



EDITAL DE PREGÃO ELETRÔNICO Nº 012/2026

ID CidadES/TCE/ES: 2026.500E0600001.01.0015.

O **ESTADO DO ESPÍRITO SANTO**, por meio da Secretaria da Fazenda do Estado do Espírito Santo, doravante denominado **SEFAZ-ES**, com sede na Av. João Batista Parra, 600 - Enseada do Suá, Vitória - ES, 29050-375, realizará licitação, na modalidade **PREGÃO**, na forma **ELETRÔNICA**, para **contratação de serviços de Security Operation Center – SOC da SEFAZ/ES**, conforme processo E-Docs nº **2025-GN6G7**, nos termos da Lei 14.133/2021, do Decreto Estadual nº 5.352-R/2023, do Decreto Estadual 5.545-R/2023, das políticas do Banco Interamericano de Desenvolvimento (GN-2349-15) e demais normas aplicáveis e, ainda, de acordo com as condições estabelecidas neste Edital.

1 - DO OBJETO E DISPOSIÇÕES ESSENCIAIS

1.1 - O objeto da presente licitação é a contratação de serviços de Security Operation Center – SOC da Secretaria de Estado da Fazenda do Espírito Santo – SEFAZ/ES, conforme especificações do Termo de Referência, Anexo I deste Edital.

1.2 - A licitação será dividida em dois itens e em um grupo, formados por mais itens, conforme tabela constante do Anexo I deste Edital, facultando-se ao licitante a participação em quantos forem de seu interesse, devendo oferecer proposta para todos os itens que compõem cada grupo.

1.3 - O orçamento da Administração é sigiloso, com fundamento no art. 24 da Lei nº 14.133/2021 e art. 44 do Decreto Estadual nº 5.352-R/2023, e será tornado público após o encerramento do envio de lances.

1.4 - Data da sessão pública: 12 de novembro de 2026, às 09:00h.

1.5 - O modo de disputa será o aberto.

1.6 - Esta licitação será julgada sob o critério de menor preço por item e grupo, conforme registrado no sistema.

1.7 - As despesas decorrentes da presente licitação correrão à conta do orçamento da SEFAZ/ES, Gestão/Unidade 220101, Fontes de Recursos 500 e 754, Programa de Trabalho 10.22.101.04.123. 0050. 2151, Elementos de Despesa 4.4.90.40 e 3.3.90.40 do orçamento da SEFAZ/ES para o exercício de 2026.

2 - DA PARTICIPAÇÃO NA LICITAÇÃO

2.1 - Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

2.1.1 - Os interessados deverão atender às condições exigidas para cadastramento até o terceiro dia útil anterior à data prevista para recebimento das propostas.



2.2 - 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, excluída 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.

2.3 - É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item 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.

2.4 - A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

2.5 - Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133/2021, para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor individual - MEI, nos limites previstos na Lei Complementar nº 123/2006 e de acordo com o disposto no art. 4º, § 1º, I, e §§ 2º e 3º, da Lei 14.133/2021.

2.6 - Não poderão disputar esta licitação:

2.6.1 - aquele que não atenda às condições deste Edital e seu(s) anexo(s);

2.6.2 - pessoas jurídicas reunidas em consórcio;

2.6.3 - 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;

2.6.4 - 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;

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

2.6.6 - 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;

2.6.7 - empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404/1976, concorrendo entre si;

2.6.8 - 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;

2.6.9 - Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato servidor público estadual, independentemente de qual seja o órgão ou entidade 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 art. 9º, § 1º, da Lei nº 14.133/2021 e arts. 221, XIX, da Lei Complementar Estadual nº 46/1994 e 35 da Constituição Estadual.

2.7 - O impedimento decorrente de sanção administrativa 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.

2.8 - Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

2.9 - O disposto nos itens acima não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

3 - DA APRESENTAÇÃO DA PROPOSTA E DOCUMENTOS DE HABILITAÇÃO

3.1 - Na presente licitação, as fases de apresentação de propostas e lances e de julgamento ocorrem antes da fase de habilitação.

3.2 - Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

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

3.3.1 - está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada 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 sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

3.3.2 - não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7º, XXXIII, da Constituição Federal;

3.3.3 - 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;



3.3.4 - 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.

3.4 - O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no art. 16 da Lei 14.133/2021.

3.5 - O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no art. 3º da Lei Complementar 123/2006, 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 14.133/2021.

3.5.1 - No item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;

3.5.2 - Nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar 123/ 2006.

3.6 - A falsidade da declaração de que trata os itens acima sujeitará o licitante às sanções previstas na Lei 14.133/2021, e neste Edital.

3.7 - Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

3.8 - 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.

3.9 - 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.

3.10 - Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

3.10.1 - a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

3.10.2 - os lances serão de envio automático pelo sistema, respeitado o seu valor final mínimo ou o seu percentual de desconto máximo, caso estabelecido, e o intervalo de que trata o subitem acima.

3.10.3 - O valor final mínimo ou o percentual de desconto final máximo parametrizado possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.



3.11 - 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.

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

4 - DO PREENCHIMENTO DA PROPOSTA

4.1 - O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos campos indicados.

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

4.3 - O licitante não poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação.

4.4 - O licitante deverá formular sua proposta, considerando as disposições do Decreto nº 4.251-R, de 21 de maio de 2018, que obriga aqueles que são contratados pela Administração Pública, a efetivar a contratação de mão-de-obra necessária à execução da obra ou serviço advinda do sistema penitenciário estadual, no percentual de 6% (seis por cento) da mão-de-obra total para a execução do objeto contratual, nos termos da Lei complementar nº 879/2017.

4.5 - 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.

4.6 - 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.

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

4.8 - O prazo de validade da proposta não será inferior a 90 (noventa) dias, a contar da data de sua apresentação.

5 - DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

5.1 - 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.



5.2 - O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

5.3 - 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.

5.4 - O lance deverá ser ofertado pelo valor unitário do item.

5.5 - Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

5.6 - O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema.

5.7 - O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de 0,1% (um décimo por cento).

5.8 - O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

5.9 - O procedimento seguirá de acordo com o modo de disputa adotado.

5.10 - Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto”, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

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

5.10.2 - A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

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

5.10.4 - 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.

5.10.5 - Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

5.11 - Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto e fechado”, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.



5.11.1 - A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

5.11.2 - Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.11.3 - No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

5.11.4 - Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.11.5 - Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

5.12 - Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa "fechado e aberto", poderão participar da etapa aberta somente os licitantes que apresentarem a proposta de menor preço ou maior percentual de desconto e os das propostas até 10% (dez por cento) superiores/inferiores àquela, em que os licitantes apresentarão lances públicos e sucessivos, até o encerramento da sessão e eventuais prorrogações.

5.12.1 - Não havendo pelo menos 3 (três) propostas nas condições definidas neste item, poderão os licitantes que apresentaram as três melhores propostas, consideradas as empatadas, oferecer novos lances sucessivos.

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

5.12.3 - A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

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

5.12.5 - 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.

5.12.6 - Após o reinício previsto no subitem supra, os licitantes serão convocados para apresentar lances intermediários.



5.13 - Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

5.14 - Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

5.15 - Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

5.16 - 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.

5.17 - Quando a desconexão do sistema eletrônico para o Pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

5.18 - Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

5.19 - Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar 123/2006.

5.19.1 - Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

5.19.2 - A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

5.19.3 - Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

5.19.4 - No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

5.20 - 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.

5.20.1 - Havendo eventual empate, o critério de desempate será aquele previsto no art. 60 da Lei 14.133/2021.



5.20.2 - Esgotados os critérios de desempate previsto em lei, o desempate poderá ocorrer por sorteio, em ato público, para o qual todos os licitantes serão convocados, vedado qualquer outro processo.

5.21 - Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o Pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

5.21.1 - 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 preço máximo definido pela Administração.

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

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

5.21.4 - O Pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 5 (cinco) horas, envie a proposta, adequada ao último lance ofertado após a negociação realizada, juntamente com os Dados Complementares, observando os modelos anexos a este Edital.

5.21.5 - É facultado ao Pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

5.22 - Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

6 - DA FASE DE JULGAMENTO

6.1 - 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 14.133/2021, legislação correlata e neste Edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

6.1.1 - SICAF;

6.1.2 - Cadastro de Fornecedores do Estado do Espírito Santo – CRC/ES;

6.1.3 - Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/ceis>);

6.1.4 - Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/cnep>).

6.2 - A consulta aos cadastros será realizada em nome da empresa licitante e também em nome de seus sócios majoritários, por força do art. 12 da Lei 8.429/1992, que prevê dentre as sanções impostas ao responsável pela prática de ato de improbidade



administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

6.3 - Constatada a existência de sanção que inviabilize a participação ou contratação, o Pregoeiro reputará o licitante desclassificado, por falta de condição de participação.

6.4 - Será também desclassificada a proposta vencedora que:

6.4.1 - conter vícios insanáveis;

6.4.2 - não obedecer às especificações técnicas contidas no Termo de Referência;

6.4.3 - apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

6.4.4 - não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

6.4.5 - apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

6.5 - O licitante deverá apresentar em sua proposta econômica, sob pena de desclassificação, a declaração de que ela 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.

6.6 - Após a verificação das condições dos itens antecedentes, os documentos de habilitação serão solicitados e apreciados e, após análise, será declarado vencedor o licitante classificado em primeiro lugar, caso tenha atendido a todas as exigências do edital.

7 - DA FASE DE HABILITAÇÃO

7.1 - Os documentos previstos no Anexo I do Termo de Referência (que consta no anexo I deste edital), necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei 14.133/2021.

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

7.2 - Os documentos exigidos para fins de habilitação deverão ser enviados, em formato digital, por meio do sistema. O Licitante vencedor deverá providenciá-los no prazo de até 02 (dois) dias úteis, contados a partir da solicitação do Pregoeiro.

7.3 - 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 14.133/2021).

7.4 - 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.

7.5 - A habilitação será verificada por meio do SICAF, nos documentos por ele abrangidos.

7.6 - 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.

7.6.1 - 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.

7.7 - A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

7.8 - Os documentos exigidos para habilitação que não estejam contemplados no SICAF serão enviados por meio do sistema, em formato digital, no mesmo prazo de envio dos documentos de habilitação.

7.9 - Para fins de habilitação, a verificação pelo órgão promotor do certame nos sítios oficiais de órgãos e entidades emissoras de certidões constitui meio legal de prova.

7.10 - Se a proposta não for aceitável, ou se o licitante não atender às exigências de habilitação, ou se recusar a assinar o contrato, o Pregoeiro examinará a oferta subsequente e a respectiva documentação de habilitação, na ordem de classificação, e assim sucessivamente, até a apuração de uma que atenda às exigências do edital.

7.11 - Nas hipóteses previstas no item anterior, o Pregoeiro poderá negociar diretamente com o proponente para que seja obtido melhor preço, tendo sempre como parâmetro a menor oferta apresentada no certame.

7.12 - Em se tratando de consórcio, os documentos de habilitação deverão ser apresentados em relação a cada empresa consorciada, observando o item sobre participação em consórcio.

8 - DOS RECURSOS

8.1 - 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 14.133/2021.

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

8.3 - Quando se tratar de decisão sobre o julgamento das propostas ou de habilitação ou inabilitação de licitante, o Pregoeiro comunicará aos licitantes, no mínimo com vinte e quatro horas de antecedência, por meio do sistema no qual a licitação foi realizada, acerca da abertura do prazo para manifestação imediata de que tratam os subitens seguintes:



8.3.1 - a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

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

8.3.3 - o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

8.3.4 - na hipótese de adoção da inversão de fases prevista no § 1º do art. 17 da Lei 14.133/2021, o prazo para apresentação das razões recursais será iniciado na data de intimação da ata de julgamento.

8.4 - Os recursos deverão ser encaminhados em campo próprio do sistema.

8.5 - 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 recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

8.6 - Os recursos interpostos fora do prazo não serão conhecidos.

8.7 - 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.

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

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

8.10 - Os autos do processo permanecerão com vista franqueada aos interessados no sistema de processo eletrônico E-Docs, no Acesso Cidadão (<https://acessocidadao.es.gov.br/>).

9 - DA ADJUDICAÇÃO E DA FORMALIZAÇÃO DA CONTRATAÇÃO

9.1 - Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório e adjudicará o objeto.

9.2 - Após a homologação, o adjudicatário será convocado para assinar o contrato ou receber o instrumento equivalente no prazo de até 05 (cinco) dias úteis.

9.2.1 - Considerando a adoção do processo eletrônico E-Docs, a assinatura será realizada mediante usuário e senha (assinatura eletrônica) no Acesso Cidadão (<https://acessocidadao.es.gov.br/>) ou através de certificado digital, conforme acordado entre as partes.

9.2.2 - Não poderão ser utilizadas formas diferentes de assinatura em um mesmo documento.



9.2.3 - No caso de assinatura eletrônica, as partes deverão providenciar uma conta verificada no Acesso Cidadão, conforme instruções contidas no endereço: <https://compras.es.gov.br/conta-verificada>.

9.3 - A Administração poderá prorrogar o prazo fixado no item anterior, por igual período, nos termos do art. 90, § 1º, da Lei 14.133/2021, quando solicitado pelo licitante vencedor, durante o seu transcurso, e desde que ocorra motivo justificado, aceito pelo ente promotor do certame.

9.4 - Para a formalização da contratação, será exigida a comprovação das condições de habilitação consignadas neste Edital, as quais deverão ser mantidas pelo licitante durante a vigência do contrato.

10 - DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

10.1 - Comete infração administrativa, nos termos do art. 155 da Lei 14.133/2021, o licitante ou adjudicatário que, com dolo ou culpa:

10.1.1 - deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo Pregoeiro durante o certame;

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

10.1.2.1 - não enviar a proposta adequada ao último lance ofertado ou após a negociação;

10.1.2.2 - recusar-se a enviar o detalhamento da proposta quando exigível;

10.1.2.3 - pedir para ser desclassificado quando encerrada a etapa competitiva;

10.1.2.4 - deixar de apresentar amostra;

10.1.2.5 - apresentar proposta ou amostra em desacordo com as especificações do edital;

10.1.3 - não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta, ou recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

10.1.4 - apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

10.1.5 - fraudar a licitação;

10.1.6 - comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

10.1.6.1 - agir em conluio ou em desconformidade com a lei;

10.1.6.2 - induzir deliberadamente a erro no julgamento;



- 10.1.6.3 - apresentar amostra falsificada ou deteriorada;
- 10.1.7 - praticar atos ilícitos com vistas a frustrar os objetivos da licitação;
- 10.1.8 - praticar ato lesivo previsto no art. 5º da Lei 12.846/2013;
- 10.2 - Reputar-se-á comportamento inidôneo, exemplificativamente, os tipificados nos arts. 337-F a 337-M do Código Penal e no art. 5º da Lei 12.846/2013, bem como a declaração falsa quanto às condições de participação e quanto ao enquadramento como ME/EPP.
- 10.3 - O licitante ou adjudicatário que cometer qualquer das infrações discriminadas ficará sujeito, sem prejuízo da responsabilidade penal e civil, às seguintes sanções:
- 10.3.1 - multa de 0,5% até 30% (trinta por cento) sobre o valor estimado para os lotes em que participou o licitante;
- 10.3.2 - impedimento de licitar e contratar; e
- 10.3.3 - declaração de inidoneidade para licitar ou contratar.
- 10.4 - As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.
- 10.5 - A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa, observando-se além da disciplina legal e regulamentar, o disposto no Termo de Contrato e/ou no Termo de Referência quanto ao procedimento e outras condições.
- 10.6 - As sanções por atos praticados durante a execução do contrato estão previstas no Termo de Contrato e/ou no Termo de Referência.

11 - DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

- 11.1 - Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da legislação ou para solicitar esclarecimento sobre os seus termos, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.
- 11.2 - A impugnação e o pedido de esclarecimento poderão ser protocolizados no órgão realizador do certame, de 9 às 18 horas, ou enviadas para o e-mail licitacao@sefaz.es.gov.br. Somente serão aceitas impugnações protocolizadas se assinadas pelo impugnante.
- 11.3 - As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.
- 11.3.1 - A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo Pregoeiro, nos autos do processo de licitação.



11.4 - Caso o Pregoeiro decida pela improcedência da impugnação ao ato convocatório, deverá encaminhar o processo para a Autoridade Competente, a quem competirá, nesse caso, ratificar ou alterar a decisão do Pregoeiro.

11.5 - Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

11.6 - Qualquer modificação no edital será divulgada pelo mesmo instrumento de publicação em que se deu o texto original, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

11.7 - A resposta à impugnação ou ao pedido de esclarecimento será divulgada por publicação em campo do Sistema de Compras do Governo Federal, no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame, ficando os interessados obrigados a acessar o endereço para a obtenção das informações prestadas.

12 - DAS DISPOSIÇÕES FINAIS

12.1 - Será divulgada ata da sessão pública no sistema eletrônico.

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

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

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

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

12.6 - 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.

12.7 - 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.

12.8 - 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.

12.9 - Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.



12.10 - O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e no Sistema de Compras do Governo Federal (www.gov.br/compras).

12.11 - Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

Anexo I – Termo de Referência e seus anexos;

Anexo II - Modelos do Edital; e

Anexo III – Minuta de Termo de Contrato.

Vitória, 26 de outubro de 2026.

Angelica Tonel Abrantes Coelho
Agente de Contratação/Pregoeira



ANEXO I – TERMO DE REFERÊNCIA

TERMO DE REFERÊNCIA PARA CONTRATAÇÃO DE SECURITY OPERATION CENTER - SOC



TERMO DE REFERÊNCIA

OBJETO: Security Operation Center - SOC para a Sefaz/ES.

IDENTIFICAÇÃO

IDENTIFICAÇÃO			
Un. Gestora:	Secretaria de Estado da Fazenda		
Área Requisitante:	Gerência de Tecnologia – GETEC		
Responsáveis:	Ualter Regis Barbosa, Luiz Carlos Lessa, Alexia Spelta Colombo		
Data de Elaboração	26/10/2026	Versão	6.0

HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
22/12/2025	1.0	Versão Preliminar do TR	Equipe de Planejamento de Contratação
26/06/2026	2.0	Versão após parecer STD	Equipe de Planejamento de Contratação
31/07/2026	3.0	Versão após ajustes SUGET	Equipe de Planejamento de Contratação
06/08/2026	4.0	Ajustes para adequação ao SIADES	Equipe de Planejamento de Contratação
30/09/2026	5.0	Versão após ajustes orçamentários	Equipe de Planejamento de Contratação
26/10/2026	6.0	Versão final para edital	Equipe de Planejamento de Contratação



1. OBJETO

1.1. Contratação de empresa especializada para prestação de serviços de Security Operation Center - SOC da Secretaria Estadual da Fazenda do Espírito Santo - SEFAZ/ES.

LOTE	ITEM	DESCRIÇÃO	TECNOLOGIA	MÉTRICA	QUANTIDADE	CATSER	COD.SIADES
1	1	EMS E5 SU EMS E3 Per User	EMS	Usuários	800	26077	11248

LOTE	ITEM	DESCRIÇÃO	TECNOLOGIA	MÉTRICA	QUANTIDADE	CATSER	COD.SIADES
2	2	Solução de Microsegmentação de rede	MICROSEG.	Workloads	1.000	26077	11248

LOTE	ITEM	DESCRIÇÃO	TECNOLOGIA	MÉTRICA	QUANTIDADE	CATSER	COD.SIADES
3	3	Solução de Gestão de Vulnerabilidades com foco em Risco e Identidade	GV	Ativos	1.800	26077	11248
	4		GVAD	Usuários	1.000	26077	11248
	5		RISK	Solução	1	26077	11248
	6	Solução de Monitoramento Avançado, Resposta a Incidentes Automatizada, Hiperautomação, Soluções aplicadas a Firewall e teste automatizado	SIEM	GB/dia	200	26077	11248
	7		DRPs	CNPJ	1	26077	11248
	8		PTA	Solução	1	26077	11248
	9	Solução de Gestão de disponibilidade	SecOps	Ativos	2.500	26077	11248
	10		Host/URL/API	Workloads	500	26077	11248
	11		SMG / SEC. AWARENESS	Usuários	1.000	26077	11248
	12	Serviços de implantação das Soluções descritas nos Itens 3 a 12	DLP	Usuários	1.000	26077	11248
	13		SERVIÇOS	Escopo Fechado	1	26972	S26972
	14		SERVIÇOS	Meses	24	27022	S27340
	15	Serviços de Monitoramento da adoção às melhores práticas de Segurança da Informação	PGV	CNPJ	1	27260	11248
	16		BIA	CNPJ	1	27260	11248
	17		PRI	CNPJ	1	27260	11248

1.2. As alterações introduzidas no Termo de Referência em relação às versões anteriores do planejamento decorreram do refinamento técnico e orçamentário da solução após a consolidação do inventário, da separação das soluções já implantadas e licenciáveis autonomamente e da necessidade de concentrar, em lote específico, as soluções e serviços interdependentes do núcleo operacional do SOC. Foram igualmente ajustados os marcos de implantação, a vigência e os critérios de medição para compatibilizar a execução progressiva, a continuidade operacional e o pagamento por entregas aceitas. A memória detalhada das alterações, com indicação da versão, conteúdo alterado e respectiva motivação, integra os autos do processo.

1.3. O parcelamento do objeto em lotes distintos observa a natureza técnica e funcional dos itens que compõem a contratação, preservando, ao mesmo tempo, a ampliação da competitividade e a lógica de integração necessária à adequada implantação e operação do Centro de Operações de Segurança - SOC. A contratação integrada do núcleo operacional de segurança permanece essencial para assegurar interoperabilidade entre



as soluções, padronização de processos, correlação de eventos, resposta coordenada a incidentes e responsabilização clara pela operação do ambiente de segurança. Contudo, determinados itens correspondem a soluções que a SEFAZ/ES já possui implantadas em seu ambiente tecnológico, demandando, nesta contratação, apenas a entrega, renovação, ampliação ou disponibilização de licenciamento, sem necessidade de nova implantação técnica ou integração complexa aos mesmos moldes dos demais serviços.

- 1.3.1. A separação desses itens em lotes específicos justifica-se porque sua contratação conjunta com serviços de implantação, operação ou sustentação poderia restringir indevidamente a competitividade, elevar custos sem correspondente benefício técnico e dificultar a obtenção da proposta mais vantajosa para a Administração. Quando o objeto consiste apenas no fornecimento de licenças para solução já existente e operacional no ambiente da SEFAZ/ES, não há dependência direta de serviços de implantação ou de reestruturação do ambiente, sendo possível sua contratação de forma autônoma, sem prejuízo à integração global do SOC.
- 1.3.2. Dessa forma, o parcelamento em lotes não representa fragmentação indevida do objeto, mas sim medida de racionalização técnica e econômica, voltada a diferenciar os itens que exigem implantação, integração, operação contínua e responsabilidade unificada daqueles que se limitam ao licenciamento de soluções previamente implantadas. Tal arranjo preserva a contratação integrada do núcleo operacional do SOC, evita sobreposição de serviços, favorece a ampla concorrência, permite melhor precificação dos componentes e assegura que a Administração contrate cada parcela do objeto de acordo com sua real necessidade, sem comprometer a segurança, a governança e a continuidade operacional do ambiente tecnológico da SEFAZ/ES.
- 1.3.3. A contratação será estruturada por lotes, com o objetivo de ampliar a competitividade, permitir a participação de fornecedores especializados e assegurar melhor aderência entre a natureza de cada parcela do objeto e o respectivo modelo de contratação. Essa diretriz aplica-se especialmente às soluções que já se encontram implementadas no ambiente tecnológico da SEFAZ/ES, para as quais a demanda principal consiste na renovação, ampliação ou disponibilização de licenças, sem necessidade de nova implantação complexa ou de transferência integral da responsabilidade operacional do SOC.
- 1.3.4. Sem prejuízo do parcelamento, a parcela de maior relevância técnica e econômica do objeto, representada pelo lote que reúne os serviços e soluções estruturantes do SOC, será contratada mediante grupamento de itens tecnicamente interdependentes. Tal agrupamento justifica-se pela sinergia operacional, necessidade de interoperabilidade entre ferramentas, correlação unificada de eventos, padronização de processos de detecção e resposta, integração com a operação 24x7 e concentração da responsabilidade técnica perante a Administração.
- 1.3.5. A divisão em três lotes foi definida após análise de autonomia técnica, mercado fornecedor, responsabilidade operacional e custo de coordenação. O Lote 1 abrange exclusivamente o upgrade de licenciamento Microsoft EMS já implantado, sem serviços de implantação. O Lote 2 abrange a continuidade do licenciamento da plataforma de microsegmentação já implantada, preservando políticas e integrações existentes. O Lote 3 reúne as soluções dos itens 3 a 12, a implantação do item 13,



a operação do item 14 e os monitoramentos dos itens 15 a 17, pois esses componentes compartilham fontes de dados, correlação de eventos, playbooks, processos 24x7, critérios de desempenho e responsabilidade integrada. A segregação dos Lotes 1 e 2 amplia a competição e evita remunerar implantação inexistente; o agrupamento do Lote 3 reduz interfaces contratuais críticas, riscos de incompatibilidade, duplicidade de responsabilidades e custos de coordenação. A escolha deverá ser reavaliada caso a pesquisa de mercado evidencie redução relevante da competição no Lote 3.

- 1.3.6. Dessa forma, o modelo adotado combina parcelamento competitivo com agrupamento técnico da parcela nuclear do SOC. Os lotes autônomos favorecem a ampla concorrência nos itens de licenciamento ou em soluções já implantadas, enquanto o lote agrupado preserva a integridade operacional do serviço, evita dispersão de responsabilidades, reduz riscos de incompatibilidade entre componentes e assegura à SEFAZ/ES um ponto claro de responsabilização pela implantação, integração, sustentação e operação do núcleo crítico de segurança cibernética.
- 1.4. Os serviços objeto desta contratação são caracterizados como comuns conforme justificativa constante do Estudo Técnico Preliminar.
- 1.5. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 5.352-R/2023.
- 1.6. A utilização das referências nominais não decorre de preferência por fabricante, mas da necessidade de preservação da continuidade operacional, da compatibilidade tecnológica e do aproveitamento dos investimentos já realizados pela Administração. A substituição dessas plataformas exigiria a reconstrução de políticas, integrações e processos já implantados, gerando custos de transição, riscos operacionais e potencial descontinuidade dos serviços, razão pela qual a solução foi enquadrada nas hipóteses de padronização e compatibilidade técnica.
- 1.7. O prazo de vigência da contratação, considerado o cronograma de execução desenvolvido, será de 24 (vinte e quatro) meses, contados da data da publicação do contrato no PNCP, podendo ser renovado a critério da administração, observando o disposto neste Termo de Referência.
 - 1.7.1. A vigência de 24 (vinte e quatro) meses mostra-se adequada à natureza, à complexidade e ao ciclo de implantação e operação do SOC, pois permite que os investimentos iniciais em configuração, integração, parametrização, transferência de conhecimento e estabilização das soluções sejam aproveitadas por período suficiente para a obtenção dos resultados esperados. Esse prazo também assegura continuidade ao monitoramento e à resposta a incidentes, favorece a maturação dos processos, a calibração das regras e a redução de falsos positivos, além de preservar o conhecimento acumulado sobre o ambiente tecnológico da SEFAZ/ES. Sob o aspecto econômico, a duração proposta dilui os custos de implantação e transição, reduz a frequência de procedimentos administrativos e de substituições de fornecedor e possibilita condições comerciais mais vantajosas, sem afastar o acompanhamento permanente do desempenho, da vantajosidade e do cumprimento das obrigações contratuais pela Administração.
 - 1.7.2. O prazo de vigência foi definido em alinhamento aos ciclos usualmente praticados pelos fornecedores para suporte, garantia, atualização tecnológica e manutenção



evolutiva das soluções contratadas. A adoção de prazo compatível com esses ciclos permite maior previsibilidade na prestação dos serviços, reduz riscos de descontinuidade de suporte durante a execução contratual e favorece condições comerciais mais vantajosas, uma vez que dilui custos de implantação, integração, operação assistida e sustentação ao longo de período suficiente para aproveitamento econômico da solução. Dessa forma, o prazo contribui para a eficiência econômica do contrato, evitando renovações excessivamente frequentes, retrabalho técnico, perda de conhecimento operacional e custos adicionais decorrentes de transições prematuras entre fornecedores ou plataformas.

1.7.3. Ademais a evolução de um SOC ocorre de forma progressiva, exigindo tempo para o aprimoramento de processos, integrações e capacidades analíticas, o que torna inadequados contratos de curta duração que interrompam esse ciclo de maturidade do projeto. Há uma curva de aprendizado relevante na compreensão do ambiente, calibração de alertas e redução de falsos positivos, cujo aproveitamento pleno demanda um horizonte contratual mais longo. Por fim, a natureza contínua e crítica do SOC requer estabilidade na prestação do serviço, evitando perda de conhecimento, descontinuidade no monitoramento e aumento de riscos operacionais.

1.7.4. Além disso, foi considerado o ganho de escala obtido com a diluição dos custos fixos ao longo do contrato, bem como a amortização dos valores pagos a título de implantação por um período mais longo.

1.8. O ciclo de vida estimado da contratação é de 10 (dez) anos, observados os limites legais aplicáveis, considerando a natureza contínua e permanente da necessidade de proteção do ambiente tecnológico da SEFAZ/ES. Esse ciclo de vida não se confunde com a vigência contratual inicial, que será de 24 (vinte e quatro) meses. Eventual continuidade da solução após esse período dependerá da adoção do instrumento jurídico cabível, conforme a legislação vigente, mediante nova análise de conveniência, oportunidade, vantajosidade e disponibilidade orçamentária pela Administração.

1.9. Em caso de divergência entre as especificações do objeto descritas no SIADES – Sistema Integrado Administrativo Digital do Espírito Santo ou no ComprasGov, e as especificações técnicas constantes neste Termo de Referência, o licitante deverá obedecer a este último, pois ele contém as especificações adequadas para a demanda a ser suprida. O catálogo de materiais servirá apenas como identificação dos itens licitados e seus respectivos códigos.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A Secretaria de Estado da Fazenda do Espírito Santo (SEFAZ-ES) desempenha papel central na sustentação econômica do Estado, atuando como guardião das informações tributárias, fiscais, contábeis, financeiras e das receitas públicas que viabilizam a continuidade das políticas governamentais. O ambiente digital que suporta essas funções é, por sua natureza, altamente sensível, complexo e estratégico. Nesse contexto, a crescente sofisticação e frequência dos ataques cibernéticos voltados especificamente para órgãos fazendários e instituições financeiras elevam exponencialmente os riscos à integridade, disponibilidade e confidencialidade dos sistemas da SEFAZ-ES. Assim, torna-se urgente a adoção de mecanismos avançados de defesa cibernética, entre os quais se destaca a implantação de um Centro de



Operações de Segurança (SOC) como elemento nuclear de proteção, monitoramento e resposta a incidentes.

- 2.2.** A SEFAZ/ES administra diariamente um volume expressivo de informações que vão muito além de dados cadastrais. O órgão lida com informações fiscais protegidas por sigilo legal, registros de arrecadação, documentos fiscais eletrônicos, dados contábeis e financeiros, transações de alto impacto e informações pessoais sensíveis de contribuintes e servidores. Qualquer comprometimento desses ativos informacionais gera repercussões não apenas internas, mas também externas, afetando diretamente a credibilidade do Estado, a confiança do contribuinte, a segurança jurídica das operações comerciais e a própria arrecadação que financia serviços essenciais como saúde, educação, segurança pública e infraestrutura.
- 2.3.** O cenário global e nacional demonstra um avanço significativo das ameaças cibernéticas que têm como alvo prioritário órgãos responsáveis por receitas públicas. Governos estaduais e federais, bem como instituições arrecadatórias de países desenvolvidos, já foram vítimas de ataques que provocaram paralisações de serviços, vazamento de dados sigilosos e prejuízos financeiros vultosos. A natureza crítica do ambiente fazendário e o valor estratégico de seus dados tornam tais órgãos alvos preferenciais para grupos criminosos especializados em ransomware, extorsão digital, sequestro de dados e ataques direcionados à manipulação de informações.
- 2.4.** A inexistência, na SEFAZ-ES, de um serviço estruturado de monitoramento contínuo, análise de eventos e resposta a incidentes gera uma lacuna significativa na capacidade institucional de identificar e neutralizar ameaças de forma tempestiva. Sem um SOC, a Secretaria opera de forma essencialmente reativa, dependendo de notificações tardias, percepções empíricas de anomalias ou da ocorrência de falhas efetivas para então iniciar a investigação e mitigação de incidentes. Essa abordagem aumenta o tempo de exposição a ataques e limita a eficácia das medidas de contenção, o que é particularmente perigoso em um ambiente crítico que precisa operar sem interrupções.
- 2.5.** A criticidade dos sistemas sob responsabilidade da SEFAZ-ES exige níveis elevados de segurança e disponibilidade. Sistemas como os de arrecadação tributária, emissão de documentos fiscais eletrônicos, folha de pagamento, gestão contábil e financeira, auditoria fiscal e controle de arrecadação são utilizados 24 horas por dia, por milhares de contribuintes, servidores e órgãos parceiros. Qualquer indisponibilidade, mesmo que breve, pode resultar em interrupção da emissão de notas fiscais, falhas na arrecadação, atrasos em repasses a municípios, paralisação de pagamentos e prejuízos estimados em milhões de reais. Em situações extremas, um ataque bem-sucedido pode suspender completamente a atividade econômica do Estado, com impactos diretos e imediatos à população.
- 2.6.** A paralisação dos sistemas de arrecadação impede a entrada de receitas, afetando diretamente a capacidade do governo de financiar saúde, educação, segurança e infraestrutura. A perda de receita não é apenas um problema operacional, mas um dano direto ao bem-estar social. A indisponibilidade dos sistemas de fiscalização e de controle impede a SEFAZ de atuar contra a sonegação fiscal, o que gera concorrência desleal e diminui a justiça tributária. A eficiência na fiscalização garante que todos os setores da sociedade contribuam de forma equitativa. A falha em um sistema crítico causa incerteza e perda de confiança por parte dos cidadãos e das empresas, que dependem da SEFAZ para operar legalmente. A previsibilidade e a estabilidade dos sistemas são essenciais para um ambiente de negócios saudável e para a credibilidade da administração pública.



A contratação desses serviços garante uma abordagem integrada e mais segura. As justificativas técnicas e tecnológicas para essa escolha se somam às razões de interesse público.

- 2.7.** A criação de um SOC endereça de forma precisa essa necessidade ao oferecer monitoramento contínuo (24x7x365), análise avançada de logs e eventos, identificação precoce de tentativas de violação, resposta orquestrada e automática a incidentes e um conjunto de serviços especializados de inteligência cibernética. Enquanto uma estrutura tradicional de segurança depende da ação humana e responde de forma pontual, um SOC opera com camadas automáticas e inteligentes de detecção, utilizando ferramentas como SIEM, SOAR, inteligência artificial, análise comportamental e bases de reputação global, tornando possível identificar ameaças invisíveis aos sistemas convencionais.
- 2.8.** A necessidade de monitoramento constante decorre do fato de que grande parte dos ataques modernos não se manifesta de forma explícita. A movimentação lateral silenciosa, a implantação de backdoors, a exfiltração discreta de dados, o acesso indevido por credenciais comprometidas e o uso de técnicas avançadas de persistência são práticas comuns em ataques direcionados, especialmente em ambientes governamentais. Tais ataques podem permanecer ocultos por semanas ou meses, comprometendo gradualmente sistemas e colhendo informações valiosas. Um SOC é a estrutura ideal para detectar esse tipo de atuação furtiva.
- 2.9.** Adicionalmente, o ambiente da SEFAZ-ES inclui milhares de endpoints, servidores críticos, redes internas diversificadas, integração com serviços em nuvem e conectividade com múltiplos órgãos públicos e empresas privadas. Essa complexidade exige uma visão centralizada sobre o tráfego de rede, sobre os eventos de autenticação, sobre o comportamento dos usuários e servidores, e sobre padrões anômalos. Sem um SOC, as equipes técnicas operam com capacidades limitadas de correlação de eventos, especialmente diante do volume cada vez maior de logs produzidos pelos sistemas.
- 2.10.** Do ponto de vista da proteção do sigilo fiscal e da privacidade de dados pessoais, a ausência de mecanismos de monitoramento, registro e resposta imediata constitui um risco direto à conformidade com normas como o Código Tributário Nacional, a Lei Geral de Proteção de Dados (LGPD), a Política Estadual de Segurança da Informação e padrões internacionais como a ISO 27001 e as recomendações do NIST. Um incidente envolvendo dados fiscais possui gravidade jurídica e institucional elevada, exigindo respostas rápidas e documentação detalhada, elementos que só podem ser garantidos por uma estrutura SOC madura.
- 2.11.** A contratação de um SOC também permite à SEFAZ-ES transicionar de um modelo de segurança centrado em ferramentas isoladas para uma abordagem integrada, inteligente e coordenada, onde soluções como firewall, antivírus, EDR, SIEM, CASB, SWG, PAM e microsegmentação trabalham de forma unificada e orquestrada. A integração reduz drasticamente o tempo de detecção (MTTD) e o tempo de resposta (MTTR), aumentando a eficácia das barreiras defensivas e reduzindo a probabilidade de incidentes graves.
- 2.12.** Entre as ameaças modernas mais críticas estão os ataques direcionados ao Active Directory, principal sistema de identidades utilizado por órgãos públicos. O AD é frequentemente o alvo inicial de grupos de ransomware, que o comprometem para obter privilégios, mover-se lateralmente e sequestrar serviços. O SOC desempenha papel central no monitoramento de sinais de comprometimento, no controle de tentativas



suspeitas de elevação de privilégios, na análise de comportamentos anômalos e na mitigação de eventos antes que causem danos irreversíveis.

