.5.	Módulo de gerenciamento ITSM - Cherwell			

9.11.5.1.	A CONTRATADA deverá configurar, customizar e adequar a solução de ITSM alinhada as necessidades da CONTRATANTE, garantindo eficiência e disponibilidade contínua;			
9.11.5.2.	É importante destacar que o suporte Cherwell poderá chegar a até 180.000 (cento e oitenta mil) usuários e 1000 (mil) usuários concorrentes, conforme a necessidade e a estratégia de implantação. O custo do software será apurado mensalmente, de modo a permitir o correto dimensionamento dos pagamentos.			
9.11.5.3.	A CONTRATADA deverá fornecer toda documentação acerca das adequações e customizações realizadas na ferramenta de ITSM à CONTRATANTE;			
9.11.5.4.	A CONTRATADA deverá realizar a passagem de conhecimento para a equipe técnica da PMESP por 10 (dez) dias úteis após a conclusão da implementação de todas as funcionalidades solicitadas e realizar a entrega de documentação relacionada;			
9.11.5.5.	A implementação das funcionalidades da ferramenta deverá ser feita em até 06 (seis) meses a partir do início da vigência contratual;			
9.11.5.6.	A CONTRATANTE deverá ter acesso ao suporte homologado pelo fabricante, via e-mail ou telefone, onde a CONTRATADA fará a abertura de eventuais chamados, na modalidade 8x5 NBD (next business day) para a solução de problemas;			
9.11.5.7.	O tempo de resposta a incidentes deverá ser de 4 (quatro) horas a partir da abertura da solicitação junto ao fabricante;			
9.11.5.8.	Após a entrega da ferramenta customizada de acordo com o solicitado, será feito uma apresentação aos Gestores Contratuais do cumprimento do serviço e comprovar o conhecimento da equipe de ITSM na ferramenta para executar as demandas da CONTRATANTE, os recursos humanos deverão poder resolver problemas, criar customizações ou melhorias e implementar novas funcionalidades à ferramenta, bem como acionar o suporte homologado pelo fabricante quando necessário, sendo vedado a CONTRATADA não execução justificada por falta de conhecimento;			
9.11.5.9.	A solução deve possuir dashboards interativos (configuráveis), visando trazer informações importantes em um único ponto de exibição, fornecendo visibilidade em tempo real do desempenho dos serviços de TI, monitoramento de incidentes, cumprimento dos SLAs, com alertas automáticos em caso de não conformidade;			
9.11.5.10.	O sistema deve permitir o registro ágil de incidentes por meio de formulários e portais de autoatendimento, com campos para categorização, priorização e atribuição automática ou manual a equipes de suporte, com base em SLA e critérios personalizados;			
9.11.5.11.	Desenvolver melhoria na comunicação junto aos usuários, visando um melhor acompanhamento no fluxo de vida dos chamados, como por exemplo com notificações automatizadas sobre o status dos incidentes, via e-mail ou notificação no portal;			
9.11.5.12.	Deverão ser criadas automatização de tarefas repetitivas quando necessário, como aprovação de solicitações ou encaminhamento de incidentes para equipes específicas;			
9.11.5.13.	Automação de mudanças recorrentes por meio da criação de templates, simplificando processos repetitivos, oferecendo rastreabilidade e histórico completo de todas as mudanças, assegurando a conformidade com normas internas e externas;			
9.11.5.14.	Deverão ser criados grupos de Acordos de Nível de Serviço (SLAs) específicos para diferentes serviços e fornecedores, além de fornecer ferramentas para acompanhar, revisar e escalar SLAs de maneira eficiente, além de gerenciar e monitorar os Indicadores – chave de Desempenho (KPIs);			

9.11.5.15.	Deverão ser calculados automaticamente o SLA e extraídos em relatório, considerando o tempo por equipe, descontando o tempo que o chamado está com status de aguardando ou pendente, contabilizando todos os tickets, tarefas e tags. O sistema deve monitorar o cumprimento dos SLAs para cada grupo e acionar notificações ou escalonamentos automáticos caso os prazos estejam próximos de serem excedidos;			
9.11.5.16.	A CONTRATADA deve entregar as funcionalidades de “Tarefas”, “Campos Multivalorados ou Tags” em pleno funcionamento, levando em consideração que um ticket pode ter mais de uma equipe atuando e mais de uma categoria e/ou subcategoria sendo verificada e tratada, portanto, deverá ter todo o histórico do ticket, como tempo de atuação de cada equipe (SLA calculado da mesma forma que o ticket principal para cada tarefa), categoria e subcategoria, tags, nome do analista responsável, tempo total e por grupo de atuação;			
9.11.5.17.	Deverão ser criados relatórios padronizados, de acordo com o solicitado pela CONTRATANTE, para apresentação das informações de forma gráfica e de relatórios detalhados de fácil compreensão, para que sejam compartilhados, tais como, SLAs, KPIs, catálogos de serviços, incidentes, solicitações de serviço, mudanças, problemas, ativos de TI;			
9.11.5.18.	A CONTRATADA deverá configurar templates de tickets para casos recorrentes que envolvam múltiplas categorias, simplificando o processo de abertura e gerenciamento;			
9.11.5.19.	A CONTRATANTE deverá entregar a funcionalidade de Criação de Guias de Atendimento (Guided Workflows) em pleno funcionamento, permitindo desta forma que através do fluxo interativo o analista que estiver criando o ticket filtre melhor a demanda, reduzindo erros de abertura de ticket, padronização e melhor performance no atendimento, esta funcionalidade deve estar disponível no autoatendimento também;			
9.11.5.20.	A CONTRATADA deverá personalizar a ferramenta para que alguns campos sejam de preenchimento obrigatório de acordo com a classificação do ticket, de acordo com as definições da CONTRATANTE;			
9.11.5.21.	A CONTRATADA deverá personalizar os perfis de atendimento, permitindo a função (botão) encaminhar, apenas aos analistas com função de dispatcher ou similar, que façam o gerenciamento dos tickets e militares com aprovação do CONTRATANTE, desta forma o chamado só poderia ser enviado aos grupos de acordo com o previamente configurado, baseado no catálogo de serviços, considerando a classificação do ticket;			
9.11.5.22.	A CONTRATADA deverá entregar em formato de relatório e dashboard informações sobre as categorias e subcategorias com maior número de tickets por determinado período, permitindo que possam ser filtradas e extraídas de diferentes formas (por categoria de cada setor, por dia, por mês e/ou período personalizado), contabilizando inclusive as tarefas e/ou tags de acordo com sua classificação;			
9.11.5.23.	Criar relatórios para controle dos analistas com relação aos chamados onde existiu atuação, criação e chamados solucionados por ele, facilitando a autogestão de chamados;			
9.11.5.24.	A CONTRATADA deverá revisar e ajustar o fluxo de mudanças, revisar todos os nomes de grupos, revisão dos integrantes dos grupos de atendimento de tickets, grupo de aprovadores de mudanças, comitê de mudanças;			
9.11.5.25.	Revisão do portal de autoatendimento, tornando mais intuitivo, habilitando todos os recursos disponíveis, deixando igual ou o mais próximo do uso da ferramenta web e/ou cliente;			

9.11.5.26.	Portal de autoatendimento intuitivo, onde os usuários finais podem registrar incidentes, solicitar serviços, consultar artigos de conhecimento, acompanhar o status de seus tickets e que resolvam problemas de forma autônoma;			
9.11.5.27.	A CONTRATADA deverá realizar a análise e, se necessário, adequação da base de dados da ferramenta implementada para que o tamanho e desempenho sejam otimizados.			
9.11.5.28.	Deverão ser criados relatórios de forma agendada para automatização de rotinas de entrega de informações para o CONTRATANTE;			
9.11.5.29.	A contratada deverá realizar a criação de relatórios para identificação de problemas recorrentes com base na análise de incidentes e tendências.			
9.11.5.30.	Realizar estudo e implementar melhorias na automação de fluxos de trabalho, as tarefas, aprovações para solicitações de serviço e encaminhamentos para diferentes equipes de suporte com base em regras de negócios, reduzindo o trabalho manual e melhorando a eficiência, através de sua interface gráfica para desenhar e implementar fluxos de trabalho personalizados, sem a necessidade de programação;			
9.11.5.31.	Deverão ser implementadas integrações com ferramentas e sistemas que a CONTRATANTE já utiliza, fazer a integração dos mesmos (como Teams, e-mail, Zabbix, Grafana, entre outros).			
9.11.5.32.	A CONTRATADA deverá elaborar um treinamento para os militares e equipes técnicas onde serão expostas a formas mais adequadas para utilização da ferramenta em pontos como abertura de chamados, atendimento de chamados, encerramento de chamados, entre outros;			
9.11.5.33.	Eventuais problemas na adequação configuração e funcionamento da ferramenta decorrente da má implementação por parte da CONTRATADA deverá ser às expensas da CONTRATADA, não restando a CONTRATANTE a cobrança de horas técnicas e/ou horas de projeto por parte da CONTRATADA;			
9.11.5.34.	Os custos decorrentes desses serviços, deverão ser previstos pela CONTRATADA, não devendo ser usado horas técnicas ou horas de projeto para tanto, salvo quando após a implantação, seja demandado pela CONTRATADA, para expansão da solução ou implementação em novos dispositivos;			
9.11.5.35.	Assegurar, durante a vigência do contrato, a manutenção do funcionamento operacional da solução Cherwell, observadas as condições normais de uso e as políticas de suporte e ciclo de vida definidas pelo fabricante, promovendo a correção de falhas técnicas comprovadamente atribuíveis à CONTRATADA, sem ônus adicional ao CONTRATANTE.			
9.11.5.36.	Disponibilizar suporte técnico à solução Cherwell, prestado pelo fabricante ou por parceiro autorizado, sujeito à vigência e às condições do contrato de suporte do fabricante, com atendimento em língua portuguesa e/ou inglesa, incluindo, quando disponíveis, o registro e acompanhamento de chamados em portal especializado, aplicação de correções, patches e atualizações liberadas pelo fabricante e acesso a novas versões, desde que disponibilizadas pelo fabricante e cobertas pelo modelo de licenciamento vigente.			
9.11.5.37.	Os custos relativos ao suporte e manutenção corretiva da solução Cherwell, conforme escopo contratado e políticas vigentes do fabricante, deverão estar contemplados no valor da planilha de decomposição da proposta, excluídas evoluções tecnológicas ou mudanças de plataforma decorrentes de decisões de descontinuidade ou alteração comercial do fabricante.			

	No caso de a solução Cherwell vir a ser enquadrada em situação de End of Life (EoL) ou End of Support (EoS) pelo fabricante durante a vigência do contrato, a CONTRATADA deverá, comunicar formalmente o CONTRATANTE, em prazo razoável, sobre o evento de descontinuidade, apresentar plano de transição tecnológica, contemplando alternativas suportadas pelo mercado e compatíveis com o ambiente existente, atuar em regime de melhores esforços, visando garantir a continuidade operacional da gestão de serviços, enquanto perdurar o suporte oficialmente disponibilizado pelo fabricante, e eventual migração para nova solução, plataforma distinta ou alteração substancial do escopo original deverá ser objeto de negociação específica entre as partes, quanto a prazos, custos e condições técnicas.			
9.11.5.38.				
9.11.6.	Módulo de monitoramento Zabbix/Grafana:			
9.11.6.1.	A CONTRATADA deverá configurar e customizar a ferramenta ZABBIX para seguir com o padrão de softwares de monitoramento já na CONTRATANTE;			
9.11.6.2.	A CONTRATADA deverá alinhar previamente com a CONTRATANTE as necessidades a fim de realizar o sizing da ferramenta e necessidade de software e hardware para início da implantação;			
9.11.6.3.	A CONTRATADA deverá fornecer toda documentação sobre a instalação, configuração, suporte, customização eventuais licenças, em língua portuguesa a CONTRATANTE;			
9.11.6.4.	A implementação da solução deverá ser realizada utilizando as melhores práticas disponíveis e em Alta Disponibilidade, com os serviços instalados de forma redundante, para que em caso de queda do servidor primário o secundário possa atuar sem indisponibilidade dos serviços para o CONTRATANTE;			
9.11.6.5.	A CONTRATANTE disponibilizará o ambiente virtual para instalação, sendo de responsabilidade da CONTRATADA o preenchimento da documentação demandada pela CONTRATANTE;			
9.11.6.6.	A CONTRATADA deverá realizar a integração entre as múltiplas bases de dados já existentes na CONTRATANTE, assim como será responsável pela ampliação da ferramenta ZABBIX, garantindo que todas as configurações, históricos de monitoramento e relatórios previamente armazenados sejam consolidados e acessíveis na nova solução. A integração deverá manter a consistência dos dados e assegurar a continuidade das operações de monitoramento sem interrupções significativas;			
9.11.6.7.	A CONTRATADA deverá realizar a implementação e tuning de monitoramento na ferramenta ZABBIX inicialmente para 5500 (cinco mil e quinhentos) dispositivos;			
9.11.6.8.	A ferramenta deve capaz de realizar o envio de alarmes através de e-mail;			
9.11.6.9.	Os dispositivos a serem monitorados na ferramenta serão diversos, heterogêneos e de fabricantes diversos, em sua maioria roteadores, switches, firewalls, access points, servidores, geradores, PABX e enlaces de rádio, devendo ser capaz de monitorar todo e qualquer dispositivo demandado pela CONTRATANTE, além dos citados nesse item, independente de fabricante;			
9.11.6.10.	Deverão ser criados grupos de prioridade dos dispositivos, para classificação da urgência e alarmes de monitoramento;			
9.11.6.11.	Deverão ser elaboradas topologias que apresentem conexões físicas e localização dos equipamentos;			
9.11.6.12.	Deve ser implementados diferentes períodos para coleta de informação dos dispositivos, de forma a criar diferentes intervalos de acordo com a urgência e impacto do dispositivo;			