- 2.13.** O e-mail continua sendo o principal vetor de ataque em nível mundial. Phishing direcionado, spoofing, engenharia social e campanhas maliciosas sofisticadas têm causado prejuízos financeiros expressivos a instituições públicas. O SOC complementa soluções tradicionais de e-mail ao fornecer detecção avançada, análise de padrões comportamentais, isolamento de anomalias e correlação com campanhas globais, aumentando significativamente a capacidade de proteção dos servidores da SEFAZ.
- 2.14.** A implantação de um SOC também permite o fortalecimento da segurança da infraestrutura de rede, incorporando práticas modernas como microsegmentação, análise de tráfego leste-oeste, identificação de movimentações laterais e contenção dinâmica de ameaças. Essa abordagem reduz drasticamente a superfície de ataque e impede que um invasor quebre uma barreira e acesse sistemas críticos internos.
- 2.15.** Outro ponto fundamental é a capacidade de o SOC fornecer visibilidade completa sobre a postura de segurança da SEFAZ-ES, facilitando auditorias, instruções de processos, respostas a órgãos de controle, elaboração de relatórios de continuidade e atualização permanente do gerenciamento de riscos. A rastreabilidade e o registro centralizado de eventos e incidentes permitem maior transparência e integridade na gestão de segurança da informação.
- 2.16.** Os quantitativos estabelecidos para os itens foram dimensionados com base na capacidade atualmente utilizada no ambiente tecnológico da SEFAZ/ES, refletindo a quantidade efetiva de usuários, ativos e workloads abrangidos pelas soluções, bem como o volume diário de dados, medido em GB/dia, já processado pelos mecanismos de monitoramento. Esses parâmetros representam a demanda operacional existente e foram adotados para assegurar cobertura adequada do ambiente, continuidade dos serviços e compatibilidade com o consumo real, evitando tanto o subdimensionamento, que poderia comprometer a proteção e o desempenho, quanto o superdimensionamento, que resultaria em custos desnecessários para a Administração.
- 2.17.** Do ponto de vista econômico, a contratação de um SOC não deve ser vista como custo, mas como investimento estratégico que reduz drasticamente despesas futuras com recuperação de incidentes, indenizações, paralisações de sistemas e danos reputacionais. O custo médio de um ataque de ransomware contra instituições públicas pode ultrapassar milhões de reais, considerando resgate, perda de dados, interrupção de serviços, trabalho emergencial e reconstrução de ambientes. Investir em SOC previne impactos incomparavelmente maiores.
- 2.18.** Além disso, a adoção de um SOC gera eficiência operacional, permitindo que equipes internas de TI e segurança dediquem-se às atividades estratégicas, à governança, à análise de riscos e ao planejamento tecnológico, enquanto o monitoramento contínuo fica a cargo de especialistas dedicados. Trata-se, portanto, de uma medida que otimiza o uso dos recursos humanos, reduz sobrecarga operacional e aumenta a capacidade de resposta organizacional.
- 2.19.** No campo da governança, a contratação de um SOC fortalece a maturidade institucional da SEFAZ, aproximando-a dos padrões mais elevados de gestão de segurança da informação adotados por órgãos federais, instituições financeiras e empresas de missão crítica. A iniciativa está alinhada ao movimento global de



transformação digital segura, promovendo confiança, transparência e conformidade regulatória.

2.20. A contratação também contribui para elevar a confiabilidade dos serviços digitais prestados ao contribuinte, reduzindo a probabilidade de indisponibilidades e aumentando a percepção de segurança sobre os portais, sistemas e serviços oferecidos pela SEFAZ. Isso reforça a imagem institucional e demonstra compromisso com a proteção do patrimônio informacional do Estado.

2.21. A contratação em análise busca atender a esse cenário por meio da implementação de soluções integradas de segurança da informação, capazes de reforçar a proteção dos ativos digitais da SEFAZ/ES, ampliar a resiliência cibernética e assegurar a continuidade das atividades fiscais. Os principais objetivos estratégicos dessa iniciativa incluem:

2.21.1. Modernização da Defesa Cibernética: Utilização de tecnologias avançadas de monitoramento, detecção e resposta a incidentes, com recursos de automação que possibilitem maior agilidade na identificação e mitigação de riscos.

2.21.2. Resiliência Operacional: Estruturação de relatórios de continuidade de negócios e de recuperação em caso de incidentes, garantindo a manutenção dos serviços públicos relacionados à arrecadação e fiscalização.

2.21.3. Proteção contra Ameaças Avançadas: Adoção de soluções específicas contra ransomware, exfiltração de dados e ataques direcionados ao ambiente de identidades, com atenção especial a sistemas críticos como o Active Directory.

2.21.4. Segurança Focada no Usuário: Reforço dos controles aplicados ao e-mail, principal vetor de ataque, aliado a programas de conscientização que aumentem a capacidade de reação dos servidores frente a tentativas de fraude e engenharia social.

2.21.5. Segurança da Infraestrutura de Rede: Implantação de técnicas de microsegmentação que reduzam a superfície de ataque, dificultem movimentações laterais e ampliem a visibilidade sobre o tráfego interno.

2.21.6. Conformidade e Regulamentação: Adequação às exigências legais e normativas, como a Lei Geral de Proteção de Dados (LGPD), a ISO 27001 e as diretrizes do NIST, fortalecendo o nível de conformidade da instituição.

2.22. Dessa forma, a iniciativa contribui para o fortalecimento da governança em segurança da informação na SEFAZ/ES, construindo um ambiente mais seguro, automatizado e alinhado às melhores práticas de mercado. Além de reduzir riscos operacionais e de reputação, a medida promove maior eficiência na gestão tributária, eleva a confiabilidade dos serviços digitais disponibilizados ao contribuinte e reafirma a responsabilidade institucional no tratamento de informações estratégicas do Estado. Nesse contexto, a contratação de uma empresa para prestação de serviços de Centro de Operações de Segurança (SOC) surge como uma ação fundamental para a proteção do patrimônio informacional, a continuidade dos serviços e a preservação da confiança da sociedade na administração pública.

2.23. O projeto tem como objetivo contratar uma empresa especializada para prover serviços de SOC, contemplando monitoramento contínuo, análise de incidentes e respostas rápidas a eventos de segurança. A iniciativa busca implementar ferramentas avançadas de detecção, correlação e mitigação de riscos, que permitam não apenas reagir, mas também antecipar possíveis vulnerabilidades. Dessa forma, a instituição



assegura maior robustez em seus processos, preserva a integridade de seus dados e promove um ambiente confiável para a execução de suas atividades estratégicas.

- 2.24.** A implantação de um Centro de Operações de Segurança (SOC) por meio de contratação de empresa especializada representa uma medida estratégica para garantir a proteção contínua das informações e ativos tecnológicos da SEFAZ-ES. Trata-se de um investimento orientado pela economicidade e pela eficiência operacional, que visa substituir múltiplas soluções pontuais e iniciativas isoladas de segurança por um modelo integrado, escalável e de alta performance. Com isso, a SEFAZ-ES passa a contar com um serviço abrangente e padronizado, capaz de atuar de forma preventiva e reativa frente a incidentes de segurança, reduzindo significativamente o risco de interrupções e prejuízos operacionais.
- 2.25.** Em que pese a separação em lotes dos licenciamentos já ativos, com o objetivo de ampliar a concorrência, a contratação do SOC unificada proporciona racionalização do parque tecnológico e da infraestrutura necessária para o monitoramento e defesa cibernética. A integração de ferramentas como SIEM, EDR, antivazamento de dados (DLP), gestão de vulnerabilidades, microsegmentação e proteção avançada de e-mail sob um mesmo contrato garante interoperabilidade, redução de redundâncias e eficiência na correlação de eventos. Além disso, o modelo de serviço gerenciado transfere ao contratado a responsabilidade pela manutenção, atualização e substituição de equipamentos e sistemas, eliminando a necessidade de aquisição e gestão direta de ativos por parte da Administração.
- 2.26.** A implantação integrada dos serviços descritos neste Estudo Técnico Preliminar, sob a governança de um Centro de Operações de Segurança (SOC), visa estabelecer um ecossistema unificado de proteção cibernética, capaz de oferecer visibilidade total, resposta automatizada e gestão de riscos contínua sobre o ambiente tecnológico da instituição.
- 2.27.** De forma geral, a integração dos serviços — como gestão de vulnerabilidades, monitoramento avançado, resposta a incidentes, proteção contra ransomware, microsegmentação e conscientização de usuários — permitirá a criação de uma camada de defesa coordenada e inteligente, operando de maneira preventiva, proativa e reativa conforme o contexto das ameaças.
- 2.28.** Entre os principais benefícios e resultados esperados, destacam-se:
- 2.28.1.** Visão centralizada de segurança e risco: a consolidação de informações oriundas de múltiplas fontes (redes, endpoints, identidades, e-mails, aplicações e usuários) permitirá a correlação automatizada de eventos, possibilitando a detecção precoce de incidentes e a priorização de respostas conforme o impacto no negócio. A operação integrada dos serviços de gestão de vulnerabilidades, monitoramento avançado, resposta a incidentes, proteção de e-mail, microsegmentação e gestão de disponibilidade proporcionará uma visão unificada do ambiente tecnológico, consolidando dados de múltiplas fontes em uma plataforma de observabilidade e análise centralizada (SIEM/SOC). Essa integração elimina silos de informação e permite a correlação automatizada de eventos, favorecendo a identificação de cadeias de ataque e anomalias em tempo real.
- 2.28.2.** Resposta rápida e automatizada a incidentes: com o uso de soluções de SIEM, XDR e orquestração (SOAR), será possível reduzir significativamente o tempo médio de detecção (MTTD) e o tempo médio de resposta (MTTR), por meio de



playbooks automatizados e integração entre ferramentas. A utilização de ferramentas de gestão de vulnerabilidades com foco em risco e identidade possibilitará a priorização de correções e controles com base no impacto real ao negócio, considerando a criticidade dos ativos e perfis de usuários. Essa abordagem orientada a risco favorece uma gestão mais eficiente dos recursos, reduzindo significativamente a superfície de ataque e fortalecendo a postura de segurança institucional.

- 2.28.3. Gestão contínua de vulnerabilidades e riscos: os serviços de gestão de vulnerabilidades e risco (GV, RISK, BIA) permitirão identificar, classificar e corrigir falhas com base em criticidade e exposição real, fortalecendo a postura de segurança e garantindo aderência a marcos regulatórios e frameworks reconhecidos (como NIST e ISO 27001). A combinação de soluções de monitoramento contínuo, detecção estendida e simulação de ataques (PTA) assegura a identificação preditiva de ameaças, incluindo ransomwares, movimentos laterais e exfiltração de dados. A resposta automatizada (SOAR) permitirá reduzir o tempo médio de detecção (MTTD) e de resposta (MTTR), minimizando o impacto de incidentes e elevando o nível de resiliência operacional.
- 2.28.4. Proteção aprimorada contra ameaças modernas: soluções avançadas de proteção contra ransomware, prevenção de vazamento de dados (DLP) e segurança de e-mail reduzirão a probabilidade de incidentes que comprometam a integridade, confidencialidade e disponibilidade das informações institucionais. O SOC integrará mecanismos de hiperautomação e orquestração (SOAR), aplicando playbooks pré-definidos para incidentes recorrentes, como phishing, DLP e ransomware. Essa automação resultará em maior eficiência operacional, reduzindo a necessidade de intervenção manual e assegurando respostas rápidas, padronizadas e auditáveis.
- 2.28.5. Aumento da disponibilidade e resiliência dos serviços: o monitoramento de disponibilidade e a microsegmentação de rede contribuirão para a continuidade operacional, limitando a propagação de ataques e garantindo a estabilidade dos serviços críticos. A adoção de soluções de proteção de endpoint (XDR), prevenção de perda de dados (DLP) e proteção de e-mail (SMG) mitigará os principais vetores de ataque cibernético, reduzindo significativamente a probabilidade de comprometimento de informações sensíveis ou interrupção de serviços.
- 2.28.6. Evolução da cultura de segurança da informação: ações de conscientização contínua (Security Awareness) e treinamentos de simulação de phishing fortalecerão o comportamento seguro dos usuários, mitigando riscos decorrentes de falhas humanas — ainda hoje um dos principais vetores de incidentes cibernéticos. A inclusão de programas de conscientização de segurança (Security Awareness) permitirá desenvolver uma cultura organizacional de segurança, reduzindo incidentes originados por erro humano — ainda o principal vetor de comprometimento em ambientes corporativos.
- 2.28.7. A monitorização de hosts, APIs e URLs críticos contribuirá para a garantia da disponibilidade e desempenho de serviços essenciais, permitindo respostas rápidas a indisponibilidades. A microsegmentação de rede, por sua vez, reduzirá o risco de propagação lateral de ataques e contribuirá para a contenção e isolamento de incidentes.



- 2.29.** De forma integrada, esses serviços permitirão que o SOC atue não apenas como um centro de monitoramento, mas como um núcleo de inteligência e resposta cibernética, capaz de antecipar ameaças, reduzir impactos operacionais e apoiar a tomada de decisão estratégica da instituição com base em dados, contexto e risco.
- 2.30.** A adoção de um SOC representa uma ação estruturante que endereça simultaneamente riscos tecnológicos, operacionais, jurídicos e reputacionais. Trata-se de medida imprescindível para assegurar a continuidade das atividades fazendárias, a proteção dos dados fiscais, a estabilidade das receitas públicas e a preservação da confiança da sociedade na administração pública. Assim, a contratação de um Centro de Operações de Segurança deve ser compreendida como uma iniciativa estratégica, indispensável e prioritária para a SEFAZ/ES.
- 2.31.** Do ponto de vista do interesse público, a adoção de uma solução integrada de segurança da informação contribui diretamente para a continuidade dos serviços públicos essenciais, como arrecadação de tributos, repasses a municípios e execução orçamentária, que dependem de sistemas estáveis e protegidos. A modernização das práticas de segurança digital fortalece a imagem institucional da SEFAZ-ES, melhora a eficiência da gestão pública e assegura que os recursos do contribuinte sejam aplicados de forma responsável e segura. Além disso, o projeto reforça o compromisso do Estado com as boas práticas de governança, transparência e proteção de dados pessoais, em consonância com a Lei Geral de Proteção de Dados (LGPD) e com as recomendações dos órgãos de controle.
- 2.32.** A contratação de um serviço especializado de SOC permitirá que a SEFAZ-ES transicione de um modelo reativo para um modelo preventivo e inteligente de segurança cibernética, utilizando tecnologias de automação, inteligência artificial e análise comportamental para antecipar e neutralizar ameaças. A medida não apenas reduz os riscos tecnológicos, mas também promove maior eficiência na utilização de recursos humanos e financeiros, evitando gastos decorrentes de incidentes e paralisações. Dessa forma, a contratação atende de maneira inequívoca ao interesse público, assegurando continuidade, integridade e confiabilidade dos serviços fiscais e financeiros prestados ao cidadão capixaba.
- 2.33.** Por fim, do ponto de vista financeiro e estratégico, espera-se que a consolidação dos serviços de segurança em um contrato único assegure melhor aproveitamento dos recursos públicos, maior transparência na execução contratual e resultados mensuráveis em termos de resiliência cibernética. O modelo proposto garante retorno efetivo sobre o investimento, reduzindo custos operacionais e fortalecendo a capacidade institucional de prevenir, detectar e responder a incidentes de forma coordenada e tempestiva. Em síntese, a contratação representa não apenas uma medida de segurança, mas também uma ação de gestão inteligente de recursos — que equilibra tecnologia, eficiência e responsabilidade fiscal, alinhando-se às diretrizes de modernização e transformação digital da SEFAZ-ES.
- 2.34.** A contratação de um Centro de Operações de Segurança é, portanto, um investimento estratégico e não apenas um custo operacional. É um passo fundamental para proteger a receita do estado, garantir a justiça fiscal e assegurar a prestação contínua de serviços essenciais à população.
- 2.35.** A decisão administrativa consiste em realizar a contratação por lotes, como medida voltada à ampliação da competitividade e à obtenção da proposta mais vantajosa,



especialmente para as soluções já implementadas na SEFAZ/ES e que demandam predominantemente licenciamento, renovação ou ampliação de uso. Contudo, a parcela de maior relevância do objeto, correspondente ao lote que concentra o núcleo operacional do SOC, será composta por agrupamento de itens em razão da sinergia técnica, da interoperabilidade indispensável entre as soluções, da necessidade de correlação integrada de eventos e da concentração de responsabilidades pela implantação, sustentação e operação dos serviços críticos de segurança cibernética.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

- 3.1.** A solução consiste na implantação de um Serviço de Centro de Operações de Segurança (Security Operation Center – SOC) para a Secretaria de Estado da Fazenda do Espírito Santo (SEFAZ-ES), contemplando um conjunto unificado e integrado de tecnologias, processos e profissionais especializados destinados à monitoração contínua, detecção avançada de ameaças, resposta rápida a incidentes e proteção abrangente de toda a infraestrutura tecnológica da instituição. Trata-se de uma solução completa, que acompanha todas as fases do ciclo de vida da segurança da informação, desde a identificação e prevenção de riscos até a contenção, análise, correção e melhoria contínua do ambiente digital. O SOC, nesse contexto, tem como missão fornecer à SEFAZ-ES um modelo moderno de defesa cibernética capaz de garantir a continuidade das operações fiscais e financeiras, preservar o sigilo dos dados sensíveis sob responsabilidade da instituição e assegurar o cumprimento das normas e melhores práticas nacionais e internacionais relacionadas à segurança da informação.
- 3.2.** A contratação abrange todas as fases do ciclo de vida do serviço, desde o planejamento, implantação, operação, monitoramento, melhoria contínua e suporte técnico, até a evolução e atualização das capacidades de defesa cibernética ao longo do período contratual. A solução se baseia em um conjunto de módulos complementares que, operando de forma integrada, constituem uma arquitetura moderna de defesa, alinhada às melhores práticas internacionais (NIST, ISO 27001, MITRE ATT&CK), e preparada para responder às ameaças cibernéticas contemporâneas — como ransomware, exfiltração de dados, ataques direcionados, abuso de identidades e exploração de vulnerabilidades.
- 3.3.** A solução tem como objetivo geral estabelecer um ecossistema integrado de proteção capaz de monitorar, analisar e correlacionar eventos de segurança provenientes de todos os ativos tecnológicos da SEFAZ-ES, detectando e bloqueando ataques em tempo real, identificando vulnerabilidades críticas, respondendo a incidentes com agilidade e gerando conhecimento estratégico para a tomada de decisão. Esse ecossistema permite que áreas técnicas e de negócio tenham visibilidade permanente sobre riscos, ameaças e fragilidades, além de possibilitar adequações contínuas às exigências legais, como LGPD, padrões NIST, ISO 27001 e diretrizes internas de governança e segurança.
- 3.4.** A CONTRATADA deverá prover solução de Security Operations Center (SOC) baseada em modelo integrado (“merge”), contemplando a unificação de tecnologias, processos e equipes em uma operação contínua 24x7, com foco na proteção ativa dos ativos de negócio. O serviço deverá incorporar capacidades de correlação avançada, automação e orquestração de respostas (SOAR), integrando ferramentas como SIEM, EDR/XDR,



firewalls e soluções de identidade, de modo a reduzir o tempo de detecção e resposta a incidentes.

- 3.5.** Deverá ainda contemplar atuação colaborativa entre funções de defesa e simulação de ataques (abordagem Purple Team), visão unificada de monitoramento (inclusive em ambientes multilocatários) e integração com mecanismos de governança de identidade para resposta automatizada. A solução deverá priorizar riscos com base no impacto ao negócio, assegurando evolução contínua da maturidade do SOC e melhoria da capacidade de detecção, análise e resposta a ameaças.
- 3.6.** A arquitetura da solução é composta por diversos módulos interdependentes que, operando de forma integrada, formam o núcleo operacional do SOC. O primeiro deles, responsável pela gestão de vulnerabilidades, realiza varreduras contínuas em todo o ambiente da SEFAZ-ES, identificando falhas técnicas, riscos relacionados a identidades, desvios de configuração e vulnerabilidades exploráveis de acordo com métricas atualizadas. Além de inventariar automaticamente os ativos, o módulo produz análises baseadas em risco e inteligência de ameaças, permitindo que a instituição priorize ações corretivas de forma alinhada à criticidade dos sistemas fiscais e financeiros.
- 3.7.** Outro componente essencial é o módulo de monitoramento avançado, resposta a incidentes e hiperautomação, que utiliza uma solução SIEM para consolidar e correlacionar logs e eventos de diferentes equipamentos, aplicações, serviços e usuários. Esse módulo incorpora mecanismos de detecção baseados no framework MITRE ATT&CK, utiliza ferramentas de análise comportamental, simulação contínua de ataques (PTA) e integra automações SOAR para executar respostas quase imediatas a incidentes. Dessa forma, os eventos detectados passam por análise especializada e são tratados de acordo com playbooks previamente definidos, reduzindo drasticamente o tempo de detecção (MTTD) e o tempo de resposta (MTTR).
- 3.8.** Complementando essa estrutura, o módulo de proteção avançada contra ransomware e ataques sofisticados atua diretamente nos endpoints e servidores, monitorando processos, comportamento, movimentações laterais e tentativas de elevação de privilégios. Ele permite bloquear automaticamente atividades suspeitas, isolar máquinas comprometidas e evitar a propagação de ameaças que possam comprometer dados fiscais ou interromper sistemas essenciais da SEFAZ-ES. A telemetria coletada alimenta o XDR, enriquecendo a capacidade analítica do SOC.
- 3.9.** A gestão de disponibilidade também faz parte da solução, garantindo monitoramento contínuo dos principais serviços da SEFAZ-ES, como APIs, URLs, sistemas fiscais e recursos de infraestrutura. Ao detectar anomalias de desempenho ou indisponibilidade, o SOC aciona mecanismos de resposta e notificação, reduzindo impactos sobre contribuintes, municípios e áreas internas que dependem de sistemas operacionais ininterruptos.
- 3.10.** A proteção do e-mail e a conscientização dos usuários compõem outra dimensão fundamental da solução. Como o e-mail é o vetor de ataque mais frequente, o SOC incorpora tecnologias de sandboxing, filtragem avançada, reputação, análise comportamental de anexos e URLs, além de iniciativas contínuas de treinamento e simulação de phishing. Essa abordagem aumenta a maturidade dos usuários, reduz o risco de ataques baseados em engenharia social e fortalece o papel do fator humano como linha de defesa.



- 3.11.** A microsegmentação de rede acrescenta uma camada estratégica ao ambiente, permitindo que servidores, aplicações e serviços sejam isolados em segmentos lógicos que dificultam a movimentação lateral de invasores. Com esse recurso, mesmo que um sistema seja comprometido, sua capacidade de alcançar outras áreas críticas é drasticamente reduzida, o que aumenta a resiliência do ambiente e reduz a superfície de ataque.
- 3.12.** A implementação e operação do SOC contam ainda com equipes especializadas disponíveis 24x7, responsáveis por monitorar o ambiente, analisar alertas, executar playbooks, acompanhar incidentes e produzir relatórios gerenciais e indicadores para as áreas técnico-estratégicas da SEFAZ-ES. Esses especialistas atuam tanto na operação diária quanto na governança de segurança, garantindo alinhamento com políticas internas e legislações aplicáveis. A operação é complementada por analistas dedicados para atendimento de requisições, manutenção de políticas, realização de ajustes técnicos e integração entre o SOC e a TI da SEFAZ.
- 3.13.** O ciclo de vida da solução envolve uma fase inicial de implantação, na qual são realizados levantamentos detalhados, configuração de ferramentas, integração de sistemas, definição de políticas, capacitação inicial e construção do baseline de segurança. Na fase operativa, inicia-se o monitoramento contínuo, análise de eventos, resposta a incidentes, gerenciamento de vulnerabilidades, geração de relatórios e reuniões periódicas de acompanhamento. A fase de evolução contempla ajustes, otimizações, ampliação da cobertura, atualização de mecanismos de detecção e melhoria contínua dos processos internos. Por fim, o ciclo prevê uma fase de desativação ou transição, garantindo entrega de documentação, relatórios finais e apoio para eventual migração a novo fornecedor ou modelo.
- 3.14.** A implantação desse SOC proporciona benefícios estratégicos significativos, como a redução de riscos operacionais, a diminuição de incidentes críticos, o aumento da proteção dos dados fiscais, a continuidade da arrecadação, a conformidade regulatória e o fortalecimento da confiança dos contribuintes nos serviços digitais oferecidos pela SEFAZ-ES. Com a modernização da defesa cibernética e a integração das diversas camadas de segurança, a solução promove um ambiente mais seguro, resiliente e eficiente, além de reduzir custos futuros relacionados a incidentes, paralisações ou perdas financeiras decorrentes de ataques.
- 3.15.** Em síntese, a solução descrita reúne tecnologias avançadas, automação, inteligência artificial, processos maduros e equipe altamente especializada para oferecer à SEFAZ-ES uma estrutura completa de defesa cibernética. Seu funcionamento integrado cobre todas as etapas do ciclo de vida da segurança, desde a prevenção até a resposta e melhoria contínua, garantindo a proteção do patrimônio informacional do Estado, a estabilidade institucional e a continuidade dos serviços essenciais que impactam diretamente a economia capixaba.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos Técnicos

- 4.1.1. Os requisitos técnicos da contratação encontram-se detalhados no ANEXO II deste Termo de Referência;



4.2. Da Sustentabilidade

- 4.2.1. Os equipamentos utilizados no âmbito do contrato deverão obedecer às normas internacionais de eficiência energética e possuir selos com Energy Star, Procel ou Green It.

4.3. Da Subcontratação

- 4.3.1. Não será admitida a subcontratação do objeto contratual por se tratar de solução integrada com alto grau de interdependência e especialização, de tal sorte que a subcontratação pode degradar a qualidade dos serviços e gerar dificuldade de responsabilização por ações tomadas dentro do escopo do contrato.
- 4.3.2. Não se entende por subcontratação o fornecimento de licenças de softwares de outros fabricantes que não a CONTRATADA, seja na modalidade de licenciamento seja ele perpétuo ou subscrição mensal, tampouco a atuação do próprio fabricante das soluções em apoio à CONTRATADA na implementação das soluções.

4.4. Da Participação de Consórcio

- 4.4.1. Não será permitida a participação de empresas que estiverem reunidas em consórcio, dadas as características específicas da solução a ser contratada.
- 4.4.2. Para os Lotes 1 e 2 o consórcio não será aceito uma vez que o objeto não apresenta complexidade relevante o suficiente para justificar a execução por mais de uma empresa.
- 4.4.3. Para o Lote 3, a vedação decorre da necessidade de atuação integrada e de responsabilização operacional centralizada por todas as soluções e serviços do núcleo do SOC. A execução do objeto exige comando operacional único, integração contínua das ferramentas, resposta coordenada a incidentes e solução imediata de falhas, sem dependência de repartição interna de atribuições entre integrantes. A participação em consórcio, neste caso concreto, aumentaria as interfaces críticas de gestão e o risco de controvérsia operacional sobre a origem e a correção de falhas.
- 4.4.3.1. A contratação de um consórcio, por sua natureza divide as responsabilidades entre as empresas consorciadas, pode criar problemas como:
- 4.4.3.2. Fragmentação da Responsabilidade: Em caso de falha de um dos componentes, a culpa pode ser transferida de uma empresa para outra dentro do consórcio. Por exemplo, uma falha na solução de Microsegmentação pode ser atribuída a um problema no software utilizado para esse fim ou no serviço de implantação e operação da solução, que por sua vez pode ter sido realizado por empresas distintas do consórcio, gerando um impasse na resolução do problema e prejudicando a operação da sala.
- 4.4.3.3. Segurança Jurídica: A contratação por meio de consórcio eleva o risco jurídico, pois em caso de descumprimento contratual, pode haver disputas judiciais entre as empresas consorciadas para definir a responsabilidade, atrasando a solução dos problemas e a aplicação de sanções.
- 4.4.4. Desta forma, para evitar esses riscos, exige-se que a empresa contratada seja a única responsável pela execução integral de cada um dos lotes do objeto, desde a instalação até a manutenção. Esse critério está em total conformidade com a Lei nº



14.133/2021, que incentiva a contratação de soluções integradas para maior eficiência e segurança.

4.5. Da Garantia de Execução

- 4.5.1. A contratação conta com garantia da contratação, nos moldes do art. 96 da Lei nº 14.133/2021, em valor correspondente a 5% (cinco por cento) do valor total do contrato.
- 4.5.2. O contratado apresentará, no prazo máximo de 10 dias, prorrogáveis por igual período, a critério do contratante, contado da vigência do contrato, comprovante de prestação de garantia, quando optar por caução em dinheiro ou títulos da dívida pública ou, ainda, pela fiança bancária, em valor correspondente a 5% (cinco por cento) do valor total do contrato.
- 4.5.3. Em caso opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.
- 4.5.4. Caso utilizada a modalidade de seguro-garantia, a apólice deverá ter validade durante a vigência do contrato e por 30 dias após o término da vigência contratual, permanecendo em vigor mesmo que o contratado não pague o prêmio nas datas convencionadas.
- 4.5.5. A apólice do seguro garantia deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.
- 4.5.6. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no contrato.
- 4.5.7. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o contratado ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.
- 4.5.8. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:
 - 4.5.8.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;
 - 4.5.8.2. Multas moratórias e punitivas aplicadas pela Administração à contratada; e
 - 4.5.8.3. Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo contratado, quando couber.
- 4.5.9. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item acima, observada a legislação que rege a matéria.
- 4.5.10. A garantia em dinheiro deverá ser efetuada em favor do contratante, em conta específica, aberta pela contratante, com correção monetária.
- 4.5.11. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia.



- 4.5.12. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.
- 4.5.13. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.
- 4.5.14. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o Contratado obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.
- 4.5.15. O Contratante executará a garantia na forma prevista na legislação que rege a matéria.
- 4.5.16. O emitente da garantia ofertada pelo contratado deverá ser notificado pelo contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais (art. 137, § 4º, da Lei nº 14.133/2021).
- 4.5.17. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep nº 662, de 11 de abril de 2022.
- 4.5.18. Extinguir-se-á a garantia com a restituição da apólice, carta fiança ou autorização para a liberação de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do contratante, mediante termo circunstanciado, de que o contratado cumpriu todas as cláusulas do contrato;
- 4.5.19. A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.
- 4.5.20. O garantidor não é parte para figurar em processo administrativo instaurado pelo contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.
- 4.5.21. O contratado autoriza o contratante a reter, a qualquer tempo, a garantia, na forma prevista neste Contrato.

4.6. Da Visita Técnica

- 4.6.1. Para fins de habilitação no certame, será exigida a realização de visita técnica obrigatória, a qual poderá ocorrer presencialmente nas instalações da SEFAZ-ES, em Vitória/ES, ou, de forma remota. Tal vistoria terá por finalidade o conhecimento do ambiente computacional e a verificação de eventuais requisitos necessários ao adequado provimento dos serviços.
- 4.6.2. A visita técnica deverá ser agendada previamente, por meio de mensagem eletrônica a suget@sefaz.es.gov.br, devendo ser realizada entre 09:00 - 11:30h e 14:00 - 16:00h em dias úteis;
- 4.6.3. No ato da visita técnica, será oportunizado à licitante o conhecimento do desenho da topologia da rede da SEFAZ-ES, bem como descrição da infraestrutura virtualizada para provimento dos serviços;



4.6.4. A visita técnica deverá ser acompanhada por representante da SEFAZ-ES designado para esse fim, o qual certificará a vistoria por meio de declaração comprobatória, conforme Anexo VIII – Termo de Visita Técnica.

4.6.5. A licitante que renunciar à Visita Técnica deverá apresentar declaração de Pleno conhecimento do objeto conforme modelo do ANEXO IX assumindo os riscos de sua decisão.

4.7. Requisitos de Qualidade, Segurança e Privacidade

4.7.1. A CONTRATADA deverá respeitar as normas nacionais de proteção de dados e informações vigentes, sobretudo considerando a possibilidade de custódia de conhecimentos, informações e dados pelo prestador de serviços, observadas as seguintes diretrizes:

4.7.1.1. Garantia de aplicabilidade da legislação brasileira sobre os princípios, diretrizes e responsabilidades relacionados à segurança da informação e à proteção de dados.

4.7.1.2. Garantia que, em qualquer hipótese, a Administração tem a tutela absoluta sobre os conhecimentos, informações e dados produzidos pelos serviços.

4.7.1.3. Vedado o uso corporativo dos conhecimentos, informações e dados pelo prestador de serviço.

4.7.1.4. Possuir Plano de Continuidade, Recuperação de Desastres e Contingência de Negócio, que possa ser testado, objetivando a disponibilidade dos dados e serviços em caso de interrupção.

4.7.1.5. Desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços.

4.7.2. A CONTRATADA deverá possuir ao menos duas das certificações de qualidade e segurança elencadas abaixo:

I. ISO/IEC 27001;

II. ISO/IEC 20000;

III. ISO/IEC 9001.

4.7.3. A CONTRATADA deverá seguir as normas internas de segurança da informação da SEFAZ, bem como suas atualizações.

4.7.4. A CONTRATADA será expressamente responsabilizada quanto à manutenção de sigilo absoluto sobre quaisquer dados, informações, e artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venham a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de aplicação de sanção e outras penalidades previstas na legislação vigente, independente da classificação de sigilo conferida pela SEFAZ a tais documentos.

4.7.5. A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, da SEFAZ sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.



- 4.7.6. Cada profissional da CONTRATADA deverá assinar termo declarando estar ciente de que a estrutura computacional disponibilizada pela SEFAZ não poderá ser utilizada para fins particulares, e que a navegação em sítios da Internet e as correspondências em meio eletrônico utilizando o endereço da SEFAZ ou acessadas a partir dos seus equipamentos poderão ser auditadas.
- 4.7.7. Cada profissional da CONTRATADA deverá assinar termo de compromisso declarando total obediência às normas de segurança vigentes ou que venham a ser implantadas, a qualquer tempo, na SEFAZ.
- 4.7.8. A CONTRATADA não poderá veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do Contrato, sem prévia autorização da Contratante;
- 4.7.9. A CONTRATADA não deverá fazer uso das informações prestadas pela Contratante para fins diversos do estrito e absoluto cumprimento do contrato em questão;
- 4.7.10. A CONTRATADA deverá garantir sigilo e inviolabilidade das conversações realizadas por meio do serviço desta contratação, respeitando as hipóteses e condições constitucionais e legais de quebra de sigilo de telecomunicações;
- 4.7.11. A CONTRATADA deverá assinar o termo de Compromisso de Manutenção de Sigilo, constante no ANEXO V deste Termo de Referência, com declaração de manutenção de sigilo e respeito às normas de segurança vigentes no órgão ou entidade em razão do trabalho vinculado ao contrato assinado.
- 4.7.12. A CONTRATADA deverá ainda providenciar o Termo de Ciência, constante no ANEXO VI, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação;
- 4.7.13. Executar o objeto em estreita observância aos ditames estabelecido pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), devendo apresentar declaração constante no ANEXO VII deste Termo de Referência acerca da Ciência e consentimento quanto ao cumprimento da LGPD.

5. MODELO DE EXECUÇÃO DO OBJETO

5.1. Condições de execução

- 5.1.1. O prazo de vigência da contratação, considerado o cronograma de execução desenvolvido, será de 24 (vinte e quatro) meses, contados da data da publicação do contrato no PNCP, podendo ser renovado a critério da administração, observando o disposto neste Termo de Referência.
- 5.1.2. **Itens 1 e 2**
- 5.1.2.1. A CONTRATADA terá até 15 (quinze) dias úteis para apresentação das licenças após o início da vigência do contrato.
- 5.1.2.2. As licenças deverão ser adicionadas diretamente no tenant da SEFAZ em cada uma das respectivas soluções.



5.1.3. Itens 3 a 17

5.1.3.1. Após a publicação do contrato no PNCP a CONTRATADA deverá no prazo de 10 (dez) dias úteis realizar a reunião inicial de “kick-off” do projeto, que deverá ser agendada previamente junto à CONTRATANTE com no mínimo 3 (três) dias de antecedência. Nela serão discutidas as premissas básicas, metodologia e pontos de atenção para o prosseguimento das fases de execução do projeto dentre outros assuntos que sejam relevantes para a execução do contrato.

5.1.3.2. Após a reunião de “kick-off” a CONTRATADA deverá apresentar em até 15 (quinze) dias o cronograma de execução do item 13 (treze) que trata da implantação das soluções descritas no item 3 (três) a 12 (doze), bem como do início das operações do Security Operation Center, item 14 (quatorze), e elaboração e acompanhamento dos itens 15 (quinze), 16 (dezesesseis) e 17 (dezessete) de monitoramento.

5.1.3.3. As licenças das soluções descritas nos itens 3 (três) a 12 (doze) deverão ser entregues em até 15 (quinze) dias úteis do início da vigência do contrato, prorrogáveis a critério da administração.

5.1.3.4. A implantação da solução como um todo de que trata o item 13 (treze), acontecerá por conta da CONTRATADA em até 90 (noventa) dias corridos contados da entrega do cronograma de execução e obedecerá no mínimo os critérios abaixo:

ITEM	DESCRIÇÃO	ENTREGA PARA ACEITE DEFINITIVO
SOLUÇÃO DE GESTÃO DE VULNERABILIDADE E EXPOSIÇÃO DE IDENTIDADE		
3	Ferramenta de Gestão de Vulnerabilidade	2 Scanners Ativos e 2 Passivos
4	Ferramenta de Gestão de Vulnerabilidade	1 Domain Controller monitorado
5	Ferramenta de Gestão de Risco	2 Relatórios
SOLUÇÃO DE MONITORAMENTO DE ATAQUES E RESPOSTA A INCIDENTES		
6	Ferramenta de detecção e resposta	Ativação da ferramenta de SIEM e criação de 05 casos de uso.
7	Ferramenta de Proteção digital de marca	Ativação de 30% das marcas monitoradas
8	PTA – Automated Penetration Testing	Execução de 2 testes
9	Ferramenta de hiperautomação para detecção e resposta a ameaças	Ativação de 30% dos ativos monitorados
SOLUÇÃO DE GESTÃO DE DISPONIBILIDADE		
10	Disponibilizar painel com 30% dos hosts licenciados.	
SOLUÇÃO DE PROTEÇÃO DE E-MAIL, CONSCIENTIZAÇÃO E PROTEÇÃO CONTRA VAZAMENTO DE INFORMAÇÕES		
11	Ferramenta de Segurança de E-mail e Conscientização	Configuração de 10 políticas e realização de 1 campanha
12	Ferramenta de Prevenção contra perda de dados	Criação de 5 políticas

5.1.3.5. A CONTRATADA apresentará uma versão preliminar do “As-Built” de implantação ao término da implantação de cada uma das soluções à CONTRATANTE que emitirá o Termo de Recebimento Provisório, conforme modelo do ANEXO IV, relativo às atividades do Item 13 (treze) – Serviços de Implantação do Security Operation Center.