9.11.6.13.	O monitoramento deve ser feito preferencialmente através do protocolo SNMPv2 ou superior, porém quando os dispositivos não suportarem essa tecnologia o monitoramento pode ser feito através do ICMP;			
9.11.6.14.	Deverá ser previsto o monitoramento de até 5500 (cinco mil e quinhentos) interfaces de equipamentos, majoritariamente proveniente do Datacenter PMESP;			
9.11.6.15.	O monitoramento e alarme deverão ser feitos para identificação de falha ou indisponibilidade dos dispositivos, assim como em relação a performance, threshold;			
9.11.6.16.	Deverão ser criados relatórios padronizados, de acordo com o solicitado pela CONTRATANTE, para apresentação das informações de forma gráfica e de fácil compreensão, a fim de serem compartilhados, tais como, performance, estatísticas, análise de comportamento (Flow) e disponibilidade.			
9.11.6.17.	Para otimizar a criação e a qualidade dos relatórios, deverá ser utilizada uma ferramenta externa com interface intuitiva, que ofereça opções de personalização e permita a geração agendada e automatizada de relatórios, atendendo aos requisitos de apresentação definidos pela CONTRATANTE garantindo padronização e eficiência;			
9.11.6.18.	Deverá possuir dashboards e relatórios interativos, permitindo ao usuário expandir, filtrar e detalhar dados diretamente no relatório.			
9.11.6.19.	Deverá agendar a geração e distribuição automática de relatórios em vários formatos (PDF, Excel, HTML, Word), poderá enviar relatórios por e-mail ou integrá-los;			
9.11.6.20.	Deverão ser criados relatórios de forma agendada para automatização de rotinas de entrega de informações para o CONTRATANTE;			
9.11.6.21.	Deverão ser criados dashboards utilizando o software Grafana, visando trazer informações importantes para um único ponto de exibição;			
9.11.6.22.	Deverão ser implementados NetFlow/SFlow em até 150 (cento e cinquenta) equipamentos, visando a identificação de desvio de comportamento na rede;			
9.11.6.23.	A implementação das funcionalidades da ferramenta deverá ser feita em até 90 (noventa) dias a partir do início da vigência contratual e disponibilização das máquinas virtuais para implementação da ferramenta;			
9.11.6.24.	Após a implementação da ferramenta a CONTRATADA deverá apresentar relatório com as informações pertinentes a implementação de todos os itens da ferramenta de monitoramento, que constam nesse documento;			
9.11.6.25.	Todos os relatórios deverão ser entregues em língua portuguesa, mesmo aqueles desenvolvidos na ferramenta, restando a CONTRATADA a adaptação desses relatórios;			
9.11.6.26.	A CONTRATANTE deverá ter acesso ao suporte oficial do fabricante, via email ou telefone, onde a CONTRATADA fará a abertura de eventuais chamados, na modalidade 8x5 NBD (next business day) para a solução de problemas; O tempo de resposta a incidentes deverá ser de 4 (quatro) horas a partir da abertura da solicitação junto ao fabricante;			
9.11.6.27.	Após a implantação da ferramenta, as atividades de monitoramento e gerenciamento serão executadas pelos recursos humanos da equipe de gerenciamento e monitoramento, os quais deverão ter treinamento na ferramenta, com comprovado conhecimento para executar as demandas da CONTRATANTE, sendo vedado a CONTRATADA não execução justificada por falta de conhecimento;			

9.11.6.28.	Após a implantação da ferramenta, com a apresentação aos Gestores Contratuais do cumprimento do serviço e atestado conhecimento da equipe de monitoramento e gerenciamento na ferramenta, os recursos humanos deverão poder resolver problemas, criar customizações ou melhorias e implementar novas funcionalidades à ferramenta de monitoramento, bem como ter acesso ao suporte da fabricante;			
9.11.6.29.	A CONTRATADA deverá realizar a integração entre o Zabbix e o Grafana, garantindo a extração e transformação dos dados monitorados, para a criação de relatórios dinâmicos, interativos e personalizáveis. Essa integração deverá proporcionar uma visualização clara e intuitiva das métricas e indicadores de desempenho, permitindo análises detalhadas e suporte à tomada de decisão estratégica. A CONTRATADA será responsável pela configuração inicial, desenvolvimento de conexões seguras e automatizadas entre as ferramentas, bem como pela criação de dashboards no Grafana que atendam às necessidades operacionais e estratégicas da CONTRATANTE, assegurando a atualização contínua dos dados monitorados.			
9.11.6.30.	Eventuais problemas no tuning, implantação, configuração e funcionamento da ferramenta decorrente da má implementação por parte da CONTRATADA deverá ser às expensas da CONTRATADA, não restando a CONTRATANTE a cobrança de horas técnicas e/ou horas de projeto por parte da CONTRATADA;			
9.11.6.31.	Os custos decorrentes desses serviços, deverão ser previstos pela CONTRATADA, não devendo ser usado horas técnicas ou horas de projeto para tanto, salvo quando após a implantação, seja demandado pela CONTRATADA, para expansão da solução ou implementação em novos dispositivos.			
9.11.6.32.	Demais informações relacionadas às bases do Zabbix existentes na CONTRATANTE estão disponíveis no APÊNDICE A12 – Zabbix;			

SECRETARIA DA SEGURANÇA PÚBLICA

POLICIA MILITAR DO ESTADO DE SÃO PAULO

APÊNDICE A05 – QUADRO RESUMO DE EXECUÇÃO (CIBERSEGURANÇA/DATA CENTER/REDES)

O Quadro Resumo de Execução tem por finalidade estabelecer o roteiro orientativo a ser observado pela Contratada, indicando as fases que deverão ser cumpridas desde o início até o atingimento de cada marco do projeto.

A implementação dos marcos — Cibersegurança, Data Center e Redes — poderá ocorrer de forma escalonada, mediante prévio acordo entre as partes, observando-se o planejamento aprovado pelo Contratante.

Tal procedimento tem por objetivo assegurar a manutenção e continuidade das atividades críticas da PMESP, evitando-se, assim, qualquer solução de continuidade ou prejuízo à execução dos serviços essenciais durante o desenvolvimento das etapas subsequentes do projeto.

FASES	MOMENTO DA REALIZAÇÃO OU ACEITAÇÃO
Assinatura do Contrato	Marco 0
Período de Transição Operacional - PTO	Até 30 (trinta) dias após a assinatura do contrato
Duração do PTO	Terá duração máxima de 2 (dois) meses e deverá garantir a migração gradual das responsabilidades para a nova contratada
Readequação do ambiente de trabalho existente	Iniciada 30 (trinta) dias corridos após o período de vigência contratual, esta readequação deve ser entregue até 15 dias corridos após o início do período de vigência contratual
Avaliação do ambiente de trabalho e apresentação junto ao corpo técnico de policiais militares das Seções	30 (trinta) dias corridos após o início do período de vigência contratual
Envio de organograma informando os membros da equipe que farão a composição do corpo técnico e gerencial	15 (quinze) dias corridos após o início do período de vigência contratual
Envio de currículos e qualificações referenciando os membros do corpo técnico e gerencial	15 (quinze) dias corridos após o início do período de vigência contratual
Questionamentos quanto ao organograma e currículos por parte da Polícia Militar	03 (três) dias corridos após o recebimento dos currículos e acesso ao organograma

Justificativa das não-conformidades por parte da CONTRATADA	03 (três) dias corridos após o recebimento dos questionamentos pela Polícia Militar
Apresentação e integração da equipe da CONTRATADA em conjunto a equipe da Polícia Militar	07 (sete) dias corridos após do início do período de vigência contratual
Transferência de conhecimento e operações da Polícia Militar para a CONTRATADA	Iniciada 07 (sete) dias corridos antes o início do período de vigência contratual, esta passagem de conhecimento deve ser concluída no início do período de vigência contratual e ser obrigatoriamente acompanhada pelo Serviço de Gestão de TIC, Serviço de Governança de TIC, Serviço de Suporte Técnico às Demandas e Mudanças de TIC de Data Center para SPD e SER, e Serviço de Suporte Técnico de Análise de Threat Hunting
Comprovação das certificações, formações acadêmicas, experiências e demais comprovações acerca das qualificações obrigatórias e desejáveis para TODOS os colaboradores alocados no contrato de prestação de serviços para a Polícia Militar	07 (sete) dias corridos antes do início do período de vigência contratual
Início do processo de monitoramento do SOC e NOC da Polícia Militar pela CONTRATADA	Início à 00:00 hora do dia ____ de ____ de 202__.
Vigência do Contrato	30 (trinta) meses, renováveis por até 120 (cento e vinte) meses a partir do início efetivo da prestação de serviços pela CONTRATADA.

SECRETARIA DA SEGURANÇA PÚBLICA

POLICIA MILITAR DO ESTADO DE SÃO PAULO

APÊNDICE A10 – Atestado de Capacidade Técnica

1. Atestados de Capacidade Técnica

1.1. A proponente deverá comprovar capacidade operacional para execução de serviço similar de complexidade tecnológica e operacional equivalente ou superior ao objeto desta contratação, ou ao item pertinente, por meio da apresentação de certidão(ões) ou atestado(s), fornecido(s) por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso, para a execução de serviços especializados de suporte técnico de cibersegurança, data center e redes, bem como de governança, gerenciamento e monitoramento, das demandas e mudanças de tecnologia da informação e comunicação e infraestrutura de data center e redes para ambiente computacional e de telecomunicações, de forma a garantir a continuidade dos serviços de TIC, conforme item 8. *Forma e critérios de seleção de regime* do Termo de Referência – TR.

ESP-DIRETORIA TEC. INFORMACAO E COMUNICACAO

Contrato 9/2025

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
9/2025	180183-ESP-DIRETORIA TEC. INFORMACAO E COMUNICACAO	SERGIO FIRMINO DA SILVA NETO	06/05/2026 17:42 (v 0.31)
Status	CONCLUIDO		

Outras informações

Categoria	Número da Contratação	Processo Administrativo
V - prestação de serviços, inclusive os técnico-profissionais especializados/Serviço continuado com dedicação exclusiva de mão de obra	141/2025	057.00495038/2025-41

1. Cláusula primeira - do objeto

TERMO DE CONTRATO
Lei nº 14.133, de 1º de abril de 2021
SERVIÇOS – LICITAÇÃO

SECRETARIA DA SEGURANÇA PÚBLICA

POLÍCIA MILITAR DO ESTADO DE SÃO PAULO

(Processo Administrativo nº 057.00422747/2025-16)

CONTRATO ADMINISTRATIVO Nº/....., CELEBRADO ENTRE O(A)
....., POR INTERMÉDIO DO(A) E
.....

O ESTADO DE SÃO PAULO, por intermédio da SECRETARIA DE SEGURANÇA PÚBLICA/POLÍCIA MILITAR DO ESTADO DE SÃO PAULO, com sede na Av Cruzeiro do Sul, 260 - 6º andar, Canindé, na cidade de São Paulo / Estado de São Paulo, inscrito no CNPJ sob o nº 04.198.514/0038-46, neste ato representado pelo Senhor CORONEL PM BEATRIZ DE ASSIS BASTOS MORASSI, inscrito(a) no CPF sob o nº 249.876.228-07, no uso da competência conferida pela legislação aplicável, doravante denominado CONTRATANTE, doravante designado(a) CONTRATADO, neste ato representado(a) por (nome e função no Contratado), inscrito(a) no CPF sob o nº, conforme atos constitutivos da fornecedora OU procuração apresentada nos autos, tendo em vista o que consta no Processo nº e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais normas da legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico nº..., mediante as condições a seguir enunciadas, de acordo com as subdivisões subsequentes na forma de cláusulas e respectivos itens que compõem este instrumento.

CLÁUSULA PRIMEIRA – OBJETO (art. 92, I e II)

1.1. O objeto do presente instrumento é a contratação de serviços especializados de suporte técnico de cibersegurança, data center e redes, bem como de governança, gerenciamento e monitoramento, das demandas e mudanças de tecnologia da informação e comunicação e infraestrutura de data center e redes para ambiente computacional e de telecomunicações, de forma a garantir a

continuidade dos serviços de TIC, a serem executados com regime de dedicação exclusiva de mão de obra conforme detalhamento e especificações técnicas deste instrumento, do Termo de Referência, da proposta do Contratado e demais documentos da contratação constantes do processo administrativo em epígrafe.

1.2. Objeto da contratação:

Item	CATMAT Contabiliza	CATMAT Compras. gov.br	Descrição – Categoria de Serviço	Qtd	HTS	Custo Mensal (R\$)	Custo 30 Meses (R\$)
1	91693	27090	Gerente de infraestrutura de tecnologia da informação	1	176	Sigiloso	Sigiloso
			Gerente de suporte técnico de tecnologia da informação	1	176	Sigiloso	Sigiloso
			Analista de sistemas de automação - Júnior	8	180	Sigiloso	Sigiloso
			Técnico de suporte ao usuário de tecnologia da informação Júnior	2	176	Sigiloso	Sigiloso
			Técnico de Rede (Telecomunicações) - Júnior	1	176	Sigiloso	Sigiloso
			Gerente de suporte técnico de tecnologia da informação	1	176	Sigiloso	Sigiloso
			Analista de suporte computacional Pleno	4	176	Sigiloso	Sigiloso
			Administrador de sistemas operacionais Sênior	4	176	Sigiloso	Sigiloso
			Administrador de sistemas operacionais Sênior	3	176	Sigiloso	Sigiloso
			Administrador de banco de dados - Sênior	1	176	Sigiloso	Sigiloso
			Administrador de banco de dados - Pleno	2	176	Sigiloso	Sigiloso
			Especialista em Cloud Sênior	1	176	Sigiloso	Sigiloso
			Gerente de segurança da informação	1	176	Sigiloso	Sigiloso
			Gerente de segurança da informação	1	176	Sigiloso	Sigiloso
			Analista de redes e de comunicação de dados Sênior	4	176	Sigiloso	Sigiloso
			Analista de redes e de comunicação de dados Pleno			Sigiloso	Sigiloso

			7	176		
		Administrador em segurança da informação - Sênior	1	176	Sigiloso	Sigiloso
		Analista de sistemas de automação - Pleno	1	176	Sigiloso	Sigiloso
		Desenvolvedor de sistemas de tecnologia da informação Sênior	1	176	Sigiloso	Sigiloso
			45		Sigiloso	Sigiloso

1.3. O presente Termo de Contrato vincula-se à seguinte documentação, que se considera parte integrante deste instrumento, independentemente de transcrição:

1.3.1. O Termo de Referência;

1.3.2. O Edital da Licitação;

1.3.3. A Proposta do contratado;

1.3.4. Eventuais anexos dos documentos supracitados.

1.4. O regime de execução deste contrato é o de empreitada por preço unitário.

2. Cláusula segunda - vigência e prorrogação

CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 30 (trinta) meses, contados da assinatura do contrato, prorrogável por até 10 (dez) anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

2.1.1. O Contratado poderá se opor à prorrogação de que trata a subdivisão acima, desde que o faça mediante documento escrito, recepcionado pelo Contratante em até 90 (noventa) dias antes do vencimento do contrato ou de cada uma das prorrogações do prazo de vigência.

2.1.2. Dentre outras exigências, a prorrogação de que trata a subdivisão acima é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração e em harmonia com os preços do mercado, conforme pesquisa a ser realizada à época do aditamento pretendido, permitida a negociação com o Contratado, observando-se, ainda, os seguintes requisitos:

- Estar formalmente demonstrado no processo que a forma de prestação dos serviços tem natureza continuada;
- Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;
- Seja juntada justificativa, por escrito, de que a Administração mantém interesse na realização do serviço;
- Haja manifestação expressa do Contratado informando o interesse na prorrogação;
- Seja comprovado que o Contratado mantém as condições iniciais de habilitação.

2.1.3. O Contratado não tem direito subjetivo à prorrogação contratual, e não poderá pleitear qualquer espécie de indenização em razão da não prorrogação do prazo de vigência contratual por conveniência do Contratante.

2.1.4. Eventuais prorrogações de contrato serão formalizadas mediante celebração de termo aditivo, respeitadas as condições prescritas na Lei nº 14.133, de 2021.

2.1.5. Nas eventuais prorrogações contratuais, custos não renováveis já pagos ou amortizados no âmbito da contratação, quando houver, deverão ser eliminados como condição para a prorrogação.

2.1.6. O contrato não poderá ser prorrogado quando o Contratado tiver sido penalizado com as sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

2.1.7. Não obstante o prazo estipulado nesta cláusula, a vigência nos exercícios subsequentes ao da celebração do contrato estará sujeita a condições resolutivas consubstanciadas:

I - na inexistência de recursos aprovados nas respectivas Leis Orçamentárias de cada exercício para atender as respectivas despesas, acarretando a extinção do contrato a partir de sua ocorrência; ou

II - na ausência de vantagem para o Contratante na manutenção do contrato, desde que o Contratante comunique ao Contratado a opção pela extinção do contrato com ao menos 2 (dois) meses de antecedência em relação à próxima data de aniversário do contrato, acarretando a extinção do contrato a partir da referida data de aniversário contratual.

2.1.8. Ocorrendo a resolução do contrato, com base em uma das condições resolutivas estipuladas na subdivisão acima desta cláusula, o Contratado não terá direito a qualquer espécie de indenização.

3. Cláusula terceira - modelos de execução e gestão contratuais

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de início, conclusão, entrega, observação e recebimento do objeto, e critérios de medição, constam no Termo de Referência, que constitui parte integrante deste Contrato.

3.2. DO REGIME DE EXECUÇÃO DOS SERVIÇOS

Os serviços objeto deste Contrato serão executados nos regimes híbrido (presencial e remoto), conforme definido pela Contratante, devendo a Contratada observar integralmente as obrigações previstas nesta Cláusula.

3.2.1. DAS OBRIGAÇÕES DA CONTRATADA NO REGIME PRESENCIAL

3.2.1.1. A Contratada deverá:

- I – disponibilizar profissionais em regime de dedicação exclusiva nas dependências da Contratante, conforme jornada e escala definidas;
- II – assegurar que os profissionais atuem presencialmente sempre que a natureza do serviço assim exigir, especialmente em atividades dependentes de intervenção física, manutenção de infraestrutura, operação de data center e tratamento de incidentes críticos;
- III – substituir, de imediato, profissionais ausentes ou que não atendam aos requisitos técnicos estabelecidos;
- IV – assegurar o cumprimento das normas internas da Contratante, incluindo políticas de segurança da informação, normas de acesso, sigilo e conduta;
- V – registrar e disponibilizar à Contratante, sempre que solicitado, evidências de presença, execução e acesso aos ambientes operacionais.

3.2.2. DAS OBRIGAÇÕES DA CONTRATADA NO REGIME REMOTO

3.2.2.1. A Contratada deverá:

- I – executar as atividades remotas com utilização de infraestrutura própria e adequada, observadas as políticas de segurança da informação definidas pela Contratante;
- II – acessar os ambientes tecnológicos da Contratante por meios seguros autorizados, incluindo VPN, autenticação multifatorial e demais mecanismos;
- III – garantir disponibilidade da equipe dentro dos horários estabelecidos, assegurando atendimento em conformidade com os níveis de serviço previstos;
- IV – registrar todas as atividades realizadas de forma remota nos sistemas e meios definidos pela Contratante;
- V – assegurar a confidencialidade e integridade das informações processadas remotamente.

3.2.3. DAS OBRIGAÇÕES DA CONTRATADA NO REGIME HÍBRIDO

3.2.3.1. A Contratada deverá:

- I – integrar a execução presencial e remota de forma contínua, mantendo coerência técnica, rastreabilidade e comunicação adequada entre as equipes;
- II – atender às convocações da Contratante para atuação presencial, sempre que necessário, inclusive em situações de urgência, auditorias, reuniões ou incidentes que exijam presença física;
- III – cumprir integralmente os prazos, indicadores e níveis de serviço, independentemente do regime utilizado;
- IV – manter mecanismos de coordenação e substituição de profissionais que contemplem ambos os regimes;
- V – assegurar que todas as entregas, registros, evidências e relatórios sejam executados e disponibilizados conforme previsto no Termo de Referência.

3.2.4. DAS OBRIGAÇÕES DA CONTRATANTE NO REGIME PRESENCIAL

3.2.4.1. A Contratante deverá:

- I – disponibilizar acesso às dependências necessárias à execução das atividades presenciais;
- II – fornecer credenciais e autorizações de acesso aos ambientes, de acordo com suas normas internas;
- III – comunicar previamente eventuais alterações nas condições físicas ou operacionais que impactem a execução dos serviços.

3.2.5. DAS OBRIGAÇÕES DA CONTRATANTE NO REGIME REMOTO

3.2.5.1. A Contratante deverá:

- I – disponibilizar os meios de acesso remoto necessários à execução dos serviços;
- II – comunicar à Contratada indisponibilidades, restrições ou incidentes que afetem o acesso remoto;
- III – disponibilizar e atualizar as políticas e diretrizes de segurança aplicáveis ao ambiente remoto.

3.2.6. DAS OBRIGAÇÕES DA CONTRATANTE NO REGIME HÍBRIDO

3.2.6.1. A Contratante deverá:

- I – definir e comunicar previamente as atividades que deverão ser realizadas presencialmente, remotamente ou em regime híbrido;
- II – estabelecer escalas e orientações operacionais, com antecedência suficiente, salvo situações emergenciais devidamente justificadas;
- III – manter canais oficiais de comunicação e acompanhamento para as equipes envolvidas;
- IV – fiscalizar a execução dos serviços, independentemente do regime de execução.

3.2.7. DAS DISPOSIÇÕES COMPLEMENTARES

- I – A alteração entre os regimes de execução não implicará revisão de preços ou condições contratuais, salvo disposição expressa e devidamente justificada.
- II – A Contratada permanece responsável pela manutenção da continuidade dos serviços, observância das normas de segurança e

cumprimento dos níveis de serviço, em qualquer regime de execução.

III – A execução dos serviços deverá observar, além do presente Contrato, o Termo de Referência, o Estudo Técnico Preliminar e as diretrizes estabelecidas pela Contratante.

4. Cláusula quarta - subcontratação

4.1. Não é admitida a cessão ou transferência, total do objeto contratual, mas é permitida a subcontratação parcial do objeto, nas seguintes condições:

4.1.1. Poderão ser subcontratadas as ferramentas para o NOC e SOC, previstas no Estudo Técnico Preliminar, conforme segue:

4.1.1.1. Módulo de Gestão e Correlação de Eventos (SIEM);

4.1.1.2. Módulo de Sistema de Logs (SisLog);

4.1.1.3. Módulo de Detecção em Endpoint (EDR);

4.1.1.4. Módulo Avançado de Detecção e Resposta (XDR);

4.1.1.5. Módulo de Teste de Penetração (PENTEST);

4.1.1.6. Módulo de Threat Intelligence (OSINT);

4.1.1.7. Módulo de Observabilidade de sistemas (APM);

4.1.1.8. Módulo de Observabilidade de redes (NPM);

4.1.1.9. Módulo de visibilidade tráfego (NPB);

4.1.1.10. Módulo de gerenciamento ITSM (Cherwell);

4.1.1.11. Módulo de monitoramento (Zabbix/Grafana).

4.1.2. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral do Contratado pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades do subcontratado, bem como responder direta e solidariamente perante o Contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

4.1.3. A subcontratação será formalizada de acordo com o seguinte procedimento:

4.1.3.1. Submissão, pelo Contratado, de pedido por escrito e fundamentado de subcontratação parcial, contendo descrição da parcela do objeto que se pretende subcontratar, acompanhado de planilha detalhada demonstrando a quantidade e o valor da parcela a ser subcontratada;

4.1.3.2. Autorização prévia do Contratante, por escrito, para a subcontratação parcial, desde que seja verificado o cumprimento dos requisitos necessários para a subcontratação;

4.1.3.3. Apresentação pelo Contratado dos documentos do subcontratado de regularidade jurídica, fiscal, social e trabalhista exigidos na habilitação do certame, bem como de documentação que comprove a capacidade técnica do subcontratado, nos termos do art. 122, § 1º, da Lei nº 14.133, de 2021;

4.1.3.4. Análise e autorização da subcontratação parcial pelo Contratante, por escrito, desde que verificado o preenchimento dos requisitos após exame da documentação do subcontratado apresentada pelo Contratado. O Contratado poderá substituir o subcontratado cuja regularidade e capacidade técnica não sejam demonstradas conforme a documentação exigida na subdivisão anterior, mantido o mesmo objeto, no prazo que lhe for assinalado pelo Contratante;

4.1.3.5. Apresentação pelo Contratado de cópia do Termo de Subcontratação ou ajuste equivalente celebrado entre o Contratado e o subcontratado, o qual será juntado aos autos do processo administrativo;

4.1.3.6. Este procedimento é aplicável às hipóteses de substituição do subcontratado, que também poderá ser solicitada pelo Contratante, devido o não atendimento do .

4.1.4. Os pagamentos serão realizados exclusivamente ao Contratado.

4.1.5. É vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau.

5. Cláusula quinta - preço

5.1. O valor mensal da contratação é de R\$ (.....), perfazendo o valor total de R\$ (.....).

5.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

5.3. O valor indicado nesta cláusula é meramente estimativo, de forma que os pagamentos devidos ao Contratado dependerão dos quantitativos efetivamente demandados, medidos e fornecidos.

6. Cláusula sexta - pagamento

6.1. O prazo para pagamento ao Contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, que constitui parte integrante deste Contrato.

7. Cláusula sétima - reajuste

7.1. Os preços inicialmente ajustados poderão ser repactuados para manutenção do equilíbrio econômico-financeiro, após o interregno de 1 (um) ano, mediante solicitação do Contratado.

7.2. O interregno mínimo de 1 (um) ano para a primeira repactuação será contado:

a. Para os custos relativos à mão de obra, vinculados à data-base da categoria profissional: a partir da data de início dos efeitos financeiros do acordo, convenção coletiva ou dissídio coletivo de trabalho ao qual a proposta estiver vinculada, relativo a cada categoria profissional abrangida pelo contrato;

b. Para os demais custos, decorrentes do mercado (não relativos a mão de obra): a partir da data da apresentação da proposta.

7.3. Nas repactuações subsequentes à primeira, o interregno mínimo de 1 (um) ano será contado a partir da data da última repactuação correspondente à mesma parcela objeto da nova solicitação.