5.1.3.6. Ao término da implantação, a CONTRATADA emitirá o “As Built” definitivo de implantação do Security Operation Center.



- 5.1.3.7. Em caso de atraso na entrega do item 13 (treze), uma prorrogação de prazo deverá ser solicitada à SEFAZ/ES de maneira justificada sob pena de aplicação de glosas no pagamento do item, sem prejuízo da aplicação das sanções cabíveis.
- 5.1.3.8. O item 14 (quatorze) – Operação do Security Operation Center - se iniciará após a comprovação por parte da CONTRATADA da entrega do item 6 (seis) - SIEM - configurado e recebendo os logs das soluções descritas nos itens 2 (dois) bem como do EDR/XDR (SentinelOne) já em operação na SEFAZ/ES.
- 5.1.3.8.1. Os serviços executados no âmbito do item 14 (quatorze) deste TR compreenderão a operação de todas as soluções descritas nos itens 3 (três) a 12 (doze) pertencentes ao lote 3 (três), bem como a operação da solução descrita no item 2 (dois - Plataforma de microsegmentação Illumio) e ainda a operação do EDR/XDR já em utilização pela SEFAZ/ES (SentinelOne)
- 5.1.3.8.2. O item será executado de maneira contínua, a partir do início da respectiva prestação dos serviços, pelo período remanescente até o término da vigência contratual.
- 5.1.3.8.3. O serviço será executado mediante registro de chamados na plataforma de ITSM da CONTRATADA de acordo com o Catálogo de serviços já existente. O Catálogo de Serviços é vivo e poderá sofrer alterações ao longo do contrato.
- 5.1.3.8.4. Todos os atendimentos registrados e encerrados no mês servirão de base para a apuração do Acordo de nível de serviços descritos no IMR e por conseguinte das eventuais glosas e valor final a ser faturado
- 5.1.3.9. Os itens 15 (quinze), 16 (dezesseis) e 17 (dezesete) terão início após a apresentação do cronograma previsto no item 5.1.3.2 e devendo os documentos previstos serem entregues no prazo de até 90 (noventa) dias corridos. Após a entrega, sua implementação deverá ocorrer de maneira contínua, com revisões semestrais dos documentos até o término da vigência contratual.
- 5.1.3.9.1. O acompanhamento da implementação deverá evidenciar mensalmente os avanços obtidos em termos reais nos níveis de maturidade de segurança e na redução da superfície de ataques, através o aumento da cobertura de táticas de ataque conhecidas e divulgadas pela Matriz MITRE ATT&CK e aderência aos conceitos e padrões do framework NIST.
- 5.1.3.10. As revisões dos documentos apresentados serão semestrais e deverão atualizar o status de implantação para realidade do momento em está sendo feita, ajustando-se os objetivos e metas para o novo ciclo de acompanhamento da implantação.

5.2. Local e horário da prestação dos serviços

- 5.2.1. Os serviços do item 13 (treze) será executado obrigatoriamente na sede da SEFAZ/ES no seguinte endereço:



5.2.1.1. Av. João Batista Parra, 600 – Enseada do Suá, Vitória-ES – CEP: 29050-375.

5.2.2. Os serviços do item 14 (quatorze) serão executados obrigatoriamente na sede da CONTRATADA.

5.2.3. Os serviços dos itens 15 (quinze), 16 (dezesesseis) e 17 (dezessete) serão executados preferencialmente na sede da CONTRATANTE, sendo admitida a execução remota ou na sede da CONTRATADA para as atividades que não exijam interação com a CONTRATANTE.

5.3. Materiais a serem disponibilizados

5.3.1. Para a perfeita execução dos serviços, a CONTRATADA deverá disponibilizar todos os materiais, equipamentos, ferramentas e utensílios necessários à perfeita realização de suas atividades, promovendo sua substituição quando necessário.

5.4. Da transição e finalização do Contrato

5.4.1. No encerramento do contrato, a CONTRATADA deverá cumprir integralmente as seguintes obrigações:

5.4.2. Planejamento e Transição:

5.4.2.1. Atender à comunicação formal de encerramento, participar do planejamento da transição e garantir a continuidade do monitoramento até o término da vigência, sem interrupção de atividades críticas.

5.4.3. Revogação de Acessos:

5.4.3.1. Apoiar a Administração na revogação de todos os acessos remotos e lógicos utilizados durante o contrato, incluindo VPN, MFA, jump servers, SIEM, firewalls, IDS/IPS, antivírus/EDR, servidores e ferramentas de chamados. Auxiliar na alteração de senhas administrativas, chaves de API e atualização de ACLs e regras de firewall.

5.4.4. Entregas Finais:

5.4.4.1. Disponibilizar relatório final de segurança com panorama de incidentes, correções aplicadas, riscos residuais e recomendações; inventário final de incidentes com evidências; runbooks atualizados; e toda a documentação técnica produzida, incluindo diagramas, arquiteturas, playbooks, dashboards e relatórios acumulados.

5.4.4.2. Toda a base de dados de incidentes deverá ser exportada em formato possível de importação pelos softwares de ITSM mais comuns do mercado, como Servece Now, Jira, GLPI, PRTG

5.4.5. Transferência de Conhecimento:

5.4.5.1. Realizar sessões de hand-over com a equipe interna ou novo fornecedor, apresentando regras de correlação do SIEM, principais fontes de logs, alertas críticos, fluxos de tratamento e ferramentas utilizadas, além de prestar orientações e treinamentos necessários à continuidade operacional.

5.4.6. Entrega de Artefatos de Segurança:



5.4.6.1. Entregar evidências de incidentes, logbooks, históricos de detecção, arquivos de regras de correlação e todos os scripts, templates e configurações desenvolvidas durante a vigência contratual.

5.4.7. Eliminação Segura de Dados:

5.4.7.1. Efetuar a destruição segura de dados, logs, dumps, backups e demais informações sensíveis obtidas no contrato, fornecendo declaração formal de eliminação conforme boas práticas de segurança, ISO 27001 e LGPD.

5.4.8. Continuidade Operacional:

5.4.8.1. Cooperar para garantir que não haja lacunas de monitoramento entre o encerramento do contrato e o início das atividades do novo SOC ou da equipe interna, incluindo apoio à eventual operação paralela quando houver substituição de fornecedor.

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

5.5.1. O prazo de garantia contratual dos serviços será de, no mínimo 12 (doze) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

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 14.133/2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.
- 6.2. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.
- 6.3. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.
- 6.4. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada 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 da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.
- 6.5. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) gestor(es) e fiscal(is) do contrato, ou pelos respectivos substitutos, na forma do Decreto Estadual nº 5.545-R/2021 e demais condições previstas para a contratação.
- 6.6. O Fiscal do contrato acompanhará a execução do objeto, assegurando o cumprimento das condições pactuadas, em especial no que se refere às especificações técnicas, prazos e qualidade dos sistemas e serviços entregues.
- 6.7. Em caso de identificação de qualquer inexecução ou irregularidade durante a execução contratual, o Fiscal deverá emitir notificações formais à contratada, determinando prazo adequado para a correção das pendências.



- 6.8.** O Fiscal deverá informar prontamente ao gestor do contrato sobre qualquer situação que demande decisão administrativa ou adoção de medidas que extrapolem sua competência, para que sejam adotadas providências corretivas ou saneadoras, de acordo com as disposições do Decreto Estadual nº 5.545-R/2023.
- 6.9.** Caso ocorram eventos ou circunstâncias que possam inviabilizar a execução contratual dentro dos prazos estabelecidos, o Fiscal deverá comunicar imediatamente o fato ao gestor do contrato, possibilitando ações preventivas ou corretivas em tempo hábil.
- 6.10.** O Fiscal deverá notificar o gestor do contrato, com antecedência razoável, sobre o término do prazo de vigência contratual, com vistas a subsidiar a decisão administrativa sobre eventual prorrogação, renovação ou encerramento do contrato.
- 6.11.** Compete ao Fiscal receber as medições dos serviços executados e analisar sua conformidade com os requisitos técnicos exigidos, apontando eventuais glosas por descumprimento do IMR, encaminhando após ao Gestor do Contrato para conferência.
- 6.12.** Caberá ao Gestor do Contrato a conferência dos valores a serem pagos solicitados pelo Fiscal, solicitar a sua correção quando necessário, e solicitar à CONTRATADA a emissão da Nota Fiscal ou documento equivalente a fim de seguir com as tratativas de pagamento.
- 6.13.** O Gestor do Contrato será responsável por acompanhar a manutenção das condições de habilitação da contratada, incluindo a regularidade fiscal e trabalhista, a análise de pagamentos, garantias, glosas, além de formalizar apostilamentos e termos aditivos, sempre que necessário, solicitando documentos comprobatórios pertinentes.
- 6.14.** Todos os atos de fiscalização e acompanhamento deverão ser registrados formalmente, preferencialmente por meio de sistema eletrônico, garantindo a rastreabilidade e a transparência das ações administrativas, conforme determina o Decreto Estadual nº 5.545-R/2023;
- 6.15.** À Contratada compete a execução dos serviços sempre que solicitado ou determinado nos termos deste Termo de Referência, encaminhar à CONTRATANTE relatório de medição dos serviços executados mensalmente, e emitir as Notas Fiscais sempre que solicitado pelo Gestor do Contrato.

7. PAPEIS E RESPONSABILIDADES

7.1. São obrigações da CONTRATANTE:

- 7.1.1. Nomear os agentes responsáveis pelo acompanhamento e fiscalização do contrato;
- 7.1.2. Receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
- 7.1.3. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis;
- 7.1.4. Liquidar o empenho e efetuar o pagamento ao Contratado, dentro dos prazos preestabelecidos em contrato e, no caso de cobrança indevida, glosar os valores considerados em desacordo com o contrato;



- 7.1.5. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;
- 7.1.6. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos, cuja criação ou alteração seja, objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.
- 7.1.7. Instruir os autos do processo administrativo com os documentos afetos ao recebimento provisório e definitivo dos bens e serviços, tais como: termo de recebimento provisório e definitivo, devidamente assinados pela equipe responsável pelo acompanhamento da execução; metodologia adotada no recebimento definitivo dos bens, contendo a definição da amostra ou a totalidade dos itens a serem testados e inspecionados (exame qualitativo); resultados dos testes de atendimento aos critérios de aceitação e das verificações de conformidade aplicados em cada serviço avaliado.
- 7.1.8. Fornecer as informações necessárias para o desenvolvimento dos serviços objeto do contrato;
- 7.1.9. Prestar as informações e esclarecimentos relativos ao objeto desta contratação que venham a ser solicitados pelo preposto do Contratado;
- 7.1.10. Observar e fazer cumprir fielmente o que estabelece este Termo de Referência, de acordo com as cláusulas contratuais, em particular no que se refere aos níveis de serviço especificados;
- 7.1.11. Providenciar as assinaturas, pelo Contratado, no Termo de Compromisso de Manutenção de Sigilo e Respeito às Normas de Segurança e no Termo de Ciência da Declaração de Manutenção de Sigilo;
- 7.1.12. Garantir, quando necessário, o acesso dos empregados do Contratado às dependências da Contratante, para execução dos serviços referentes ao objeto contratado, após o devido cadastramento dos referidos empregados;
- 7.1.13. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;
- 7.1.14. Notificar o Contratado da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;
- 7.1.15. Aferir a produtividade efetivamente alcançada, para fins de pagamento.

7.2. São obrigações da CONTRATADA:

- 7.2.1. Fornecer o objeto da contratação, atendendo às normas e condições deste Termo de Referência, em especial no que se refere à implantação, operação e níveis de serviço, não sendo admitida qualquer modificação em sua execução sem prévia autorização da Contratante;



- 7.2.2. Indicar formalmente e por escrito, no prazo máximo de 3 dias úteis após a assinatura do contrato, junto à Contratante, um preposto idôneo com poderes de decisão para representar o Contratado, principalmente quanto a eficiência e agilidade da execução dos serviços objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato;
- 7.2.3. Na hipótese de afastamento do preposto, definitivamente ou temporariamente, o Contratado deverá comunicar ao Gestor do Contrato por escrito o nome e a forma de comunicação de seu substituto até o fim do próximo dia útil.
- 7.2.4. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;
- 7.2.5. Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;
- 7.2.6. Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;
- 7.2.7. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;
- 7.2.8. Manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;
- 7.2.9. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;
- 7.2.10. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;
- 7.2.11. Fazer a transição contratual, efetuando a transferência de conhecimento, e todas as documentações inerentes aos serviços executados, quando for o caso;
- 7.2.12. Manter seus funcionários capacitados e treinados para os padrões, ferramentas e processos utilizados no ambiente da Contratante;
- 7.2.13. Executar o objeto em estreita observância aos ditames estabelecido pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).
- 7.2.14. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais;
- 7.2.15. Fornecer e utilizar os materiais, equipamentos e ferramentas necessários, na qualidade e quantidade adequadas especificadas neste Termo de Referência e em sua proposta;
- 7.2.16. Propiciar todos os meios e facilidades necessárias à fiscalização da Solução de Tecnologia da Informação pela Contratante, cujo representante terá poderes para



sustar o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária;

- 7.2.17. Prestar as informações e os esclarecimentos que venham a ser solicitados pela Contratante, por intermédio de preposto designado para acompanhamento.
- 7.2.18. Paralisar, por determinação da Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de dados, de pessoas ou bens de terceiros;
- 7.2.19. Apresentar Nota Fiscal/Fatura com a descrição dos serviços prestados, nas condições deste Termo de Referência, como forma de dar início ao processo de pagamento pela Contratante;
- 7.2.20. Assumir as responsabilidades pelos encargos fiscais e comerciais resultantes da adjudicação da licitação oriunda deste Termo de Referência;
- 7.2.21. Responsabilizar-se pelo cumprimento das obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade à Contratante;
- 7.2.22. Assumir inteira responsabilidade técnica e operacional do objeto contratado, não podendo, sob qualquer hipótese, transferir a outras empresas a responsabilidade por problemas de funcionamento do serviço;
- 7.2.23. Caso o problema de funcionamento do serviço detectado tenha a sua origem fora do escopo do objeto contratado, o Contratado repassará para a Contratante as informações técnicas com a devida análise fundamentada que comprovem o fato, sem qualquer ônus para a Contratante;
- 7.2.24. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo Fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;
- 7.2.25. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado ao Estado ou à entidade estadual, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos ao Contratado, o valor correspondente aos danos sofridos;
- 7.2.26. Responder por quaisquer interferências de estranhos nos acessos em serviço, bem como zelar pela integridade da comunicação;
- 7.2.27. Acatar as orientações da Contratante, sujeitando-se à mais ampla e irrestrita fiscalização, prestando os esclarecimentos solicitados e atendendo às reclamações formuladas;
- 7.2.28. Prestar esclarecimentos à Contratante sobre eventuais atos ou fatos noticiados que se refiram ao Contratado, independente de solicitação;
- 7.2.29. Comunicar à Contratante, por escrito, qualquer anormalidade nos serviços e prestar os esclarecimentos julgados necessários;
- 7.2.30. Sujeitar-se aos acréscimos e às supressões contratuais estabelecidos na forma do art. 125 da Lei nº 14.133, de 2021, quais sejam, os acréscimos ou as supressões



que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor atualizado do contrato;

- 7.2.31. Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do Contrato, sem prévia autorização da Contratante;
- 7.2.32. Não fazer uso das informações prestadas pela Contratante para fins diversos do estrito e absoluto cumprimento do contrato em questão;
- 7.2.33. Garantir sigilo e inviolabilidade das conversações realizadas por meio do serviço desta contratação, respeitando as hipóteses e condições constitucionais e legais de quebra de sigilo de telecomunicações;
- 7.2.34. Assinar o termo de Compromisso de Manutenção de Sigilo, com declaração de manutenção de sigilo e respeito às normas de segurança vigentes no órgão ou entidade em razão do trabalho vinculado ao contrato assinado.
- 7.2.35. Pela mesma razão o Contratado deverá providenciar o Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação;
- 7.2.36. Responder, integralmente, por perdas e danos que vier a causar à Contratante ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou de prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita;
- 7.2.37. Prestar esclarecimentos técnicos sobre a execução dos serviços, sempre que solicitados pela CONTRATANTE;
- 7.2.38. Manter seus funcionários capacitados e treinados para os padrões, ferramentas e processos utilizados no ambiente da CONTRATANTE;
- 7.2.39. Repassar todos os documentos produzidos e gerados no contexto da sua execução, incluindo códigos-fonte, documentação de programas, diagramas e especificações;
- 7.2.40. Cumprir outras obrigações que se apliquem, de acordo com o objeto da contratação.

8. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

8.1. Do Recebimento

- 8.1.1. O recebimento dos itens 1 (um) a 12 (doze) se dará mediante comprovação da ativação de todas as licenças dos softwares no ambiente, devendo a CONTRATANTE emitir Termo de Recebimento Definitivo destes itens, conforme modelo constante do ANEXO IV.
 - 8.1.1.1. Será considerada comprovada a entrega da licença mediante sua efetiva disponibilização no ambiente indicado pela CONTRATANTE, acompanhada da documentação emitida pelo fabricante ou canal de distribuição autorizado que permita à fiscalização verificar a quantidade contratada, o período de vigência e a regularidade do licenciamento.
- 8.1.2. O item 13 (treze) será recebido de maneira parcelada e proporcional ao percentual da implantação efetivamente alcançado, mediante a entrega, pela CONTRATADA à



CONTRATANTE, dos “As Built” de implantação previsto no item 5.1.3.5. Após a análise da documentação apresentada, a CONTRATANTE emitirá o Termo de Recebimento Provisório, conforme modelo constante do ANEXO IV, relativo às atividades executadas.

8.1.2.1. A CONTRATANTE terá prazo de 10 (dez) dias a partir da emissão do Termo de Recebimento Provisório para a análise do “As-Built” e solicitação de correções caso necessário.

8.1.2.2. Havendo necessidade de correção das informações ou adequação dos serviços, a CONTRATADA terá 10 (dez) dias corridos para entrega da versão final do “As-Built” de implantação com toda a documentação produzida acerca da solução implementada.

8.1.2.3. Após o recebimento do “As-Built” definitivo a CONTRATANTE emitirá o Termo de Recebimento Definitivo do item 13 (treze) do objeto contratual conforme modelo do ANEXO V em até 5 (cinco) dias úteis.

8.1.3. O item 14 (quatorze) será recebido mensalmente mediante apresentação de relatório de medição até o 5º (quinto) dia útil do mês subsequente ao da execução dos serviços;

8.1.3.1. O relatório de medição deverá constar no mínimo:

- Atividades realizadas no mês;
- Incidentes registrados e resolvidos;
- Número de chamados abertos;
- Atividades de manutenção realizadas e suas devidas comprovações;
- Demais atividades realizadas no período;
- Apuração do IMR e valores de glosa caso haja;
- Demais informações previstas no ANEXO II – Requisitos Técnicos

8.1.3.2. O recebimento dos serviços previstos neste item ocorrerá de forma proporcional à execução e aceitação das etapas de implantação previstas no item 13 (treze) sendo recebidos efetivamente 10% do item 14 (quatorze) para cada solução implementada e transferida para a operação.

8.1.3.3. Havendo necessidade de correção das informações ou adequação dos serviços, a CONTRATADA terá 10 (dez) dias corridos para entrega da versão final do Relatório de Medição e/ou adoção das medidas cabíveis.

8.1.4. Os itens 15 (quinze), 16 (dezesesseis) e 17 (dezessete) serão recebidos parcialmente na razão de 50% do valor do item pela entrega dos documentos conforme descrito no ANEXO II. Após a entrega dos documentos os demais 50% serão recebidos mensalmente mediante apresentação de relatório de acompanhamento de implantação das medidas recomendadas nos documentos de referência, bem como pela revisão semestral dos documentos.

8.1.5. Os serviços poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 10 (dez)



dias, a contar da notificação por escrito da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

- 8.1.6. Caso haja irregularidades que impeçam o recebimento provisório, o fiscal, conforme o caso, deverá solicitar ao contratado, por escrito, as respectivas correções.
- 8.1.7. O descumprimento deste prazo ensejará na aplicação de glosas conforme cláusulas de IMR previstas no item 18 do ANEXO II.
- 8.1.8. Após o recebimento provisório, o fiscal deverá manifestar-se sobre o cumprimento das exigências de caráter técnico da conformidade do material recebido com as exigências contratuais, visando subsidiar o gestor do contrato no recebimento definitivo.
- 8.1.9. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133/2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertence à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.
- 8.1.10. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.
- 8.1.11. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança dos serviços nem a responsabilidade ético-profissional pela perfeita execução do contrato.
- 8.1.12. O recebimento provisório poderá ser dispensado nos casos em que a fiscalização consiga emitir sumariamente o termo de recebimento definitivo pela simplicidade ou quantidade recebida do objeto.

8.2. Nota Fiscal

- 8.2.1. Para fins de exame da Nota Fiscal, o fiscal deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:
- O prazo de validade;
 - A data da emissão;
 - Os dados do contrato e do órgão contratante;
 - O período respectivo de execução do contrato;
 - O valor a pagar; e
 - Eventual destaque do valor de retenções tributárias cabíveis.
- 8.2.2. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, 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;



8.2.3. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal.

8.2.4. O Contratado deverá apresentar nota fiscal/fatura que registre o valor dos bens/serviços, o valor líquido da nota e o valor dos impostos sujeitos a retenção na fonte, inclusive o ISSQN (quando for o caso) e o destaque do Imposto de Renda na Fonte (conforme disposto na IN/RFB 1.234/2012, ou a que vier a substituí-la, e no Decreto Estadual 5.460-R/2023), os quais serão retidos e recolhidos diretamente pela Administração contratante.

8.3. Do Prazo de Pagamento

8.3.1. O pagamento será efetuado no prazo máximo de até dez dias úteis, contados do recebimento da nota fiscal, nos termos do art. 31 do Decreto Estadual nº 5545-R/2023.

8.3.2. Decorrido o prazo indicado no item anterior, incidirá multa financeira nos seguintes termos:

$$VM = VF \times \frac{12}{100} \times \frac{ND}{360}$$

Onde:

VM = Valor da Multa Financeira.

VF = Valor da Nota Fiscal referente ao mês em atraso.

ND = Número de dias em atraso.

8.3.3. Incumbirão à Contratada a iniciativa e o encargo do cálculo minucioso da fatura devida, a ser revisto e aprovado pela Contratante, juntando-se o cálculo da fatura.

8.3.4. A liquidação das despesas obedecerá rigorosamente ao estabelecido na Lei 4.320/1964, assim como na Lei Estadual 2.583/1971.

8.3.5. Se houver alguma incorreção na Nota Fiscal/Fatura, esta será devolvida à Contratada para correção, ficando estabelecido que o prazo para pagamento será contado a partir da data de apresentação na nova Nota Fiscal/Fatura, sem qualquer ônus ou correção a ser paga pela Contratante.

8.4. Da Forma de Pagamento

8.4.1. Os itens 1 (um) a 12 (doze) terão pagamento anualizado após a entrega das licenças conforme cronograma de desembolsos constante no tópico 10.2 deste Termo de Referência.

8.4.2. O item 13 (treze) será pago de maneira parcelada de acordo com o percentual de avanço da implantação.

8.4.2.1. A CONTRATADA terá direito ao pagamento proporcional, calculado conforme a quantidade de soluções efetivamente implementadas, integradas quando aplicável, e formalmente aceitas pela CONTRATANTE, observados os critérios de recebimento previstos no item 5.1.3.4, da seguinte forma:

- **10%** após a implantação do item 6 (seis), incluindo a correlação dos dados provenientes do lote 2 (dois) e da solução de EDR/XDR SentinelOne já em operação na SEFAZ/ES;



- **10%** adicionais para cada uma das demais soluções efetivamente implantadas e aceitas pela CONTRATANTE, correspondentes aos itens 3 (três) a 5 (cinco) e 7 (sete) a 12 (doze).

8.4.3. O item 14 (quatorze) será pago mensalmente no mês subsequente ao da prestação dos serviços após recebimento dos respectivos relatórios de medição.

8.4.3.1. Até que seja concluída a implantação A CONTRATADA terá direito ao pagamento proporcional, calculado conforme a quantidade de soluções efetivamente implementadas, integradas quando aplicável, e formalmente aceitas pela CONTRATANTE, observados os critérios de recebimento previstos no item 5.1.3.4, da seguinte forma:

- **10%** do valor mensal após a implantação do item 6 (seis), incluindo a correlação dos dados provenientes do lote 2 (dois) e da solução de EDR/XDR SentinelOne já em operação na SEFAZ/ES;
- **10%** do valor mensal adicionais para cada uma das demais soluções efetivamente implantadas e aceitas pela CONTRATANTE, correspondentes aos itens 3 (três) a 5 (cinco) e 7 (sete) a 12 (doze).

8.4.3.2. Após o término da implantação o pagamento integral do valor do item ocorrerá mensalmente no mês subsequente à execução dos serviços.

8.4.4. Os itens 15 (quinze), 16 (dezesesseis) e 17 (dezessete) terão 50% (cinquenta por cento) dos seus valores pagos mediante entrega e aceite dos documentos de Referência (PGV/BIA/PRI) e 50% (cinquenta por cento) restantes, pagos mensalmente pelo acompanhamento das ações de implantação de medidas recomendadas nos documentos, bem como pela atualização dos documentos conforme cronograma de desembolso dos itens de pagamento contínuo disponível no tópico 10.2 deste TR.

8.4.5. Todo faturamento ocorrerá somente após a emissão do respectivo Termo de Recebimento Definitivo, mediante solicitação do Gestor do Contrato.

8.4.6. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

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

8.4.8. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

8.4.9. 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.

8.5. Critérios de pagamento por grupo de itens

Itens	Forma de fornecimento	Medição e aceite	Pagamento	Renovação
1 a 12	Disponibilização integral do quantitativo contratado em cada ciclo de subscrição.	Comprovação da ativação integral das licenças e de sua disponibilidade durante o ciclo.	Pagamento condicionado à comprovação da disponibilização e ativação do quantitativo contratado no respectivo ciclo.	Admitida conforme o ciclo contratual e o ciclo de vida do projeto.



13	Execução parcelada por marcos físicos de implantação.	Aceite progressivo dos marcos concluídos, conforme os critérios do Termo de Referência.	Pagamento por marco físico efetivamente executado e aceito, até a implementação completa.	Não renovável.
14	Prestação continuada da operação do SOC.	Medição mensal dos serviços, níveis de serviço e resultados alcançados.	Pagamento mensal após aferição e aceite da medição, observadas eventuais glosas.	Admitida conforme o ciclo contratual e o ciclo de vida do projeto.
15 a 17	Entrega inicial por produto, seguida de acompanhamento continuado.	Aceite da entrega inicial e medições mensais da evolução das atividades.	Pagamento da entrega inicial correspondente à 50% do valor total do item e pagamentos mensais subsequentes dos 50% restantes.	Não renovável.

9. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E FORMA DE FORNECIMENTO

9.1. Forma de Seleção e Critério de Julgamento da Proposta

- 9.1.1. O fornecedor será selecionado por meio da realização de procedimento de Licitação, na modalidade Pregão, sob a forma Eletrônica, com adoção do critério de julgamento pelo menor preço por Lote.
- 9.1.2. A adoção desse critério justifica-se tecnicamente porque os itens agrupados em cada lote possuem interdependência funcional, complementaridade tecnológica e necessidade de compatibilidade operacional entre si, de modo que a contratação por lote preserva a coerência da solução, reduz riscos de incompatibilidades, evita sobreposição de responsabilidades entre fornecedores distintos e favorece a integração, a implantação, a sustentação e a operação coordenada dos componentes da solução.
- 9.1.3. Especificamente em relação itens 1 (um) e 2 (dois) a segregação em lotes distintos justifica-se pelo fato de a SEFAZ/ES já possuir tais soluções instaladas, configuradas e operacionalizadas em seu parque tecnológico, demandando, nesta contratação, apenas a aquisição, renovação ou ampliação das respectivas licenças de uso. Assim, não há necessidade de contratação de serviços de implantação, configuração inicial, integração técnica complexa ou migração de ambiente para esses itens, uma vez que sua utilização ocorrerá sobre infraestrutura e arranjos operacionais já existentes.
- 9.1.4. A separação desses itens evita a vinculação indevida de licenças autônomas a serviços de implantação que não serão executados, favorece a competitividade, permite precificação mais adequada ao objeto efetivamente demandado e assegura economicidade à Administração, sem prejuízo da continuidade operacional, da compatibilidade tecnológica e da integração dessas soluções ao ambiente de segurança da SEFAZ/ES.
- 9.1.5. Além disso, o julgamento pelo menor preço por lote permite à Administração obter a proposta economicamente mais vantajosa para cada conjunto tecnicamente relacionado, mantendo a competitividade entre licitantes aptos a fornecer a integralidade do lote, sem comprometer a padronização, a rastreabilidade, a governança e a responsabilização pela entrega dos resultados esperados.



9.1.6. Tal critério foi escolhido por representar o menor dispêndio para a Administração, uma vez que atendidas todas as características técnicas o menor preço representará a otimização máxima do valor percebido do objeto.

9.2. Da Forma de Fornecimento

9.2.1. O objeto será fornecido através do regime de empreitada por preço global conforme os seguintes critérios:

9.2.1.1. itens 1 a 12: disponibilização integral do quantitativo contratado para cada ciclo de subscrição, com comprovação de ativação e natureza continuada ao longo da vigência, podendo ser renovado a cada ciclo de subscrição;

9.2.1.2. item 13: execução parcelada por marcos físicos de implantação, finalizando após a implementação completa de todas as soluções previstas no TR, não cabendo a sua renovação;

9.2.1.3. item 14: prestação continuada e medição mensal, sendo renovável de acordo com o ciclo contratual e Ciclo de vida do projeto;

9.2.1.4. itens 15 a 17: entrega inicial por produto e fornecimento do objeto parcelado.

9.2.1.5. A forma de fornecimento foi definida de modo a refletir a natureza específica de cada grupo de itens.

9.2.1.6. Para os itens 1 a 12, a disponibilização integral do quantitativo em cada ciclo de subscrição assegura a ativação completa das licenças e a continuidade de uso durante a vigência, admitindo renovação nos ciclos subsequentes.

9.2.1.7. Para o item 13, a execução parcelada por marcos físicos permite acompanhar e aceitar progressivamente a implantação das soluções, encerrando-se com sua implementação integral, por se tratar de entrega não renovável.

9.2.1.8. Quanto ao item 14, a prestação continuada, com medição mensal, é compatível com a operação permanente do SOC e permite aferir regularmente os níveis de serviço e os resultados alcançados, sendo passível de renovação conforme o ciclo contratual e o ciclo de vida do projeto.

9.2.1.9. Já os itens 15 a 17 combinam uma entrega inicial por produto com acompanhamento continuado e medições semestrais, adequando o pagamento à entrega dos produtos e à comprovação periódica da evolução das atividades.

9.2.1.10. Esse arranjo evita a aplicação de uma única forma de fornecimento a objetos com características distintas, estabelece critérios de entrega e medição compatíveis com licenciamento, implantação, operação e monitoramento e permite que o recebimento e o pagamento ocorram conforme a efetiva disponibilização, implantação ou prestação de cada item.

9.2.1.11. Assim, as formas de fornecimento previstas favorecem o controle da execução, a continuidade operacional, a previsibilidade orçamentária e a gestão dos riscos, sem condicionar entregas autônomas à conclusão simultânea de componentes com prazos, ciclos e critérios de aceite diferentes.



9.3. Das Exigências de Habilitação

- 9.3.1. A qualificação técnica exigida tem por finalidade comprovar que a licitante possui experiência compatível com a natureza, a complexidade, a criticidade e a escala do objeto pretendido, especialmente no que se refere ao fornecimento, implantação, integração, operação, sustentação e suporte de soluções e serviços de segurança da informação associados a ambiente de Security Operation Center - SOC.
- 9.3.2. Considerando que a contratação envolve tecnologias interdependentes, monitoramento contínuo, resposta a incidentes, tratamento de informações sensíveis e atuação sobre sistemas críticos da SEFAZ/ES, a comprovação de capacidade técnica mostra-se indispensável para mitigar riscos de inexecução, falhas operacionais, indisponibilidade dos serviços, baixa qualidade das entregas e comprometimento da continuidade das atividades fazendárias.
- 9.3.3. As exigências de habilitação técnica foram definidas em função da elevada criticidade do ambiente monitorado, da necessidade de operação contínua em regime 24x7x365, do tratamento de informações protegidas por sigilo fiscal e da necessidade de integração entre múltiplas tecnologias de segurança cibernética. As certificações e atestados exigidos destinam-se exclusivamente a demonstrar capacidade técnico-operacional e técnico-profissional compatível com a complexidade do objeto, nos termos do art. 67 da Lei nº 14.133/2021.
- 9.3.4. A exigência da qualificação econômico-financeira é justificada como uma medida de proteção ao interesse público e de segurança contratual, pois visa garantir que a empresa contratada possua a solidez financeira necessária para executar o objeto integralmente e cumprir todas as suas obrigações, incluindo encargos trabalhistas e sociais, mitigando o risco de paralisação do contrato por insolvência e evitando a responsabilização subsidiária da SEFAZ/ES.
- 9.3.5. Ambas estão detalhadas no ANEXO I deste Termo de Referência.

10. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

10.1. Custo Estimado da Contratação

10.1.1. O custo estimado total da contratação é de **R\$ xx.xxx.xxx,xx (xxxxxxx milhões xxxxxxxxxxxx reais e xxxxxxxxxxxx centavos)**, conforme custos unitários apostos na tabela abaixo:

LOTE	ITEM	DESCRIÇÃO	TECNOLOGIA	MÉTRICA	QTD	VLR. UNIT	VLR. MENSAL	VLR. TOTAL
1	1	EMS E5 SU EMS E3 Per User	EMS	Usuários	800			

LOTE	ITEM	DESCRIÇÃO	TECNOLOGIA	MÉTRICA	QTD	VLR. UNIT	VLR. MENSAL	VLR. TOTAL
2	2	Solução de Microsegmentação de rede	MICROSEG.	Workloads	1.000		N/A	

LOTE	ITEM	DESCRIÇÃO	TECNOLOGIA	MÉTRICA	QTD	VLR. UNIT	VLR. MENSAL	VLR. TOTAL
3	3	Solução de Gestão de Vulnerabilidades com foco em Risco e Identidade	GV	Ativos	1800		N/A	
	4		GVAD	Usuários	1000		N/A	
	5		RISK	Solução	1		N/A	
	6	Solução de Monitoramento Avançado, Resposta a Incidentes Automatizada, Hiperautomação, Soluções aplicadas a Firewall e teste automatizado	SIEM	GB/dia	200		N/A	
	7		DRPs	CNPJ	1		N/A	
	8		PTA	Solução	1		N/A	
	9		SecOps	Ativos	2500		N/A	



10	Solução de Gestão de disponibilidade	Host/URL/API	Workloads	500		N/A	
11	Solução Integrado de Proteção de E-mail, Conscientização de Usuários e Prevenção de Vazamento de Informações	SMG/ SEC. AWAR	Usuários	1000		N/A	
12		DLP	Usuários	1000		N/A	
13	Serviços de implantação das Soluções descritas nos Itens 3 a 12	SERVIÇOS	Escopo Fechado	1		N/A	
14	Serviços de Operação do Security Operation Center	SERVIÇOS	Meses	24	N/A		
15		PGV	CNPJ	1	N/A		
16	Serviços de Monitoramento da adoção às melhores práticas de Segurança da Informação	BIA	CNPJ	1	N/A		
17		PRI	CNPJ	1	N/A		

10.1.2.A estimativa de preços da presente contratação foi elaborada com base em metodologia estruturada, observando os princípios da economicidade, razoabilidade e vantajosidade para a Administração Pública, conforme preconiza a Lei nº 14.133/2021.

10.1.3.A composição dos valores considerou unidades de medida específicas para cada item (ativos, usuários, GB de ingestão, endpoints, horas técnicas, entre outros), bem como a complexidade técnica, criticidade do ambiente e nível de serviço exigido (24x7x365). Adicionalmente, foram considerados fatores como escala da solução, necessidade de integração entre ferramentas e características do ambiente da SEFAZ/ES, conforme descrito neste Termo de Referência.

10.1.4.Para o Lote 1, a cotação foi obtida diretamente junto ao fabricante da solução e validada por meio do Catálogo de Soluções Digitais da Microsoft para a Secretaria de Governo Digital. Essa fonte foi considerada adequada por refletir referência oficial do fabricante, aderente ao modelo de licenciamento pretendido, às condições comerciais praticadas para soluções Microsoft no âmbito da Administração Pública e às características específicas do item a ser adquirido.

10.1.5.Para o Lote 2, o preço também foi obtido com base em contrato já em andamento com a SEFAZ/ES, considerado pertinente por envolver solução já instalada e operacionalizada no parque tecnológico atual. Essa fonte foi adotada por refletir o custo real e atual de licenciamento de solução equivalente no próprio ambiente da Administração, sem incorporar custos de implantação que não integram a demanda.

10.1.6.Para o Lote 3, a estimativa de preços foi obtida por meio de cotação junto a empresa especializada no segmento de segurança cibernética, reconhecida como referência no mercado pela atuação em soluções compatíveis com o objeto pretendido, especialmente em gestão de vulnerabilidades, exposição de identidades, análise de riscos e demais capacidades associadas ao fortalecimento da maturidade de ambientes de Security Operation Center - SOC.

10.1.7.A utilização dessa fonte mostra-se tecnicamente adequada diante da especificidade, complexidade e criticidade do lote, que envolve solução especializada, aderência a práticas consolidadas de mercado e integração ao ambiente de segurança da SEFAZ/ES. A cotação obtida reflete valores praticados por fornecedor com expertise no segmento, contribuindo para uma estimativa realista, rastreável e compatível com o escopo técnico e com o nível de especialização requerido para a contratação.

10.1.8.Dessa forma, a pesquisa de preços dos Lotes 1, 2 e 3 foi estruturada a partir de fontes diretamente relacionadas ao objeto e ao contexto de uso da SEFAZ/ES: referência oficial de fabricante validada em catálogo institucional para o Lote 1,



contratos vigentes da própria Secretaria para os Lotes 2 e cotação de empresa especializada e reconhecida no mercado de segurança cibernética para o Lote 3.

10.1.9. Tal metodologia confere consistência, rastreabilidade e aderência técnica à estimativa, além de reforçar a economicidade ao considerar preços compatíveis com soluções já adotadas ou tecnicamente equivalentes às necessidades da Administração.

10.2. Do Cronograma de Desembolso

DESCRIÇÃO		1º ANO		2º ANO		TOTAL
		1º mês	Demais Meses	1º mês	Demais Meses	
1	EMS E5 SU EMS E3 Per User – SEM					
2	Solução de Microsegmentação de rede - MICROSEG.					
3	Solução de Gestão de Vulnerabilidades com foco em Risco e Identidade - GV					
4	Solução de Gestão de Vulnerabilidades com foco em Risco e Identidade - GVAD					
5	Solução de Gestão de Vulnerabilidades com foco em Risco e Identidade - RISK					
6	Solução de Monitoramento Avançado, Resposta a Incidentes Automatizada, Hiperautomação, Soluções aplicadas a Firewall e teste automatizado - SIEM					
7	Solução de Monitoramento Avançado, Resposta a Incidentes Automatizada, Hiperautomação, Soluções aplicadas a Firewall e teste automatizado - DRPs					
8	Solução de Monitoramento Avançado, Resposta a Incidentes Automatizada, Hiperautomação, Soluções aplicadas a Firewall e teste automatizado - PTA					
9	Solução de Monitoramento Avançado, Resposta a Incidentes Automatizada, Hiperautomação, Soluções aplicadas a Firewall e teste automatizado - SecOps					
10	Solução de Gestão de disponibilidade - Host/URL/API					
11	Solução Integrado de Proteção de E-mail, Conscientização de Usuários, Prevenção a Vazamento de Informações SMG/ SEC.AWAR					
12	Solução Integrado de Proteção de E-mail, Conscientização de Usuários e Prevenção de Vazamento de Informações - DLP					
13*	Serviços de implantação das Soluções descritas nos Itens 3 a 12					
14**	Serviços de Operação do Security Operation Center					
15	Serviços de Monitoramento da adoção às melhores práticas de Segurança da Informação - PGV					
16	Serviços de Monitoramento da adoção às melhores práticas de Segurança da Informação - BIA					
17	Serviços de Monitoramento da adoção às melhores práticas de Segurança da Informação - PRI					

TOTAL

*Os pagamentos iniciais do item 13 serviços de implantação das soluções descritas nos itens 3 a 12 serão impactados pelo ritmo da implantação e ocorrerão conforme critérios descritos nos itens 5.1.3.4 e 8.4.2 deste TR. Desta forma seu valor foi trazido para o primeiro mês de contrato de forma exemplificativa a fim de demonstrar sua ocorrência uma única vez ao longo do contrato.

** Os pagamentos iniciais do item 14 serviço de operação do Security Operation Center serão impactados pelo ritmo da implantação e ocorrência conforme critérios descritos nos itens 5.1.3.4 e 8.4.3. Desta forma os valores foram demonstrados no cronograma de maneira exemplificativa.

DATALHAMENTO DO PAGAMENTO MENSAL (ESTIMADO)

		Mês 1	Mês 2	Mês 3	Mês 4	Mês 5	Mês 6	Mês 7	Mês 8	Mês 9	Mês 10	Mês 11	Mês 12
14*	Pgto Total	N/A	N/A	N/A									
	Pgto Único	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Pgto Mensal												
15	Pgto Total	N/A	N/A	N/A									
	Pgto Único	N/A	N/A	N/A		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Pgto Mensal	N/A	N/A	N/A	N/A								
16	Pgto Total	N/A	N/A	N/A									
	Pgto Único	N/A	N/A	N/A		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Pgto Mensal	N/A	N/A	N/A	N/A								
17	Pgto Total	N/A	N/A	N/A									
	Pgto Único	N/A	N/A	N/A		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Pgto Mensal	N/A	N/A	N/A	N/A								



		Mês 13	Mês 14	Mês 15	Mês 16	Mês 17	Mês 18	Mês 19	Mês 20	Mês 21	Mês 22	Mês 23	Mês 24
14	Pgto Total												
	Pgto Único	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Pgto Mensal												
15	Pgto Total												
	Pgto Único	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Pgto Mensal												
16	Pgto Total												
	Pgto Único	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Pgto Mensal												
17	Pgto Total												
	Pgto Único	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Pgto Mensal												

11. ADEQUAÇÃO ORÇAMENTÁRIA

11.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento. A contratação será atendida pela seguinte dotação:

Gestão/Unidade: 220101

Fonte de Recursos: 500 e 704

Programa de Trabalho: 10.22.101.04.121.0050.1106

Elemento de Despesa: 44.90.52 – 44.90.40 – 33.90.40

Plano Interno: Modernização, Atualização E Inovação De Equipamentos, Processos E Sistemas

12. SANÇÕES ADMINISTRATIVAS

12.1.1. Estarão sujeitos às sanções administrativas previstas em contrato, sem prejuízo da aplicação dos demais dispositivos legais, respeitadas a gradação e contraditório:

12.1.1.1. A indisponibilidade injustificada do serviço por período superior a 4 (quatro) horas;

12.1.1.2. A omissão ou atraso na comunicação de incidente;

12.1.1.3. A violação de sigilo;

12.1.1.4. O tratamento de dados fora da finalidade;

12.1.1.5. A perda ou alteração indevida de evidências;

12.1.1.6. A não manutenção de licenças e suporte;

12.1.1.7. A execução por profissional sem qualificação exigida;

12.1.1.8. E a recusa injustificada de transição contratual

12.1.1.9. O descumprimento de IMR com a apresentação do indicador IDG insatisfatório;

12.1.1.10. O descumprimento reiterado do IMR com a apresentação do indicador IDG por 3 (três) ou mais vezes seguidas como regular.

12.2. As sanções de que trata este tópico estarão previstas em tópico específico do contrato.



Vitória, 26 de outubro de 2026.

Ualter Regis Barbosa

Subgerente de Infraestrutura Tecnológica

Alexia Spelta Colombo

Subgerente de Gestão de Tecnologia da
Informação

Aprovo:

Luiz Carlos Lessa

Gerente de Tecnologia da Informação



ANEXO I DO TR – REQUISITOS DE HABILITAÇÃO

Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

1. HABILITAÇÃO JURÍDICA

1.1. 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;

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

12.12 - 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>;

1.3. Sociedade empresária, sociedade limitada unipessoal ou sociedade identificada como empresa individual de responsabilidade limitada: 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;

1.4. 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 n.º 77, de 18 de março de 2020.

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

1.6. 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;

1.7. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

1.8. Agricultor familiar: Declaração de Aptidão ao Pronaf – DAP ou DAP-P válida, ou, ainda, outros documentos definidos pela Secretaria Especial de Agricultura Familiar e do Desenvolvimento Agrário, nos termos do art. 4º, §2º do Decreto nº 10.880, de 2 de dezembro de 2021.

1.9. Produtor Rural: matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física, nos termos da Instrução Normativa RFB n. 971, de 13 de novembro de 2009 (arts. 17 a 19 e 165).

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



2. HABILITAÇÃO FISCAL, SOCIAL E TRABALHISTA

- 2.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ) ou no Cadastro de Pessoas Físicas (CPF), conforme o caso;
- 2.2. Prova de inscrição no cadastro de contribuintes estadual e/ou municipal relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
 - 2.2.1. Caso o fornecedor seja considerado isento dos tributos estaduais ou municipais relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.
 - 2.2.2. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar 123/2006 estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.
- 2.3. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão negativa ou positiva com efeito de negativa, expedida conjuntamente pela Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente aos créditos tributários federais e à Dívida Ativa da União por elas administrados, inclusive aqueles relativos à Seguridade Social;
- 2.4. Prova de regularidade com a Fazenda Estadual (onde for sediada a empresa e a do Estado do Espírito Santo, quando a sede não for deste Estado);
- 2.5. Prova de regularidade com a Fazenda Pública Municipal da sede da licitante;
- 2.6. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS), mediante certidão expedida pela Caixa Econômica Federal;
- 2.7. Prova de regularidade 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;
- 2.8. Caso o objeto contratual venha a ser cumprido por filial da licitante, os documentos exigidos neste item também deverão ser apresentados pela filial executora do contrato, sem prejuízo para a exigência de apresentação dos documentos relativos à sua matriz.
- 2.9. Nos casos de microempresas, empresas de pequeno porte ou equiparadas, não se exige comprovação de regularidade fiscal para fins de habilitação, mas somente para formalização da contratação, observadas as seguintes regras:
 - 2.9.1. A licitante deverá apresentar, à época da habilitação, todos os documentos exigidos para efeito de comprovação de regularidade fiscal, mesmo que apresentem alguma restrição.
 - 2.9.2. Havendo alguma restrição na comprovação da regularidade fiscal ou trabalhista, é assegurado o prazo de 5 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente for declarado vencedor do certame, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.



- 2.9.3. O prazo a que se refere o item anterior poderá, a critério da Administração Pública, ser prorrogado por igual período.
- 2.9.4. Em caso de atraso por parte do órgão competente para emissão de certidões comprobatórias de regularidade fiscal, ou trabalhista, a licitante poderá apresentar à Administração outro documento que comprove a extinção ou suspensão do crédito tributário, respectivamente, nos termos dos arts. 156 e 151 do Código Tributário Nacional, acompanhado de prova do protocolo do pedido de certidão.
- 2.9.5. Na hipótese descrita no inciso anterior, a licitante terá o prazo de 10 (dez) dias, contado da apresentação dos documentos a que se refere o parágrafo anterior, para apresentar a certidão comprobatória de regularidade fiscal ou trabalhista.
- 2.9.6. O prazo a que se refere o item anterior poderá, a critério da Administração Pública, ser prorrogado por igual período, uma única vez, se demonstrado pela licitante a impossibilidade de o órgão competente emitir a certidão.
- 2.9.7. A formalização da contratação fica condicionada à regularização da documentação comprobatória de regularidade fiscal e trabalhista, nos termos dos incisos anteriores, sob pena de decadência do direito à contratação, sem prejuízo da aplicação das sanções legais, sendo facultado à Administração convocar as licitantes remanescentes e com elas contratar, observada a ordem de classificação, ou revogar a licitação.

3. HABILITAÇÃO TÉCNICA

- 3.1. Comprovação de aptidão para execução de serviço de complexidade equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, emitidos por pessoas jurídicas de direito público ou privado, ou regularmente emitidos pelo conselho profissional competente, quando for o caso.
- 3.2. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:
- 3.2.1. Atestado (s) de Capacidade Técnica fornecido (s) por Pessoa Jurídica de Direito Público ou Privado, que comprovem desempenho pela licitante de serviços compatíveis em características, quantidades e prazos, com no mínimo 50% (cinquenta por cento), que deverão estar explicitadas conforme constante a seguir.
- 3.2.2. Para o lote 1**
- 3.2.2.1. Considerar-se-á compatível o atestado que comprove o fornecimento de licenciamento microsoft EMS para pelo menos 400 usuários.
- 3.2.3. Para o lote 2**
- 3.2.3.1. Considerar-se-á compatível o atestado que comprove o fornecimento de licenciamento de ferramenta de microssegmentação de rede para no mínimo 500 usuários
- 3.2.4. Para o Lote 3**
- 3.2.4.1. Considerar-se-á compatível o atestado que comprove a prestação de **SERVIÇO GERENCIADOS DE SEGURANÇA** em regime de 24 (vinte quatro)



horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, com duração mínima de 12 (doze) meses:

- a) 1 (um) ou mais atestado(s) de capacidade técnica, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, em nome da licitante, que comprove(m) a prestação de Serviços Gerenciados de Segurança (MMS – Managed Security Services) por meio de SOC (Security Operation Center) redundante no Brasil, operado pela contratada;
 - b) Atestado (s) de Capacidade Técnica (ACT) em nome da licitante, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, e que comprove que a licitante tenha realizado experiência na prestação de serviços de gestão de vulnerabilidades, incluindo o monitoramento e o tratamento das vulnerabilidades encontradas em ambientes;
 - c) Atestado (s) de Capacidade Técnica (ACT) em nome da licitante, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, e que comprove que a licitante tenha realizado experiência na prestação de serviços de administração de solução de Gerenciamento e Correlação de Eventos de Segurança da Informação – SIEM;
 - d) Atestado (s) de Capacidade Técnica (ACT) em nome da licitante, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, e que comprove que a licitante tenha realizado experiência na prestação de serviços de administração de solução de extended detection and response;
 - e) Atestado (s) de Capacidade Técnica (ACT) em nome da licitante, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, e que comprove que a licitante tenha realizado o fornecimento de solução de Data Loss Prevention – DLP;
 - f) Atestado (s) de Capacidade Técnica (ACT) em nome da licitante, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, e que comprove que a licitante tenha realizado fornecimento de serviço gerenciamento de firewall;
 - g) Atestado (s) de Capacidade Técnica (ACT) em nome da licitante, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, e que comprove que a licitante tenha realizado fornecimento de serviço de digital risk Protection (DRP);
 - h) Atestado (s) de Capacidade Técnica (ACT) em nome da licitante, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, e que comprove que a licitante tenha realizado serviços de conscientização de segurança;
 - i) Atestado (s) de Capacidade Técnica (ACT) em nome da licitante, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, e que comprove que a licitante tenha realizado serviços de operações de cibersegurança;
- 3.2.4.2. A LICITANTE deverá apresentar, no mínimo, 01 (um) atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, comprovando a prestação satisfatória de serviços compatíveis com o objeto desta contratação, contemplando, no mínimo, 3 (três) dos serviços previstos



neste instrumento convocatório, executados em ambiente operacional integrado de segurança cibernética (SOC), com atuação correlacionada entre múltiplas disciplinas de monitoramento, detecção, resposta e gestão de eventos de segurança

3.2.5. A LICITANTE deverá apresentar uma planilha de comprovação de atendimento dos Atestados contendo todas as informações conforme tabela abaixo:

APRESENTAÇÃO DO ATESTADO DE CAPACIDADE TÉCNICA							
	OBJETO	Número do Contrato	Descrição do Serviço	Período de Prestação de serviço	Emissão do Atestado	Nome do servidor/responsável	Contato
3.2.4.1							
Alínea A							
Alínea B							
Alínea C							
Alínea D							
Alínea E							
Alínea F							
Alínea G							
Alínea H							
Alínea I							

3.2.5.1. O atestado deverá conter a identificação do signatário preferencialmente em papel timbrado do declarante, no caso de atestado emitido por pessoa jurídica de direito privado, ficando reservado à Equipe de Licitação o direito de solicitar cópias dos contratos ou nota fiscal a que se referem tais documentos.

3.2.5.2. A licitante deverá comprovar, através de consultas ao site do fabricante ou através de declaração dele, que é parceira de todas as soluções e que está apta e autorizada a comercializar os produtos ofertados;

3.2.5.3. Deverá ser apresentado, na fase de assinatura de contrato, as certificações dos profissionais, bem como a comprovação de vínculo entre a CONTRATADA e os profissionais que participarão da implantação, gestão continuada, suporte e gerenciamento do projeto, respeitando o quantitativo mínimo estabelecido abaixo.

- a) Um Profissional: Gerência de projeto PMP/PMI o Prince2 Practitioner;
- b) Um Profissional: Certificado pela solução de SIEM ofertada;
- c) Um Profissional: Certificado pela solução de Gestão de Vulnerabilidade ofertada;
- d) Um Profissional: Certificado pela solução Microsegmentação ofertada;
- e) Um Profissional: Certificado pela solução XDR utilizada na SEFAZ;
- f) Um Profissional: Certificado pela solução DLP;
- g) Um Profissionais: Certificado pela solução E-mail Security ofertada;
- h) Um ou mais profissionais que detenha, individualmente ou em conjunto, no mínimo 3 (três) das seguintes certificações de segurança: GCIH, GCIA, GCFA, GMON, GCDA, CompTIA CySA+, CompTIA Security+, CISSP,



CISM, CEH ou OSCP;

- 3.2.5.4. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados de serviços executados de forma concomitante, pois essa situação equivale, para fins de comprovação de capacidade técnico-operacional, a uma única contratação.
- 3.2.5.5. Os atestados de capacidade técnica podem ser apresentados em nome da matriz ou da filial da empresa licitante.
- 3.2.5.6. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, entre outros documentos.
- 3.2.5.7. A licitante deve, juntamente com a proposta comercial, apresentar os manuais, catálogos, folders, ou outros documentos técnicos, ou ainda, links públicos oficiais da solução exigida ou do serviço exigido, para comprovação do atendimento às características técnicas especificadas neste Termo de Referência;
- 3.2.5.8. Deverá ser fornecido uma planilha em formato xlsx, docx ou pdf, junto à proposta comercial com a comprovação de todos os itens das especificações técnicas indicando documento ou link público com seu devido trecho e página.
- 3.2.5.9. No conjunto de documentos apresentados pela licitante (folders/catálogos), para fins de aceitação pela SEFAZ-ES deverá vir indicando corretamente, o item, especificação, link ou documento, página e trecho que comprove o atendimento de cada item/subitem das especificações técnicas descritas nos serviços a serem ofertado, conforme modelo abaixo.

Especificação	Link ou Documento	Página	Item / Trecho

4. HABILITAÇÃO ECONÔMICO-FINANCEIRA

- 4.1. **Certidão negativa de insolvência civil** expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de sociedade simples ou de pessoa física, desde que admitida a sua participação na licitação;
- 4.2. **Certidão negativa de falência** expedida pelo distribuidor da sede do licitante, para as demais pessoas jurídicas;
- 4.3. Caso a licitante se encontre em processo de **recuperação judicial ou extrajudicial**, deverá apresentar certidão emitida pela instância judicial competente certificando que a interessada está apta econômica e financeiramente a participar da licitação, além de cumprir todos os demais requisitos de habilitação exigidos por este Edital.
- 4.4. **Balanço Patrimonial (BP) e Demonstração de Resultado de Exercício (DRE) dos 2 (dois) últimos exercícios sociais, comprovando:**



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

$$ILG = \frac{\text{ATIVO CIRCULANTE (AC)} + \text{REALIZÁVEL A LONGO PRAZO (RLP)}}{\text{PASSIVO CIRCULANTE (PC)} + \text{PASSIVO NÃO CIRCULANTE (PNC)}}$$

$$ISG = \frac{\text{ATIVO TOTAL (AT)}}{\text{PASSIVO CIRCULANTE (PC)} + \text{PASSIVO NÃO CIRCULANTE (PNC)}}$$

$$ILC = \frac{\text{ATIVO CIRCULANTE (AC)}}{\text{PASSIVO CIRCULANTE (PC)}}$$

4.4.2. Quando qualquer dos índices for igual ou inferior a 1 (um), poderá o licitante atender ao requisito de habilitação demonstrando patrimônio líquido não inferior a 10% (dez por cento) do valor estimado da contratação.

- 4.5.** Os documentos referidos acima (BP e DRE) serão os já exigíveis na forma da lei, com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital (ECD) ao SPED ou, se a empresa não estiver obrigada ao SPED, observando a data de exigibilidade do art. 1.078, I, do Código Civil.
- 4.6. Declaração assinada por profissional habilitado da área contábil**, apresentada pelo licitante, demonstrando o atendimento dos índices e coeficientes para cada exercício a que se referem as demonstrações contábeis, bem como demonstrando o patrimônio líquido mínimo exigido no último exercício.
- 4.7.** 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.
- 4.8.** 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.
- 4.9.** No caso de consórcio, se admitida a sua participação no edital, deverá haver a demonstração, por cada consorciado, do atendimento aos índices contábeis definidos neste Edital.



ANEXO II DO TR - REQUISITOS TÉCNICOS

LOTE 1

1. EMS E5 SU EMS E3 Per User

- 1.1.** O item 1, referente ao licenciamento EMS E5 SU EMS E3 Per User, tem por objetivo realizar o upgrade da solução Microsoft Enterprise Mobility + Security atualmente contratada e utilizada pela SEFAZ/ES na modalidade EMS E3 para o nível EMS E5, ampliando as capacidades já existentes de proteção, governança, monitoramento e resposta a riscos relacionados a identidades digitais, dispositivos, aplicações, dados corporativos e acessos ao ambiente tecnológico institucional.
- 1.2.** Atualmente, a SEFAZ/ES já possui ambiente estruturado com a solução EMS E3, integrada aos processos de gestão de identidades, controle de acesso, proteção de dispositivos, políticas de conformidade e governança dos recursos corporativos Microsoft. A evolução para o EMS E5 não representa substituição de tecnologia, mas sim ampliação funcional da plataforma já contratada, preservando as configurações existentes, os fluxos operacionais estabelecidos, o conhecimento técnico acumulado pelas equipes internas e a compatibilidade com o ecossistema tecnológico atualmente em uso.
- 1.3.** A contratação do upgrade por meio de licenciamento Step-up mostra-se tecnicamente adequada e economicamente vantajosa, pois permite o aproveitamento integral da base já licenciada, evitando custos, riscos e esforços associados à substituição de plataforma, reimplantação de controles, migração de políticas, revalidação de integrações e capacitação ampla das equipes para solução distinta. Essa abordagem reduz a complexidade operacional, preserva a padronização tecnológica do ambiente e assegura a continuidade dos serviços de segurança já suportados pela plataforma Microsoft.
- 1.4.** O EMS E5 agrega funcionalidades avançadas de segurança e governança, especialmente voltadas à proteção de identidades, análise de riscos, detecção de comportamentos anômalos, resposta a acessos suspeitos, proteção de informações sensíveis e fortalecimento dos mecanismos de conformidade. Tais capacidades são aderentes à necessidade da SEFAZ/ES de elevar sua maturidade em segurança cibernética, ampliar a proteção contra uso indevido de credenciais, reduzir a superfície de ataque e apoiar a operação integrada do SOC com informações qualificadas sobre identidades, acessos e riscos.
- 1.5.** Dessa forma, a manutenção da plataforma Microsoft EMS com evolução do nível E3 para E5 justifica-se pela necessidade de preservação da compatibilidade técnica, continuidade operacional, interoperabilidade com o ambiente já implantado, padronização tecnológica e obtenção da solução mais vantajosa para a Administração. Por se tratar de licenciamento complementar de solução previamente contratada e operacional, o item deve ser tratado de forma autônoma em lote próprio, sem necessidade de nova implantação técnica, sem prejuízo da integração com os demais componentes do SOC e com os processos de segurança da informação da SEFAZ/ES.
- 1.6.** A CONTRATADA deverá fornecer exclusivamente o licenciamento EMS E5 SU EMS E3 Per User, correspondente ao part number CE6-00004 destinado à evolução da solução EMS E3 já contratada e implantada no ambiente da SEFAZ/ES. Por se tratar de upgrade/licenciamento complementar de solução previamente existente, não caberá à CONTRATADA a execução de atividades de implantação, configuração, migração ou



parametrização da solução, limitando-se sua obrigação à disponibilização regular das licenças contratadas.

LOTE 2

2. SOLUÇÃO DE MICROSSEGMENTAÇÃO DE REDE

2.1. Requisitos gerais

- 2.1.1. Contratação de uma solução de Microsegmentação, visando implementar controles granulares de tráfego entre sistemas, aplicações e usuários, reduzir a superfície de ataque, conter movimentações laterais de possíveis invasores e assegurar que os ativos críticos da SEFAZ-ES sejam protegidos de acordo com seu nível de sensibilidade e relevância para a continuidade do negócio.
- 2.1.2. O modelo de licenciamento da solução ofertada deverá ser flexível. A eventual migração de licenças entre ativos (ex.: entre máquinas físicas, virtuais, containers ou instâncias em nuvem) deverá ser permitida sem necessidade de notificação prévia ou autorização do fabricante, desde que o quantitativo total de licenças em uso não ultrapasse o volume contratado.
- 2.1.3. Atualmente encontra-se implantada e operacional no ambiente tecnológico da SEFAZ a solução de microsegmentação do fabricante Illumio, integrada aos processos de segurança, políticas de segmentação, fluxos operacionais e arquitetura de proteção cibernética da instituição;
- 2.1.4. A solução atualmente utilizada proporcionou à SEFAZ elevado nível de visibilidade sobre os fluxos internos de comunicação entre sistemas e aplicações, permitindo o mapeamento detalhado de dependências operacionais, identificação de comunicações indevidas e implementação de controles de segmentação compatíveis com os requisitos de segurança do ambiente institucional;
- 2.1.5. A utilização da solução contribuiu significativamente para o fortalecimento da capacidade de contenção de movimentação lateral de ameaças cibernéticas, bem como para a adoção de políticas mais restritivas e aderentes ao princípio do menor privilégio entre ativos e aplicações corporativas;
- 2.1.6. A plataforma atualmente implantada encontra-se integrada à arquitetura de segurança da SEFAZ, incluindo regras de segmentação já definidas, grupos de aplicações mapeados, etiquetas de classificação operacional, políticas de comunicação homologadas e processos internos de governança e resposta a incidentes;
- 2.1.7. A eventual substituição da solução atualmente utilizada poderá acarretar impactos técnicos e operacionais relevantes, incluindo:
 - 2.1.7.1. necessidade de reconstrução integral das políticas de segmentação existentes;
 - 2.1.7.2. remapeamento de dependências entre aplicações e serviços;
 - 2.1.7.3. reclassificação de workloads e ativos protegidos;
 - 2.1.7.4. revalidação das regras de comunicação atualmente homologadas;
 - 2.1.7.5. aumento da complexidade operacional durante o processo de transição;
 - 2.1.7.6. risco de indisponibilidade ou interrupção indevida de comunicações legítimas entre aplicações críticas;



2.1.7.7. e comprometimento temporário da visibilidade operacional atualmente existente sobre os fluxos internos do ambiente computacional;

2.1.8. Considerando:

2.1.8.1. a necessidade de preservação da arquitetura de segmentação lógica já implantada;

2.1.8.2. a manutenção das políticas de segurança atualmente estabelecidas;

2.1.8.3. a continuidade operacional dos mecanismos de controle de comunicação interna do ambiente;

2.1.8.4. a mitigação de riscos associados à reconstrução de políticas e remapeamento de dependências aplicacionais;

2.1.8.5. o aproveitamento do esforço técnico e operacional já realizado na implementação da solução;

2.1.8.6. a necessidade de manutenção da interoperabilidade entre os componentes de segurança já existentes;

2.1.8.7. os custos técnicos, operacionais e administrativos decorrentes de eventual substituição integral da plataforma atualmente implantada;

2.1.8.8. o conhecimento técnico adquirido pelas equipes responsáveis pela operação da solução;

2.1.8.9. e o disposto no art. 11, inciso I, art. 18, §1º, inciso VIII, e art. 40, inciso V, alínea "b", da Lei nº 14.133/2021, que autorizam a adoção de padronização como mecanismo de eficiência administrativa, economicidade, compatibilidade técnica e obtenção da solução mais vantajosa para a Administração Pública;

2.1.9. Em razão da necessidade de preservação da continuidade operacional, compatibilidade técnica, interoperabilidade da arquitetura de segurança e manutenção dos mecanismos de segmentação já implementados, deverá ser fornecida mediante licenciamento da plataforma Illumio atualmente existente no ambiente da SEFAZ, observando os quantitativos e características técnicas definidos neste instrumento convocatório.

LOTE 3

Todos os requisitos solicitados deverão ser atendidos por qualquer das soluções apresentadas que componham o escopo do Lote 3. Não há obrigação de que cada requisito seja necessariamente atendido pela ferramenta na qual esteja descrito, será admitido o atendimento de requisitos através da composição de funcionalidades de ferramentas distintas, desde que todos estejam integrados entre si e entra as demais ferramentas deste lote.

SOLUÇÃO DE GESTÃO DE VULNERABILIDADES COM FOCO EM RISCO E IDENTIDADE

3. SOLUÇÃO DE GESTÃO DE VULNERABILIDADES

3.1. Dos requisitos gerais

3.1.1. O objetivo é atuar de maneira preventiva e contínua na detecção de eventuais vulnerabilidades de segurança da informação presentes na infraestrutura e nas



aplicações da SEFAZ-ES, reduzindo os riscos de exploração por ataques cibernéticos que possam se valer de falhas já conhecidas.

- 3.1.2. O licenciamento deverá ser obrigatoriamente de propriedade da CONTRATADA e não poderá ser do tipo open source (software livre);
- 3.1.3. A solução deve realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance);
- 3.1.4. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede
- 3.1.5. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;
- 3.1.6. A solução deve ser licenciada pelo número de endereços IP ou dispositivos (assets);
- 3.1.7. A solução deve fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externos ou de terceiros;
 - 3.1.7.1. Caso a solução dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela CONTRATADA.
- 3.1.8. A solução deverá suportar API (Application Programming Interface) baseada em REST (Representational State Transfer) para automação de processos e integração com aplicações terceiras.
- 3.1.9. A solução deve possuir integração via API no mínimo as seguintes linguagens: Python, Powershell, Ruby, javascript, Java, Swift e PHP;
- 3.1.10. A solução deve possuir métodos de consulta via api e envio, tais como: HTTP METHOD (POST, GET, PUT AND DELETE);
- 3.1.11. A solução deve incluir a opção para agentes instalados e licenciados em estações de trabalho e servidores, para varredura diretamente no sistema operacional;
- 3.1.12. Tais agentes devem ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades;
- 3.1.13. A solução deve permitir o agrupamento de scanners para facilitar o gerenciamento e aplicação de políticas;
- 3.1.14. A solução deve realizar a varredura tanto de dispositivos na rede interna, dispositivos expostos a demais redes externas, tanto quanto dispositivos em nuvens públicas como Azure, AWS ou GCP;
- 3.1.15. O escaneamento para os dispositivos expostos deve ser realizados através de SCANS (ENGINE) do próprio fabricante alocados no Brasil;
- 3.1.16. Os scanners e sensores agentes deverão ser gerenciados por uma única plataforma, de maneira centralizada;
- 3.1.17. O acesso a console de gerenciamento deve ser fornecida para pelo menos 10 usuários simultâneos;
- 3.1.18. A solução deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM);
- 3.1.19. A solução deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção;



- 3.1.20. A solução deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (outputs);
- 3.1.21. A solução deve fornecer controle de acesso baseado em função (RBAC- Role Based Access Control) para controlar o acesso do usuário a conjuntos de dados e funcionalidades;
- 3.1.22. A solução deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e dashboards;
- 3.1.23. A solução deve ter a capacidade de excluir determinados endereços IP do escopo de qualquer varredura ou scan;
- 3.1.24. A solução deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito;
- 3.1.25. A solução deve suportar métodos de autenticação usando bases de autenticação local, e SAML (Security Assertion Markup Language) para uso de SSO (Single Sign-On);
- 3.1.26. A solução deve ser capaz de orquestrar scanners ilimitados dentro da infraestrutura;
- 3.1.27. A solução não deve impor nenhum limite de quantidade de scanners implementados dentro da infraestrutura;
- 3.1.28. A solução deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de e-mail;
- 3.1.29. A solução deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características:
 - 3.1.29.1. Sistema Operacional, Endereço IP, DNS, NetBIOS Host, MAC, AWS Instance Type, AWS EC2 Name, Software instalado, Azure VM ID, AWS Region, Google Cloud Instance ID, Azure Resource ID, Ativos avaliados.

3.2. Dos requisitos e relatórios e painéis gerenciais

- 3.2.1. A solução deverá possuir painéis gerenciais (dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados;
- 3.2.2. Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento;
- 3.2.3. Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução;
- 3.2.4. Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um exploit disponível e informações do ativo;
- 3.2.5. A solução deve permitir a customização de dashboards/relatórios;
- 3.2.6. A solução deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas;
- 3.2.7. A solução deve ser capaz de produzir relatórios, pelo menos, nos seguintes formatos: HTML, PDF e CSV;
- 3.2.8. A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos;



- 3.2.9. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);
- 3.2.10. A solução deve suportar o envio automático de relatórios para destinatários específicos;
- 3.2.11. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
- 3.2.12. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;

3.3. Das varreduras

- 3.3.1. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como appliances virtuais;
- 3.3.2. A solução deve suportar varredura com e sem agente, de maneira ativa e passiva, distribuídas em diferentes localidades e regiões e gerenciar todos por uma console central;
- 3.3.3. A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de vulnerabilidades;
- 3.3.4. Tais agentes devem realizar conexões para o sistema gerenciamento através de protocolo seguro;
- 3.3.5. A solução deve ser configurável para permitir a otimização das configurações de varredura;
- 3.3.6. A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;
- 3.3.7. A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
- 3.3.8. A solução deve se integrar com solução de gerenciamento de acessos privilegiados para autenticação nos dispositivos, no mínimo, os seguintes:
 - 3.3.8.1. CyberArk;
 - 3.3.8.2. BeyondTrust;
 - 3.3.8.3. Thycotic;
 - 3.3.8.4. Delínea;
- 3.3.9. A solução deve suportar o agendamento de scans personalizados, incluindo a capacidade de executar varreduras em tempos designados, com frequência pré-determinada;
- 3.3.10. A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de scan;
- 3.3.11. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
- 3.3.12. A solução deve ser capaz de realizar em tempo real a descoberta de vulnerabilidades nas seguintes tecnologias:



- 3.3.12.1. Cloud Services;
- 3.3.12.2. Data Leakage;
- 3.3.12.3. Database;
- 3.3.12.4. IoT;
- 3.3.12.5. Mobile Devices;
- 3.3.12.6. Operating System;
- 3.3.12.7. Peer-To-Peer;
- 3.3.12.8. SCADA;
- 3.3.12.9. Web Servers;
- 3.3.12.10. Web Clients;

3.3.13. A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;

3.3.14. A solução deve em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede;

3.4. Da análise e priorização de vulnerabilidades

3.4.1. A solução deve ser capaz de exibir ambos severidade e pontuação, com base em CVSS (Common Vulnerability Scoring System) e inteligência de ameaças;

3.4.2. A solução deve utilizar sistema de pontuação e priorização das vulnerabilidades que utilize no mínimo:

3.4.3. CVSS Impact Score;

3.4.4. Idade da Vulnerabilidade;

3.4.5. Maturidade de códigos de exploração da vulnerabilidade encontrada;

3.4.6. Frequência de uso da vulnerabilidade em ataques e campanhas atuais;

3.4.7. Disponibilidade do código de exploração da vulnerabilidade;

3.4.8. Presença de módulos de exploração de vulnerabilidade em frameworks automatizados de exploração de vulnerabilidades como CANVAS, Metasploit e Core Impact;

3.4.9. Popularidade da vulnerabilidade em fóruns e comunicações na Darkweb;

3.4.10. O mecanismo de priorização deve ser sujeito a modificações e atualizações diárias com base em inteligência de ameaças e observação de tendências na Internet;

3.5. Da inteligência de vulnerabilidades centralizada

3.5.1. A solução deve fornecer acesso integrado e em tempo real a um banco de dados de vulnerabilidades abrangente, alimentado por múltiplas fontes, incluindo:

3.5.2. Conhecimento interno do time de pesquisa do fabricante.

3.5.3. Avisos de fornecedores/fabricantes de softwares e hardwares.

3.5.4. GitHub Advisory Database.

3.5.5. National Vulnerability Database (NVD).

- 3.5.6. Deve ser acessível diretamente pela plataforma de Gestão de Vulnerabilidades, sem a necessidade de ferramentas externas ou integrações complexas.
- 3.5.7. O banco de dados de vulnerabilidades deve ser atualizado continuamente com as últimas informações de vulnerabilidades, garantindo a detecção de ameaças emergentes.
- 3.5.8. A solução deve incluir categorias de vulnerabilidades curadas pelo time de pesquisa do fabricante, combinando indicadores de risco conhecidos com insights especializados para destacar as vulnerabilidades mais críticas e relevantes para o ambiente da SEFAZ.
- 3.5.9. Deverá oferecer categorias de vulnerabilidades pré-definidas e atualizadas, permitindo a priorização e ação rápida em relação às vulnerabilidades críticas, conforme as seguintes categorias:
- 3.5.10. Ameaças Emergentes: Identificação e destaque de vulnerabilidades que estão sendo ativamente monitoradas pelo fabricante da solução, devido ao seu potencial de exploração iminente.
- 3.5.11. Vulnerabilidades Conhecidas da CISA (Cybersecurity and Infrastructure Security Agency): Integração com o Catálogo de Vulnerabilidades Conhecidas da CISA, permitindo a identificação e priorização de vulnerabilidades que são conhecidas por serem exploradas ativamente.
- 3.5.12. Exibição das 50 principais vulnerabilidades com base na Classificação de Prioridade do fabricante, levando em consideração a gravidade, a probabilidade de exploração, existência e maturidade do Exploit.
- 3.5.13. Vulnerabilidades Persistentemente Exploradas: vulnerabilidades que são consistentemente exploradas por atores de ameaças ao longo do tempo.
- 3.5.14. Vulnerabilidades exploradas por Ransomware: Identificação de vulnerabilidades que são comumente exploradas em ataques de Ransomware.
- 3.5.15. Vulnerabilidades Recentemente Exploradas: Identificação de vulnerabilidades que receberam cobertura significativa da imprensa e evidências de exploração ativa.
- 3.5.16. Em Destaque nas Notícias: Identificação de vulnerabilidades que foram amplamente relatadas na imprensa, indicando um alto nível de conscientização pública e potencial de exploração.
- 3.5.17. A solução deve permitir a correlação entre vulnerabilidades conhecidas e a exposição real dos ativos identificando quais sistemas e aplicações são afetados por vulnerabilidades críticas e baseados em categorias.
- 3.5.18. Deve fornecer ao administrador a capacidade de filtrar e pesquisar vulnerabilidades com base em categorias, bem como em outros critérios, como gravidade, data de publicação e ativos afetados.
- 3.5.19. A solução deve permitir a geração de relatórios e painéis personalizáveis que exibem informações sobre as vulnerabilidades em cada categoria, permitindo o monitoramento e a análise da postura de segurança.
- 3.5.20. Deve fornecer informações sobre os incidentes de segurança recentes associados as vulnerabilidades.