7.3.1. Entende-se como última repactuação a data em que iniciados seus efeitos financeiros, independentemente daquela em que apostilada.

7.4. A repactuação poderá ser dividida em tantas parcelas quantas forem necessárias, observado o princípio da anualidade do reajuste de preços da contratação, podendo ser realizada em momentos distintos para discutir a variação de custos que tenham sua anualidade resultante em datas diferenciadas, como os decorrentes de mão de obra e os decorrentes dos insumos necessários à execução dos serviços (art. 135, § 4º, da Lei nº 14.133, de 2021).

7.5. Quando a contratação envolver mais de uma categoria profissional, a repactuação dos custos contratuais decorrentes da mão de obra poderá ser dividida em tantos quantos forem os acordos, convenções ou dissídios coletivos de trabalho das respectivas categorias (art. 135, § 5º, da Lei nº 14.133, de 2021).

7.6. É vedada a inclusão, por ocasião da repactuação, de benefícios não previstos na proposta inicial, exceto quando se tornarem obrigatórios por força de lei, acordo, convenção ou dissídio coletivo de trabalho.

7.7. Na repactuação, o Contratante não se vinculará às disposições contidas em acordos, convenções ou dissídios coletivos de trabalho que tratem de obrigações e direitos que somente se aplicam aos contratos com a Administração Pública, de matéria não trabalhista, de pagamento de participação dos trabalhadores nos lucros ou resultados do Contratado, ou que estabeleçam direitos não previstos em lei, como valores ou índices obrigatórios de encargos sociais ou previdenciários, bem como de preços para os insumos relacionados ao exercício da atividade (art. 135, §§ 1º e 2º, da Lei nº 14.133, de 2021).

7.8. Quando a repactuação solicitada pelo Contratado se referir aos custos da mão de obra, o Contratado efetuará a demonstração analítica da variação dos custos por meio de Planilha de Custos e Formação de Preços, acompanhada da apresentação do novo acordo, convenção coletiva ou sentença normativa da categoria profissional abrangida pelo contrato que fundamenta a repactuação.

7.8.1. A repactuação para reajustamento do contrato em razão de novo Acordo, Convenção ou Dissídio Coletivo de Trabalho visa a repassar integralmente a variação de custos da mão de obra decorrente desses instrumentos.

7.9. Quando a repactuação solicitada pelo Contratado se referir aos demais custos, decorrentes do mercado (não relativos a mão de obra), a respectiva variação será apurada mediante a aplicação do índice de reajustamento IPC/FIPE, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, observando a data de referência e o interregno mínimo definidos nesta cláusula, com base na seguinte fórmula:

$R = V (I - I^0) / I^0$, onde:

R = Valor do reajustamento procurado;

V = Valor contratual correspondente à parcela dos custos decorrentes do mercado (não relativos a mão de obra) a ser reajustada;

Iº = índice inicial - refere-se ao índice de custos ou de preços correspondente à data de apresentação da proposta ou à data do último reajustamento aplicado;

I = Índice relativo ao mês do reajustamento

7.9.1. No caso de atraso ou não divulgação do índice de reajustamento, o Contratante pagará ao Contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo; fica o Contratado obrigado a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

7.9.2. Nas aferições finais, o índice utilizado para a repactuação dos custos decorrentes do mercado (não relativos a mão de obra) será, obrigatoriamente, o definitivo.

7.9.3. Caso o índice estabelecido venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

7.9.4. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente dos custos decorrentes do mercado (não relativos a mão de obra), por meio de termo aditivo.

7.10. Independentemente do requerimento de repactuação dos custos decorrentes do mercado (não relativos a mão de obra), o Contratante verificará, a cada anualidade, se houve deflação do índice adotado que justifique o recálculo dos custos em valor menor, promovendo, em caso positivo, a redução dos valores correspondentes da planilha contratual.

7.11. Os efeitos financeiros da repactuação decorrente da variação dos custos contratuais de mão de obra vinculados aos acordos, às convenções ou aos dissídios coletivos de trabalho retroagirão, quando for o caso, à data do início dos efeitos financeiros do novo acordo, convenção ou sentença normativa que fundamenta a repactuação.

7.12. Os novos valores contratuais decorrentes das repactuações poderão se iniciar em data futura, desde que assim acordado entre as

partes, sem prejuízo da contagem da anualidade para concessão das repactuações futuras.

7.13. Os efeitos financeiros da repactuação ficarão restritos exclusivamente aos itens que a motivaram, e apenas em relação à diferença porventura existente.

7.14. O pedido de repactuação deverá ser formulado durante a vigência do contrato e antes de eventual prorrogação ou encerramento contratual, sob pena de preclusão.

7.15. Caso, na data da prorrogação contratual, ainda não tenha sido celebrado o novo acordo, convenção coletiva ou dissídio coletivo da categoria, ou ainda não tenha sido possível ao Contratante ou ao Contratado proceder aos cálculos devidos, deverá ser inserida cláusula no termo aditivo de prorrogação para resguardar o direito futuro à repactuação, a ser exercido tão logo se disponha dos valores reajustados, sob pena de preclusão.

7.16. A extinção do contrato não configurará óbice para o deferimento da repactuação solicitada tempestivamente, hipótese em que será concedida por meio de termo indenizatório.

7.17. O Contratante decidirá sobre o pedido de repactuação em até 90 (noventa) dias, contado a partir da data em que for apresentada, pelo Contratado, solicitação acompanhada de documentação contendo demonstração analítica da variação dos custos a serem repactuados (art. 92, § 6º, c/c o art. 135, § 6º, da Lei nº 14.133, de 2021).

7.17.1. O prazo referido na subdivisão anterior não se iniciará enquanto o Contratado não cumprir os atos ou apresentar a documentação solicitada pelo Contratante para a comprovação da variação dos custos.

7.18. A repactuação de preços será formalizada por apostilamento.

7.19. As repactuações não interferem no direito das partes de solicitar, a qualquer momento, a manutenção do equilíbrio econômico-financeiro inicial do contrato com base no disposto no art. 124, inciso II, alínea “d”, da Lei nº 14.133, de 2021.

7.20. Se ocorrer repactuação para valor maior, o Contratado deverá complementar a garantia contratual que tenha sido anteriormente prestada, caso exigida neste instrumento, de modo que se mantenha a proporção inicial em relação ao valor contratado.

7.21. Caso ocorra majoração da tarifa de transporte público, será facultada a revisão de item relativo a valores pagos a título de vale-transporte, constante da Planilha de Custos e Formação de Preços que constitui parte integrante do presente Contrato, desde que comprovada pelo Contratado a sua efetiva repercussão sobre os preços contratados. Caso sejam preenchidos os requisitos legais, a revisão dos custos relativos ao vale-transporte será formalizada por termo aditivo a este Contrato.

8. Cláusula oitava - obrigações do contratante

8.1. São obrigações do Contratante:

8.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e a documentação que o integra;

8.1.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.1.3. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, a expensas do Contratado;

8.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

8.1.5. Comunicar ao Contratado para emissão de Nota Fiscal relativa à parcela incontroversa, para efeito de liquidação e pagamento, se houver parcela incontroversa no caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, observando-se o art. 143 da Lei nº 14.133, de 2021;

8.1.6. Efetuar o pagamento ao Contratado do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

8.1.7. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

8.1.8. Não praticar atos de intervenção indevida na gestão interna do Contratado, tais como (art. 48 da Lei nº 14.133, de 2021):

I) indicar pessoas expressamente nominadas para executar direta ou indiretamente o objeto contratado;

II) fixar salário inferior ao definido em lei ou em ato normativo a ser pago pelo Contratado;

III) estabelecer vínculo de subordinação com funcionário do Contratado;

IV) definir forma de pagamento mediante exclusivo reembolso dos salários pagos;

V) demandar a funcionário do Contratado a execução de tarefas fora do escopo do objeto da contratação;

VI) realizar outras exigências que constituam intervenção indevida da Administração na gestão interna do Contratado;

8.1.9. Cientificar o órgão de representação judicial da Procuradoria Geral do Estado para adoção das medidas cabíveis quando necessária medida judicial diante do descumprimento de obrigações pelo Contratado;

8.1.10. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste, observado o prazo de 01 (um) mês para decisão, a contar da conclusão da instrução do requerimento, admitida a prorrogação motivada, por igual período, e excepcionada a hipótese de disposição legal ou cláusula contratual que estabeleça prazo específico;

8.1.11. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo Contratado no prazo máximo de 01 (um) mês, contado a partir da conclusão da instrução do requerimento, sendo admitida a prorrogação motivada desse prazo por igual período, e observado o disposto no parágrafo único do artigo 131 da Lei nº 14.133, de 2021;

8.1.12. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais (§ 4º, do art. 137, da Lei nº 14.133, de 2021);

8.1.13. Comunicar o Contratado na hipótese de posterior alteração do projeto pelo Contratante, se o caso estiver enquadrado na situação disciplinada pelo art. 93, § 3º, da Lei nº 14.133, de 2021;

8.1.14. Observar que constitui responsabilidade da Administração Pública garantir as condições de segurança, higiene e salubridade dos trabalhadores, quando o trabalho for realizado em suas dependências ou local previamente convencionado em contrato;

8.1.15. Observar, no tratamento de dados pessoais de profissionais, empregados, prepostos, administradores e/ou sócios do

Contratado, a que tenha acesso durante a execução do objeto a que se refere a cláusula primeira deste contrato, as normas legais e regulamentares aplicáveis, em especial, a Lei nº 13.709, de 14 de agosto de 2018, com suas alterações subsequentes.

8.2. O prazo para resposta ao pedido de restabelecimento do equilíbrio econômico-financeiro não se iniciará enquanto o Contratado não cumprir os atos ou apresentar a documentação solicitada pelo Contratante para adequada instrução do requerimento.

8.3. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus profissionais, prepostos ou subordinados.

9. Cláusula nona - obrigações do contratado

9.1. O Contratado deve cumprir todas as obrigações estabelecidas em lei, e aquelas constantes deste Contrato e da documentação que o integra, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

9.1.1. Designar e manter preposto aceito pelo Contratante para representar o Contratado na execução do contrato;

9.1.1.1. A indicação ou a manutenção do preposto do Contratado poderá ser recusada pelo Contratante, desde que devidamente justificada, hipótese em que o Contratado deverá designar outro para o exercício da atividade;

9.1.2. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II, da Lei nº 14.133, de 2021) e prestar todo esclarecimento ou informação por eles solicitados;

9.1.3. Alocar os profissionais necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados, utilizando os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e à legislação de regência;

9.1.4. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

9.1.5. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado diretamente à Administração ou a terceiros em razão da execução do contrato, não excluindo nem reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida na documentação que integra este instrumento, o valor correspondente aos danos sofridos;

9.1.6. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do Contratante, de agente público que desempenhe(ou) função na licitação ou que atue na fiscalização ou gestão do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

9.1.7. Quando não for possível a verificação da regularidade no Sistema de Cadastramento Unificado de Fornecedores – Sicaf, ou em outros meios eletrônicos hábeis de informações, ou em documentação apresentada pelo Contratado para cumprimento da disciplina da fiscalização administrativa do Termo de Referência, o Contratado deverá atender a notificação para entregar ao setor responsável pela fiscalização do contrato, no prazo de 5 (cinco) dias úteis, os seguintes documentos: 1) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 2) certidões que comprovem regularidade fiscal perante as Fazendas Estadual/Distrital e/ou Municipal/Distrital do domicílio ou sede do Contratado que tenham sido exigidas para fins de habilitação na documentação que integra este instrumento; 3) Certidão de Regularidade do FGTS – CRF; e 4) Certidão Negativa, ou positiva com efeitos de negativa, de Débitos Trabalhistas;

9.1.8. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, ou Dissídio Coletivo de Trabalho das categorias abrangidas pelo contrato, e por todas as obrigações e encargos trabalhistas, previdenciários, fiscais, sociais, comerciais e os demais previstos em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante, nos termos do artigo 121 da Lei nº 14.133, de 2021;

9.1.9. Comunicar ao Fiscal do contrato, assim que possível, qualquer ocorrência anormal ou acidente que se verifique no local da execução dos serviços;

9.1.10. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do objeto;

9.1.11. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros;

9.1.12. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato;

9.1.13. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina;

9.1.14. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do Termo de Referência, observando-se o disposto no Capítulo VII do Título III da Lei nº 14.133, de 2021;

9.1.15. Não permitir a utilização de qualquer trabalho do menor de 16 (dezesesseis) anos, exceto na condição de aprendiz para os maiores de 14 (quatorze) anos, nem permitir a utilização do trabalho do menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre;

9.1.16. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

9.1.17. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas em outras normas específicas (art. 116 da Lei nº 14.133, de 2021);