3.6. Da análise de risco do ambiente

- 3.6.1. A solução deve gerar um score que combine dados de vulnerabilidades com a



criticidade dos ativos do ambiente computacional;

- 3.6.2. O cálculo da pontuação deve ser dinâmico e representar o risco de exposição cibernética da organização, baseada nas pontuações de exposição dos ativos, auxiliando na comunicação eficaz do risco cibernético para líderes e partes interessadas.
- 3.6.3. O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;
- 3.6.4. Deve ser capaz de calcular a criticidade dos ativos da organização;
- 3.6.5. A solução deve ser capaz de realizar um benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor;
- 3.6.6. A solução deve prover visão sobre quais ações de remediação reduzem o maior nível de risco do ambiente;
- 3.6.7. A solução deve também permitir a visualização de ações de remediação agregadas para visão consolidada de redução de risco;
- 3.6.8. Deve permitir modificar a qualquer momento o tipo de indústria para comparação.
Ex: Mudar de Setor Público para Mercado Financeiro;
- 3.6.9. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;
- 3.6.10. A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo);
- 3.6.11. A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos;
- 3.6.12. A solução deve oferecer uma capacidade de comparação (benchmarking) da pontuação referente a exposição cibernética com outros players da mesma indústria assim como outras empresas do mercado;
- 3.6.13. A solução deve permitir um acompanhamento histórico do nível de exposição da organização;
- 3.6.14. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução;
- 3.6.15. A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade;
- 3.6.16. A solução deve permitir a segregação lógica entre áreas distintas da empresa afim de obter a pontuação referente exposição cibernética por área;

3.7. Do gerenciamento da análise de ataques exploráveis

- 3.7.1. Deve disponibilizar visibilidade nas técnicas de ataque baseado no framework MITRE ATT&CK;



- 3.7.2. Deve identificar qual a criticidade do ataque, em no mínimo: baixo, médio e alto;
- 3.7.3. Deve permitir a visualização gráfica dos caminhos de ataque, permitindo uma análise detalhada e intuitiva dos vetores de exploração.
- 3.7.4. Deve prover a evidência relacionada a descoberta do ataque;
- 3.7.5. Deve mostrar o objeto relacionado ao ataque, de origem e de destino;
- 3.7.6. Deve apresentar informações detalhadas relacionadas a mitigação para o ataque em análise;
- 3.7.7. Deve prover quais ferramentas e possíveis malwares associados ao ataque;
- 3.7.8. Deve disponibilizar de forma gráfica via console de gerenciamento as conexões entre os objetos do ataque;
- 3.7.9. Deve disponibilizar uma biblioteca com 'Queries' para a busca de objetos no mínimo os seguintes segmentos:
 - 3.7.9.1.1. Rede;
 - 3.7.9.1.2. Endpoint;
 - 3.7.9.1.3. Active Directory;
 - 3.7.9.1.4. Permissão;
 - 3.7.9.1.5. Ransomware;
 - 3.7.9.1.6. Vetores;
 - 3.7.9.1.7. Credenciamento;
- 3.7.10. Deve suportar todas as táticas de ataques mapeadas no framework MITRE ATT&CK;
- 3.7.11. Deve permitir analisar, ao menos, os seguintes caminhos das superfícies de ataques:
 - 3.7.11.1. Aplicações WEB (DAST);
 - 3.7.11.2. Nuvem;
 - 3.7.11.3. Active Directory;
 - 3.7.11.4. Infraestrutura (Desktops, Servidores).
- 3.7.12. Deve apresentar os resultados em forma ilustrativa (Dashboard).
- 3.7.13. O Dashboard deve oferecer uma visão dos seus ativos vulneráveis considerando:
 - 3.7.13.1. Número de ativos críticos vulneráveis;
 - 3.7.13.2. Número de caminhos de ataque que levam a esses ativos críticos;
 - 3.7.13.3. Número de descobertas abertas e sua gravidade;
 - 3.7.13.4. Matriz para visualizar caminhos com diferentes combinações de valores alvo;
 - 3.7.13.5. Lista de tendências de caminhos de ataque.
- 3.7.14. Deve listar as diferenças entre os intervalos de tempo e mostrar uma seta direcional a fim de indicar se o valor aumentou ou diminuiu.

- 3.7.15. Deve permitir que o caminho de ataque leve a um ativo crítico.
- 3.7.16. Deve apresentar o número total alcançado de ativos críticos;
- 3.7.17. Deve apresentar uma tendência dos caminhos de ataque, listando os caminhos de ataques mais populares.
- 3.7.18. Deve ser possível identificar o host suspeito;
- 3.7.19. Deve ser possível identificar o usuário suspeito;
- 3.7.20. Deve ser possível identificar o IP suspeito;
- 3.7.21. Deve permitir visualização em modo ilustrativo do caminho de ataque;
- 3.7.22. Deve ser possível identificar qual a técnica utilizada pelo atacante, tais como:
 - 3.7.22.1. Network Sniffing;
 - 3.7.22.2. LSASS Memory;
 - 3.7.22.3. Remote Desktop Protocol;
 - 3.7.22.4. Exploração de serviços remotos;
 - 3.7.22.5. System Services Discovery;
 - 3.7.22.6. Modificação da Política de Grupo;
 - 3.7.22.7. Mecanismo de Controle de Elevação de Abuso.
- 3.7.23. Deve permitir a comunicação com o framework MITRE ATT&CK ®.
- 3.7.24. Deve trazer o número de identificação MITRE ATT&CK para a descoberta;
- 3.7.25. A descoberta no MITRE ATT&CK deve abordar as seguintes ações:
- 3.7.26. A técnica MITRE ATT&CK associada ao achado.
- 3.7.27. A origem da descoberta.
- 3.7.28. O alvo da descoberta.
- 3.7.29. O status para indicar a ação tomada na descoberta, por exemplo, 'Em andamento'.
- 3.7.30. Deve ser possível exportar uma descoberta como CSV.
- 3.7.31. Deve ser possível arquivar uma descoberta.
- 3.7.32. Deve ser possível ver o histórico do log da descoberta.
- 3.7.33. Deve permitir alterar o status do caminho de ataque descoberto para, pelo menos:
 - 3.7.33.1. Em Progresso;
 - 3.7.33.2. Em Revisão;
 - 3.7.33.3. Feito;

3.8. Da descoberta de ativos

- 3.8.1. A solução deve ser capaz de realizar escaneamento de descoberta de rede utilizando os seguintes critérios como alvo: IP, CIRD e Range;
- 3.8.2. A solução deve disponibilizar modelos de escaneamento de descoberta, ajustável, com os seguintes tipos de scan:
 - 3.8.2.1. Enumeração de Hosts;



- 3.8.2.2. Identificação de Sistema Operacional (SO);
- 3.8.2.3. Port Scan (Portas comuns);
- 3.8.2.4. Port Scan (Todas as portas);
- 3.8.2.5. Customizado;
- 3.8.3. A solução deve permitir realizar escaneamento de descoberta customizado podendo ser parametrizado de acordo com a necessidade;
- 3.8.4. A parametrização do escaneamento de descoberta deve, no mínimo, conter os seguintes requisitos:
 - 3.8.4.1. Descoberta de Host;
 - 3.8.4.2. Ping o host remoto;
 - 3.8.4.3. Usar descoberta rápida;
 - 3.8.4.4. Métodos de ping;
 - a) ARP;
 - b) TCP;
 - c) ICMP;
 - d) UDP;
 - e) HTTP/HTTPS Ping;
 - f) Varredura/Ping Sweep controlado.
 - 3.8.4.5. Escaneamento de descoberta de dispositivos de OT/SCADA;
 - 3.8.4.6. Escaneamento de descoberta em redes de impressora;
 - 3.8.4.7. Escaneamento em redes Novell;
 - 3.8.4.8. Tecnologia de Wake-on-LAN;
 - 3.8.4.9. Port Scanning;
 - 3.8.4.10. Portas
 - a) Considerar portas não escaneadas como fechadas;
 - b) Range de portas a serem escaneadas;
 - 3.8.4.11. Enumerar Portas locais:
 - a) SSH (netstat);
 - b) WMI (netstat);
 - c) SNMP;
 - 3.8.4.12. Descoberta de Serviços:
 - c) Sondar todas as portas para encontrar serviços;
 - d) Procurar por serviços baseado em SSL/TLS;
 - e) Enumerar todas as cifras SSL/TLS;
- 3.8.5. A solução deve realizar descoberta de ativo de forma passiva e adicionado automaticamente na console de gerenciamento;



3.8.6. A solução deve descobrir passivamente quando um host é adicionado na rede;

3.9. Do inventário de ativos e mapeamento de exposição

3.9.1. Deve consolidar todos os ativos da organização em uma única interface, incluindo dispositivos, contas de usuário, softwares, ativos em nuvem e aplicações SaaS, facilitando a análise e gestão centralizada.

3.9.2. A solução deve calcular dinamicamente uma pontuação de exposição para cada ativo, variando de 0 a 1000, indicando o nível de risco associado. Pontuações mais altas representarão maior exposição.

3.9.3. Deve atribuir uma classificação de criticidade a cada ativo, em uma escala de 1 a 10, auxiliando na priorização de medidas de segurança com base na importância do ativo para a organização.

3.9.4. Permitir a criação e aplicação de etiquetas (tags), tanto estáticas quanto dinâmicas, para categorizar e organizar ativos conforme critérios específicos, como localização, função ou nível de risco.

3.9.4.1. As tags devem suportar o agrupamento de ativos on premises, recursos em nuvem, identidades e aplicações Web.

3.9.4.2. A solução deve gerar para cada agrupamento, uma pontuação de risco associado, bem como a porcentagem de contribuição para a pontuação global da SEFAZ.

3.9.5. A solução deve oferecer a capacidade de adicionar sinais de exposição personalizados para monitorar combinações específicas de riscos que possam impactar a organização, permitindo uma gestão proativa das fraquezas (vulnerabilidades, configurações incorretas e permissões excessivas);

3.9.6. A plataforma deve permitir a integração com fontes de dados externas e ferramentas de terceiros para uma análise mais aprofundada da exposição e remediação de riscos.

3.9.7. Deve garantir que as informações sobre os ativos sejam atualizadas sempre que um ativo é identificado em uma varredura, mantendo a precisão e relevância dos dados no inventário.

3.9.8. Deve possibilitar a detecção de combinações específicas de vulnerabilidades, exposições de identidade e ameaças que, juntas, aumentam significativamente o risco para a organização.

3.9.9. A plataforma deve possuir uma biblioteca de sinais de exposição pré-definidos pelo fabricante da solução, permitindo às equipes de segurança iniciar rapidamente a identificação de cenários de risco críticos.

3.9.10. A solução deve possibilitar criar sinais de exposição personalizados, utilizando consultas específicas ou processamento de linguagem natural (NLP), adaptando a detecção de riscos às necessidades específicas do negócio.

3.9.11. Deve possibilitar o monitoramento contínuo das violações associadas a cada sinal de exposição, com apresentação de tendências e porcentagens de mudança nos últimos 7 dias, auxiliando na identificação de padrões emergentes.

3.9.12. A plataforma deve possuir uma listagem detalhada dos ativos afetados por cada sinal de exposição, incluindo informações como nome do ativo, pontuação de exposição e detalhes específicos das fraquezas identificadas.



- 3.9.13. Deve possuir funcionalidades para arquivar, editar, duplicar ou excluir sinais de exposição personalizados, proporcionando flexibilidade no gerenciamento dos sinais conforme a evolução das necessidades de segurança.
- 3.9.14. A solução deve utilizar inteligência artificial para fornecer explicações detalhadas sobre cada sinal de exposição e seus ativos impactados, facilitando a compreensão e a tomada de decisões informadas pelas equipes de segurança.
- 3.9.15. A plataforma deve unificar as informações de inventário de todos os módulos da solução, com integração nativa ou via API, permitindo uma gestão centralizada e integrada das exposições cibernéticas.

3.10. Da avaliação de vulnerabilidade

- 3.10.1. A solução deve ser capaz de realizar testes sem a necessidade de agentes instalados no dispositivo destino para detecção de vulnerabilidades;
- 3.10.2. A solução deve detectar e classificar através de severidades, riscos e vulnerabilidades;
- 3.10.3. A solução deve também fornecer informações detalhadas sobre a natureza da vulnerabilidade, evidências da existência da vulnerabilidade e recomendações para mitigá-los;
- 3.10.4. A solução deve incluir uma saída detalhada das vulnerabilidades descobertas como versões de DLL esperadas e encontradas;
- 3.10.5. A solução deve ser compatível com CVE e fornecer pelo menos 10 anos de cobertura CVE;
- 3.10.6. A solução deve identificar vulnerabilidades específicas para o Active Directory com os seguintes padrões de verificação:
- 3.10.6.1. Contas administrativas vulneráveis a Kerberoasting attack;
 - 3.10.6.2. Utilização de criptografia vulnerável com autenticação Kerberos;
 - 3.10.6.3. Contas com pré-autenticação do Kerberos desabilitada;
 - 3.10.6.4. Verificação de usuários com a opção de nunca expirar a senha com a opção habilitada;
 - 3.10.6.5. Verificar validação de fragilidades do tipo "Unconstrained Delegation";
 - 3.10.6.6. Verificação de "Pre-Windows 2000 Compatible Access";
 - 3.10.6.7. Verificação de validade de chaves mestras "Kerberos KRBTGT";
 - 3.10.6.8. Verificação de "SID History Injection";
 - 3.10.6.9. Verificação de "Printer Bug Exploit";
 - 3.10.6.10. Verificação de "Primary Group ID";
 - 3.10.6.11. Verificação de usuários com Passwords em branco;
- 3.10.7. A solução deve suportar o uso de SMB e WMI para verificação de sistemas Microsoft Windows;
- 3.10.8. A solução deve ser capaz de realizar a varredura credenciada de sistemas Windows com acesso ao registro remoto, seja por ativação automática do serviço durante a varredura, seja mediante habilitação prévia do serviço pelo administrador como pré-



requisito;

- 3.10.9. Quando a solução ativar automaticamente o serviço de registro remoto para fins de varredura credenciada, deve ser capaz de restaurá-lo ao seu estado anterior ao término da varredura, admitindo-se, alternativamente, procedimento operacional equivalente de restauração do serviço orientado pela CONTRATADA;
- 3.10.10. O scanner deve oferecer suporte a shell seguro (SSH) com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix;
- 3.10.11. A solução deve suportar o uso do netstat (Linux) e WMI (Windows) para uma enumeração rápida e precisa de portas em um sistema quando as credenciais são fornecidas;
- 3.10.12. O scanner deve oferecer suporte a shell seguro (SSH) com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix;
- 3.10.13. A solução deve suportar o uso do netstat (Linux) e WMI (Windows) para uma enumeração rápida e precisa de portas em um sistema quando as credenciais são fornecidas:
- 3.10.13.1. A solução deve possibilitar a verificação remota de portas, além da enumeração local de portas, para ajudar a determinar se algum mecanismo de controle de acesso está sendo utilizado;
- 3.10.14. A solução deve fornecer auditoria de patch (MS Bulletins) para as principais versões de Windows;
- 3.10.15. A solução deve fornecer auditoria de patch para todos os principais sistemas operacionais Unix incluindo Mac OS, Linux, Solaris e IBM AIX;
- 3.10.16. A solução deve fornecer varredura para aplicativos comerciais diversos e proprietários, incluindo, mas não limitando-se a: Java, Adobe, Oracle, Apple, Microsoft, Check Point, Palo Alto Networks, Cisco, Fortinet, Trellic, etc;
- 3.10.17. A solução deve incluir classificação de severidades de acordo com o padrão Sistema Comum de Pontuação de Vulnerabilidade Versão (CVSS2 e CSVSS 3);
- 3.10.18. A solução deve fornecer informações acerca da disponibilidade de códigos de exploração das vulnerabilidades encontradas em frameworks de exploração para as plataformas mais populares: Core, Metasploit e Canvas;
- 3.10.19. A solução deve informar se a vulnerabilidade pode e está sendo ativamente explorada por código malicioso (malware);
- 3.10.20. A solução deve possuir importação de arquivos .YARA;
- 3.10.21. Deve ser capaz de identificar e classificar vulnerabilidades de máquinas virtuais em nuvem pública em infraestruturas como serviço nas plataformas AWS, Microsoft Azure e Google Cloud;

3.11. Da auditoria de configuração

- 3.11.1. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;
- 3.11.2. A solução deve fornecer benchmarks de auditoria de segurança e configuração

para conformidade regulatória e outros padrões de práticas recomendadas pela área ou fabricantes;

3.11.3. A solução deve realizar verificações de auditoria contendo as de segurança, com indicação de sucesso ou falha, baseado nos principais frameworks reconhecidos pela indústria, pelo menos os seguintes:

- 3.11.3.1. Center for Internet Security Benchmarks (CIS);
- 3.11.3.2. Defense Information Systems Agency (DISA) STIGs;
- 3.11.3.3. Health Insurance Portability and Accountability Act (HIPAA);
- 3.11.3.4. Payment Card Industry Data Security Standards (PCI DSS).

3.11.4. A solução deve fornecer auditoria de soluções de proteção de endpoint (antivírus, antimalware ou EDR), verificando presença, status de execução, status de inicialização e atualidade das assinaturas ou do mecanismo de detecção, com suporte aos principais fabricantes de mercado;

3.11.5. A solução deve fornecer auditorias de configuração com base benchmarks em CIS (Center for Internet Security) L1 e L2, para ambos os sistemas operacionais Microsoft Windows e Linux;

3.11.6. A solução deve permitir auditoria de conformidade em servidores Windows, Linux, Bancos de Dados SQL Server, a fim de determinar se estão configurados de acordo com os principais Framework de segurança como, por exemplo, CIS e DISA;

3.11.7. A solução deve oferecer validação e suporte a SCAP (Security Content Automation Protocol);

3.12. Do gerenciamento de superfície de ataque

3.12.1. Requisitos Gerais

- 3.12.1.1. Deve possuir Interface intuitiva com dashboards personalizáveis e relatórios automáticos.
- 3.12.1.2. Possuir integração com outras ferramentas de segurança, como SIEMs e plataformas de gerenciamento de vulnerabilidades.
- 3.12.1.3. Para varredura aprofundada de uma aplicação web exposta, deve possuir integração para iniciar uma varredura pela solução de DAST da própria plataforma ou possuir integração nativa com a solução de Web Application Scanning.
- 3.12.1.4. Deve possuir conformidade com normas e padrões de segurança reconhecidos, como ISO 27001, NIST e LGPD.

3.12.2. Descoberta e Mapeamento de Ativos

- 3.12.2.1. Possuir identificação automática e contínua de ativos expostos na internet, incluindo domínios, subdomínios, endereços IP, portas abertas e serviços.
- 3.12.2.2. Para detecção de ativos expostos, deve ainda permitir integração com a Cloudflare, AWS, Microsoft Azure e Google Cloud Platform.
- 3.12.2.3. Deve ter capacidade de correlacionar ativos a partir de ASN, registros DNS, certificados SSL/TLS e outros dados públicos.
- 3.12.2.4. Possuir atualização frequente da superfície de ataque, com ciclos diários



ou quinzenais.

3.12.3. Classificação e Contextualização de Ativos

- 3.12.3.1. Deve coletar e possuir organização de metadados de ativos, incluindo versão de software, tecnologias utilizadas e localização geográfica.
- 3.12.3.2. Deve possuir filtros avançados para classificação de ativos por risco, tipo e criticidade.
- 3.12.3.3. Possuir capacidade de agrupar e categorizar ativos conforme necessidade do órgão contratante.
- 3.12.3.4. Deve possuir sensores na Internet para detectar domínios semelhantes com os monitorados pela plataforma. Além disso, deve permitir a adição dos domínios e subdomínios semelhantes encontrados ao inventário da solução.

3.12.4. Avaliação de Riscos e Detecção de Vulnerabilidades

- 3.12.4.1. Deve possuir identificação automática de vulnerabilidades em ativos expostos.
- 3.12.4.2. Deve correlacionar bancos de dados de vulnerabilidades públicos e proprietários, como CVE, NVD e outras fontes de ameaças conhecidas.
- 3.12.4.3. Deve possuir análise de riscos baseada em criticidade, com recomendações de mitigação priorizadas.
- 3.12.4.4. Deve avaliar a postura de segurança e o risco com verificação de vulnerabilidade dos ativos descobertos externos a organização.
- 3.12.4.5. Permitir acompanhar as alterações selecionadas, por meio de alertas automáticos, em conformidade, tecnologia e exposição.

3.12.5. Integração com Plataformas e Automação

- 3.12.5.1. APIs abertas para integração com sistemas de gerenciamento de vulnerabilidades, SIEMs e plataformas de Threat Intelligence.
- 3.12.5.2. Possibilidade de exportação de relatórios em formatos padronizados (CSV, JSON, PDF).
- 3.12.5.3. Suporte à automação de respostas a incidentes e workflows de segurança.
- 3.12.5.4. Conexão com sistemas de monitoramento de DNS e reputação de IPs para detecção de domínios comprometidos ou maliciosos.
- 3.12.5.5. Capacidade de correlacionar dados com feeds de Threat Intelligence, identificando ameaças emergentes associadas aos ativos descobertos.

3.12.6. Relatórios e Auditoria

- 3.12.6.1. Geração automática de relatórios customizáveis para auditorias, conformidade e gestão de riscos.
- 3.12.6.2. Deve possuir registros detalhados de todas as ações realizadas na plataforma para fins de auditoria e rastreabilidade.

3.13. Solução de análise dinâmica de vulnerabilidades para aplicações web



- 3.13.1. A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;
- 3.13.2. A solução deve ser capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);
- 3.13.3. A solução deve avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (payment card industry data security standard);
- 3.13.4. A solução deve suportar as diretivas PCI ASV 5.5 para definição de escopo de análise da aplicação;
- 3.13.5. A solução deve suportar as diretivas PCI ASV 6.1 para definição de balanceadores de carga das aplicações bem como suas configurações para inclusão no relatório de resultados;
- 3.13.6. A solução deve possuir templates prontos de varreduras entre simples e extensos;
- 3.13.7. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:
 - 3.13.7.1. Cookies, Headers, Formulários e Links;
 - 3.13.7.2. Nomes e valores de parâmetros da aplicação;
 - 3.13.7.3. Elementos JSON e XML;
 - 3.13.7.4. Elementos DOM.
- 3.13.8. A solução deve permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;
- 3.13.9. A solução deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;
- 3.13.10. A solução deve excluir determinadas URLs da varredura através de expressões regulares;
- 3.13.11. A solução deve excluir determinados tipos de arquivos através de suas extensões;
- 3.13.12. A solução deve instituir no mínimo os seguintes limites:
 - 3.13.12.1. Número máximo de URLs para crawl e navegação;
 - 3.13.12.2. Número máximo de diretórios para varreduras;
 - 3.13.12.3. Número máximo de elementos DOM;
 - 3.13.12.4. Tamanho máximo de respostas;
 - 3.13.12.5. Limite de requisições de redirecionamentos;
 - 3.13.12.6. Tempo máximo para a varredura;
 - 3.13.12.7. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;
 - 3.13.12.8. Número máximo de requisições HTTP por segundo;
- 3.13.13. A solução deve detectar congestionamento de rede e limitar os seguintes aspectos da varredura:
 - 3.13.13.1. Limite em segundos para timeout de requisições de rede;



- 3.13.13.2. Número máximo de timeouts antes que a varredura seja abortada;
- 3.13.14. A solução deve agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
- 3.13.15. A solução deve enviar notificações através de no mínimo E-mail e SMS;
- 3.13.16. A solução deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques;
- 3.13.17. A solução deve avaliar sistemas web utilizando protocolos HTTP e HTTPS;
- 3.13.18. A solução deve possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizado a ser enviada durante os testes;
- 3.13.19. A solução deve ser compatível com avaliação de web services REST e SOAP;
- 3.13.20. Deverá suportar no mínimo os seguintes esquemas de autenticação:
 - 3.13.20.1. Autenticação básica (digest);
 - 3.13.20.2. NTLM;
 - 3.13.20.3. Forma de login;
 - 3.13.20.4. Autenticação de Cookies;
 - 3.13.20.5. Autenticação através de Selenium;
 - 3.13.20.6. Autenticação através de Bearer;
- 3.13.21. A solução deve importar scripts de autenticação selenium previamente configurados pelo usuário;
- 3.13.22. A solução deve customizar parâmetros Selenium como delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos;
- 3.13.23. A solução deve exibir os resultados das varreduras em tendência temporal para acompanhamento de correções e introdução de novas vulnerabilidades;
- 3.13.24. A solução deve exibir os resultados agregados de acordo com as categorias do OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project);
- 3.13.25. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
- 3.13.26. Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes;
- 3.13.27. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc), deve evidenciar nos detalhes do evento encontrado:
 - 3.13.27.1. Payload injetado;
 - 3.13.27.2. Evidência em forma de resposta da aplicação;
 - 3.13.27.3. Detalhes da requisição HTTP;
 - 3.13.27.4. Detalhes da resposta HTTP;



3.13.28. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;

3.13.29. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;

3.13.30. A solução deve possuir suporte a varreduras de componentes para no mínimo:

3.13.30.1. Wordpress, Blog Designer Plugin for Wordpress, Event Calendar Plugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat, Apache Tomcat JK connecto, Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla.

3.14. Solução para segurança para nuvem pública, multi-cloud, aderente ao conceito de cnapp (cloud-native application protection platform)

3.14.1. Arquitetura

3.14.1.1. A solução de Segurança deve ser fornecida no modelo SaaS;

3.14.1.2. Deve suportar Múltiplas Regiões;

3.14.1.3. A solução deve fornecer segregação de Dados por Instância;

3.14.1.4. A solução deve utilizar criptografia dos dados em trânsito com TLS 1.2;

3.14.1.5. Para todos os dados armazenados, a solução deve utilizar criptografia com AES-256;

3.14.1.6. O fabricante da plataforma deve garantir Backup e Proteção dos dados armazenados;

3.14.1.7. A plataforma da solução deve ter Certificação SOC 2 Type II e ISO/IEC 27001;

3.14.1.8. A solução deve ser compatível com o conceito de CNAPP, incluindo as seguintes disciplinas:

- a) Cloud Security Posture Management;
- b) Kubernetes Security Posture Management;
- c) Cloud Identity and Entitlement Management;
- d) Infrastructure as a Code;
- e) Cloud Workload Protection Platform;
- f) Cloud Detection and Response;
- g) Identity and Access Management;
- h) Inventário multi-cloud;
- i) Workflow para acesso temporário;
- j) Data Security Posture Management;
- k) Artificial Intelligence Security Posture Management;

3.14.1.9. A solução deve apresentar facilidade de onboarding e conexão continua com as nuvens públicas da AWS, GCP, Microsoft Azure e OCI;

- a) O Onboarding deve ser guiado e de simples implementação;



- b) A solução deve possuir conexão com os provedores de identidades através de APIs;
- c) A conexão com as nuvens públicas deve ser através de APIs sem a necessidade de instalação de agentes (modelo agentless);
- d) A solução deve ter a capacidade de realizar onboarding de contas individuais das nuvens públicas;
- e) A solução deve ter a capacidade de realizar onboarding de Organizações/Tenancies;
- f) A solução deve ter a capacidade de identificar inclusão e exclusão de contas em organizações sem intervenção do administrador;
- g) A solução deve replicar a hierarquia organizacional de contas de nuvens públicas;
- h) A solução deve realizar o onboarding de regiões distintas;
- i) A comunicação deve ser contínua com as nuvens para prover informações atualizadas.

3.14.1.10. A solução deve possuir integração com APIs com as seguintes características:

- a) Suporte a APIs no formato GraphQL;
- b) Possuir Endpoints para as APIs nas mesmas regiões de hospedagem;
- c) APIs para Onboarding e Offboarding;
- d) APIs para consulta ao inventário;
- e) APIs para consultas e interação com os problemas encontrados;
- f) APIs para pesquisas de permissionamento entre todos os recursos de nuvem avaliados;
- g) APIs para gerenciamento de usuários com acesso a console;
- h) APIs para consultas de vulnerabilidades;
- i) APIs para consultas de inventário de software;
- j) APIs para auditoria de acessos a console;

3.14.1.11. Deve ser compatível com as seguintes plataformas:

- a) Provedores de Nuvem Pública: Suporte a Azure; Suporte a GCP; Suporte a AWS; Suporte a OCI;
- b) Provedores de Identidade (IdPs):
- c) Suporte a Entra ID;
- d) Suporte a Google Workspace;
- e) Suporte a Ping Identity;
- f) Suporte a OKTA;
- g) Suporte a One Login;

3.14.1.12. Plataformas de Containers:



- a) Suporte a Clusters EKS;
 - b) Suporte a Clusters AKS;
 - c) Suporte a Clusters GKE;
 - d) Suporte a OpenShift Local Clusters;
 - e) Suporte a Kubernetes Local Clusters;
- 3.14.1.13. Linguagens de IaC (Infrastructure as a code):
- a) Suporte a Terraform;
 - b) Suporte a CloudFormation;
- 3.14.1.14. Repositórios de Código IaC:
- a) Suporte a Azure DevOps;
 - b) Suporte a Bitbucket;
 - c) Suporte a GitHub;
 - d) Suporte a GitLab;
- 3.14.1.15. CI/CD Pipelines (esteiras de desenvolvimento):
- a) Suporte a Jenkins Pipeline;
 - b) Suporte a Terraform CloudRun;
 - c) Suporte a Generic Docker Pipeline;
- 3.14.1.16. Deve permitir as seguintes integrações nativas:
- a) Ferramentas de Attack Path;
 - b) Ferramentas de Attack Path Analysis;
 - c) Ferramentas de Colaboração;
 - d) Slack;
 - e) Microsoft Teams;
- 3.14.1.17. Ferramentas de Inventário:
- a) Ferramentas de Inventário unificado de ativos com descoberta por múltiplos métodos;
 - b) Ferramentas de Avaliação de Risco;
 - c) Ferramentas de visão executiva de exposição ao risco com índice agregado e evolução histórica
- 3.14.1.18. Ferramentas de Correlação de Logs e Eventos – SIEM:
- a) Datadog;
 - b) Qradar;
 - c) Splunk;
 - d) SQS;
- 3.14.1.19. Ferramentas de Ticketing:



- a) Jira Cloud;
- b) Service Now;

3.14.1.20. A solução deve possuir integração customizável via Webhooks;

3.14.2. Administração de Interface Web

3.14.2.1. A solução deve apresentar Dashboards com, no mínimo, as seguintes funcionalidades:

3.14.2.2. Visualização das conexões ativas (nuvens públicas e cluster on premises);

3.14.2.3. Visualização do inventário multi-cloud consolidado, agrupando por tipo de recursos;

3.14.2.4. Contabilizar todos os recursos inventariados, permitindo drill-down;

3.14.2.5. Alertas de políticas não atendidas, por criticidade;

3.14.2.6. Monitoramento de Tendências;

3.14.2.7. Conformidade com padrões de compliance;

3.14.2.8. Contextualização de problemas diversos num mesmo recurso;

3.14.2.9. Apresentação de Quick Wins;

3.14.2.10. Identificação de Recursos públicos;

3.14.2.11. Identificação de Senhas e Credenciais expostas;

3.14.2.12. Recursos que possuem Dados, incluindo o tipo de dado;

3.14.2.13. Detecção de Anomalias;

3.14.2.14. Vulnerabilidades;

3.14.2.15. Contas/assinaturas/projects/compartments com maiores riscos;

3.14.2.16. Capacidade de drill down em todos os dashboards

3.14.3. Funcionalidades da Interface

3.14.3.1. A solução deve possibilitar login integrado via SSO;

3.14.3.2. A solução deve ter a capacidade de criar hierarquia de contas através de folders;

3.14.3.3. A solução deve limitar o acesso dos usuários à plataforma através de Roles;

3.14.3.4. A solução deve ter a capacidade de definir escopos de acesso;

3.14.3.5. A solução deve auditar as atividades do usuário e manter logs de acesso;

3.14.3.6. A solução deve ter permitir a criação de campos customizados no inventário;

3.14.3.7. A solução deve permitir a criação de TAGs / Labels customizadas;

3.14.3.8. A solução de possibilitar a definição dos ranges de IPs internos / corporativos;

3.14.3.9. A solução deve possibilitar o Drill down em qualquer item;



- 3.14.3.10. A solução deve permitir a aplicação de filtros em qualquer recurso;
- 3.14.3.11. A solução deve marcar automaticamente os recursos com problemas sérios;
- 3.14.3.12. A solução deve marcar automaticamente os recursos com características importantes;
- 3.14.3.13. Capacidade de detecção de problemas e erros de configuração através de políticas.
- 3.14.3.14. A solução deve possuir um conjunto de políticas pré-definidas;
- 3.14.3.15. Deve possuir, no mínimo, os seguintes tipos de políticas:
 - a) Detecção de Anomalias;
 - b) Políticas Customizadas;
 - c) Dados e Armazenamento;
 - d) Identidade de Permissionamento;
 - e) Kubernetes;
 - f) Virtualização, Clusters, e Funções Serverless;
 - g) Logs e Auditoria;
 - h) Chaves e Senhas;
 - i) Proteção de Workloads;
 - j) Gerenciamento da nuvem pública;
 - k) Redes e networking;
- 3.14.3.16. A solução deve avaliar o ambiente de maneira contínua e ininterrupta
- 3.14.3.17. A solução deve descrever o problema ou não conformidade da política
- 3.14.3.18. A solução deve ter a capacidade de indicar o passo-a-passo para resolução do problema;
- 3.14.3.19. A solução deve tomar ações para cada alerta/política disparado;
- 3.14.3.20. Toda política da plataforma deve ter um indicador de criticidade;
- 3.14.3.21. A solução deve indicar automaticamente a severidade do problema;
- 3.14.3.22. Os indicadores de severidade devem ser dinâmicos e podem ser alterados conforme a contextualização do problema;
- 3.14.3.23. A solução deve monitorar o desempenho das atividades de remediação;
- 3.14.3.24. A solução deve disparar alerta para qualquer política;
- 3.14.3.25. A solução deve possibilitar automatizar ações disparadas por um alerta;
- 3.14.3.26. A solução deve permitir enviar o problema por e-mail para outro usuário;
- 3.14.3.27. A solução deve permitir a customização de políticas com as seguintes características:
 - a) Capacidade de customizar políticas sem necessidade de escrever código;



- b) Capacidade de definir o escopo de avaliação de uma política
 - c) Capacidade de customizar políticas para monitorar recursos específicos
 - d) Capacidade de customizar políticas para monitorar Networking;
 - e) Capacidade de customizar políticas para monitorar Atividades;
 - f) Capacidade de customizar políticas para monitorar Permissões;
 - g) Capacidade de reutilização de políticas;
- 3.14.3.28. A solução deve permitir transformar a política disparada em uma exceção à regra;
- 3.14.3.29. A solução deve identificar automaticamente a resolução do problema.
- 3.14.3.30. A solução deve permitir marcar o problema como resolvido manualmente.
- 3.14.3.31. A solução deve descrever a remediação para o problema apresentando e, quando possível, disponibilizar scripts para automatização (cloudformation e terraform);
- 3.14.3.32. A solução deve permitir a remediação automatizada através de um clique;
- 3.14.3.33. A solução deve permitir automatizar remediação através de integrações;
- 3.14.3.34. A solução deve possibilitar reabrir um problema fechado anteriormente;
- 3.14.3.35. A solução deve Capacidade de marcar o problema como importante.
- 3.14.4. Relatórios**
- 3.14.4.1.1. A solução deve disponibilizar templates para criação de relatórios.
- 3.14.4.1.2. A solução deve permitir, no mínimo, os seguintes tipos de relatórios:
- a) Log de Atividades
 - b) Chaves de Acesso
 - c) Atribuições de funções e permissionamentos
 - d) Compliance
 - e) Inventário
 - f) Gerenciamento da nuvem pública
 - g) Erros de configuração.
 - h) Problemas em aberto (ativos ou reabertos)
 - i) Vulnerabilidades
- 3.14.4.2. A solução deve permitir customizar relatórios;
- 3.14.4.3. A solução deve possibilitar definir o escopo de alvo para o relatório;
- 3.14.4.4. A solução deve permitir programar a geração dos relatórios;
- 3.14.4.5. Deve possibilitar a exportação dos dados em formato PDF e CSV;
- 3.14.4.6. A solução deve armazenar relatórios históricos
- 3.14.5. Principais requisitos para Avaliação de Conformidade (CSPM e KSPM)**
- 3.14.5.1. A solução deve avaliar a postura de conformidade em relação às normas



suportadas;

- 3.14.5.2. A solução deve gerar relatório de conformidade com escopo customizável;
- 3.14.5.3. A solução deve avaliar a conformidade em clusters Kubernetes locais (on premisses);
- 3.14.5.4. A solução deve avaliar a conformidade em cluster Kubernetes na nuvem pública;
- 3.14.5.5. A solução deve permitir criar e/ou customizar padrões de compliance;
- 3.14.5.6. A solução deve gerar relatório de conformidade para toda a organização.
- 3.14.5.7. A solução deve inventariar os seguintes tipos de recursos multi-cloud para avaliação de conformidade:
 - a) Inteligência Artificial e Machine Learning;
 - b) Computacionais e Virtualização;
 - c) Containers;
 - d) Dados;
 - e) Identidades e Privilégios;
 - f) IoT;
 - g) Kubernetes;
 - h) Gerenciamento;
 - i) Networking;
 - j) Segurança;
- 3.14.5.8. A solução deve suportar os seguintes padrões de conformidade:
 - a) AWS Well Architected
 - b) Proprietário do Fabricante
 - c) CIS AKS 1.2
 - d) CIS AWS 2.0 e 3.0
 - e) CIS Azure 2.0
 - f) CIS EKS 1.2
 - g) CIS GCP 1.3 e 2.0
 - h) CIS GKE 1.3
 - i) CIS Kubernetes 1.8
 - j) CIS Openshift 1.5
 - k) CSA CCM 4.0
 - l) Essential Eight
 - m) GDPR
 - n) HIPAA
 - o) NIST 800-171 Rev2



- p) NIST 800-53 Rev5
- q) NYDFS 23 NYCBR 500
- r) PCI DSS 4.0
- s) SOC2 Type II
- t) AWS FSBP v1.0
- u) ISMS-P (Korea)
- v) LGPD (Brasil)
- w) MITRE ATT&CK v13
- x) NIST CFS 1.1
- y) ISO 27001:2022
- z) Microsoft Cloud Security Benchmark v1
- aa) CIS OCI 2.0
- bb) NIST SP 800-190

4. AVALIAÇÃO DE IDENTIDADES E PERMISSIONAMENTO (CIEM E IAM)

4.1. Requisitos Gerais

- 4.1.1. A solução deve possibilitar consultas de permissionamento efetivo entre dois recursos;
- 4.1.2. A solução deve apresentar dashboard específico para identidades;
- 4.1.3. A solução deve detectar identidades inativas;
- 4.1.4. A solução deve detectar o uso efetivo de permissionamento com base nas atividades registradas;
- 4.1.5. A solução deve comparar o permissionamento efetivo com o utilizado, identificando permissionamento excessivo, parcialmente excessivo e utilizado;
- 4.1.6. A solução deve avaliar o permissionamento para identidades federadas;
- 4.1.7. A solução deve avaliar o permissionamento efetivo para o aninhamento de identidades, funções e recursos;
- 4.1.8. A solução deve apresentar graficamente as permissões efetivas;
- 4.1.9. A solução deve apresentar graficamente quais recursos podem herdar o permissionamento;
- 4.1.10. A solução deve mostrar em detalhes as políticas anexadas ao recurso, e seu histórico de alterações;
- 4.1.11. A solução deve marcar automaticamente identidades privilegiadas;
- 4.1.12. A solução deve marcar automaticamente identidades com privilégios excessivos;
- 4.1.13. A solução deve identificar permissionamento de terceiros;
- 4.1.14. A solução deve identificar permissionamento do tipo cross-account;



- 4.1.15. A solução deve mapear o permissionamento efetivo: ações x recursos
- 4.1.16. A solução deve classificar automaticamente o permissionamento por severidade, baseado na extensão do acesso;
- 4.1.17. A solução deve permitir visualizar a permissão efetiva dos recursos, incluindo SCP, boundaries e demais regras de exceção;
- 4.1.18. Classificar automaticamente o permissionamento por categorias:
 - a) Escalação de Privilégios;
 - b) Gestão de Permissionamento;
 - c) Acesso a Dados;
 - d) Gestão da Infraestrutura de nuvem;
 - e) Reconhecimento da infraestrutura;
- 4.1.19. A solução deve possuir sugestão automática de política de menor privilégio;
- 4.1.20. A solução deve permitir automatizar ação corretiva;
- 4.1.21. A solução deve ter a capacidade de disparar alertas;
- 4.1.22. A solução deve possibilitar criar políticas de menor privilégio baseadas no acesso efetivo em uma janela de tempo configurável;
- 4.1.23. A solução de possibilitar aplicar correção com um clique;

4.2. Proteção de Workload e detecção de vulnerabilidades (CWPP)

- 4.2.1. A solução deve encontrar malware no ambiente;
- 4.2.2. A solução deve scanear os workloads via API, sem necessidade de agentes;
- 4.2.3. A solução deve scanear os workloads utilizando a própria infra do contratante.
- 4.2.4. Os Scans devem possuir recorrência diária;
- 4.2.5. A solução deve possibilitar excluir contas específicas como alvos dos scans;
- 4.2.6. A solução deve scanear imagens de containers;
- 4.2.7. A solução deve ter a capacidade de excluir binários (hashes);
- 4.2.8. A solução deve identificar vulnerabilidades nos workloads avaliados;
- 4.2.9. A solução deve apresentar o score CVSS;
- 4.2.10. A solução deve apresentar um score de priorização proprietário;
- 4.2.11. A solução deve indicar se existe exploit para a vulnerabilidade indicada;
- 4.2.12. A solução deve identificar automaticamente quando uma correção for aplicada.;
- 4.2.13. A solução deve permitir exportar as informações em um formato comum CSV;

4.3. Detecção de anomalias e atividades

- 4.3.1. A solução deve detectar padrões incomuns de acesso a recursos, incluindo dados
- 4.3.2. A solução deve possuir detecção de Gerenciamento ou alteração de permissões e privilégios;
- 4.3.3. A solução deve detectar alterações nas configurações de rede;

- 4.3.4. A solução deve possuir detecção de Reconhecimento da infraestrutura;
- 4.3.5. A solução deve armazenar todo o log de atividades das várias nuvens públicas;
- 4.3.6. A solução deve normalizar o log permitindo consultas multi-cloud e multi-IIdP;
- 4.3.7. A solução deve possibilitar utilizar filtros diversos para pesquisar no log;
- 4.3.8. A solução deve apresentar o log de maneira amigável e em interface gráfica;
- 4.3.9. A solução deve apresentar o log original (raw event);

4.4. Avaliação de IaC

- 4.4.1. A solução deve identificar problemas em produção e relacioná-los ao código de origem;
- 4.4.2. A solução deve manter o sincronismo entre o recurso e o código de origem no repositório;
- 4.4.3. A solução deve manter o sincronismo entre o recurso e o código de origem no pipeline;
- 4.4.4. A solução deve possibilitar linkar o código de origem aos recursos em produção através do inventário;
- 4.4.5. A solução deve ter a capacidade de remediar diretamente no código IaC via Pull request.
- 4.4.6. A solução deve scanear automaticamente os repositórios de IaC;
- 4.4.7. A solução deve scanear por demanda, durante a pipeline, o código IaC;
- 4.4.8. A solução deve permitir customizar os scans definindo quais políticas serão utilizadas;
- 4.4.9. A solução deve possibilitar executar o scan localmente, em formato docker, provendo compatibilidade genérica com demais pipelines;
- 4.4.10. A solução deve scanear automaticamente o repositório que receber um commit de código.
- 4.4.11. A solução deve consolidar os resultados na console ou executar localmente, em modo verbose Only;

4.5. Avaliação do uso e IA (inteligência Artificial)

- 4.5.1. A solução deve inventariar os recursos de Inteligência Artificial e Machine Learning;
- 4.5.2. A solução deve identificar as melhores práticas de configuração;
- 4.5.3. A solução deve ter armazenar e avaliar os logs de atividades;
- 4.5.4. A solução deve identificar graficamente o permissionamento para uso dos recursos de IA;

4.6. Avaliação do uso de Dados em nuvem pública (DSPM)

- 4.6.1. A solução deve possibilitar avaliar as melhores práticas de proteção de dados;
- 4.6.2. A solução deve inventariar recursos para identificar a presença de dados;
- 4.6.3. A solução deve classificar automaticamente os tipos de dados;
- 4.6.4. A solução deve identificar a severidade do dado;



- 4.6.5. A solução deve marcar automaticamente os dados com labels e etiquetas;
- 4.6.6. A solução deve armazenar o log de acesso aos repositórios;
- 4.6.7. A solução deve identificar o permissionamento de acesso aos recursos com dados;

4.7. Solução de análise em ambiente Microsoft Active Directory

- 4.7.1. A solução deve identificar fraquezas ocultas em configurações dedicadas ao Active Directory e Entra ID (Microsoft Azure Active Directory);
- 4.7.2. A solução deve possuir ações preventivas de hardening para o Active Directory;
- 4.7.3. A solução deve identificar ataque específicos para a estrutura do Active Directory;
- 4.7.4. A solução deve possuir funcionalidade para analisar em detalhes cada configuração incorreta que acarreta riscos de segurança – com uma linguagem simples, contextualizando tal risco para os times envolvidos;
- 4.7.5. A solução deve possuir recomendações de correção para cada configuração incorreta no Active Directory;
- 4.7.6. A solução deve avaliar relações de confiança perigosas entre florestas e domínios;
- 4.7.7. A solução deve capturar as mudanças que ocorrem no AD e demonstrar na console de administração;
- 4.7.8. A solução deve possuir dashboard com os principais ataques e vulnerabilidades por domínio;
- 4.7.9. A solução deve permitir a correlação de mudanças no Active Directory e desvios de segurança;
- 4.7.10. A solução deve analisar em detalhes um ataque explorando as descrições através do framework MITRE ATT&CK;
- 4.7.11. A solução deve prover interface web para gerenciamento de todas as funcionalidades;
- 4.7.12. A solução deve possuir capacidade nativa de criação de dashboards customizados;
- 4.7.13. A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;
- 4.7.14. A solução não deve realizar alterações no Active Directory, seus objetos e atributos;
- 4.7.15. A solução não deve armazenar ou sincronizar nenhuma credencial de objetos do Active Directory;
- 4.7.16. A solução deve suportar ambientes com múltiplas florestas e domínios;
- 4.7.17. A solução deve suportar monitoramento contínuo de ambientes com Active Directory com o nível funcional de floresta e domínio a partir do 2003;
- 4.7.18. A solução deve suportar reter os eventos coletados por no mínimo um ano;
- 4.7.19. A solução deve descobrir e mapear a superfície de ataque do Active Directory e seus domínios monitorados com os seguintes padrões:
 - a) A coleta de informações do Active Directory deve operar em modo somente leitura sobre o diretório, sem realizar qualquer alteração em objetos, atributos ou políticas, e sem causar indisponibilidade ou degradação



relevante de desempenho dos controladores de domínio. Admite-se qualquer arquitetura de coleta, com ou sem componente de software instalado nos controladores de domínio, desde que homologada pelo fabricante e previamente aprovada pela contratante, devendo o licitante descrever em sua proposta os componentes a serem instalados, os requisitos de recurso e o consumo esperado, passíveis de verificação em prova de conceito;

- b) A solução deve seguir as boas práticas de menor privilégio, a conta de serviço utilizada para conexão com o Active Directory, sendo o menor nível de acesso esperado para a conta de serviço como parte do grupo Domain User;
- c) Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles;

4.7.20. A solução deve analisar continuamente a postura de segurança do AD, minimamente avaliando:

- a) Validação de domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como *NTLMv1*;
- b) Validação do uso recente da conta de administrador padrão;
- c) Validação de contas dormentes;
- d) Validação de direitos perigosos configurados no *Schema* do AD;
- e) Validação de relação de confiança perigosa com outras *Florestas* e *Domínios*;
- f) Validação de contas que possuem um atributo perigoso de histórico SID (*SID History*);
- g) Validação da última alteração de senha do KDC;
- h) Validação de possível senha em *clear-text*;
- i) Validação de contas de serviço com SPN (*Service Principal Name*) que fazem parte de grupos privilegiados;
- j) Validação em permissões de objetos raiz que permitem ataques do tipo DCSync;
- k) Validação de políticas de senha fracas aplicadas aos usuários;
- l) Validação de permissões em GPOs sensíveis associadas aos *Containers Configuration, Sites, Root Partition* e *OUs* sensíveis como *Domain Controllers*;
- m) Controladores de domínio gerenciados por usuários ilegítimos;

4.7.21. A solução deve identificar vulnerabilidades e configurações incorretas do AD à medida que são introduzidas sendo:

- a) Identificar todas as vulnerabilidades e configurações incorretas no AD;
- b) Monitorar relações de confiança perigosas em toda a estrutura AD;
- c) Apresentar ameaças e alterações sem a necessidade de scans estáticos e



programados no Active Directory e sua infraestrutura;

- d) Apresentar as ameaças e alterações em tempo real ou em menos de cinco minutos;

4.7.22. Detecção e resposta a ataques:

- a) Monitorar continuamente indicadores de possível ataque ao Active Directory, contemplando, no mínimo: replicação indevida de dados do diretório (DCSync); uso indevido de credenciais e de tickets Kerberos, inclusive Pass-the-Hash, Pass-the-Ticket e forja de tickets (Golden Ticket); obtenção de credenciais a partir de contas de serviço e de contas sem pré-autenticação Kerberos (Kerberoasting e AS-REP Roasting); e tentativas de adivinhação de senha por força bruta e por pulverização de senhas. Cada indicador deve identificar a conta, o objeto e o controlador de domínio envolvidos, admitida a apresentação da correspondência com framework público de táticas e técnicas adversárias (MITRE ATT&CK).
- b) Detecção de ataques ao AD em tempo real ou em menos de um minuto;
- c) Análise detalhada do ataque, apresentando ativo de origem, vetor de ataque, controlador de domínio afetado, técnica aplicada;
- d) Apresentação de ataques em uma linha do tempo;
- e) Investigar ameaças, reproduzir ataques e procurar por backdoors;
- f) Permitir busca ágil de eventos específicos na base da solução através de queries customizadas;

4.7.23. A solução deve ser capaz de enviar alertas por e-mail;

4.7.24. A solução nativamente deve ser capaz de se integrar com SIEM através de protocolo SYSLOG;

4.7.25. A solução deve ser capaz de filtrar e enriquecer os eventos que serão enviados para o SIEM;

4.7.26. A solução deve possuir conjunto de APIs REST, todas as chamadas disponíveis devem estar contidas na documentação;

4.7.27. A solução deve permitir a criação de listas de exclusões, suportando minimamente Exclusão por domínios do AD monitorados e por itens analisados;

4.7.28. A solução deve ser licenciada pelo número de usuários habilitados;

4.8. Gerenciamento de Risco de Identidades

4.8.1. Deve classificar identidades do maior para o menor risco, utilizando análises avançadas, otimizando a alocação de recursos e aprimorando a postura geral de segurança.

4.8.2. Deve disponibilizar uma visão aprofundada de cada identidade por meio de múltiplas perspectivas, incluindo contas associadas, fraquezas identificadas, dispositivos conectados, privilégios de acesso e padrões de atividade.

4.8.3. Deve Fornecer insights que permitem às equipes de segurança identificar e remediar vulnerabilidades associadas a identidades de alto risco, implementar políticas de controle de acesso mais eficazes, detectar e responder rapidamente a potenciais ameaças



internas.

- 4.8.4. A solução deve consolidar contas do Active Directory e Entra ID sob uma entidade unificada, utilizando atributos como endereços de e-mail e UPNs para associação precisa.
- 4.8.5. Deve fornecer dashboards para visualização, busca e gestão de informações de identidade, com foco em métricas de segurança como fraquezas e exposição a ataques.
- 4.8.6. A solução deve avaliar de forma contínua as exposições relacionadas a identidades, como configurações incorretas, permissões excessivas e relacionamentos de confiança arriscados, permitindo a priorização e mitigação de riscos antes que sejam explorados.
- 4.8.7. Deve possuir sistema de pontuação baseado em inteligência artificial que avalia e classifica cada identidade com base em vulnerabilidades inerentes e riscos herdados, auxiliando na priorização de esforços de remediação.
- 4.8.8. Possuir capacidade de monitorar continuamente a infraestruturas de identidade híbridas (Active Directory e Entra ID), fornecendo alertas em tempo real sobre novas fraquezas e técnicas avançadas de ataque, permitindo respostas rápidas e eficazes.
- 4.8.9. Deve possibilitar integração nativa com os módulos de gerenciamento de vulnerabilidade e segurança em Nuvem, permitindo uma visão holística dos riscos relacionados à identidade dentro da superfície geral de ataque da organização.
- 4.8.10. Deve permitir exportar descobertas e dados em formato .CSV, permitindo personalização das exportações para mostrar colunas específicas conforme necessário.

5. GESTÃO DE RISCO ESTRATÉGICO DE CYBER SEGURANÇA

5.1. Requisitos gerais

- 5.1.1. A solução de avaliação e quantificação da maturidade dos controles de segurança da informação e de quantificação do impacto financeiro deverá prestar suporte à CONTRATANTE, permitindo avaliar a resiliência dos ativos de tecnologia em relação a determinados tipos de ataques conhecidos no mercado, considerando os atacantes e as técnicas, processos e procedimentos por eles utilizados, bem como priorizar os investimentos com base no resultado da avaliação e na importância dos controles para os processos de negócio.
- 5.1.2. A ferramenta deve permitir realizar assessment de risco considerando questionário de até 180 questões para qualificação dos riscos.
- 5.1.3. A ferramenta deve ser essencialmente baseada em Web, acessível por navegador padrão de mercado, sem necessidade de instalação de plugins ou de clientes proprietários na estação do usuário. A ferramenta não deve ter limitações de usuários;
- 5.1.4. A ferramenta deve possibilitar uma visão holística das avaliações, facilitando os avaliadores a terem uma visão do nível de riscos identificados em todas as avaliações;
- 5.1.5. A ferramenta deve possuir layout amigável e intuitivo;
- 5.1.6. Módulo de quantificação de maturidade, riscos e impacto financeiro
- 5.1.7. O módulo de análise dos controles de segurança da informação deve:
 - 5.1.7.1. Realizar avaliações de risco cibernético dos vários componentes da



CONTRATANTE, bem como para toda a organização, conforme necessário. Também ser possível avaliar a maturidade para uma variedade de padrões e estruturas usando insumos humanos e de ativos tecnológicos;

- 5.1.8. Permitir avaliações flexíveis e customizáveis, baseado na localidade, indústria e outras informações financeiras da CONTRATANTE;
- 5.1.9. Identificar riscos externos com a inteligência de ameaças estratégicas e correlacionar com a avaliação de risco cibernético em andamento;
- 5.1.10. Comunicar seus riscos cibernéticos em termos financeiros claros em uma linguagem comum entre as partes interessadas técnicas e não técnicas;
- 5.1.11. Permitir que as partes interessadas da organização, em todos os níveis, tenham visão a painéis executivos com o resultado das avaliações;
- 5.1.12. Realizar avaliações de maturidade de segurança da informação baseado nas principais normativas e *frameworks* de mercado como ISO/IEC 27.001, NIST CSF, PCI-DSS, CIS Controls, entre outros;
- 5.1.13. Realizar as avaliações através de questionários abrangentes com, no mínimo, os principais grupos de controles de segurança da informação:
 - a) Segmentação de Rede,
 - b) Controle de Acesso à Rede,
 - c) Firewall,
 - d) Banco de dados,
 - e) Firewalls e proxies de aplicativos,
 - f) Desenvolvimento Seguro,
 - g) Proteção de aplicativos,
 - h) Testes de Intrusão,
 - i) Verificação de Conteúdo de Rede & Filtragem - Mail / Arquivos,
 - j) WAF,
 - k) Navegação segura do usuário,
 - l) Verificação de Conteúdo de Rede & Filtragem - Tráfego Web,
 - m) Endpoint Anti Malware,
 - n) Política e mapeamento de classificação de dados,
 - o) Criptografia de dados,
 - p) DLP,
 - q) Criptografia de rede,
 - r) Controle de mídia removível,
 - s) Gestão de Ativos,
 - t) Política e Controle de Software Autorizado,
 - u) Proteção do servidor, dispositivos de rede e Endpoints,



- v) Gerenciamento de Vulnerabilidades,
 - w) Coleta e Análise de Inteligência Externa,
 - x) Revisões de segurança,
 - y) Honeypots, Honeynets, etc.,
 - z) SIEM,
 - aa) Anti-phishing,
 - bb) Forense,
 - cc) Detecção de comportamento anômalo do usuário,
 - dd) Detecção de anomalias de tráfego de rede,
 - ee) Autenticação, Gerenciamento de Usuários & Autorização,
 - ff) Gerenciamento de contas privilegiadas,
 - gg) Estrutura e políticas de gerenciamento de segurança,
 - hh) Procedimentos de recrutamento e RH,
 - ii) Gestão de Fornecedores,
 - jj) Gestão de Mudanças,
 - kk) Procedimentos e Práticas de Segurança Física,
 - ll) Conscientização e Treinamento,
 - mm) Gerenciamento de dispositivos móveis (MDM),
 - nn) Integridade dos dados e Privacidade;
- 5.1.14. Permitir a criação de questionários customizados;
- 5.1.15. Permitir o compartilhamento dos questionários com os proprietários/responsáveis pelos grupos de controles;
- 5.1.16. Quantificação do possível impacto financeiro em caso de um incidente de segurança da informação, tendo como base:
- a) Valor base do negócio como faturamento anual, média salarial e uma média de investimentos em segurança da informação;
 - b) Indústria;
 - c) Geolocalização política;
 - d) Prioridade dos ativos relevantes para o negócio;
 - e) Fator de risco.
- 5.1.17. Permitir a geração de painéis (dashboards) executivos, baseado nas avaliações de maturidade de segurança, da importância dos controles para os processos de negócio, do cenário de ameaças, painéis (dashboards) de análise dos riscos, baseados na tríade Confidencialidade, Integridade e Disponibilidade dos controles de segurança da informação e processos de negócio, e painéis (dashboards) técnicos, com os detalhes individuais da maturidade de todos os controles avaliados;
- 5.1.18. Geração de relatórios detalhados, em nível executivo e/ou técnico, demonstrando

o nível de maturidade dos controles, os riscos aos processos de negócio, o nível de aderência a normativas e *frameworks* conhecidos de mercado, entre outros.

5.1.19. Gerar relatórios com recomendações de ações para mitigação dos riscos apontados durante a avaliação;

5.2. Módulo de análise de arquivos de configuração dos ativos de tecnologia

5.2.1. Análise de Maturidade Cibernética que permite validar, melhorar e aumentar as avaliações da maturidade dos ativos de tecnologia, avaliando se esses ativos estão com as melhores práticas de segurança da informação aplicadas;

5.2.2. Permitir integração com as tecnologias e fornecedores conhecidos de mercado, como:

- a) AWS,
- b) Microsoft Azure,
- c) Google Cloud Platform,
- d) Check Point,
- e) CrowdStrike,
- f) Fortigate, McAfee,
- g) Palo Alto,
- h) Symantec,
- i) Windows 10-11 Enterprise,
- j) Windows Server 2016-2022,
- k) CentOS Linux 7-8,
- l) Cisco IOS 17.x,
- m) Google Chrome,
- n) Microsoft Edge,
- o) Oracle MySQL Enterprise Edition 5.6-5.7-8.0,
- p) Google Kubernetes Engine (GKE),
- q) Amazon Elastic Kubernetes Service (EKS),
- r) Kubernetes 1.20-1.23

5.2.3. Avaliar indicadores técnicos de segurança dos ativos baseados nos fabricantes ou *frameworks* conhecidos de mercado, como Cis Benchmark, entre outros;

5.2.4. Compatibilidade com normativas e *frameworks* conhecidos de mercado, como:

- a) ISO/IEC 27.001,
- b) NIST CSF,
- c) PCI-DSS,
- d) CIS Controls,
- e) HIPPA,



f) GDPR.

5.3. Módulo de simulação de retorno dos investimentos em segurança da informação

5.3.1. Priorizar os investimentos em segurança da informação, baseado nos controles mais importantes para o negócio;

5.4. Módulo de verificações e análises de inteligência de ameaças

5.4.1. Coletar feeds de dados de ameaças de milhares de fontes, incluindo Deep e Dark Web, e analisar os itens de inteligência ou "eventos cibernéticos" dentro deles para criar tendências estratégicas de inteligência em relação a invasores, métodos de ataque, ativos direcionados, indústrias impactadas e regiões geopolíticas;

5.4.2. Monitorar continuamente o nível de atividade do agente de ameaças e do método de ataque em uma região e indústria geopolítica específica;

5.4.3. Agregar capacidades e critérios quantitativos que, quando combinados no motor de cálculo, calculam a Probabilidade de Sucesso (PoS) de um ataque específico, alimentado por um invasor específico em um determinado ativo, levando em consideração algumas métricas, como:

5.4.3.1. O nível de atividade combinado de uma variedade de diferentes agentes de ameaças;

5.4.3.2. Utilizando vários métodos de ataque (exigindo habilidades e recursos proporcionais para utilizar);

5.4.3.3. Atingir os objetivos (comprometendo a Confidencialidade, Integridade e Disponibilidade dos processos do negócio);

5.4.3.4. Sobre ativos comerciais direcionados e atraentes;

5.4.3.5. Intrusão das defesas agregadas de classes de controles.

SOLUÇÃO DE MONITORAMENTO AVANÇADO, RESPOSTA A INCIDENTES AUTOMATIZADA, HIPERAUTOMAÇÃO, SOLUÇÕES APLICADAS A FIREWALL E TESTE AUTOMATIZADO

6. SOLUÇÃO DE MONITORAMENTO DE ATAQUES E RESPOSTA AUTOMATIZADA

6.1. Requisitos gerais

6.1.1. O objetivo é realizar o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados à SEFAZ-ES, por meio da aplicação de diferentes tecnologias e processos de segurança da informação. Serão utilizadas ferramentas de detecção e resposta gerenciada para identificar e conter ameaças em tempo real; mecanismos de proteção contra riscos digitais voltados à prevenção de vazamento de credenciais, perfis falsos e uso indevido da marca; soluções de simulação controlada de ataques, que permitem avaliar e validar continuamente a resiliência dos controles de segurança; além de tecnologias de monitoramento de tráfego de rede, capazes de detectar comportamentos suspeitos e movimentações laterais de ataque. De forma integrada, esses recursos viabilizam o correlacionamento de logs e o acompanhamento de comportamentos anômalos em aplicações, serviços e infraestrutura da SEFAZ-ES, possibilitando a identificação criteriosa de eventos de segurança que, quando necessário, serão classificados como incidentes e tratados dentro de um processo cíclico e rigoroso de



gestão, assegurando rápida identificação, resposta e mitigação de ameaças cibernéticas.

Grupo de Serviço	Serviço
Monitoramento de Ataques Cibernéticos	Eventos de Informação
	Eventos de Aviso
	Eventos de Exceção

6.2. Sobre A Ferramenta De Detecção E Resposta

- 6.2.1. Para execução deste serviço, a CONTRATADA deverá utilizar e ser capaz de fornecer, operar, sustentar e suportar soluções de monitoramento que atendam o descritivo técnico a seguir.
- 6.2.2. O licenciamento deverá ser de propriedade da CONTRATADA, com suporte técnico e atualizações contratados junto ao fabricante durante toda a vigência. Não será aceita solução mantida exclusivamente por comunidade, sem fabricante responsável e sem contrato de suporte, admitindo-se soluções comerciais cujo código seja disponibilizado sob licença aberta, desde que o fornecimento se dê por subscrição comercial do fabricante.
- 6.2.3. A plataforma utilizada deverá ter capacidade de operar com volumes massivos de dados em tempo real utilizando algoritmos de aprendizagem de automático de máquina "Machine Learning" e deve contar com casos de uso para detectar ameaças avançadas;
- 6.2.4. Deverá ser escalável e tolerante a falhas, capaz de ingerir centenas de terabytes por dia e suportar a retenção de eventos de segurança por longo período;
- 6.2.5. Junte-se a eventos ao longo do tempo usando modelos Kill Chain para a análise de eventos de maior risco;
- 6.2.6. Permitir o hunting rápido de ameaças por meio da pesquisa em linguagem natural.
- 6.2.7. A solução deve estar classificada como líder no quadrante mágico de "Security Information and Event Management" do Gartner em 2024, 2025; ou no quadrante mágico de "Observability Platforms" de 2026.
- 6.2.8. A solução deve ter recursos de "Multi-tenant";
- 6.2.9. Deve ter as certificações SOC 2 TYPE II e ISO 27001;
- 6.2.10. Deve garantir retenção dos logs na console de gerenciamento por 365 (trezentos e sessenta e cinco) dias, sendo 90 dias em modo hot, ou seja, disponível para consultas rápidas pela equipe de operação da CONTRATADA;
- 6.2.11. Deve ter alta disponibilidade e mecanismos de recuperação de desastres;
- 6.2.12. Deve permitir o gerenciamento da largura de banda para a transmissão de dados entre os coletores e os servidores de gerenciamento;
- 6.2.13. Deve executar o armazenamento em cache local e/ou em buffer nos coletores para garantir que nenhum dado seja perdido em trânsito no caso de um problema de rede ou um pico no volume do evento;
- 6.2.14. Deve oferecer suporte ao mascaramento de dados por meio de controles de acesso granulares baseados em funções, para ofuscar qualquer informação de usuário potencialmente sensível na camada de interface do usuário;
- 6.2.15. Deve suportar controle de acesso baseado em função granular (RBAC) com suporte a administração delegada, tanto para as funcionalidades na interface do usuário



quanto acesso aos dados e configurações;

- 6.2.16. Deve incluir uma ferramenta de Security Data Lake baseada em big data em uma arquitetura aberta e escalável e com capacidade de coletar e reter dados por períodos estabelecidos para fins de conformidade e investigação;
- 6.2.17. Deve oferecer suporte à integração com várias fontes de eventos usando métodos de syslog, formatos de log estruturados (CEF, LEEF, MEF, JSON, XML), arquivos, bancos de dados (conexão JDBC), conexão API (AWS, Azure, Google Cloud, SVN, Office 365, entre outros), WMI, consultas LDAP/LDAPS, dados e fluxo (Netflow e sFlow), Hadoop, Registros não estruturados (Regex), agentes de terceiros (snare);
- 6.2.18. Deve permitir a integração com diferentes tipos de fontes de dados, como dados de identidade, logs de atividades / transações, logs de eventos de segurança, fluxos de rede, log de aplicativos / plataformas de nuvem, permissões de acesso, fontes de inteligência de ameaças, dados não estruturados e metadados de ativos;
- 6.2.19. Deve permitir conexão a sistemas externos de gerenciamento de identidade, minimamente para Active Directory / LDAP ou soluções de IAM (gestão de identidade), minimamente para Aveksa/Sailpoint, sistemas de RH, minimamente para Peoplesoft/Workday, para realizar o enriquecimento contextual de eventos adicionando identidade do usuário;
- 6.2.20. Deve ser capaz de se conectar nativamente através de APIs ou outros meios com serviços em nuvem como Salesforce, Amazon Web Services S3 e Cloudtrail, BOX, Microsoft Azure, Office 365, Google Apps, Google Cloud, Netskope, ServiceNow, entre outros.
- 6.2.21. Deve ter uma interface que permita modificar conectores, analisadores (parsers) existentes ou construir novos analisadores (parsers) na mesma interface de usuário;
- 6.2.22. Deve ter conectores, analisadores (parsers) pré-configurados, prontos para uso, mas que possam ser modificados conforme necessário. A análise, normalização e categorização dos coletores devem ser totalmente personalizáveis na interface do usuário.
- 6.2.23. Deve ter uma API RESTful de serviços para integração bidirecional com outras tecnologias possibilitando a integração entre aplicações (ambiente interno e externo);
- 6.2.24. Deve fornecer integração com pelo menos 5 fontes de inteligência de ameaças inclusas no valor do serviço ofertado;
- 6.2.25. Deve possuir a funcionalidade de UEBA (User and Entity Behavior Analytics);
- 6.2.26. Deve realizar o enriquecimento dos eventos com dados contextuais sobre eventos no momento da captura e ingestão de dados adicionando aos eventos:
- 6.2.26.1. Identidade do usuário;
 - 6.2.26.2. Contexto de negócios
 - 6.2.26.3. Metadados de ativos;
 - 6.2.26.4. Informações de rede;
 - 6.2.26.5. Localização Geográfica;
 - 6.2.26.6. Dados de inteligência de ameaças;

- 6.2.27. Deve ter conteúdo pré-empacotado de casos de uso e modelos de ameaças prontos para uso para detecção avançada de ameaças, como:
- 6.2.27.1. Detecção de ameaças internas (insider threat) utilizando técnicas de aprendizagem de máquina;
 - 6.2.27.2. Detecção de ameaças cibernéticas (cyber threat) utilizando técnicas de aprendizagem de máquina;
 - 6.2.27.3. Detecção de ameaças na nuvem (cloud threat) utilizando técnicas de aprendizagem de máquina;
- 6.2.28. Deve fornecer recursos abrangentes para modelar e ajustar a pontuação de risco com base no perfil do usuário e/ou entidade, gravidade da ameaça e sequência/combinção de eventos que ocorrem durante um período;
- 6.2.29. Deve permitir a modelagem de risco a partir da interface do usuário de acordo com as prioridades da SEFAZ-ES;
- 6.2.30. Deve ter modelos de ameaças que permitam agrupar eventos realizados por um usuário ou entidade que duram dias, semanas, meses e assim por diante. Essas atividades devem ser exibidas como uma cadeia de eliminação com cada evento categorizado em estágios predefinidos.
- 6.2.31. Deve ter algoritmos preditivos para identificar usuários de risco (por exemplo, usuários prestes a deixar a organização);
- 6.2.32. Deve fornecer análises para diferentes tipos de anomalias, como relacionadas ao tempo, volume de transferência de dados, origem do evento relacionado, destino do evento relacionado, anomalias por usuário e grupo de pares, anomalias relacionadas à localização geográfica / velocidade terrestre, bem como rastrear usuários ou outras entidades nas listas de observação;
- 6.2.33. Deve ter algoritmos de aprendizagem supervisionados para detectar ameaças de malware avançadas, como DGA, ataques de phishing/spam e muito mais;
- 6.2.34. Deve haver técnicas de análise de raridade de eventos pelas quais atividades suspeitas que não foram vistas antes possam ser identificadas;
- 6.2.35. Deve ter técnicas de análise de tráfego para identificar padrões de beaconing, agentes de usuários incomuns, conexões com URLs incomuns, conexões com domínios DGA etc.;
- 6.2.36. Deve fornecer a capacidade de definir políticas baseadas em regras para detectar ameaças conhecidas. Essas ameaças conhecidas devem ser usadas como intensificadores de risco e combinadas com as verificações “não assinadas” nos modelos de ameaças;
- 6.2.37. Deve haver modelagem de ameaças que permita a identificação de ameaças compostas, que se observadas isoladamente podem ser de baixo risco, porém, quando combinadas, são indicativas de um evento de alto risco;
- 6.2.38. Deve reduzir o número de falsos positivos aplicando recursos avançados de aprendizado de máquina para aprender o que é normal e o que não é normal no ambiente monitorado;
- 6.2.39. Deve ter relatórios de ameaças que forneçam visibilidade da postura de segurança cibernética. Por exemplo: usuários de alto risco, ativos de alto risco, principais ameaças,



principais IPs maliciosas etc.;

- 6.2.40. Deve ter relatórios que forneçam visibilidade sobre as operações de segurança. Por exemplo, para dispositivos VPN, os relatórios devem incluir as melhores sessões de VPN por duração, os principais eventos de saída de dados, a distribuição dos eventos de login por geografia, as principais tentativas de login com falha e assim por diante;
- 6.2.41. Deve ter relatórios de conformidade alinhados com requisitos de conformidade específicos, minimamente para PCI, SOX, HIPPA, GDPR, ISO27002;
- 6.2.42. Deve ter relatórios de resumo executivo de violações, incidentes e operações;
- 6.2.43. Deve ter relatórios sobre a atividade do usuário;
- 6.2.44. Deve permitir que os dados sejam exibidos com diferentes tipos de gráficos: gráfico de linhas, gráfico de barras, gráfico de pizza, mapa geográfico, tabelas, gráfico empilhados, gráfico N principais, gráficos de bolhas, gráficos de relacionamento de origem e destino;
- 6.2.45. Deve permitir a visualização de dados através de links que permitam vincular qualquer conjunto de atributos e visualização a relação entre eles;
- 6.2.46. O serviço deve possuir solução para análise de artefatos maliciosos que minimamente contemple as funcionalidades a seguir:
 - 6.2.46.1. Analisar mais de 1000 indicadores comportamentais de um artefato;
 - 6.2.46.2. Realizar análise estatística e dinâmica para avaliar se o artefato é malicioso ou não;
 - 6.2.46.3. Deve suportar a análise, no mínimo, de executáveis e bibliotecas do Windows (EXE, DLL, PE32, MSI), scripts e conteúdo ativo (JS, JSE, VBE, WSF, BAT, HTA), documentos ofimáticos (Microsoft Office e PDF), arquivos compactados e imagens de disco (ZIP, JAR, ISO), atalhos (LNK), marcações e páginas (MHTML, XML) e URLs. Os formatos de uso regional restrito (HWP, JTD e CHM) passam a ser desejáveis e não constituem critério de desclassificação;
 - 6.2.46.4. Deve ter solução Autônoma para Avaliação de Ameaças;
 - 6.2.46.5. Deve ter curation de inteligência de ameaças;
 - 6.2.46.6. Deve ter automação de detecção pós-facto;
 - 6.2.46.7. Deve ter melhoria na eficiência do soc;
 - 6.2.46.8. Deve ter automação de respostas cibernéticas rápidas;
 - 6.2.46.9. Deve ter detecção multivetorial;
 - 6.2.46.10. Deve ter detecção por ioc (indicadores de comprometimento);
 - 6.2.46.11. Deve ter detecção por ttp (táticas, técnicas e procedimentos);
 - 6.2.46.12. Deve ter relatórios de conscientização de ameaças;
 - 6.2.46.13. Deve ter integração de inteligência própria;
 - 6.2.46.14. Deve ter relatórios de detecção de ameaças;
 - 6.2.46.15. Deve ter criação automática de incidentes;
 - 6.2.46.16. Deve ter relatórios de ameaças personalizados;



- 6.2.46.17. Deve ter redução do tempo médio de resposta;
- 6.2.46.18. Deve ter avaliação de exposição a ameaças emergentes;
- 6.2.47. Deverá permitir a criação, edição e gerenciamento de playbooks de segurança através de interface gráfica intuitiva;
- 6.2.48. A plataforma deverá disponibilizar console web unificada para gerenciamento de todas as funcionalidades;
- 6.2.49. Deverá suportar arquitetura multi-tenant, permitindo segregação lógica entre diferentes organizações ou departamentos;
- 6.2.50. A solução deverá permitir a criação, a edição, o versionamento e a reutilização de playbooks de automação, por meio de interface gráfica de baixo código do tipo arrastar e soltar ou por linguagem declarativa documentada pelo fabricante (por exemplo, YAML ou JSON), admitindo-se qualquer das formas, desde que a CONTRATADA assuma integralmente a construção, a manutenção e a documentação dos playbooks durante toda a vigência contratual, sem custo adicional para a CONTRATANTE. Deverá disponibilizar blocos de ação pré-configurados incluindo, no mínimo: Actions, Integrations, Utilities, Flow Control e Custom;
- 6.2.51. A plataforma deverá permitir a validação automática de playbooks, verificando conectividade entre blocos e parâmetros obrigatórios;
- 6.2.52. Deverá possibilitar a configuração de regras de disparo (triggering rules) associadas a políticas de segurança;
- 6.2.53. A solução deverá permitir a execução de lógica customizada dentro dos fluxos de automação, por linguagem de script suportada pelo fabricante ou por chamada a serviço externo via API;
- 6.2.54. Deverá possibilitar a adição e configuração de múltiplas instâncias de integração para cada tipo de ferramenta;
- 6.2.55. Deverá permitir o envio de notificações por e-mail com conteúdo dinâmico para aprovação de ações;
- 6.2.56. solução deverá possibilitar a configuração de timeout para processos de aprovação;
- 6.2.57. Deverá suportar diferentes tipos de resposta incluindo: Single-select, Multi-select e Text Value;
- 6.2.58. plataforma deverá disponibilizar funcionalidade de debugger para execução e teste de playbooks contra alertas;
- 6.2.59. Deverá permitir a validação de playbooks antes da implantação em produção;
- 6.2.60. A solução deverá possibilitar testes de regras de disparo (triggering rules) antes da ativação;
- 6.2.61. A interface deverá permitir funcionalidades de Undo (desfazer) e Redo (refazer) durante a edição de playbooks;
- 6.2.62. A plataforma deverá permitir a visualização legível do fluxo do playbook e de suas execuções, por representação gráfica com recursos de ampliação e redução, ou por visualização estruturada do fluxo;
- 6.2.63. Deverá possibilitar a expansão e colapso de painéis de configuração para



otimização do espaço de trabalho;

6.3. Requisitos de processamento de dados

- 6.3.1. A solução deverá ser capaz de extrair e processar detalhes de alertas (Get Alert Details) incluindo endereços IP de origem e destino;
- 6.3.2. Deverá permitir o processamento de múltiplos endereços IP simultaneamente em eventos de violação;
- 6.3.3. A plataforma deverá suportar expressões regulares para tomada de decisão e processamento de dados;

6.4. Gerenciamento contínuo de exposição a ameaças

- 6.4.1. O objetivo é realizar testes contínuos e sistemáticos de exposição a ameaças, utilizando ferramenta de gerenciamento contínuo de exposição, com o intuito de avaliar a eficácia do SIEM, XDR e de todo o processo de monitoramento, detecção e resposta a incidentes. A atividade deverá identificar lacunas de cobertura, validar regras de correlação, bem como fornecer relatórios executivos e técnicos que subsidiem a melhoria contínua da postura de segurança cibernética da CONTRATANTE.