- 9.1.18. Comprovar o cumprimento da reserva de cargos a que se refere a subdivisão acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único, da Lei nº 14.133, de 2021);
- 9.1.19. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato, respondendo, administrativa, civil e criminalmente por sua indevida divulgação e incorreta ou inadequada utilização;
- 9.1.20. Arcar com o ônus decorrente de eventual equívoco no dimensionamento de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros, mas que sejam previsíveis em seu ramo de atividade;
- 9.1.21. Cumprir as disposições legais e regulamentares federais, estaduais e municipais que interfiram na execução do objeto, bem como as normas de segurança do Contratante;
- 9.1.22. Assegurar aos seus trabalhadores ambiente de trabalho, inclusive equipamentos e instalações, em condições adequadas ao cumprimento das normas de saúde, segurança e bem-estar no trabalho;
- 9.1.23. Garantir o acesso do Contratante, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do objeto;
- 9.1.24. Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram o Termo de Referência, no prazo determinado;
- 9.1.25. Prestar os serviços conforme os parâmetros e rotinas estabelecidos, utilizando todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, e normas da legislação;
- 9.1.26. Disponibilizar ao Contratante os empregados devidamente uniformizados e identificados por meio de crachá, além de provê-los com os Equipamentos de Proteção Individual - EPI, quando for o caso;
- 9.1.27. Fornecer os uniformes a serem utilizados por seus empregados, conforme disposto no Termo de Referência, sem repassar quaisquer custos a estes;
- 9.1.28. Apresentar relação mensal dos empregados que expressamente optarem por não receber o vale-transporte;
- 9.1.29. Efetuar o pagamento dos salários dos empregados alocados na execução contratual mediante depósito na conta bancária de titularidade do trabalhador, em agência situada na localidade ou região metropolitana em que ocorre a prestação dos serviços, de modo a possibilitar a conferência do pagamento por parte do Contratante. Em caso de impossibilidade de cumprimento desta disposição, o Contratado deverá apresentar justificativa, a fim de que o Contratante analise sua plausibilidade e possa verificar a realização do pagamento;
- 9.1.30. Autorizar o Contratante, no momento da assinatura do contrato, a fazer o desconto nas faturas e realizar os pagamentos dos salários e demais verbas trabalhistas diretamente aos trabalhadores, bem como a fazer o desconto das contribuições previdenciárias e do FGTS, quando não demonstrado o cumprimento tempestivo e regular dessas obrigações, até o momento da regularização, sem prejuízo das sanções cabíveis;
- 9.1.31. Não permitir que o empregado designado para trabalhar em um turno preste seus serviços no turno imediatamente subsequente;
- 9.1.32. Atender às solicitações do Contratante quanto à substituição dos profissionais alocados, no prazo fixado pelo fiscal do contrato, nos casos em que ficar constatado descumprimento das obrigações relativas à execução do serviço, conforme descrito no Termo de Referência;
- 9.1.33. Instruir seus profissionais quanto à necessidade de acatar as normas internas da Administração;
- 9.1.34. Instruir seus profissionais a respeito das atividades a serem desempenhadas, alertando-os a não executarem atividades não abrangidas pelo contrato, devendo o Contratado relatar ao Contratante toda e qualquer eventual ocorrência neste sentido, a fim de evitar desvio de função;
- 9.1.35. Instruir seus empregados, no início da execução contratual, quanto à obtenção das informações de seus interesses junto aos órgãos públicos, relativas ao contrato de trabalho e obrigações a ele inerentes, adotando, entre outras, as seguintes medidas:
- 9.1.35.1. Viabilizar o acesso de seus empregados, via internet, por meio de senha própria, aos sistemas da Previdência Social e da Receita do Brasil, quando disponível, com o objetivo de verificar se as suas contribuições previdenciárias foram recolhidas, no prazo máximo de 60 (sessenta) dias, contados do início da prestação dos serviços ou da admissão do empregado;
- 9.1.35.2. Viabilizar a emissão do cartão cidadão pela Caixa Econômica Federal para todos os empregados que necessitem dessa providência para acesso às informações de seu interesse, no prazo máximo de 60 (sessenta) dias, contados do início da prestação dos serviços ou da admissão do empregado, admitindo-se que essa providência seja substituída por outro meio comprovadamente eficaz de acesso a essas informações;
- 9.1.36. Oferecer todos os meios necessários aos seus empregados para a obtenção de extratos de recolhimentos de seus direitos sociais, preferencialmente por meio eletrônico, quando disponível;
- 9.1.37. Não se beneficiar do regime tributário do Simples Nacional em caso de enquadramento em uma das vedações da Lei Complementar nº 123, de 14 de dezembro de 2006;
- 9.1.37.1. Quando for o caso, se caracterizado enquadramento em uma das vedações da Lei Complementar nº 123, de 2006, o Contratado deverá requerer ao órgão fazendário competente a sua exclusão do Simples Nacional até o último dia útil do mês subsequente àquele em que ocorrida a situação de vedação, nos termos do artigo 30, caput, inciso II, e § 1º, inciso II, do mesmo diploma legal, apresentando ao Contratante a comprovação da exclusão ou o seu respectivo protocolo;
- 9.1.38. Realizar os serviços de manutenção e assistência técnica no(s) seguinte(s) local(is) ... [inserir endereço(s)];
- 9.1.38.1. O técnico deverá se deslocar ao local da repartição, salvo se o Contratado tiver unidade de prestação de serviços em distância de até [...] [inserir distância conforme avaliação técnica] do local demandado.
- 9.1.39. Realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo ser exigida do Contratado, inclusive, a capacitação dos técnicos do Contratante ou do novo fornecedor que continuará a execução dos serviços;
- 9.1.40. Ceder ao Contratante todos os direitos patrimoniais relativos ao objeto contratado, o qual poderá ser livremente utilizado e/ou alterado em outras ocasiões, sem necessidade de nova autorização do Contratado;
- 9.1.40.1. Considerando que o objeto da contratação envolve a elaboração de projeto relativo a obra imaterial de caráter tecnológico, insuscetível de privilégio, a cessão de todos os direitos patrimoniais a que se refere a subdivisão anterior inclui o fornecimento de todos os dados, documentos e elementos de informação pertinentes à tecnologia de concepção, desenvolvimento, fixação em suporte físico de

qualquer natureza e aplicação da obra, nos termos do § 1º do art. 93 da Lei nº 14.133, de 2021.

9.2. Em atendimento à Lei nº 12.846, de 2013, e ao Decreto estadual nº 69.588, de 2025, o Contratado se compromete a conduzir os seus negócios de forma a coibir fraudes, corrupção e quaisquer outros atos lesivos à Administração Pública, nacional ou estrangeira, de modo que o Contratado não poderá oferecer, dar ou se comprometer a dar a quem quer que seja, tampouco aceitar ou se comprometer a aceitar de quem quer que seja, por conta própria ou por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou benefícios de qualquer espécie relacionados de forma direta ou indireta ao objeto deste contrato, o que deve ser observado, ainda, pelos seus prepostos, colaboradores e eventuais subcontratados, caso permitida a subcontratação.

9.2.1. O descumprimento das obrigações previstas na subdivisão acima poderá submeter o Contratado à extinção unilateral do contrato, a critério do Contratante, sem prejuízo da aplicação das sanções penais e administrativas cabíveis e, também, da instauração do processo administrativo de responsabilização de que tratam a Lei nº 12.846, de 2013, e o Decreto estadual nº 69.588, de 2025.

9.3. O Contratado obriga-se a não admitir a participação, na execução deste contrato, de:

9.3.1. agente público de órgão ou entidade licitante ou contratante, ou terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica, nos termos dos §§ 1º e 2º do artigo 9º da Lei nº 14.133, de 2021;

9.3.2. pessoa que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, nos termos do inciso IV do artigo 14 e/ou parágrafo único do artigo 48 da Lei nº 14.133, de 2021;

9.3.3. pessoas que se enquadrem nas demais vedações previstas no artigo 14 da Lei nº 14.133, de 2021.

9.4. O Contratado deverá observar a vedação constante do Decreto estadual nº 68.829, de 4 de setembro de 2024.

9.5. Deverá ser apresentado as certificações ISO 20.000:2020 e 27.001:2022;

9.6. Na hipótese do fornecedor comprovar a posse de somente uma das certificações requeridas, a contratação será permitida, desde que assuma o compromisso de apresentar a certificação remanescente no prazo máximo e improrrogável de 12 (doze) meses, a contar da data da assinatura do contrato, sendo que o não cumprimento desta condição implicará nas penalidades contratuais previstas.

9.7. Apresentação da declaração formal da licitante que possui o(s) profissional(is) abaixo, com as respectivas certificações e experiências previstas no Estudo Técnico Preliminar, detentor(es) de atestado de responsabilidade técnica por execução de serviço(s) de características abaixo:

9.7.1. 01 (um) Especialista em Cloud - Arquiteto de solução;

9.7.2. 01 (um) Analista de sistemas operacionais Windows (Sênior);

9.7.3. 01 (um) Analista de sistemas operacionais Linux (Sênior);

9.7.4. 01 (um) Administrador de Banco de Dados (DBA);

9.7.5. 01 (um) Administrador Notes (Sênior);

9.7.6. 01 (um) Analista de redes (N3);

9.7.7. 01 (um) Administrador em Segurança da Informação (Threat Hunting).

9.7.8. As certificações mencionadas no Estudo Técnico Preliminar são obrigatórias, ou seja, somente serão aceitos profissionais que as possuam, não sendo aceitos aqueles que possuírem apenas comprovação da experiência nos conhecimentos e atividades que elas comportam.

9.7.9. Deverá ser apresentada a comprovação de experiência exigidas conforme a função, bem como certificações em até 30 (trinta) dias após a assinatura do contrato.

10. Cláusula décima - obrigações pertinentes a LGPD

10.2. No âmbito da execução do objeto deste contrato, o Contratado deve cumprir a Lei nº 13.709, de 14 de agosto de 2018, com suas alterações subsequentes (Lei Geral de Proteção de Dados Pessoais - LGPD), as demais normas legais e regulamentares aplicáveis à proteção de dados pessoais, inclusive regulamentos editados pela Agência Nacional de Proteção de Dados, e deve observar as instruções por escrito do Contratante no tratamento de dados pessoais.

10.2.1. O Contratado deve assegurar que o acesso a dados pessoais seja limitado aos empregados, prepostos ou colaboradores que necessitem conhecer/acessar os dados pertinentes, na medida em que sejam estritamente necessários para as finalidades deste contrato, e cumprir a legislação aplicável, assegurando que todos esses indivíduos estejam sujeitos a compromissos de confidencialidade ou obrigações profissionais de confidencialidade.

10.2.2. Considerando a natureza dos dados tratados, as características específicas do tratamento e o estado atual da tecnologia, assim

como os princípios previstos no caput do artigo 6º da Lei nº 13.709, de 2018, o Contratado deve adotar, em relação aos dados pessoais, medidas de segurança, técnicas e administrativas aptas a proteger os dados e informações de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

10.2.3. Considerando a natureza do tratamento, o Contratado deve, enquanto operador de dados pessoais, implementar medidas técnicas e organizacionais apropriadas para o cumprimento das obrigações do Contratante previstas na Lei nº 13.709, de 2018.

10.2.4. O Contratado deve:

10.2.4.1. notificar o Contratante na primeira oportunidade possível, ao receber requerimento de um titular de dados, na forma prevista no artigo 18 da Lei nº 13.709, de 2018; e

10.2.4.2. quando for o caso, auxiliar o Contratante na elaboração da resposta ao requerimento a que se refere a subdivisão anterior.

10.2.5. O Contratado deve notificar ao Contratante, na primeira oportunidade possível, a ocorrência de incidente de segurança relacionado a dados pessoais, fornecendo informações suficientes para que o Contratante cumpra quaisquer obrigações de comunicar à autoridade nacional e aos titulares dos dados a ocorrência do incidente de segurança sujeita à Lei nº 13.709, de 2018.

10.2.6. O Contratado deve adotar as medidas cabíveis para auxiliar na investigação, mitigação e reparação de cada um dos incidentes de segurança.

10.2.7. O Contratado deve auxiliar o Contratante na elaboração de relatórios de impacto à proteção de dados pessoais, observado o disposto no artigo 38 da Lei nº 13.709, de 2018, no âmbito da execução deste Contrato.

10.2.8. Na ocasião do encerramento deste contrato, o Contratado deve, imediatamente, ou, mediante justificativa, em até 10 (dez) dias úteis da data de seu encerramento, devolver todos os dados pessoais ao Contratante ou eliminá-los, conforme decisão do Contratante, inclusive eventuais cópias de dados pessoais tratados no âmbito deste contrato, certificando por escrito, ao Contratante, o cumprimento desta obrigação.

10.2.9. O Contratado deve colocar à disposição do Contratante, conforme solicitado, toda informação necessária para demonstrar o cumprimento do disposto nesta cláusula, e deve permitir auditorias e contribuir com elas, incluindo inspeções, pelo Contratante ou auditor por ele indicado, em relação ao tratamento de dados pessoais.

10.2.10. O Contratado responderá por quaisquer danos, perdas ou prejuízos causados ao Contratante ou a terceiros decorrentes do descumprimento da Lei nº 13.709, de 2018 ou de instruções do Contratante relacionadas a este contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização do Contratante em seu acompanhamento.

10.2.11. Caso o objeto da presente contratação envolva o tratamento de dados pessoais com fundamento no consentimento do titular de que trata o inciso I do artigo 7º da Lei nº 13.709, de 2018, deverão ser observadas pelo Contratado ao longo de toda a vigência do contrato todas as obrigações específicas vinculadas a essa hipótese legal de tratamento de dados pessoais, conforme instruções por escrito do Contratante.

10.2.12. É vedada a transferência de dados pessoais, pelo Contratado, para fora do território do Brasil.

10.2.13. O Contratado não poderá realizar subcontratação, tampouco divulgar dados pessoais a qualquer subcontratado, ou substituir subcontratado, exceto se previamente autorizada de forma específica e por escrito pelo Contratante.