7. GERENCIAMENTO DE INTELIGÊNCIA APLICADO À SEGURANÇA

7.1. Requisitos Gerais

- 7.1.1. A ferramenta tem por objetivo realizar o monitoramento contínuo de fontes externas nacionais e internacionais incluindo Fóruns, Redes Sociais, Mídias Sociais, Nuvens Públicas e Grupos Hackers com o intuito de identificar motivações, intenções e atividades de possíveis adversários que representem riscos à CONTRATANTE. O escopo de monitoramento abrange a Internet de superfície, profunda e escura, permitindo antecipar ameaças e fornecer subsídios estratégicos para a prevenção de incidentes de segurança.
- 7.1.2. A CONTRATADA deve realizar o monitoramento contínuo de fontes externas nacionais e internacionais, como Fóruns, Redes Sociais, Mídias Sociais, Nuvens Públicas e Grupos Hackers para identificação de motivações, intenções e atividades de possíveis adversários que possam causar impactos à CONTRATANTE, seja na INTERNET profunda, escura ou de superfície.
- 7.1.3. A solução deverá ser licenciada para no mínimo os ativos digitais descritos abaixo:

Descrição	Quantidade
Domínios principais	1
Subdomínios	15
Endereços IP públicos	92
Ativos em nuvem expostos	0
Marcas e termos	10
Pessoas VIP	7
Aplicativos móveis	0
Perfis oficiais em redes sociais	3
Portais e páginas de login	15
Usuários da plataforma	7

- 7.1.4. Os Serviços de Proteção de Riscos Digitais, doravante SPRD, devem suportar quatro grandes pilares: mapeamento, monitoramento, curadoria e mitigação.



7.1.5. São apresentadas, a seguir, especificações técnicas mínimas dos serviços a serem ofertados referentes ao objeto. Os termos “possui”, “permite”, “suporta” e “é” implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo “ou” implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo “e” implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

- a) Mapeamento, tem por objetivo coletar, identificar e entender os ativos digitais sob risco.
- b) Monitoramento, visa o monitoramento contínuo e ininterrupto dos ativos digitais, com o objetivo de documentar, contextualizar, enriquecer e priorizar os riscos e alertas com capacidade de reportar detalhes de incidentes permitindo a tomada de decisão inteligente em relação a tais riscos.
- c) Curadoria, visa ter um time especializado para acompanhar e validar os resultados do monitoramento em agendas recorrentes com o cliente para garantir a melhoria contínua dos resultados, captura melhor do contexto do cliente, eliminando falsos alertas, contribuindo no ajuste de novos contextos de buscas e sugerindo novos ativos para potencializar o monitoramento.
- d) Mitigação, visa a reduzir o risco dos ativos digitais, através dos alertas enviados aos clientes, envio de relatórios (executivo e técnico), procedimentos de remoção de conteúdo infrator, boletins periódicos de inteligência ou sugestão de configurações do ambiente para mitigar riscos identificados pela plataforma durante a fase de monitoramento.
- e) Todos os serviços descritos pertencem a um único objeto e bloco de contratação denominado SPRD. Todas as características e requisitos exigidos nesse termo de referência serão confirmadas em prova de conceito ou diligência, presencial ou remota.

7.2. Mapeamento De Ativos

7.2.1. O SPRD deve ser capaz de entregar à CONTRATANTE a visualização de todos os termos/ativos monitorados e permitir o seu gerenciamento, como por exemplo, sua ativação, desativação, exclusão ou a adição de novos ativos.

7.2.2. O SPRD não deve ter limite de monitoramento de termos, nem de alertas gerados a partir destes.

7.2.3. O SPRD deve ser capaz de contextualizar o tipo de ativo, a fim de que seja possível criar regras específicas para cada caso ou tipo de ativo.

7.2.4. O SPRD deve possuir capacidade para entender no mínimo as seguintes classes de ativos:

- a) Domínios: Nome que serve para localizar e identificar conjuntos de computadores na internet. O nome de domínio foi concebido com o objetivo de facilitar a memorização dos endereços de computadores na Internet.
- b) Marcas: A marca registrada, nome fantasia, nome do produto, nome de fachada, razão social, termo ou expressão que identifique o CONTRATANTE.



- c) BIN: Números do cartão de crédito para identificar o banco emissor e a conta do cliente. Os primeiros seis dígitos, liderados pelo primeiro dígito que identifica a bandeira do cartão, são coletivamente conhecidos como o número de identificação do emissor e denominados números de identificação bancária.
- d) Endereço IP: Endereço de Protocolo da Internet, do inglês Internet Protocol address, é um rótulo numérico atribuído a cada dispositivo conectado a uma rede de computadores que utiliza o Protocolo de Internet para comunicação.
- e) Pessoa: Informação de identificação pessoal de empregado ou pessoa de interesse para monitoramento de riscos digitais dirigidos a pessoa física.
- f) Aplicativos móveis: monitoramento de aplicativos relacionados à CONTRATANTE em lojas oficiais e não oficiais, identificados por nome, desenvolvedor, identificador de pacote ou equivalente.

7.2.5. O SRPD deve:

- a) Permitir que o ativo em monitoramento seja apenas desabilitado, para que pare de gerar alertas sem precisar ser excluído da console.
- b) Apresentar em sua tela de gestão de ativos a lista completa de ativos cadastrados, estejam eles habilitados ou desabilitados, contendo o tipo de ativo, o nome do ativo e a quantidade de eventos que este ativo já recebeu.
- c) Permitir visualizar em formato resumido a distribuição das quantidades de ativos por severidade, tipo e status.
- d) Realizar a identificação proativa de eventos relacionados a ativos VIP, como APKs, BINs, domínios, endereços IPv4, marcas e outros ativos críticos. Essa funcionalidade permite o monitoramento contínuo, assegurando a detecção de possíveis ameaças ou atividades anômalas que possam comprometer a segurança e a integridade desses ativos estratégicos.

7.3. Monitoramento

7.3.1. Seguindo um processo de monitoramento contínuo de nossos sensores em regime 24x7 a CONTRATADA deve entregar à CONTRATANTE em forma de relatórios e notificações:

7.3.2. Deverá identificar, reconhecer, coletar, analisar, processar, organizar e apresentar informações disponíveis e acessíveis, de forma automatizada e personalizada, em conversas, mídias e redes sociais, demais páginas da internet de superfície, profunda e oculta, fóruns, redes de compartilhamento de textos e códigos-fonte, aplicativos de mensageria, lojas de aplicativos, feeds, páginas de comércio eletrônico, bem como monitorar outros serviços de descoberta e monitoração e quaisquer outras fontes de informação disponíveis e acessíveis.

7.3.3. As informações devem ser apresentadas a CONTRATANTE no formato de evento, contextualizado com o tipo de risco associado de maneira automática, sem depender de que a CONTRATANTE parametrize consultas, queries, ou qualquer tipo de ação que não



seja usar o serviço. Toda customização da plataforma para monitoramento, gestão, geração de alertas, e configurações adicionais correm por responsabilidade da CONTRATADA.

7.3.4. Os eventos disponíveis no SPRD devem estar contextualizados e estarem disponíveis com base em suas características indicando o tipo de evento a que ele se relaciona, sendo no mínimo os seguintes tipos ou semelhantes:

- a) Menção ao cliente, Linguagem Ofensiva, Fraude Cibernética, Exposição de Credenciais, Personificação a um perfil de mídia social, Exposição de chaves, Phishing.
- b) Correlacionar as informações coletadas, utilizando plataforma de big data para processamento visando normalizar informações, gerando listas acionáveis de inteligência contra ameaças.
- c) A plataforma deve por exemplo ter a capacidade de ao encontrar um dump de senhas que cite credenciais da CONTRATANTE, apresentar evidência referente apenas a CONTRATANTE ao invés de apresentar o dump completo para que a CONTRATANTE pesquise manualmente.
- d) Ao verificar por exemplo uma conversa de grupo ou fórum de fraudes menciona a CONTRATANTE, a CONTRATADA deve apresentar somente as mensagens do contexto de risco à CONTRATANTE e não a conversa completa contendo itens que não são relevantes para a CONTRATANTE.
- e) A plataforma deve reconhecer, no mínimo, as seguintes categorias de informação, ou equivalentes: (i) credenciais e senhas; (ii) chaves, tokens e segredos de API, de aplicações e de provedores de nuvem; (iii) chaves privadas e arquivos de configuração de sistemas; (iv) dados pessoais (CPF, email, currículos); (v) dados de cartões de pagamento, inclusive BIN; (vi) URLs, endereços IP e convites de grupos de mensageria; (vii) ferramentas e contas utilizadas em fraude (ex.: validadores de credenciais e contas de passagem).

7.3.5. Deverá realizar coleta, no mínimo, nas seguintes categorias de fontes: (i) principais redes sociais e plataformas de vídeo utilizadas no Brasil; (ii) aplicativos de mensageria com grupos e canais de acesso público; (iii) lojas de aplicativos oficiais e não oficiais; (iv) sites de compartilhamento de textos, arquivos e códigos-fonte; (v) marketplaces e sites de reclamação de consumidores; (vi) fóruns e mercados da deep e dark web. A cobertura de fontes específicas poderá ser realizada por coleta automatizada ou por monitoramento sob demanda da equipe de inteligência, e a CONTRATANTE poderá solicitar a inclusão de novas fontes durante a execução contratual.

7.3.6. Informar anomalias nos registros de nomes dos domínios monitorados ("whois", registros DNS, etc).

7.3.7. Deve realizar a degravação (transcrição) de áudios publicados em, no mínimo, 1 (uma) plataforma de mensageria monitorada que apresentem correspondência com os critérios pesquisados, transformando-os em evento que contenha a respectiva transcrição. A degravação poderá ser realizada por mecanismo próprio da solução ou por meio dos recursos nativos de transcrição disponibilizados pelas próprias plataformas de comunicação monitoradas, sendo em qualquer caso obrigatória a inclusão do texto transcrito no evento.



- 7.3.8. Na transcrição dos áudios e nos vídeos analisados, deverá ser possível destacar informações relevantes de acordo com os ativos digitais definidos pelo CONTRATANTE.
- 7.3.9. O áudio (completo), bem como seus metadados, onde foi encontrado algum resultado, deve ser capturado, identificado e disponibilizado para análise.
- 7.3.10. Deve realizar a análise de conteúdo de imagens, permitindo que imagens contendo ameaça a algum dos ativos digitais da CONTRATANTE (ex.: captura de tela de credencial de acesso, documento interno ou uso indevido da identidade visual) sejam detectadas e notificadas. A análise poderá ser realizada por reconhecimento óptico de caracteres (OCR) ou por outras metodologias de análise que alcancem o mesmo resultado.
- 7.3.11. Todos os incidentes reportados devem conter informações de log sendo possível determinar:
- a) O ativo digital ao qual aquele determinado incidente se refere;
 - b) A data e hora em que houve a coleta da informação;
 - c) A data e hora em que a informação se transformou em um risco exibido na console do CONTRATANTE.
 - d) A prioridade do risco determinada pelo SPRD.
- 7.3.12. O tipo do incidente e a sua origem.
- 7.3.13. O SPRD deve disponibilizar as informações das pesquisas por, no mínimo: intervalo de data, status, severidade, categoria, contexto, metadados e tipo da fonte.
- 7.3.14. Para as quantidades de ativos digitais presentes neste termo de referência, não poderá haver limitação da quantidade de alertas gerados pelo serviço da CONTRATADA.
- 7.3.15. As ocorrências devem possuir um campo de descrição em que os analistas possam contextualizar as informações associadas.
- 7.3.16. Diretamente a partir de um incidente aberto pela ferramenta deve ser possível solicitar o serviço de remoção de conteúdo infrator (takedown) caso o cliente tenha contratado essa opção.
- 7.3.17. O serviço deverá realizar a detecção de domínios registrados que possam oferecer riscos de serem utilizados de forma maliciosa, através do registro de domínios com variações comuns de nome, permutações de caracteres e outros (typosquatting, nomes de domínios similares).
- 7.3.18. Deve possibilitar a descoberta de páginas de phishing ativas utilizando o nome, a marca e a identidade visual da CONTRATANTE.
- 7.3.19. Deve possibilitar a descoberta de páginas de phishing ativamente, a partir da detecção de clones das aplicações da CONTRATANTE, independentemente de onde estes estejam sendo executados.
- 7.3.20. Deve possuir regras ou casos de uso pré-definidos para detecção, cobrindo no mínimo: phishing, domínios similares, personificação de marca e de pessoas, vazamento de credenciais e de dados, exposição de chaves e segredos, fraude e aplicativos falsos. A relação de casos de uso deverá constar de documentação do fabricante.
- 7.3.21. Permitir a criação e acompanhamento de Incidentes de Segurança, de forma manual ou automática.



- 7.3.22. Possuir a capacidade de criação de interpretadores (coletores) para aplicações proprietárias e/ou não conhecidas. Caso a CONTRATANTE solicite a criação de coletores exclusivos para seu uso, o custo de desenvolvimento será negociado a parte.
- 7.3.23. Deve possuir foco no sistema financeiro brasileiro com fontes relevantes relacionadas a grupos de fraudadores.
- 7.3.24. Deve permitir a inclusão e o monitoramento de novos grupos dos aplicativos de mensageria, incluindo grupos que eventualmente sejam solicitados pela CONTRATANTE.
- 7.3.25. Extrair, no mínimo, os seguintes metadados de cada mensagem: autor, aplicativo de origem e data e hora, com precisão de segundos, dos momentos de envio e coleta.
- 7.3.26. Monitorar, redes de compartilhamento de textos e a plataforma de compartilhamento de códigos.
- 7.3.27. O serviço não deverá possuir limitação na capacidade de análise de ativos digitais.
- 7.3.28. O módulo de monitoramento deve permitir o uso de regras YARA ou equivalente, inclusive, permitindo o cadastro de regras por solicitação da CONTRATANTE.
- 7.3.29. Para eventos do tipo Informação, não é requerido qualquer tipo de ação, podendo estes serem apenas mantidos temporariamente na solução para posteriormente serem descartados.
- 7.3.30. Deve existir a garantia por parte da CONTRATADA, que uma interface humana, ou seja, uma analista que pertence ao grupo de monitoramento de ataques, esteja validando e impedindo o envio de falsos positivos para a CONTRATANTE.
- 7.3.31. Deve oferecer canais de comunicação integrados para funcionários do CONTRATANTE, requisitarem e receberem devolutivas de incidentes detectados pela solução.
- 7.3.32. Deve possuir módulo de visualização de eventos, seus tipos e suas respectivas severidades, através de dashboard. Onde possa ser possível filtrar minimamente por período e realizar o download do mesmo em formato PDF, DOCX e HTML.
- 7.3.33. Nos detalhes de todos os eventos apresentados pela solução de SPRD, deve ser possível verificar, no mínimo, o horário da detecção ou coleta e o horário de disponibilização na console da CONTRATANTE, sendo os demais marcos do processamento rastreáveis por meio de histórico do evento, log de auditoria ou API.
- 7.3.34. A configuração de alertas deve permitir a criação de notificações granulares a partir dos eventos da plataforma. Entre os critérios que devem estar disponíveis para configuração de alertas estão:
- a) Categoria do Evento;
 - b) Tipo do Evento;
 - c) Severidade;
 - d) Filtro de palavra-chave.

7.4. Mitigação

- 7.4.1. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de sites maliciosos, sites que contenham phishing ou sites/domínios que disparem phishing que



utilizem o nome, a marca ou a imagem, mesmo que similar (com intuito de confundir), os clientes da CONTRATADA.

- 7.4.2. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de perfis falsos de funcionários (Executivos) e da própria empresa em redes sociais;
- 7.4.3. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer tipos de informação disponíveis e acessíveis que violem os direitos de uso do CLIENTE ou que permitam burlar os meios de proteção desses direitos;
- 7.4.4. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer tipos de informação disponíveis e acessíveis quando for identificada a tentativa de ataque a reputação da instituição ou ainda a tentativa de captura de credenciais do CLIENTE.
- 7.4.5. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer informações em redes sociais (Facebook, Twitter, LinkedIn, Instagram, YouTube etc. que tenham relação com o CLIENTE e não seja autorizado por essa instituição.
- 7.4.6. Possibilitar a realização do serviço de TAKEDOWN para retirar das principais lojas de aplicativos para mobile (Google Play Store, Apple Store, etc.) os aplicativos falsos e maliciosos distribuídos fora das lojas oficiais comumente conhecidas.
- 7.4.7. Possibilitar a realização do serviço de TAKEDOWN para retirar conteúdo com documentos, informações confidenciais, informações de cartões de crédito, divulgações relacionadas a produtos e sistemas do CLIENTE, divulgações relacionadas a clientes e empregados do CLIENTE, além do monitoramento de sites de compartilhamento de arquivos e informações, sites de compartilhamento de textos (Pastebin, Ghostbin, entre outros) presentes na internet superficial.
- 7.4.8. A CONTRATADA deverá emitir um alerta, atualizado conforme andamento, para acompanhamento do processo de TAKEDOWN de cada ocorrência.
- 7.4.9. A CONTRATADA deverá disponibilizar um painel para consulta e análise de ocorrências (em andamento e finalizadas) do serviço de TAKEDOWN. Deve permitir consultas por intervalo de tempo, tipos de ocorrências e demais critérios relevantes na análise das ocorrências.
- 7.4.10. O serviço de TAKEDOWN deverá ser fornecido sem limitação de quantidade de solicitações durante toda a vigência contratual, com acompanhamento de cada ocorrência até a conclusão e relatório mensal das solicitações realizadas.
- 7.4.11. Todo serviço de TAKEDOWN deve ser acompanhado de um especialista, a fim de garantir assertividade de todo o processo.

8. FERRAMENTA DE TESTE AUTOMATIZADO DE PENETRAÇÃO

- 8.1. A solução deverá permitir execução automatizada de testes de intrusão em ambientes internos e externos.
- 8.2. A solução deverá ser licenciada para suportar 30 IP's simultâneos e 5 aplicações Web simultâneas
- 8.3. A solução deverá permitir execução recorrente, programada ou sob demanda.
- 8.4. A solução deverá permitir execução controlada de cenários de ataque sem causar indisponibilidade significativa dos serviços da CONTRATANTE.



- 8.5.** A solução deverá permitir validação técnica de vulnerabilidades por meio de execução controlada de exploração.
- 8.6.** A solução não deverá limitar-se à identificação passiva de vulnerabilidades, devendo permitir encadeamento contextualizado de ações com base nas exposições identificadas.
- 8.7.** A solução deverá permitir priorização de riscos com base em impacto técnico validado.
- 8.8.** A solução deverá ser oferecida como software implantável no ambiente da CONTRATANTE.
- 8.9.** A solução deverá suportar implantação:
- 8.9.1. em ambiente on-premise
 - 8.9.2. em ambientes virtualizados
 - 8.9.3. em nuvem pública
 - 8.9.4. em arquitetura híbrida
- 8.10.** A solução deverá possuir interface web segura para gerenciamento centralizado.
- 8.11.** A solução deverá suportar execução paralela de múltiplas tarefas de teste.
- 8.12.** A solução deverá disponibilizar API REST para integração com sistemas externos.
- 8.13.** A solução deverá permitir operação em ambientes com ou sem acesso à Internet.
- 8.14.** A solução deverá registrar estado operacional durante cada execução, incluindo ativos descobertos, credenciais obtidas, permissões alcançadas e caminhos de ataque testados
- 8.15.** Realizar descoberta automática de ativos e superfícies de ataque.
- 8.16.** Identificar hosts ativos, serviços expostos e tecnologias utilizadas.
- 8.17.** Mapear ativos internos e externos dentro do escopo definido.
- 8.18.** Atualizar continuamente o inventário de ativos descobertos.
- 8.19.** Identificar relações entre ativos que possam compor caminhos de ataque.
- 8.20.** Identificar vulnerabilidades técnicas associadas aos ativos descobertos.
- 8.21.** Correlacionar vulnerabilidades identificadas com possíveis caminhos de ataque.
- 8.22.** Identificar configurações inseguras, serviços expostos e fraquezas de autenticação.
- 8.23.** Mapear vulnerabilidades identificadas a referências públicas quando aplicável.
- 8.24.** Permitir contextualização do risco com base na exposição real do ambiente.
- 8.25.** Execução automática de exploração de vulnerabilidades quando tecnicamente viável e autorizado.
- 8.26.** Demonstração técnica da explorabilidade da vulnerabilidade identificada.
- 8.27.** Encadeamento de múltiplas vulnerabilidades para construção de cenários de ataque realistas.
- 8.28.** Execução controlada de escalada de privilégios quando aplicável.
- 8.29.** Simulação de movimentação lateral controlada entre segmentos de rede.



- 8.30.** Coleta controlada de evidências técnicas que comprovem o impacto da exploração.
- 8.31.** Construção de cadeias de ataque (Attack Paths) baseadas nas exposições identificadas.
- 8.32.** Demonstração visual das etapas de exploração executadas.
- 8.33.** Correlação entre ativos, vulnerabilidades e permissões obtidas durante o ataque.
- 8.34.** Execução de cenários multi-etapas envolvendo descoberta, exploração, escalada de privilégios e movimentação lateral.
- 8.35.** Identificação de caminhos alternativos de comprometimento quando múltiplas exposições estiverem presentes.
- 8.36.** A solução deverá suportar:
- 8.36.1. Testes Blackbox.
 - 8.36.2. Testes Graybox.
 - 8.36.3. Testes autenticados.
 - 8.36.4. Testes em aplicações Web e APIs.
 - 8.36.5. Testes em ambientes Active Directory.
 - 8.36.6. Simulação de movimentação lateral.
 - 8.36.7. Simulação controlada de coleta de credenciais.
 - 8.36.8. Simulação controlada de exfiltração de dados.
 - 8.36.9. Pivoting autorizado entre segmentos de rede.
 - 8.36.10. Validação de exposições em ambientes de nuvem pública.
- 8.37.** A solução deverá operar segundo ciclo estruturado contendo, no mínimo:
- 8.37.1. Definição de escopo.
 - 8.37.2. Descoberta de ativos.
 - 8.37.3. Identificação de vulnerabilidades.
 - 8.37.4. Validação técnica por exploração controlada.
 - 8.37.5. Priorização baseada em impacto real.
 - 8.37.6. Apoio à remediação.
 - 8.37.7. Revalidação após aplicação de correções.
- 8.38.** Comparação histórica entre execuções sucessivas.
- 8.38.1. A solução deverá permitir integração com:
 - 8.38.2. Soluções SIEM.
 - 8.38.3. Soluções EDR ou XDR.
 - 8.38.4. Ferramentas de gestão de vulnerabilidades.
 - 8.38.5. Sistemas ITSM.
 - 8.38.6. Plataformas DevSecOps.



- 8.38.7. Exportação de eventos via Syslog ou API.
- 8.38.8. Correlação entre resultados de teste e alertas gerados por ferramentas de segurança.
- 8.39. Deverão conter, no mínimo os seguintes relatórios técnico:
 - 8.39.1. vulnerabilidades identificadas
 - 8.39.2. vulnerabilidades exploradas
 - 8.39.3. evidências técnicas da exploração
 - 8.39.4. cadeia de ataque executada
 - 8.39.5. recomendações de mitigação
- 8.40. Deverão conter no mínimo os seguintes relatórios executivos:
 - 8.40.1. Indicador de exposição validada
 - 8.40.2. Evolução histórica da postura de segurança
 - 8.40.3. Priorização de riscos baseada em impacto ao negócio
 - 8.40.4. Mapeamento MITRE ATT&CK
- 8.41. Os relatórios deverão estar disponíveis em formato PDF, HTML ou CSV.
- 8.42. A solução definição de escopo de execução por ativo ou segmento de rede.
- 8.43. definição de janelas de execução.
- 8.44. registro completo das ações executadas.
- 8.45. interrupção segura das execuções quando necessário.
- 8.46. controle de intensidade e profundidade dos testes.

9. HIPERAUTOMAÇÃO PARA DETECÇÃO E RESPOSTA A AMEAÇAS

- 9.1. A ferramenta tem por objetivo analisar em tempo real ameaças ao ambiente de TI da CONTRATANTE, por meio do processamento de metadados de rede e aplicações (como Netflows, DNS, Proxy, Firewall e caixas de spam). Deve permitir a coleta e integração independente de fornecedores, abrangendo infraestrutura local, dispositivos remotos, servidores e nuvens públicas, sem necessidade de hardware dedicado. Além disso, deve possibilitar integração com SIEMs e ferramentas de resposta a incidentes, bem como fornecer APIs abertas para ingestão de metadados, garantindo visibilidade centralizada e suporte ágil à identificação e mitigação de riscos.
- 9.2. A solução ofertada não poderá ser do tipo open source (software livre);
- 9.3. A solução deve oferecer, em modo SaaS, a capacidade de medir o comprometimento dos ativos de TI em tempo real;
- 9.4. O serviço deve ser obrigatoriamente sustentado por uma arquitetura nativa em nuvem (Software as a Service), eliminando qualquer necessidade de a CONTRATANTE manter hardware local, servidores de banco de dados ou realizar atualizações de software de gestão.



- 9.5.** A solução deve ter a capacidade de se integrar, nativamente, com mais de 50 (cinquenta) soluções de tecnologia (infraestrutura e segurança).
- 9.6.** Deve ser disponibilizada uma API pública de ingestão de informações (leitura), com documentação completa e publicada, para extração de métricas e indicadores estratégicos para ferramentas de Business Intelligence (BI) e dashboards customizados da CONTRATANTE.
- 9.7.** A plataforma deverá fornecer esta API aberta de comunicação entre soluções de infraestrutura e segurança.
- 9.8.** A plataforma não deve exigir um licenciamento extra para consumo de APIs, a fim de não gerar custos adicionais para a CONTRATANTE.
- 9.9.** O portal deve fornecer um dashboard de saúde da telemetria, alertando proativamente quando um ativo crítico parar de enviar logs ou quando houver falha na normalização dos dados (parsing).
- 9.10.** Este painel deverá trazer no mínimo os seguintes indicadores executivos e operacionais com seus respectivos quantitativos, permitindo à CONTRATANTE auditar visualmente a relação de eficácia da operação ao longo do tempo:
- 9.10.1. Volume de incidentes abertos;
 - 9.10.2. Novos incidentes ou exposições;
 - 9.10.3. Incidentes ou exposições resolvidos;
 - 9.10.4. Incidentes ou exposições não-resolvidos;
 - 9.10.5. Risco inerente;
 - 9.10.6. Risco residual;
 - 9.10.7. Curva de tendência;
 - 9.10.8. Quantidade total de eventos alertas ou indicadores coletados;
 - 9.10.9. Dispositivos afetados;
 - 9.10.10. Setores comprometidos;
 - 9.10.11. Volume de incidentes respondidos e/ou de ações de remediação executadas;
 - 9.10.12. Histórico de atividades;
 - 9.10.13. Quantidade de artefatos de inteligência de ameaças que foram enviados para as tecnologias integradas;
 - 9.10.14. Tempo médio de detecção e resposta aos incidentes.
- 9.11.** Os dados exportados devem fornecer gráficos de linha do tempo e curva de tendência categorizando ameaças, anomalias ou exposições e a distribuição de atividades adversas por grupos de endpoints, facilitando a localização de segmentos e áreas de risco.
- 9.12.** A plataforma de gestão não poderá ser baseada em softwares do tipo open-source, ou in-house, visando garantir suporte e SLAs diretos do fabricante em situações de crise.
- 9.13.** A solução deve ser licenciada pelo número de ativos tecnológicos a serem monitorados e/ou pelo número de controles de segurança integrados, sem custo adicional por integração.



- 9.14.** Entende-se como um ativo, toda e qualquer solução que se comunica na rede utilizando protocolos de comunicação, como por exemplo TCP/IP.
- 9.15.** A arquitetura deve permitir a implantação de uma quantidade ilimitada de coletores virtuais, conectores e integrações nativas com outras soluções de segurança, sem que isso gere custos adicionais de licenciamento por componente de infraestrutura.
- 9.16.** Independente da alteração da volumetria de informações coletadas ao longo do período contratado, a plataforma deve ser escalável de forma automática, evitando perda de dados e logs, trazendo rastreabilidade
- 9.17.** A quantidade de integrações com outras soluções deve ser ilimitada.
- 9.18.** O fornecedor deve ter certificação SOC2 Type II para confirmar que o serviço SaaS utiliza as melhores práticas em termos de:
- 9.18.1. Privacidade
 - 9.18.2. Segurança
 - 9.18.3. Disponibilidade
 - 9.18.4. Confidencialidade
 - 9.18.5. Integridade de processamento
- 9.19.** A solução deve ser capaz de processar as fontes de telemetria de outras soluções de infraestrutura e segurança, independentemente do formato.
- 9.20.** A coleta de dados deve ser agnóstica aos fornecedores que a organização possui em sua infraestrutura.
- 9.21.** A solução deve permitir a integração com múltiplas ferramentas para coleta de telemetria, como por exemplo, minimamente as seguintes plataformas:
- 9.21.1. Rede
 - 9.21.1.1. Firewall;
 - 9.21.1.2. VPN;
 - 9.21.1.3. Proxy;
 - 9.21.1.4. Plataformas de Microsegmentação;
 - 9.21.1.5. Packet brokers.
 - 9.21.2. Endpoint
 - 9.21.2.1. Servidores DNS;
 - 9.21.2.2. Estações de Trabalho;
 - 9.21.2.3. Servidores.
 - 9.21.3. Cloud
 - 9.21.3.1. Amazon AWS;
 - 9.21.3.2. Google GCP;
 - 9.21.3.3. Microsoft Azure;
 - 9.21.4. E-mail



- 9.21.4.1. Office365;
- 9.21.4.2. Google Workspace.

9.21.5. Identidade

- 9.21.5.1. Active Directory.

9.22. A solução deve ter a capacidade de coletar, processar e analisar as consultas DNS da organização para identificar quais dos ativos estão tentando se comunicar com a infraestrutura do atacante.

9.23. A solução deve ser capaz de coletar, processar e analisar dados absorvidos de plataformas como Microsoft Office 365, identificando quem está atacando a organização e como.

9.24. A solução deve ser capaz de coletar, processar e analisar metadados de rede e de identidade relativos a dispositivos locais e remotos, incluindo estações de trabalho e servidores, sendo livre a arquitetura de coleta adotada (agentes de endpoint, sensores de rede físicos ou virtuais, espelhamento de tráfego, TAP, packet broker, encaminhamento de logs ou integração por API), desde que todos os componentes necessários sejam fornecidos, instalados e mantidos pela CONTRATADA sem custo adicional.

- 9.24.1. Caso a arquitetura ofertada empregue agentes, estes devem ser compatíveis com as versões de Windows, Windows Server, ChromeOS, MacOS e das principais distribuições Linux corporativas que estiverem suportadas pelos respectivos fabricantes à época da contratação.

9.25. Para o processo de coleta das fontes de telemetria, a CONTRATADA deve fornecer, instalar, configurar e manter todos os componentes necessários (agentes, coletores virtuais, sensores físicos ou virtuais, appliances ou conectores de log e de API), sem custo adicional para a CONTRATANTE. Caberá à CONTRATANTE disponibilizar os recursos de virtualização, as portas de espelhamento, TAP ou packet broker e os acessos lógicos exigidos pela arquitetura ofertada, os quais deverão estar integralmente descritos na proposta técnica da licitante.

9.26. A coleta de dados deve ser orientada a metadados, evitando o armazenamento ou análise de pacotes completos de dados, garantindo eficiência e menor sobrecarga de rede.

9.27. O monitoramento deve oferecer uma visão abrangente das comunicações de toda a rede, incluindo e não se limitando a:

- 9.27.1. Estações de trabalho;
- 9.27.2. Servidores;
- 9.27.3. Equipamentos de rede;
- 9.27.4. Equipamentos IoT.

9.28. A solução deve armazenar dados históricos por até 2 (dois) anos.

9.29. As informações coletadas das fontes devem ser armazenadas em infraestrutura em nuvem de fabricantes, que responderão pela guarda primária, pelo controle de acesso e pela proteção dos dados, não se admitindo que a operação da solução dependa de infraestrutura de armazenamento provida pela CONTRATANTE.



- 9.29.1. Será admitida a exportação dos metadados e eventos para a solução de SIEM contratada no item 6 deste mesmo lote, para fins de retenção estendida, correlação e auditoria.
- 9.30.** Deve-se existir a exportação destas informações diretamente da plataforma durante todo o período em que estiver armazenado.
- 9.31.** Caso a arquitetura ofertada utilize coletor, conector ou componente virtual equivalente, este deve suportar, no mínimo, os seguintes virtualizadores:
- 9.31.1. Hyper-V;
 - 9.31.2. VMware ESXi;
 - 9.31.3. VMware Workstation.
- 9.32.** A solução deve identificar em tempo real e retrospectivamente comprometimentos confirmados e comportamentos maliciosos na rede.
- 9.33.** A solução deve ter a capacidade de classificar o tipo da ameaça confirmada o o indicador tratado no mínimo, porém não se limitando aos exemplos a seguir:
- 9.33.1. Anonymizer;
 - 9.33.2. C&C (Comando e Controle);
 - 9.33.3. Malware;
 - 9.33.4. Mining;
 - 9.33.5. Network Scan;
 - 9.33.6. Phishing;
 - 9.33.7. Spam
- 9.34.** A solução deve ter a capacidade de identificar anomalias e eventos suspeitos, no mínimo, porém não se limitando aos exemplos a seguir:
- 9.34.1. DGA (Algoritmo de Geração de Domínios);
 - 9.34.2. Tunelamento de DNS;
 - 9.34.3. Tentativas de logins não-usuais;
 - 9.34.4. Tentativas de brute-force de rede;
 - 9.34.5. Tentativas de brute-force de identidade.
- 9.35.** A plataforma deve empregar capacidades avançadas e contínuas de Inteligência Artificial (IA) e Aprendizado de Máquina (Machine Learning) para separar comportamentos normais de atividades incomuns, identificando atividades suspeitas de maneira proativa.
- 9.36.** Os motores analíticos e de triagem utilizados pela plataforma devem adotar e aplicar técnicas reconhecidas de aprendizado de máquina supervisionado e não supervisionado, documentadas pelo fabricante, tais como:
- 9.36.1. Latent Dirichlet Allocation (LDA);
 - 9.36.2. Isolation Forest (Floresta de Isolamento);
 - 9.36.3. Random Forest (Floresta Aleatória);
 - 9.36.4. Recurrent Neural Networks (Redes Neurais Recorrentes);



9.36.5. Ensemble Methods (Métodos de Aprendizado em Conjunto);

9.36.6. Ou outros algoritmos e modelos equivalentes.

9.37. A solução deve permitir a adição de novas fontes de inteligência cibernética da CONTRATANTE, incluindo o conceito BYOTI ('Bring Your Own Threat Intelligence')."

9.37.1. Analisadores supervisionados de Machine Learning e Inteligência Artificial.

9.37.2. Analisadores não supervisionados de Machine Learning e Inteligência Artificial.

9.37.3. Análise retrospectiva em todos os dados que foram coletados e armazenados nos últimos 2 (dois) anos.

9.37.4. Sempre que novos artefatos ou Indicadores de Comprometimento (IoCs) forem incorporados à base de inteligência da CONTRATADA ou base customizada, a solução deverá realizar, de forma automatizada, uma análise retrospectiva (hunting) para identificar possíveis interações com tais ameaças no ambiente da CONTRATANTE, abrangendo os últimos 2 (dois) anos.

9.37.5. Além da identificação do vetor inicial de contato, a solução deve detalhar os ativos e usuários comprometidos, indicando a unidade de negócio afetada e o nível de risco associado à organização sempre que a informação estiver disponível nas fontes integradas.

9.37.6. Não deverá possuir limitação quanto ao volume ou à frequência de execuções de análises retrospectivas (huntings) realizadas pela solução.

9.38. A solução deve identificar com precisão a origem e a propagação de incidentes no ambiente da CONTRATANTE, atendendo aos seguintes requisitos:

9.38.1. Rastreabilidade de Endpoints: Identificar o ponto de origem e todos os dispositivos e usuários afetados pelo comprometimento, permitindo o mapeamento completo do vetor de ataque, incluindo a identificação de ameaças provenientes de e-mails maliciosos;

9.38.2. Arquitetura Sem Agentes: A visibilidade e detecção descritas devem ser realizadas sem a necessidade de instalação de agentes nos endpoints, softwares adicionais nos ativos de rede ou aquisição de hardware proprietário dedicado para esse fim;

9.38.3. Enriquecimento com Inteligência de Ameaças: Para cada ameaça detectada ou indicador tratado, a solução deve fornecer metadados detalhados de Threat Intelligence, incluindo quando disponíveis:

9.38.3.1. Identificação do ator ou grupo de ameaça;

9.38.3.2. Geolocalização e infraestrutura de origem;

9.38.3.3. Status operacional (se o artefato malicioso permanece ativo ou online) ou nível de confiança atualizado do artefato malicioso.