10.2.14. O Contratado deve tomar medidas razoáveis para assegurar que empregados, prepostos ou colaboradores de qualquer subcontratado que necessitem conhecer/acessar dados pessoais relacionados à execução deste contrato estejam sujeitos a compromissos de confidencialidade ou obrigações profissionais de confidencialidade, e cumprir, no tocante à subcontratação, todas as disposições aplicáveis da Lei nº 13.709, de 2018.

10.2.15. A subcontratação, mesmo quando autorizada pelo Contratante, não exime o Contratado das obrigações decorrentes deste contrato, de modo que o Contratado permanecerá por elas integralmente responsável perante o Contratante, inclusive na hipótese de descumprimento dessas obrigações por subcontratado.

11. Cláusula décima primeira - garantia de execução

11.1. Não haverá exigência de garantia contratual da execução.

12. Cláusula décima segunda - infrações e sanções administrativas

12.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado que:

- a. der causa à inexecução parcial do contrato;
- b. der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c. der causa à inexecução total do contrato;
- d. ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- e. apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- f. praticar ato fraudulento na execução do contrato;
- g. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

12.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

I. Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

II. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

III. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima deste Contrato, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021);

IV. Multa:

As sanções serão aplicadas em conformidade com a Resolução nº SSP-05/2026, publicada no diário oficial do Estado de São Paulo em 02MAR26, que integra este instrumento (**Anexo III do Edital**), após regular processo administrativo.

iv.1) A sanção de multa prevista no inciso II do caput do art. 156 da Lei nº 14.133, de 2021, calculada na forma deste Contrato, não poderá ser inferior a 0,5% (cinco décimos por cento) nem superior a 30% (trinta por cento) do valor do contrato (§ 3º do art. 156 da Lei nº 14.133, de 2021).

12.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021).

12.4. A multa poderá ser aplicada cumulativamente com as demais sanções previstas neste Contrato ([art. 156, § 7º, da Lei nº 14.133, de 2021](#)).

12.4.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021).

12.4.2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).

12.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no **caput** e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

12.6. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

- a) a natureza e a gravidade da infração cometida;
- b) as peculiaridades do caso concreto;
- c) as circunstâncias agravantes ou atenuantes;
- d) os danos que dela provierem para o Contratante;
- e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

12.7. As sanções são autônomas e a aplicação de uma não exclui a de outra.

12.8. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na referida Lei (art. 159 da Lei nº 14.133, de 2021).

12.9. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos na Lei nº 14.133, de 2021, ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, a pessoa jurídica sucessora ou a empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o sancionado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160 da Lei nº 14.133, de 2021).

12.10. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ele aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal (Art. 161 da Lei nº 14.133, de 2021).

12.11. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021

13. Cláusula décima terceira - da extinção contratual

13.1. O contrato poderá ser extinto na forma, pelos motivos e com as consequências previstos nos artigos 137 a 139 e 155 a 163 da Lei nº 14.133, de 2021.

13.1.1. O Contratado reconhece desde já os direitos do Contratante nos casos de extinção por ato unilateral da Administração, prevista no artigo 138 da Lei nº 14.133, de 2021.

13.1.2. O contrato poderá ser extinto por algum dos motivos previstos no artigo 137 da Lei nº 14.133, de 2021, devendo a extinção ser formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa.

13.1.3. A alteração social ou modificação da finalidade ou da estrutura da empresa não ensejará a extinção contratual se não restringir sua capacidade de concluir o contrato.

13.1.3.1. Se a operação societária de que trata a subdivisão acima implicar mudança em pessoa jurídica contratada, deverá ser formalizada alteração subjetiva por termo aditivo.

13.2. O termo de extinção, sempre que possível, será precedido da indicação de:

13.2.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

13.2.2. Relação dos pagamentos já efetuados e ainda devidos;

13.2.3. Indenizações e multas.

13.3. A extinção do contrato não configura óbice para o reconhecimento de eventual desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, caput, da Lei n.º 14.133, de 2021).

13.4. O descumprimento total ou parcial das obrigações e responsabilidades assumidas pelo Contratado, incluindo o descumprimento das obrigações trabalhistas, não recolhimento das contribuições sociais, previdenciárias ou para com o FGTS, ou a não manutenção das condições de habilitação pelo Contratado, ensejará a aplicação de sanções administrativas, previstas neste instrumento e na legislação vigente, podendo culminar em extinção contratual, por ato unilateral e escrito do Contratante, com base nos artigos 50, 121 e 137 da Lei nº 14.133, de 2021.

13.5. Quando da extinção da contratação, o fiscal administrativo deverá verificar o pagamento pelo Contratado das verbas rescisórias ou os documentos que comprovem que os empregados serão realocados em outra atividade de prestação de serviços do Contratado, sem que ocorra a extinção do contrato de trabalho.

13.5.1. Até que o Contratado comprove o disposto na subdivisão anterior, o Contratante reterá:

13.5.1.1. a garantia contratual, caso exigida na documentação que integra este instrumento - prestada com cobertura para os casos de descumprimento das obrigações de natureza trabalhista e previdenciária, incluídas as verbas rescisórias -, a qual será executada para reembolso dos prejuízos sofridos pela Administração, nos termos da legislação que rege a matéria (art. 121, § 3º, I, e art. 139, III, "b", da Lei n.º 14.133, de 2021); e

13.5.1.2. os valores das Notas fiscais ou Faturas correspondentes, até que a situação seja regularizada.

13.6. Na hipótese da subdivisão anterior, não havendo quitação das verbas trabalhistas por parte do Contratado no prazo de 15 (quinze) dias, o Contratante poderá efetuar o pagamento das verbas trabalhistas diretamente aos empregados do Contratado que tenham participado da execução dos serviços objeto do contrato, deduzindo o respectivo valor do pagamento devido ao Contratado (art. 121, § 3º, inciso IV, da Lei nº 14.133, de 2021).

13.7. O Contratante poderá ainda:

13.7.1. nos casos de obrigação de pagamento de multa pelo Contratado, reter a garantia prestada a ser executada (art. 139, III, "c", da Lei n.º 14.133, de 2021), conforme legislação que rege a matéria, caso tenha ocorrido exigência de prestação de garantia na documentação que integra este instrumento; e

13.7.2. nos casos em que houver necessidade de ressarcimento de prejuízos causados à Administração, nos termos do inciso IV do art. 139 da Lei n.º 14.133, de 2021, reter os eventuais créditos existentes em favor do Contratado decorrentes do contrato.

13.8. Se for constatada irregularidade no procedimento licitatório ou na execução contratual, caso não seja possível o saneamento, a decisão pelo Contratante sobre a suspensão da execução ou sobre a declaração de nulidade do contrato somente será adotada na hipótese em que se revelar medida de interesse público, observado o disposto nos artigos 147 a 149 da Lei nº 14.133, de 2021, conferindo-se ao Contratado oportunidade para prévia manifestação e participação na instrução.

14. Cláusula décima quarta - dotação orçamentária

14.1. No presente exercício, as despesas decorrentes desta contratação correrão à conta de recursos específicos consignados no respectivo Orçamento do Estado, na dotação abaixo discriminada:

I. Gestão/Unidade: DTIC – Diretoria de Tecnologia da Informação e Comunicação;

II. Fonte de Recursos: 10010001;

III. Programa de Trabalho: 180433;

IV. Elemento de Despesa: 339039;

V. Plano Interno: Plano de ação nº 13/46 – PR13.

VI. Nota de Empenho:

14.2. Quando a execução do contrato ultrapassar o presente exercício, a dotação relativa ao(s) exercício(s) financeiro(s) subsequente (s) será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

15. Cláusula décima quinta - dos casos omissos

15.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

16. Cláusula décima sexta - alterações

- 16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 16.133, de 2021.
- 16.2. O Contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários no objeto, a critério exclusivo do Contratante, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.
- 16.3. Se o contrato não contemplar preços unitários para serviços cujo aditamento se fizer necessário, esses serão fixados por meio da aplicação da relação geral entre os valores da proposta e o do orçamento-base da Administração sobre os preços referenciais ou de mercado vigentes na data do aditamento, respeitados os limites estabelecidos no artigo 125 da Lei nº 16.133, de 2021.
- 16.4. Eventuais alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, respeitadas as disposições da Lei nº 16.133, de 2021, admitindo-se que, nos casos de justificada necessidade de antecipação de seus efeitos, a formalização do aditivo ocorra no prazo máximo de 1 (um) mês (art. 132 da Lei nº 16.133, de 2021).
- 16.5. Caso haja alteração unilateral do contrato que aumente ou diminua os encargos do Contratado, o equilíbrio econômico-financeiro inicial será restabelecido no mesmo termo aditivo.
- 16.6. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 16.133, de 2021.

17. Cláusula décima sétima - publicação

17.1 Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, *caput*, da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 22º, do Decreto Estadual 68.155, de 2023..

18. Cláusula décima oitava - foro

18.1. Fica eleito o Foro da Comarca da Capital do Estado de São Paulo para dirimir quaisquer questões que decorrerem deste Termo de Contrato, que não puderem ser resolvidas na esfera administrativa, conforme art. 92, § 1º, da Lei nº 14.133, de 2021.

E assim, por estarem as partes justas e contratadas, foi lavrado o presente instrumento em 01 (uma) via, que, lido e achado conforme pelo Contratado e pelo Contratante, vai por eles assinado para que produza todos os efeitos de Direito, sendo assinado também pelas testemunhas abaixo identificadas.

[Local], [dia] de [mês] de [ano]. OU [Local], data da última assinatura eletrônica das partes.

Representante legal do CONTRATANTE

Representante legal do CONTRATADO

TESTEMUNHAS:

1-

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

MARCELO FUMIO TAMASHIRO

Equipe de apoio



DIÁRIO OFICIAL DO ESTADO DE SÃO PAULO

Publicado na Edição de 2 de março de 2026 | Caderno Executivo | Seção Atos Normativos

RESOLUÇÃO SSP-05/2026

Regulamenta a aplicação das sanções previstas na Lei Federal nº 14.133/2021, no âmbito da Secretaria da Segurança Pública.

O **SECRETÁRIO DA SEGURANÇA PÚBLICA**, no exercício de suas atribuições legais e regulamentares, e, considerando as significativas alterações introduzidas pela Lei Federal nº 14.133, de 1º de abril de 2021 (LLCA), às licitações e contratações públicas, bem como a necessidade de disciplinar a aplicação de sanções, nos termos dos artigos 155 a 163 desse diploma legal,

RESOLVE:

CAPÍTULO I - DAS DISPOSIÇÕES INICIAIS

Artigo 1º - A aplicação de sanções aos licitantes e contratados, em decorrência de infrações cometidas em procedimentos licitatórios, em contratações administrativas e em outros ajustes regidos pela LLCA obedecerá ao disposto nesta Resolução.

Artigo 2º - São consideradas infrações para os fins desta Resolução:

- I - dar causa à inexecução parcial do contrato;
- II - dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
- III - dar causa à inexecução total do contrato;
- IV - deixar de entregar a documentação exigida para o certame;
- V - não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
- VI - não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
- VII - ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;
- VIII - apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;
- IX - fraudar a licitação ou praticar ato fraudulento na execução do contrato;
- X - comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- XI - praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

XII - praticar ato lesivo previsto no artigo 5º da Lei nº 12.846, de 1º de agosto de 2013.

Artigo 3º - As sanções administrativas aplicáveis são:

I - advertência;

II - multa;

III - impedimento de licitar e contratar com a Administração Pública Direta e Indireta do Estado de São Paulo, pelo prazo máximo de 3 (três) anos;

IV - declaração de inidoneidade para licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) e máximo de 6 (seis) anos.

Artigo 4º - Além das sanções previstas no artigo 3º desta Resolução, incidirá em multa de mora o contratado que der causa ao atraso injustificado na execução do contrato, na forma prevista em edital ou em contrato.

Parágrafo único. A aplicação de multa de mora não impedirá que a Administração a converta em compensatória e promova a extinção unilateral do contrato com a aplicação cumulada de outras sanções previstas nesta Resolução.

Artigo 5º - Na aplicação das sanções a que se refere o artigo 2º desta Resolução, serão considerados:

I - a natureza e a gravidade da infração cometida;

II - as peculiaridades do caso concreto;

III - as circunstâncias agravantes ou atenuantes;

IV - os danos à Administração que advierem da infração cometida;

V - a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

§1º - São consideradas circunstâncias agravantes:

1 - a existência de registro do licitante ou contratado no E-Sanções ou na Relação de Apenados do TCESP, em vigência no momento do cometimento da infração, em decorrência de penalidade aplicada no âmbito da Secretaria da Segurança Pública, nos 12 (doze) meses anteriores ao fato ensejador da sanção;

2 - a desclassificação ou inabilitação por descumprimento das exigências do edital, quando for notória a impossibilidade de atendimento ao estabelecido;

3 - a inércia deliberada do licitante ou do contratado em face das diligências destinadas a esclarecer ou a complementar a instrução do processo licitatório ou o inadimplemento de obrigações contratuais;

4 - a falsidade de declaração, apresentada pelo licitante, de que é beneficiário de tratamento diferenciado concedido em legislação específica;

5 - a reincidência na infração;

6 - a imprescindibilidade do bem ou serviço contratado para o funcionamento de serviços públicos ou satisfação de necessidade coletiva.

§ 2º - São consideradas circunstâncias atenuantes:

1 - a falha escusável do licitante ou contratado;

2- a apresentação de documentação que contenha vícios ou omissões para os quais não tenha contribuído o licitante ou o contratado e que não sejam de fácil identificação por estes últimos;

3- a juntada de documentação que, embora não tenha atendido às exigências do edital, foi encaminhada de forma equivocada, sem indício de má-fé;

4 - a adoção de medidas destinadas a mitigar os efeitos danosos da conduta infracional.

Artigo 6º - Considera-se reincidência a repetição de conduta prevista no artigo 2º desta Resolução, sancionada por decisão administrativa irrecorrível.

Parágrafo único - Para efeito de reincidência, não prevalece a sanção anterior, se entre a data da decisão administrativa definitiva e aquela da prática posterior houver decorrido período superior a 5 (cinco) anos.

CAPÍTULO II - DAS SANÇÕES

Seção I – Da Advertência

Artigo 7º - A advertência será aplicada exclusivamente ao contratado que der causa à inexecução parcial do contrato, da qual não advenha grave dano à Administração, quando não se justificar a imposição de penalidade mais grave.

Parágrafo único - Será considerada inexecução parcial sem grave prejuízo à Administração aquela relacionada ao descumprimento de cláusulas contratuais, que não comprometa o cumprimento da execução contratual, bem como não cause dano ao interesse público.

Seção II – Da Multa prevista no inciso II do artigo 3º desta Resolução

Artigo 8º - A multa prevista no inciso II do artigo 3º desta Resolução não poderá ser inferior a 0,5% (cinco décimos por cento) nem superior a 30% (trinta por cento) do valor do contrato licitado ou celebrado e poderá ser aplicada a todas as infrações tratadas por esta Resolução.

Artigo 9º - Em caso de inexecução parcial do ajuste será aplicada a multa prevista no inciso II do artigo 3º desta Resolução, na seguinte conformidade:

I - aquisição de bens, contratação de prestação de serviços não contínuos e obras e serviços de engenharia: de 10% (dez por cento) a 20% (vinte por cento) do valor total do contrato;

II - serviços e fornecimentos contínuos: de 10% (dez por cento) a 20% (vinte por cento) do valor anual do contrato;

Artigo 10 – Em caso de inexecução total do ajuste será aplicada a multa prevista no inciso II do artigo 3º desta Resolução, na seguinte conformidade:

I - aquisição de bens, contratação de prestação de serviços não contínuos e obras e serviços de engenharia: de 20% (vinte por cento) a 30% (trinta por cento) do valor total do contrato;

II - serviços e fornecimentos contínuos: de 20% (vinte por cento) a 30% (trinta por cento) do valor anual do contrato.

Artigo 11 – A multa prevista no inciso II do artigo 3º desta Resolução será aplicada nos termos e percentuais abaixo indicados:

I - deixar de entregar a documentação exigida para o certame: de 5% (cinco por cento) a 10% (dez por cento) sobre o valor total do contrato;

II - não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado: de 10% (dez por cento) a 20% (vinte por cento) sobre o valor total do contrato;

III - não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta: de 20% (vinte por cento) a 30% (trinta por cento) sobre o valor total do contrato;

IV - apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato: de 20% (vinte por cento) a 30% (trinta por cento) sobre o valor total do contrato;

V - fraudar a licitação ou praticar ato fraudulento na execução do contrato: de 20% (vinte por cento) a 30% (trinta por cento) sobre o valor total do contrato;

VI - comportar-se de modo inidôneo ou cometer fraude de qualquer natureza: de 20% (vinte por cento) a 30% (trinta por cento) sobre o valor total do contrato;

VII - praticar atos ilícitos visando a frustrar os objetivos da licitação: de 20% (vinte por cento) a 30% (trinta por cento) sobre o valor total do contrato;

VIII - praticar ato lesivo previsto no artigo 5º da Lei nº 12.846, de 1º de agosto de 2013: de 20% (vinte por cento) a 30% (trinta por cento) sobre o valor total do contrato.

Artigo 12 - Nas hipóteses de inexecução parcial ou total do contrato, a autoridade competente deverá deliberar, formalmente, quanto à vantajosidade da manutenção do contrato vigente ou inaugurar, imediatamente, os procedimentos para a extinção do contrato.

Seção III – Da multa de mora prevista no artigo 4º desta Resolução

Artigo 13 - Em caso de atraso injustificado na execução do contrato será aplicada a multa de mora prevista no artigo 4º desta Resolução:

I - sobre o valor da parcela inadimplida;

II - a partir do primeiro dia útil seguinte ao término do prazo estipulado para cumprimento da obrigação.

§1º- A multa de mora prevista no *caput* deste artigo será:

1 - no caso de aquisição de bens ou de prestação de serviços não contínuos:

a) 0,5% (meio por cento) ao dia, para atraso de até 60 (sessenta) dias;

b) após 60 (sessenta) dias, ficará caracterizada a inexecução parcial ou total do contrato, sem prejuízo de eventual extinção unilateral em prazo inferior, conforme o caso.

2 - no caso de serviços e fornecimentos contínuos:

a) 0,5% (meio por cento) ao dia, para atraso de até 60 (sessenta) dias;

b) após 60 (sessenta) dias, ficará caracterizada a inexecução parcial ou total do contrato, conforme o caso, sem prejuízo de eventual extinção unilateral em prazo inferior, dadas as características do serviço prestado ou bem adquirido.

3 - no caso de obras e serviços de engenharia:

- a) 0,7% (sete décimos por cento) ao dia, para atraso de até 30 (trinta) dias;
- b) 1% (um por cento) ao dia, para atraso de até 30 (trinta) dias, no caso de reincidência;
- c) após 30 (trinta) dias, ficará caracterizada a inexecução parcial ou total do contrato, conforme o caso, sem prejuízo de eventual extinção unilateral em prazo inferior, dadas as características do serviço prestado.

§ 2º – Os prazos referidos nos itens 1 a 3 do §1º deste artigo serão contados em dias corridos.

§ 3º – A multa de mora poderá:

- 1 - ser convertida na multa sancionatória prevista no inciso II do artigo 3º desta Resolução;
- 2 - ser aplicada em conjunto com as demais sanções previstas nesta Resolução;
- 3 - ensejar a extinção unilateral do contrato.

Seção IV – Do Impedimento de Licitar e Contratar

Artigo 14 - A sanção de impedimento de licitar e contratar com a Administração Pública Direta e Indireta do Estado de São Paulo, será aplicada ao contratado ou licitante pelas infrações nos termos abaixo, quando não se justificar a imposição de declaração de inidoneidade, pelos seguintes prazos, respeitado o prazo máximo de 3 (três) anos:

I - de 3 (três) meses a 9 (nove) meses pela conduta de deixar de entregar a documentação exigida para o certame;

II - de 6 (seis) meses a 18 (dezoito) meses pela conduta de:

- a) não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
- b) não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
- c) retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

III - de 12 (doze) meses a 3 (três) anos, pela conduta de dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

IV - de 2 (dois) anos a 3 (três) anos, pela conduta de dar causa à inexecução total do contrato.

Seção V – Da Declaração de Inidoneidade para Licitar ou Contratar

Artigo 15 – A declaração de inidoneidade para licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos será aplicada ao contratado ou licitante pelas infrações nos termos abaixo, pelos seguintes prazos, devendo ser observado o prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos:

I - de 3 (três) anos a 5 (cinco) anos, pela conduta de praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

II - de 4 (quatro) anos a 6 (seis) anos pela conduta de:

- a) apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;
- b) fraudar a licitação ou praticar ato fraudulento na execução do contrato;
- c) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- d) praticar ato lesivo previsto no artigo 5º da Lei nº 12.846, de 1º de agosto de 2013.

Parágrafo único - A sanção prevista no *caput* será aplicada quando justificada a imposição de penalidade mais grave pela prática das seguintes condutas, pelos seguintes prazos:

I - de 3 (três) anos a 5 (cinco) anos pela conduta de:

- a) dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
- b) deixar de entregar a documentação exigida para o certame;
- c) não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
- d) não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
- e) ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado.

II - de 4 (quatro) anos a 6 (seis) anos, pela conduta de dar causa à inexecução total do contrato;

CAPÍTULO III - DAS COMPETÊNCIAS

Artigo 16 - O Dirigente da Unidade Gestora Executora (UGE) será competente para:

- I - instaurar os processos sancionatórios e de responsabilização;**
- II - aplicar as sanções de advertência e multa nos casos de inexecução parcial do contrato que não resulte em grave dano à Administração, quando não se justificar a imposição de penalidade mais grave;**
- III - aplicar as sanções decorrentes de infrações no procedimento licitatório para constituição de Sistema de Registro de Preços, do descumprimento do pactuado na ata de registro de preço, em relação à sua demanda registrada, ou do descumprimento das obrigações contratuais, em relação às suas próprias contratações;**
- IV - aplicar as penalidades decorrentes do descumprimento do pactuado na ata de registro de preço, na condição de órgão participante, em relação à sua demanda registrada, ou do descumprimento das obrigações contratuais, em relação às suas próprias contratações.**

Parágrafo único - Os atos previstos neste artigo serão formalizados mediante despacho motivado, com a devida indicação dos fundamentos fáticos e jurídicos.

Artigo 17 - O Dirigente da Unidade Orçamentária (UO) será competente para aplicar:

- I - sanção de multa pelas seguintes condutas:**

- a) dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
- b) dar causa à inexecução total do contrato;
- c) deixar de entregar a documentação exigida para o certame;
- d) não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
- e) não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
- f) ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;
- g) apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;
- h) fraudar a licitação ou praticar ato fraudulento na execução do contrato;
- i) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- j) praticar atos ilícitos com vistas a frustrar os objetivos da licitação;
- k) praticar ato lesivo previsto no artigo 5º da Lei nº 12.846, de 1º de agosto de 2013.

II - a sanção de impedimento de licitar e contratar pelas seguintes condutas:

- a) dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
- b) dar causa à inexecução total do contrato;
- c) deixar de entregar a documentação exigida para o certame;
- d) não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
- e) não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
- f) ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado.

Artigo 18 - Compete exclusivamente ao Secretário de Segurança Pública a aplicação da sanção de declaração de inidoneidade para licitar ou contratar, prevista no artigo 15 desta resolução, que será precedida de análise pelo órgão jurídico da Pasta.

CAPÍTULO IV - DA APURAÇÃO DE INFRAÇÕES E APLICAÇÃO DE SANÇÕES ADMINISTRATIVAS

Seção I - Das espécies de processo para aplicação das sanções

Artigo 19 - A aplicação das sanções objeto desta Resolução obedecerá ao seguinte:

I - para as sanções previstas nos incisos I a II do artigo 3º, desta Resolução e para a multa de mora será instaurado processo sancionatório;

II - para as sanções previstas nos incisos III e IV, do artigo 3º, desta Resolução, será instaurado processo de responsabilização, a ser conduzido por comissão composta de 2 (dois) ou

mais servidores estáveis.

§1º - O processo sancionatório e o processo de responsabilização terão início com o registro da infração.

§2º - O processo sancionatório e o processo de responsabilização deverão ser instaurados junto ao SEI/SP - Sistema Eletrônico de Informações do Estado de São Paulo - nos termos do Decreto nº 67.641, de 10 de abril de 2023, e ser relacionados, apensados ou anexados ao processo principal, de forma que a consulta a ambos possa ser simultânea.

§3º - O processo sancionatório e o processo de responsabilização deverão ser instruídos com as peças extraídas do processo principal identificadas individualmente, evitando a reunião de vários documentos em um único arquivo.

§4º - Com o início do processo sancionatório ou do processo de responsabilização, deverão ser notificados os emitentes das garantias que houver.

Seção II - Do registro da infração

Artigo 20 - Constatada a prática das infrações previstas nesta Resolução, no transcorrer do procedimento licitatório ou durante a execução do contrato, o fato deverá ser relatado formalmente ao Dirigente da UGE para que exerça o controle preventivo e delibere sobre o prosseguimento.

§1º - O relato formal da infração constitui um dever do agente público que tomar conhecimento do fato.

§ 2º - O relato formal da infração deverá conter os seguintes elementos:

- 1 - descrição da conduta irregular praticada pelo licitante ou contratado;
- 2 - motivação do ato, com enquadramento da situação fática às infrações previstas nesta Resolução;
- 3 - memorial de cálculo da multa, com base nesta Resolução;
- 4 - proposta de aplicação das sanções, nos termos desta Resolução.

§ 3º - O relato formal da infração será lavrado em documento digital, por meio do SEI/SP ou outro que venha a substituí-lo.

§ 4º - Compete:

1 - ao agente de contratação, bem como ao presidente da comissão de contratação, conforme o caso, o relato formal da infração cometida durante a licitação.

2 - ao gestor e a qualquer fiscal do contrato o relato formal da infração cometida durante a execução contratual.

§ 5º - Em sendo o relato formal da infração lavrado pelo fiscal do contrato, este deverá ser remetido preliminarmente ao gestor do contrato, para que exerça o controle preventivo do ato.

Seção III - Do processo sancionatório para aplicação de advertência

Artigo 21 - À vista de relato formal sobre inexecução parcial do contrato, sem grave dano à Administração, o dirigente da UGE determinará, mediante despacho fundamentado, a abertura do processo sancionatório para aplicação de advertência.

§ 1º - O despacho fundamentado consistirá na conferência e aprovação da aplicação da sanção.

§2º - Após seu despacho fundamentado o Dirigente de UGE encaminhará os autos ao gestor do contrato, para que intime o interessado para apresentar defesa no prazo de 15 (quinze) dias úteis, contados da data do recebimento da intimação.

§ 3º - Expirado o prazo para manifestação do interessado, a autoridade competente proferirá decisão fundamentada.

Seção IV - Do processo sancionatório para aplicação da multa prevista no artigo 2º, inciso II desta Resolução e da multa de mora prevista no 3º desta Resolução

Artigo 22 - À vista de relato formal sobre a prática de infração sujeita à multa ou à multa de mora, o Dirigente da UGE determinará, mediante despacho fundamentado, a abertura do processo sancionatório.

§1º - O despacho fundamentado consistirá na conferência e aprovação da aplicação da multa proposta no relato formal.

§2º - Após seu despacho fundamentado o Dirigente de UGE encaminhará os autos ao gestor do contrato, para que intime o interessado para apresentar defesa no prazo de 15 (quinze) dias úteis, contados da data do recebimento da intimação.

§3º - Expirado o prazo para manifestação do interessado, a autoridade competente proferirá decisão fundamentada.

§4º - Mantida a aplicação da penalidade, o interessado deverá ser intimado para ciência e, se for o caso, para pagamento da multa, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação para o recolhimento, devendo comprová-lo nos autos do processo sancionatório.

Seção V - Do processo de responsabilização para aplicação das penalidades de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar.

Artigo 23 - À vista de relato formal sobre a prática de infração sujeita às penalidades de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar, o Dirigente da UGE determinará, mediante despacho fundamentado, a abertura do processo de responsabilização, nos termos do artigo 19, inciso II desta Resolução.

§1º - O despacho fundamentado consistirá:

- 1 - Na conferência da penalidade proposta no relato formal;
- 2 - Na constituição de comissão composta de 2 (dois) ou mais servidores estáveis, de acordo com o artigo 19, inciso II desta Resolução.

§2º - A comissão referida no inciso II do §1º deste artigo:

- 1 - avaliará fatos e circunstâncias conhecidos;
- 2 - intimará o interessado para, no prazo de 15 (quinze) dias úteis contados da intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

3 - notificará os emitentes das garantias exigidas no contrato sobre o início do processo de responsabilização para apuração de descumprimento de cláusulas contratuais, nos termos do artigo 137, § 4º, da LLCA.

Artigo 24 - Se estiverem presentes indícios que recomendem, desde logo, a rescisão unilateral do contrato, deverá o interessado ser intimado de ambas as consequências da infração constatada.

Artigo 25 - Na hipótese de deferimento de pedido de produção de novas provas ou de juntada de provas julgadas indispensáveis pela comissão, o interessado poderá apresentar alegações finais, no prazo de 15 (quinze) dias úteis, contados da data da intimação.

Artigo 26 - Serão indeferidas pela comissão, mediante decisão fundamentada, provas ilícitas, impertinentes, desnecessárias, protelatórias ou intempestivas.

Artigo 27 - Finalizada a produção de provas ou expirado o prazo para alegações finais, a comissão elaborará relatório pormenorizado dos fatos no prazo máximo de 15 (quinze) dias úteis.

Artigo 28 - Os processos de responsabilização deverão ser remetidos, após o término da fase de instrução, à autoridade competente para fins de avaliação da regularidade do seu processamento.

Parágrafo único - Constatada a regularidade, a autoridade competente proferirá decisão, salvo nos casos de declaração de inidoneidade para licitar ou contratar, hipótese em que os autos serão remetidos ao órgão de assessoramento jurídico preliminarmente à decisão do Titular da Pasta.

Seção VI - Dos recursos

Artigo 29 - Da decisão que aplicar as sanções de advertência, multa, multa de mora e impedimento de licitar e contratar, caberá recurso, no prazo de 15 (quinze) dias úteis, a contar da intimação.

Parágrafo único - O recurso deverá ser dirigido à autoridade que tiver proferido a decisão recorrida que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis contados do recebimento dos autos.

Artigo 30 - Da decisão que aplicar a sanção de inidoneidade para licitar e contratar, caberá apenas pedido de reconsideração, que deverá ser apresentado no prazo de 15 (quinze) dias úteis, contados da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contados do seu recebimento pela autoridade competente.

Artigo 31 - O recurso e o pedido de reconsideração suspenderão o ato ou a decisão recorrida, até que sobrevenha decisão final da autoridade competente.

Artigo 32 - Na elaboração de suas decisões, a autoridade competente será auxiliada pelo órgão de assessoramento jurídico, que deverá dirimir dúvidas e subsidiá-la com as informações necessárias.

Seção VII - Das intimações

Artigo 33 - A intimação dos atos previstos nesta Resolução será feita ao preposto ou ao representante legal do interessado, conforme o caso, mediante mensagem eletrônica formal por meio do SEI/SP ao endereço de e-mail registrado no Sistema de Cadastramento Unificado de Fornecedores (SICAF).

Parágrafo único - Resultando infrutífera a intimação a que refere o *caput* deste artigo, será esta efetuada por meio de publicação no Diário Oficial do Estado de São Paulo.

CAPÍTULO V - DAS DISPOSIÇÕES FINAIS

Artigo 34 - A imposição das sanções previstas nesta Resolução não impede a propositura de ação judicial visando à reparação integral do dano causado.

Artigo 35 - Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

Artigo 36 - Aplica-se na contagem dos prazos previstos nesta Resolução o disposto no artigo 183 da LLCA.

Artigo 37 - A prescrição ocorrerá em 5 (cinco) anos, contados da ciência da infração pela Administração, e será:

I - interrompida pela instauração do processo de responsabilização a que se refere o *caput*

deste artigo;

II - suspensão pela celebração de acordo de leniência previsto na Lei nº 12.846, de 1º de agosto de 2013;

III - suspensão por decisão judicial que inviabilize a conclusão da apuração administrativa.

Artigo 38 - Os atos previstos como infrações administrativas na LLCA ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei Federal nº 12.846, de 1º de agosto de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na referida lei.

Artigo 39 - A personalidade jurídica poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos na LLCA ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, a pessoa jurídica sucessora ou a empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o sancionado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

Artigo 40 - Esta Resolução deverá integrar, obrigatoriamente, como anexo, os instrumentos convocatórios de licitação, os contratos e os instrumentos equivalentes, inclusive nas hipóteses de dispensa ou inexigibilidade de licitação.

Artigo 41 - Esta Resolução entrará em vigor na data de sua publicação, produzindo efeitos em relação aos certames e contratos regidos pela Lei Federal nº 14.133/2021.

OSVALDO NICO GONÇALVES
Secretário da Segurança Pública

POLÍCIA MILITAR DO ESTADO DE SÃO PAULO
Diretoria de Tecnologia da Informação e Comunicação - DTIC
MODELO REFERENTE A PLANILHA DE PROPOSTA

OBJETO: Contratação de serviços especializados de suporte técnico de cibersegurança, data center e redes, bem como de governança, gerenciamento e monitoramento, das demandas e mudanças de tecnologia da informação e comunicação e infraestrutura de data center e redes para ambiente computacional e de telecomunicações, de forma a garantir a continuidade dos serviços de TIC.

Item	CATMAT Contabiliz a	CATMAT Compras. serviço	Descrição – Categoria de Serviço	Qtd	HTS	Custo Mensal (R\$)	Custo 30 Meses (R\$)
1	91693	27090	Gerente de infraestrutura de tecnologia da informação	1	176	Sigiloso	Sigiloso
			Gerente de suporte técnico de tecnologia da informação	1	176	Sigiloso	Sigiloso
			Analista de sistemas de automação - Júnior	8	180	Sigiloso	Sigiloso
			Técnico de suporte ao usuário de tecnologia da informação Júnior	2	176	Sigiloso	Sigiloso
			Técnico de Rede (Telecomunicações) - Júnior	1	176	Sigiloso	Sigiloso
			Gerente de suporte técnico de tecnologia da informação	1	176	Sigiloso	Sigiloso
			Analista de suporte computacional Pleno	4	176	Sigiloso	Sigiloso
			Administrador de sistemas operacionais Sênior	4	176	Sigiloso	Sigiloso
			Administrador de sistemas operacionais Sênior	3	176	Sigiloso	Sigiloso
			Administrador de banco de dados - Sênior	1	176	Sigiloso	Sigiloso
			Administrador de banco de dados - Pleno	2	176	Sigiloso	Sigiloso
			Especialista em Cloud Sênior	1	176	Sigiloso	Sigiloso
			Gerente de segurança da informação	1	176	Sigiloso	Sigiloso
			Gerente de segurança da informação	1	176	Sigiloso	Sigiloso
			Analista de redes e de comunicação de dados Sênior	4	176	Sigiloso	Sigiloso
			Analista de redes e de comunicação de dados Pleno	7	176	Sigiloso	Sigiloso
			Administrador em segurança da informação - Sênior	1	176	Sigiloso	Sigiloso
			Analista de sistemas de automação - Pleno	1	176	Sigiloso	Sigiloso
			Desenvolvedor de sistemas de tecnologia da informação Sênior	1	176	Sigiloso	Sigiloso
				45		Sigiloso	Sigiloso

ANEXO V

MODELO DE DECLARAÇÃO

ANEXO V.1

MODELO DE DECLARAÇÃO EXIGIDA PARA HABILITAÇÃO

(em papel timbrado do licitante)

Eu, _____, portador do CPF nº _____, na condição de representante legal de _____ (nome empresarial ou denominação), interessado em participar do Pregão Eletrônico nº 90.041/2025, Processo nº 057.00495038/2025-41, DECLARO, sob as penas da Lei, que o licitante:

a) cumpre as normas relativas à saúde e segurança no trabalho, nos termos do parágrafo único do artigo 117 da Constituição Estadual; e

b) atenderá, na data da contratação, ao disposto no artigo 5º-C e se compromete a não disponibilizar empregado que incorra na vedação prevista no artigo 5º-D, ambos da Lei nº 6.019, de 1974, com redação dada pela Lei nº 13.467, de 2017, quando o caso.

(Local e data).

(Nome/assinatura do representante legal)

ANEXO VI

MODELOS REFERENTES À VISTORIA PRÉVIA

ANEXO VI.1

DECLARAÇÃO DE CONHECIMENTO DO LOCAL E DAS CONDIÇÕES DA REALIZAÇÃO DO OBJETO DA LICITAÇÃO PRECEDIDA DE VISTORIA (elaborada pelo licitante)

Eu, _____, portador do CPF nº _____, na condição de representante legal de _____ (nome empresarial ou denominação), interessado em participar do Pregão Eletrônico nº 90.041/2025, DECLARO que o licitante tem conhecimento do(s) local(is) e das condições da realização do objeto da licitação, e **que realizou vistoria prévia no(s) local(is) em que será realizado o objeto da licitação**, colhendo todas as informações e subsídios necessários para a elaboração da sua proposta.

O licitante está ciente desde já que, em conformidade com o estabelecido no Edital, não poderá pleitear em nenhuma hipótese modificações nos preços, prazos ou condições ajustadas, tampouco alegar quaisquer prejuízos ou reivindicar quaisquer benefícios sob a invocação de insuficiência de dados ou informações sobre o(s) local(is) em que será realizado o objeto da licitação.

(Local e data)

(nome/assinatura do representante legal)

ANEXO VI.2

DECLARAÇÃO DE CONHECIMENTO DO LOCAL E DAS CONDIÇÕES DA REALIZAÇÃO DO OBJETO DA LICITAÇÃO (elaborada pelo licitante)

Eu, _____, portador do CPF nº _____, na condição de representante legal de _____ (nome empresarial ou denominação), interessado em participar do Pregão Eletrônico nº 90.041/2025, Processo nº 057.00495038/2025-41, DECLARO que o licitante tem conhecimento do(s) local(is) e das condições da realização do objeto da licitação, **que não realizou a vistoria prévia prevista no Edital** e que, mesmo ciente da possibilidade de fazê-la e dos riscos e consequências envolvidos, optou por formular a proposta sem realizar a vistoria prévia que lhe havia sido facultada.

O licitante está ciente desde já que, em conformidade com o estabelecido no Edital, não poderá pleitear em nenhuma hipótese modificações nos preços, prazos ou condições ajustadas, tampouco alegar quaisquer prejuízos ou reivindicar quaisquer benefícios sob a invocação de insuficiência de dados ou informações sobre o(s) local(is) em que será realizado o objeto da licitação.

(Local e data)

(nome/assinatura do representante legal)

ANEXO VI.3

DECLARAÇÃO DE CONHECIMENTO PLENO DAS CONDIÇÕES E PECULIARIDADES DA CONTRATAÇÃO (elaborada pelo licitante)

Eu, _____, portador do CPF nº _____, na condição de responsável técnico de _____ (nome empresarial ou denominação), interessado em participar do Pregão Eletrônico nº 90.041/2025, Processo nº 057.00495038/2025-41, DECLARO que o licitante tem conhecimento pleno das condições e peculiaridades da contratação, **que não realizou a vistoria prévia prevista no Edital** e que, mesmo ciente da possibilidade de fazê-la e dos riscos e consequências envolvidos, optou por formular a proposta sem realizar a vistoria prévia que lhe havia sido facultada.

O licitante está ciente desde já que, em conformidade com o estabelecido no Edital, não poderá pleitear em nenhuma hipótese modificações nos preços, prazos ou condições ajustadas, tampouco alegar quaisquer prejuízos ou reivindicar quaisquer benefícios sob a invocação de insuficiência de dados ou informações sobre o(s) local(is) em que será realizado o objeto da licitação.

(Local e data)

(nome/assinatura/qualificação do responsável técnico)