9.38.4. A solução deve fornecer o contexto completo de todos os Indicadores de Comprometimento (IoCs) detectados, incluindo, mas não se limitando a:

9.38.4.1. Família de malware

9.38.4.2. Atribuição de atores de ameaça (quando disponível);

9.38.4.3. Severidade;



- 9.38.4.4. Táticas, técnicas e procedimentos (TTPs) associados, baseado no Mitre ATT&CK.
- 9.38.5. A solução deve entregar, no mínimo, os seguintes artefatos (caso aplicáveis) para cada incidente detectado ou indicador tratado e deve ter a opção de fazer o download destas informações diretamente da plataforma:
- 9.38.5.1. Domínio(s);
 - 9.38.5.2. URL(s);
 - 9.38.5.3. IP(s) resolvido(s);
 - 9.38.5.4. Arquivo(s) relacionado(s) e sua(s) respectiva(s) hash(es);
 - 9.38.5.5. Amostra(s) de malware(s) relacionado(s);
 - 9.38.5.6. Data de quando a ameaça foi descoberta;
 - 9.38.5.7. Data da última vez que a ameaça foi reportada.
- 9.38.6. A solução deve fornecer contexto para cada incidente com referências internas e externas para entender a natureza do incidente.
- 9.38.7. Após a detecção e triagem autônoma de um incidente, a solução deverá orquestrar respostas automáticas por meio de integração com a infraestrutura de segurança existente do CONTRATANTE, incluindo, mas não se limitando a Firewall, Proxy, EDR/XDR, Antimalware, Plataformas de Microsegmentação, Proteção de DNS e Infraestruturas de Nuvem Pública.
- 9.38.8. A execução da resposta e contenção deverá ocorrer de forma nativa nos componentes de infraestrutura de rede e segurança já existentes. A solução deve obrigatoriamente permitir a mitigação de ameaças de maneira orquestrada via integração (API), sendo vedadas soluções cuja única capacidade de bloqueio dependa exclusivamente da instalação de agentes proprietários nos dispositivos finais (endpoints) ou que exijam a gerência direta e manual sobre o ativo para a efetivação da resposta.
- 9.38.9. Como parte deste processo, a plataforma deverá prover e distribuir inteligência de ameaças (Threat Intelligence) contextualizada para os sistemas integrados, a fim de enriquecer e justificar as políticas de bloqueio aplicadas.
- 9.38.10. A solução deverá possuir, funcionalidade de bloqueio automático por meio de integração com os principais fabricantes de firewall do mercado, contemplando, no mínimo, os seguintes:
- 9.38.10.1. Palo Alto;
 - 9.38.10.2. Fortinet;
 - 9.38.10.3. Checkpoint;
 - 9.38.10.4. Sophos;
 - 9.38.10.5. Cisco/Meraki;
 - 9.38.10.6. Watchguard;
 - 9.38.10.7. Sonicwall;
 - 9.38.10.8. Juniper;
 - 9.38.10.9. PFsense;



- 9.38.10.10. Barracuda;
- 9.38.10.11. Forcepoint;
- 9.38.10.12. Cato Networks.

9.38.11. A solução deverá possuir, funcionalidade de bloqueio automático por meio de integração com os principais fabricantes de antimalware e EDR do mercado, contemplando, no mínimo, os seguintes:

- 9.38.11.1. CrowdStrike;
- 9.38.11.2. Microsoft Defender;
- 9.38.11.3. Sophos Endpoint;
- 9.38.11.4. SentinelOne
- 9.38.11.5. Trend Micro
- 9.38.11.6. Bitdefender
- 9.38.11.7. Checkpoint Harmony
- 9.38.11.8. Cisco Secure Endpoint
- 9.38.11.9. Cylance
- 9.38.11.10. VMware Carbon Black;
- 9.38.11.11. Sonicwall;
- 9.38.11.12. Symantec on-premises;
- 9.38.11.13. Kaspersky on-premises.
- 9.38.11.14. ESET on-premises.

9.38.12. A solução deverá possuir, funcionalidade de bloqueio automático por meio de integração com os principais fabricantes de web proxy do mercado, contemplando, no mínimo, os seguintes:

- 9.38.12.1. Zscaler ZIA;
- 9.38.12.2. Netskope SWG;
- 9.38.12.3. McAfee SWG;
- 9.38.12.4. Iboss Zero Trust;
- 9.38.12.5. Akamai SIA;
- 9.38.12.6. Forcepoint SWG;

9.38.13. A solução deverá possuir, funcionalidade de bloqueio automático por meio de integração com os principais fabricantes de proteção de DNS do mercado:

9.38.14. A solução deverá possuir, funcionalidade de bloqueio automático por meio de integração com os principais fabricantes de nuvem pública do mercado, contemplando, no mínimo, os seguintes:

- 9.38.14.1. Amazon AWS;
- 9.38.14.2. Microsoft Azure;
- 9.38.14.3. Google GCP.



9.38.15. A solução deverá possuir, funcionalidade de bloqueio automático por meio de integração com os principais fabricantes de microsegmentação do mercado, contemplando, no mínimo, os seguintes:

9.38.15.1. Illumio;

9.38.15.2. Guardicore.

9.38.16. Além do ecossistema nativo de orquestração deve ser disponibilizada uma API documentada. Esta API deve permitir a automação da contenção e a exportação de artefatos (IoCs) advindos de incidentes confirmados para componentes de terceiros.

9.38.17. As funcionalidades de mitigação e bloqueio não deverão ser limitadas à técnica de TCP Reset.

9.38.18. A solução deve empregar métodos de bloqueio eficazes em nível de infraestrutura (Firewalls, Proxy, EDR, Antimalware) que impeçam novas tentativas de conexão e que sejam agnósticos ao protocolo de transporte utilizado, garantindo proteção contra ameaças persistentes e que utilizam múltiplos vetores de comunicação.

9.38.19. Sempre que um novo IoC for integrado a partir de uma base customizada, a solução deverá disparar as seguintes ações de forma automatizada:

9.38.20. Executar protocolos de resposta autônoma para cada IoC detectado, visando a mitigação imediata da ameaça no ambiente.

9.38.21. Iniciar e concluir um processo de threat hunting retrospectivo em toda a base histórica de eventos dos últimos 2 (dois) anos.

9.38.22. Sempre que uma nova solução for adquirida pela CONTRATANTE a solução da CONTRATADA deverá integrar-se bidirecionalmente e de forma automática à nova solução adquirida pela CONTRATANTE, coletando os artefatos maliciosos por ela identificados e incorporando-os às suas políticas de bloqueio, bem como fornecendo-lhe os artefatos maliciosos vigentes em sua própria base de indicadores, contemplados, em ambos os fluxos, no mínimo, aqueles observados nos incidentes ocorridos nos últimos 3 (três) dias.

9.38.23. A solução deve possuir capacidade de gerenciamento dinâmico do ciclo de vida dos Indicadores de Comprometimento (IoCs), garantindo a precisão das detecções e a otimização dos recursos de segurança da CONTRATANTE:

9.38.23.1. A plataforma deve ser capaz de identificar, quando um artefato ou recurso anteriormente malicioso deixar de representar uma ameaça ativa, reclassificando-o para evitar falsos positivos.

9.38.23.2. Uma vez identificado o fim do ciclo de vida de uma ameaça, a solução deve atualizar automaticamente as ferramentas de segurança integradas, removendo proteções e regras de bloqueio obsoletas.

9.38.23.3. A automação descrita deve visar a economia de recursos de processamento nos ativos de rede e segurança, mantendo apenas as políticas de proteção estritamente necessárias e vigentes.

9.38.23.4. Mesmo após a desclassificação de um IoC como malicioso, a solução deve alertar caso contatos residuais com este recurso persistam no ambiente, sinalizando a necessidade de revisão técnica de ativos possivelmente comprometidos de forma latente.



- 9.38.24. A solução deve fornecer um portal web acessível por meio dos navegadores Google Chrome, Mozilla Firefox, Microsoft Edge ou Safari, nas versões oficiais mais recentes disponíveis.
- 9.38.25. A solução deve disponibilizar interface web centralizada para monitoramento contínuo, apresentando indicadores objetivos sobre a postura de segurança e eficiência operacional:
- 9.38.25.1. Painel com indicadores quantitativos de incidentes abertos, total de dispositivos (endpoints) afetados e setores comprometidos.
 - 9.38.25.2. Exibição do volume de incidentes ou exposições abertos, novos IoCs incorporados à defesa e o quantitativo de horas de trabalho economizadas pela equipe interna, devido à automação.
 - 9.38.25.3. Gráficos de linha do tempo categorizando ameaças por tipo (Malware, Phishing, C&C, Network Scan) ou categorias equivalentes e volume de tráfego analisado.
 - 9.38.25.4. Identificação visual da distribuição de contatos adversos por grupos de endpoints e setores, permitindo localizar rapidamente áreas de maior risco.
- 9.38.26. A solução deve ter a opção de filtros de data pré-definidos.
- 9.38.26.1. Hoje;
 - 9.38.26.2. Ontem;
 - 9.38.26.3. Últimos 7 (sete) dias;
 - 9.38.26.4. Últimos 30 (trinta) dias.
- 9.38.27. A solução deve ter a opção de filtros por um período personalizado.
- 9.38.28. A solução deve ter a opção de filtros de dados relacionados com incidentes.
- 9.38.28.1. Tipos de incidentes;
 - 9.38.28.2. Quantidade de endpoints;
 - 9.38.28.3. Quantidade de contatos;
 - 9.38.28.4. Data de criação.
- 9.38.29. A solução deve ter a possibilidade usar linguagem natural em sua filtragem para executar pesquisas no histórico dos incidentes.
- 9.38.30. A solução deve permitir o agrupamento dos ativos de informação de acordo com as necessidades da organização, através de marcação e/ou etiquetas.
- 9.38.31. A solução deve incluir a frequência dos contatos maliciosos por dia da semana e por hora do dia. Também deve mostrar a distribuição do ataque com base em etiquetas previamente configuradas (por exemplo, usuário remoto, escritório central, IOT).
- 9.38.32. O portal web deve permitir a criação de novos usuários da organização com no mínimo as seguintes funções:
- 9.38.32.1. Administrador;
 - 9.38.32.2. Somente leitura.



9.38.33. A solução deve fornecer as informações dos acessos ao portal e quais as respectivas atividades e configurações realizadas de, pelo menos, os últimos 180 (cento e oitenta) dias a fins de auditoria contendo, pelo menos, as seguintes informações:

- 9.38.33.1. Usuário;
- 9.38.33.2. Função;
- 9.38.33.3. Tipo de atividade;
- 9.38.33.4. Data/hora da atividade.

9.38.34. O Portal deve permitir o monitoramento dos coletores implantados na rede, por exemplo:

- 9.38.34.1. Status da Máquina Virtual da Solução;
- 9.38.34.2. Status das Integrações com Dispositivos (Firewall, Proxy, DNS e Email);
- 9.38.34.3. Status dos agentes instalados (Servidores e Estações de Trabalho).

9.38.35. Caso a arquitetura ofertada empregue agentes, sensores ou coletores, o portal deve permitir o monitoramento desses componentes de coleta implantados no ambiente, trazendo as seguintes informações:

- 9.38.35.1. Nome da máquina ou do componente;
- 9.38.35.2. Nome e versão do sistema operacional ou do firmware;
- 9.38.35.3. Versão do componente de coleta;
- 9.38.35.4. Grupo ou segmento ao qual pertence.

9.38.36. A plataforma deve oferecer mecanismos de autenticação forte, exigindo um segundo fator de autenticação (2FA) para a validação do acesso e garantia da integridade das credenciais dos usuários da preferência da organização, sejam eles Google Authenticator, Microsoft Authenticator e outros.

9.38.37. A solução deve ter a capacidade de Integração via SSO para autenticação em seu portal web com pelo menos:

- 9.38.37.1. Active Directory;
- 9.38.37.2. Entra ID;
- 9.38.37.3. OKTA;
- 9.38.37.4. Thales;
- 9.38.37.5. Cyberark;
- 9.38.37.6. Keycloak.

9.38.38. A solução deve possuir arquitetura de integração com ferramentas de terceiros, permitindo o encaminhamento de alertas e o gerenciamento centralizado de incidentes por meio de conector nativo ou de mecanismo documentado de API REST, webhook ou syslog, cabendo à CONTRATADA implantar e manter a integração sem custo adicional, contemplando no mínimo, mas não se limitando, aos seguintes ecossistemas:

- 9.38.38.1. SIEM Splunk;
- 9.38.38.2. SIEM IBM QRadar;



- 9.38.38.3. SIEM Microsoft Sentinel;
- 9.38.38.4. SIEM Google SecOps;
- 9.38.38.5. SIEM Wazuh;
- 9.38.38.6. XSOAR Cortex Palo Alto;
- 9.38.38.7. Microsoft Teams
- 9.38.38.8. Google Chat
- 9.38.38.9. Slack
- 9.38.38.10. ITSM ServiceNow
- 9.38.38.11. ITSM Jira
- 9.38.38.12. ITSM ConnectWise PSA
- 9.38.38.13. ITSM GLPI
- 9.38.39. Após a identificação de um incidente, a solução deve enviar notificação automática para o e-mail do administrador da plataforma ou para os usuários conforme determinado.
- 9.38.40. A solução deve enviar relatórios técnicos e executivos via e-mail com informações sobre as atividades da operação contendo, no mínimo:
 - 9.38.40.1. Métricas operacionais;
 - 9.38.40.2. Métricas de performance;
 - 9.38.40.3. Quantidade de incidentes tratados e respondidos;
 - 9.38.40.4. Soluções que receberam ajuste de políticas;
 - 9.38.40.5. Distribuição de incidentes por impacto no negócio;
 - 9.38.40.6. Máquinas mais afetadas;
 - 9.38.40.7. Quantidade de incidentes tratados e respondidos.
- 9.38.41. A solução deve permitir a exportação em formato CSV do inventário dos ativos monitorados e dos componentes de coleta implantados na rede (agentes, sensores ou coletores), conforme a arquitetura ofertada.
- 9.38.42. A solução deve permitir a exportação de incidentes no formato CSV e STIX.
- 9.38.43. A solução deve incluir a análise de cada incidente com base na Matriz do MITRE ATT&CK de conhecimento de táticas e técnicas adversas baseadas em observações do mundo real.
- 9.38.44. A solução deve incluir a análise global das táticas e técnicas do MITRE ATT&CK usadas por atacantes na organização. Este recurso deve permitir que a organização veja como os atacantes estão tentando acessar na nossa rede, dando a visibilidade necessária para ajustar nossa pilha de segurança cibernética, para melhorar a eficiência e a eficácia de nossas defesas cibernéticas.
- 9.38.45. A solução deve permitir configurar a periodicidade da entrega dos relatórios:
 - 9.38.45.1. Diário
 - 9.38.45.2. Semanal
 - 9.38.45.3. Quinzenal



9.38.45.4. Mensal.

- 9.38.46. A solução deve fornecer informações sobre o número médio de incidentes reportados em um período de tempo determinado.
- 9.38.47. A solução deve fornecer informações sobre o tempo médio de resposta (MTTR) a incidentes reportados em um período de tempo determinado.
- 9.38.48. A solução, dentro dos KPIs fornecidos automaticamente, deve ter a capacidade de mostrar, pelo menos, o tempo médio de resposta da organização a um incidente ou por um período de tempo determinado, bem como o número médio de incidentes registrados diariamente.
- 9.38.49. A solução deve fornecer informações que evidenciem a eficiência operacional que a organização está alcançando, através da economia operacional expressa em horas de trabalho dos analistas de segurança.
- 9.38.50. A solução deve fornecer informações sobre o tempo médio de resolução de incidentes reportados em um período de tempo determinado.
- 9.38.51. A solução deve fornecer métricas sobre a quantidade de artefatos maliciosos ou indicadores de comprometimento que foram incluídos em políticas de bloqueio de soluções terceiras integradas;
- 9.38.52. A solução deve fornecer de forma gráfica a informação associada à distribuição do tráfego coletado/analísado em função da popularidade dos domínios contatados;

10. SOLUÇÃO DE GESTÃO DE DISPONIBILIDADE

10.1. Requisitos Gerais

- 10.1.1. Tem por objetivo monitorar, de forma contínua e ininterrupta, a disponibilidade dos dispositivos (servidores) locais responsáveis por sustentar as soluções contempladas neste edital, garantindo seu pleno funcionamento a qualquer tempo.
- 10.1.2. A CONTRATADA também deverá definir e realizar de forma periódica, ações proativas de ajustes da ferramenta de monitoramento para entregar maior visibilidade e disponibilidade dos ativos.
- 10.1.3. Deverá ser fornecido monitoramento de hosts com no mínimo visualização dos seguintes parâmetros:
- 10.1.3.1. Detalhamento dos hosts ativos (up);
 - 10.1.3.2. Detalhamento dos hosts desativados (down);
 - 10.1.3.3. Detalhamentos de todos os hosts monitorados;
- 10.1.4. Ainda sobre os hosts monitorados, deverá apresentar dashboard com no mínimo as seguintes informações:
- 10.1.4.1. Identificação do Host;
 - 10.1.4.2. IP;
 - 10.1.4.3. Porta de rede utilizada;
 - 10.1.4.4. Informação da community SNMP
- 10.1.5. Deverá ser fornecido monitoramento de links com no mínimo visualização dos

seguintes parâmetros:

- 10.1.5.1. Detalhamento dos links ativos (up);
- 10.1.5.2. Detalhamento dos links desativados (down);
- 10.1.5.3. Detalhamentos de todos os links monitorados;

10.1.6. Deverá possuir dashboard de monitoramento geral, com no mínimo as seguintes capacidades de visualização:

- 10.1.6.1. Permitir o monitoramento contínuo da disponibilidade de dispositivos (hosts), com identificação de estados UP e DOWN em tempo real.
- 10.1.6.2. Exibir indicadores consolidados com quantitativo global de hosts:
- 10.1.6.3. Total de hosts monitorados
- 10.1.6.4. Total de hosts disponíveis (UP)
- 10.1.6.5. Total de hosts indisponíveis (DOWN)
- 10.1.6.6. Possibilitar a atualização automática da disponibilidade com periodicidade configurável (em segundos).
- 10.1.6.7. Identificar, registrar e exibir incidentes ativos em tempo real.
- 10.1.6.8. Classificar incidentes por níveis de criticidade (ex.: crítico, alto, médio, baixo).
- 10.1.6.9. Apresentar quantitativo consolidado de incidentes ativos por categoria.
- 10.1.6.10. Permitir o detalhamento do incidente até o nível do ativo afetado.
- 10.1.6.11. Suportar integração com sistemas de ITSM (ex: abertura automática de chamados).
- 10.1.6.12. Monitorar o tempo de resposta (latência) dos ativos de rede e servidores.
- 10.1.6.13. Exibir os tempos em milissegundos (ms), com ordenação por maior criticidade.
- 10.1.6.14. Permitir configuração de thresholds para classificação:
 - 10.1.6.14.1. Normal
 - 10.1.6.14.2. Alerta
 - 10.1.6.14.3. Crítico
- 10.1.6.15. Monitoramento de consumo de CPU:
 - 10.1.6.15.1. Monitorar a utilização de CPU dos ativos em percentual (%).
 - 10.1.6.15.2. Exibir ranking dos ativos com maior consumo.
 - 10.1.6.15.3. Permitir definição de limites configuráveis de alerta.
 - 10.1.6.15.4. Suportar coleta em intervalos inferiores a 1 minuto.
- 10.1.6.16. Monitoramento de consumo de memória:
 - 10.1.6.16.1. Monitorar o consumo de memória RAM em percentual (%).
 - 10.1.6.16.2. Identificar automaticamente ativos com utilização elevada.



- 10.1.6.16.3. Exibir painel comparativo entre múltiplos servidores.
- 10.1.6.16.4. Possibilitar histórico de consumo para análise de tendências.
- 10.1.6.17. Monitoramento de consumo de disco:
 - 10.1.6.17.1. Monitorar utilização de discos em percentual (%).
 - 10.1.6.17.2. Identificar volumes críticos (ex.: acima de 90%).
 - 10.1.6.17.3. Permitir visualização ordenada pelos maiores consumos.
 - 10.1.6.17.4. Suportar monitoramento de múltiplos volumes por host.
- 10.1.7. Deverá possuir dashboard de monitoramento geral de alertas, com no mínimo as seguintes capacidades de visualização:
 - 10.1.7.1. Detalhamento por nome do host
 - 10.1.7.2. Severidade do alerta
 - 10.1.7.3. Descrição do problema
 - 10.1.7.4. Data e hora do alarme
 - 10.1.7.5. Capacidade de realizar filtragem de alarme por intervalo de horário e data;
- 10.1.8. Deverá possuir monitoramento de Firewalls, contendo no mínimo os seguintes parâmetros:
 - 10.1.8.1. Nome do appliance/host;
 - 10.1.8.2. Status do appliance;
 - 10.1.8.3. Utilização de CPU;
 - 10.1.8.4. Utilização de Memória;
 - 10.1.8.5. Sessões ativas;
 - 10.1.8.6. Tráfego por interface;
 - 10.1.8.7. Tráfego de VPN;
 - 10.1.8.8. Gráfico de perda de pacotes (Packet Loss);
- 10.1.9. Deverá possuir monitoramento de servidores, contendo no mínimo os seguintes parâmetros:
 - 10.1.9.1. A solução deverá permitir o monitoramento individualizado de servidores, com exibição do nome do servidor monitorado.
 - 10.1.9.2. A solução deverá indicar, em tempo real, o status de disponibilidade do servidor, incluindo estados como UP e DOWN.
 - 10.1.9.3. A solução deverá monitorar e alertar sobre o status do agente de coleta instalado no servidor, identificando condições de indisponibilidade como "Agent Down".
 - 10.1.9.4. A solução deverá apresentar o tempo de disponibilidade contínua (uptime) do servidor em formato detalhado, incluindo dias, horas, minutos e segundos.
 - 10.1.9.5. A solução deverá realizar monitoramento de conectividade via ICMP (ping), demonstrando o status ao longo do tempo em linha temporal contínua.



- 10.1.9.6. A solução deverá exibir histórico de disponibilidade ICMP com granularidade mínima de minutos.
- 10.1.9.7. A solução deverá apresentar indicadores visuais de estado (ex.: ACTIVE) para conectividade de rede.
- 10.1.9.8. A solução deverá monitorar o consumo de CPU em tempo real, apresentando os dados em formato percentual.
- 10.1.9.9. A solução deverá disponibilizar visualização gráfica do consumo de CPU ao longo do tempo (séries temporais).
- 10.1.9.10. A solução deverá apresentar medidores gráficos de consumo para CPU, com indicação visual de limites operacionais.
- 10.1.9.11. A solução deverá permitir identificação do valor atual de utilização de CPU (ex.: 5,50%).
- 10.1.9.12. A solução deverá monitorar o consumo de memória RAM em tempo real, com exibição em percentual.
- 10.1.9.13. A solução deverá disponibilizar gráfico histórico de consumo de memória.
- 10.1.9.14. A solução deverá apresentar medidores para consumo de memória, com indicação visual de faixas de uso.
- 10.1.9.15. A solução deverá identificar automaticamente variações de consumo de memória ao longo do tempo.
- 10.1.9.16. A solução deverá apresentar gráfico histórico de uso de disco em percentual.
- 10.1.9.17. A solução deverá permitir visualização simultânea de múltiplos volumes de armazenamento.
- 10.1.9.18. A solução deverá exibir estatísticas detalhadas por métrica, incluindo:
- 10.1.9.18.1. Valor médio (Mean)
 - 10.1.9.18.2. Último valor coletado (Last)
 - 10.1.9.18.3. Valor máximo (Max)
 - 10.1.9.18.4. Valor mínimo (Min)
- 10.1.9.19. A solução deverá permitir identificação nominal dos volumes monitorados (ex.: "/", "/boot/efi").
- 10.1.9.20. A solução deverá possibilitar a correlação entre métricas de CPU, memória e disco para análise de desempenho.
- 10.1.9.21. A solução deverá permitir a definição de intervalos de tempo para análise (ex.: última 1 hora).
- 10.1.9.22. A solução deverá oferecer recurso de atualização automática dos dados (refresh configurável).
- 10.1.9.23. A solução deverá permitir filtragem e seleção dinâmica de hosts monitorados.
- 10.1.9.24. A solução deverá apresentar dashboards operacionais centralizados com informações consolidadas e detalhadas por servidor.



10.1.9.25. A solução deverá utilizar codificação visual por cores para indicar estados e níveis de criticidade.

10.1.9.26. A solução deverá possibilitar identificação rápida de degradação de serviços com base em indicadores de desempenho e disponibilidade.

SOLUÇÃO DE PROTEÇÃO DE E-MAIL, CONSCIENTIZAÇÃO E PROTEÇÃO CONTRA VAZAMENTO DE INFORMAÇÕES

11. SECURE MAIL GATEWAY E SEC.AWARENESS

11.1. Requisitos Gerais

11.1.1. Contratação de uma solução de Proteção de E-mail (Email Security), Conscientização de Usuários (Security Awareness) e prevenção de exfiltração de dados, visando proteger o ambiente de mensagens eletrônicas contra ameaças cibernéticas, impedir a saída não autorizada de informações sensíveis e, simultaneamente, elevar o nível de conhecimento dos usuários da SEFAZ-ES no que diz respeito às boas práticas de segurança da informação.

11.1.2. A CONTRATADA deverá prover, por meio de softwares e serviços especializados, uma solução de proteção de e-mail, conscientização de usuários e , visando aumentar a resiliência cibernética da CONTRATANTE.

11.1.3. A CONTRATADA deverá realizar a entrega de uma plataforma robusta de segurança de e-mail, capaz de bloquear ameaças como spam, phishing, malware e Business Email Compromise (BEC), bem como uma solução de conscientização, com recursos de campanhas de phishing educativo, treinamentos interativos, quizzes e relatórios de desempenho. Neste contexto, a CONTRATADA será responsável pelos serviços de implantação, configuração, personalização e sustentação da solução, garantindo sua plena eficácia, alinhamento com as boas práticas de segurança da informação e aderência ao ambiente operacional do CONTRATANTE.

11.1.4. As ferramentas e soluções utilizadas para prestação do serviço supracitado deverão ser agrupadas, a saber:

11.1.5. Solução de Proteção de E-mail: Solução utilizada pela CONTRATADA para proteger todo o ciclo de comunicações eletrônicas no ambiente do CONTRATANTE, desde a recepção até a entrega de mensagens. A plataforma deve oferecer recursos para bloqueio de ameaças como phishing, malware, spam e e-mails de impostores (BEC), fornecendo visibilidade centralizada sobre incidentes, relatórios gerenciais e orientações para mitigação de riscos. Assim, busca-se reduzir a exposição cibernética da CONTRATANTE e fortalecer sua postura de segurança;

11.1.6. Solução de Conscientização de Usuários: Solução utilizada pela CONTRATADA para capacitar os usuários finais da CONTRATANTE a reconhecerem e reportarem ameaças cibernéticas em tempo real. A plataforma deve oferecer treinamentos próprios e possibilidade de personalizá-los, ajustando o conteúdo às necessidades específicas de cada público. Com isso, busca-se transformar o usuário em uma forte linha de defesa contra phishing e outros tipos de ataques, por meio de avaliações de risco, engajamento contínuo e relatórios de incidentes que auxiliam na rápida contenção de ameaças;

11.1.7. Independente das soluções supracitadas, todas as soluções e/ou ferramentas utilizadas para prestação do serviço deverão obrigatoriamente seguir os requisitos, a



saber:

- 11.1.7.1. Deverão ser ofertadas exclusivamente soluções proprietárias, licenciadas e mantidas por fabricante ou fornecedor formalmente responsável por seu suporte, atualização e evolução tecnológica, não sendo admitidas soluções baseadas em software livre ou open source;
- 11.1.7.2. Os serviços deverão ser prestados por meio de soluções providas através da nuvem;
- 11.1.7.3. Devem englobar a alocação de todos os softwares necessários à consecução das atividades de segurança da informação e ao atendimento das especificações técnicas do objeto durante o prazo de vigência do contrato, incluindo garantia, manutenção, atualização dos produtos e monitoramento de segurança em regime de 24 (vinte quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano;
- 11.1.7.4. Os softwares devem ser ofertados em suas versões mais estáveis e atualizadas e devem estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço;
- 11.1.7.5. Admite-se o atendimento do conjunto de requisitos especificados mediante composição de soluções de fabricantes distintos, desde que o licitante comprove a interoperabilidade entre os componentes ofertados e assuma integralmente a responsabilidade pela operação do conjunto;
- 11.1.7.6. Todo o licenciamento do conjunto de soluções deverá ser por usuário, ou seja, não limitado por módulo/solução.

11.2. SOLUÇÃO DE PROTEÇÃO DE E-MAIL - SMG

- 11.2.1. A solução deverá ser fornecida em Cloud (Nuvem) com servidores dedicados e em
- 11.2.2. alta disponibilidade com operação contínua em regime 24x7.
- 11.2.3. A solução deverá possuir certificação SOC 2 Type II e comprovar adequação ao tratamento de dados pessoais em transferências internacionais, por meio de adesão ao EU-US Data Privacy Framework, de cláusulas contratuais padrão da União Europeia ou de certificação equivalente reconhecida internacionalmente, tais como ISO/IEC 27001, ISO/IEC 27701 ou CSA STAR, observada ainda a conformidade com a Lei nº 13.709/2018 (LGPD).
- 11.2.4. A solução deverá possuir avaliação CSA STAR Level 1 Self-Assessment.
- 11.2.5. Deverá ter disponibilidade de 99,9%;
- 11.2.6. Deverá ter efetividade em bloqueio de spam de ao menos 99%;
- 11.2.7. Deverá possuir suporte e monitoramento 24x7X365;
- 11.2.8. A solução deve ser capaz de integrar com as seguintes plataformas de correio eletrônico:
 - 11.2.8.1. Office 365 (incluindo Teams, OneDrive e SharePoint);
 - 11.2.8.2. Google G-Suite;
- 11.2.9. Deve possuir capacidade de configuração em cluster em alta disponibilidade.
- 11.2.10. A solução deve ser capaz de proteger ao menos, quinze domínios de correio



eletrônico na mesma console.

- 11.2.11. A solução deve possibilitar a configuração de filtragens de entrada e saída de e-mail.
- 11.2.12. A solução deve ser capaz de configurar políticas distintas de filtragem para entrada e saída de e-mails.
- 11.2.13. A solução deve suportar sincronização via protocolo NTP e NTP seguro (Network Time Protocol).
- 11.2.14. Deve possuir a capacidade de implementar comunicação segura via TLS (Transport Layer Security).
- 11.2.15. Deve possuir capacidade de configurar criptografia TLS por domínio e por política.
- 11.2.16. Deve seguir a RFC 821 para o recebimento e envio de mensagens.
- 11.2.17. Deve possuir console de gráfica (GUI) para administração centralizada com acesso via HTTPS.
- 11.2.18. Deverá conter mecanismos pre-delivery e pos-delivery. Por pre-delivery entende-se a capacidade de bloquear e-mails antes que eles sejam entregues à caixa postal do usuário. Por post-delivery a capacidade de atuar mesmo depois que o e-mail foi entregue à caixa postal.
- 11.2.18.1. A solução deve possuir mecanismo de quarentena com acesso direto dos usuários. Não será aceito soluções que ao invés da quarentena usam apenas as pastas de lixo/spam/junk ou de mensagens apagadas.
- 11.2.18.2. A solução deve possuir um sistema de reputação proprietário para a detecção de spam/phishing, não sendo aceitos sistemas opensource.
- 11.2.18.3. A solução deve bloquear mensagens que forem enviadas por IP com baixa reputação ou considerados spammers. A consulta da base de reputação de IP (Blacklist) deve ser proprietária do fabricante.
- 11.2.18.4. A solução deve categorizar e bloquear uma ameaça, no mínimo, nos seguintes grupos/níveis: Phishing, Adulto, Spam, Malware e Bulk (greymail).
- 11.2.18.5. Para cada um dos grupos/níveis (Phishing, Spam, Malware e Bulk (Greymail)) deve ser possível a customização individual no nível desejável da taxa de bloqueio.
- 11.2.18.6. Deve ser possível criar políticas por:
- a) Endereço IP
 - b) Classes de endereços Ips
 - c) Domínios
 - d) Usuário
 - e) Grupo de usuários
- 11.2.18.7. Deve possuir block list e safe list globais (definidas para toda a organização) e pessoais (definidas pelo usuário final).
- 11.2.18.8. A O fabricante da solução deverá participar do programa Microsoft Active Protections Program (MAPP);



11.2.18.9. A solução deve possibilitar a configuração de políticas de antispam novas conforme a necessidade.

11.2.18.10. Deve ser capaz de configurar políticas de e-mail analisando, no mínimo, trinta diferentes condições de critérios, podendo ser utilizado as expressões lógicas “E” ou “OU”, podendo ser combinadas com mais de um critério na mesma política.

11.2.18.11. Deve ser possível configurar critérios de filtragem de mensagens no mínimo, nos seguintes campos:

- 11.2.18.11.1. Tamanho Arquivo Anexo;
- 11.2.18.11.2. Quantidade de arquivo anexos;
- 11.2.18.11.3. Quantidade de arquivos contidos em um único arquivo comprimido;
- 11.2.18.11.4. Metadata do arquivo anexo;
- 11.2.18.11.5. Campo MFROM do remetente e destinatário;
- 11.2.18.11.6. Campo FROM do remetente e destinatário;
- 11.2.18.11.7. Extensão do arquivo anexo;
- 11.2.18.11.8. Nome Arquivo anexo;
- 11.2.18.11.9. Tamanho do arquivo comprimido;
- 11.2.18.11.10. Conteúdo HTML contida no corpo do e-mail;
- 11.2.18.11.11. Qualquer TAG HTML contida no corpo do e-mail;
- 11.2.18.11.12. Número de destinatários;
- 11.2.18.11.13. Linguagem utilizada no corpo do e-mail;
- 11.2.18.11.14. Código do país origem de envio do e-mail;
- 11.2.18.11.15. Tempo do registro do domínio utilizado nos campos FROM ou MFROM;
- 11.2.18.11.16. Detectar se e-mail é criptografada;
- 11.2.18.11.17. Campo HELO do enviado;
- 11.2.18.11.18. Quantidade de conexões SMTP de um único IP;

11.2.18.12. Para cada política de antispam criada, deve ser possível designar a opção de “quarentenar” mensagens em pastas de quarentena diferentes.

11.2.18.13. Deve possuir os seguintes métodos de entrega:

- 11.2.18.13.1. Continuar;
- 11.2.18.13.2. Bloquear, possibilitado a modificação do código e texto de retorno - mensagem ao enviado;
- 11.2.18.13.3. Descartar de forma silenciosa;
- 11.2.18.13.4. Entregar agora, realizando o by-pass nos filtros existentes;
- 11.2.18.13.5. Enviar uma cópia da mensagem a outro destinatário;
- 11.2.18.13.6. Encaminhar e-mail a outro destino como por exemplo, sandbox externa ou ambiente de arquivando;



- 11.2.18.14. Ao tomar uma ação referente a uma mensagem (bloquear, continuar, descartar etc.), deve ser possível editar:
- 11.2.18.14.1. Assunto da mensagem;
 - 11.2.18.14.2. Enviar a mensagem, porém removendo o arquivo anexo;
 - 11.2.18.14.3. Adicionar qualquer tag no header da mensagem;
- 11.2.18.15. Deve possuir tecnologia para prevenção de ataques do tipo “Bounce Messages”.
- 11.2.18.16. Deve possuir suporte a DMARC (Domain Message Authentication Reporting & Conformance) para e-mails entrante, garantindo a validação e integridade do e-mail recebido.
- 11.2.18.17. Possuir funcionalidade de controle de tráfego SMTP de saída garantindo que e-mails em grandes volumes enviadas por apenas um remetente sejam controladas e bloqueadas se necessário.
- 11.2.18.18. Deve possuir filtragem de Ataques de Diretório, ou seja, realizar a verificação de endereços de e-mail destino válidos e, caso seja inexistente, a solução deve bloquear o e-mail.
- 11.2.18.19. Deve possuir a possibilidade de criar regras baseada em dicionário de palavras ofensivas ou inapropriadas. Dicionário deve ser configurável para a língua Português Brasil.
- 11.2.18.20. Deve possuir tecnologia para detecção de ataques de spoofing de domínio.
- 11.2.18.21. Deve ser capaz de bloquear e-mails contendo arquivos anexos protegidos por senha ou cifrados.
- 11.2.18.22. Deve ter a capacidade de bloquear arquivos anexos por extensão, tipo real do arquivo (True Type File).
- 11.2.18.23. Deverá possibilitar inserir avisos (tags) nos e-mails a partir de critérios como:
- 11.2.18.23.1. Remetente externo;
 - 11.2.18.23.2. Remetente desconhecido;
 - 11.2.18.23.3. Domínio novo;
 - 11.2.18.23.4. Falha de DMARC;
 - 11.2.18.23.5. Mensagem suspeita/insegura;
 - 11.2.18.23.6. Remetente falsificado (impersonated);
- 11.2.18.24. As tags de mensagem suspeita/insegura deverão estar baseadas nas seguintes avaliações:
- 11.2.18.24.1. Remetente incomum;
 - 11.2.18.24.2. Reputação do website ou domínio;
 - 11.2.18.24.3. Reputação do provedor de SaaS;
 - 11.2.18.24.4. Conteúdo e temas de mensagem comumente usados para phishing;



- 11.2.18.25. Deve fornecer uma funcionalidade de “círculo de confiança” para usuários “VIP”, na qual e-mails de remetentes sem relacionamento anterior com o usuário VIP são identificados para revisão pelo usuário ou por terceiros.
- 11.2.18.26. Deve possibilitar que o tempo de retenção de logs para análise dos eventos ocorridos seja de no mínimo 30 dias.
- 11.2.18.27. Deve contar com proteção contra e-mails fraudulentos (BEC) baseado em machine learning e em LLM (Large Language Model).
- 11.2.18.28. A solução deve possuir proteção de antimalware com análise por sandbox sem limite de envio de arquivos.
- 11.2.18.29. Deve possuir proteção contra-ataques do tipo zero-hour, baseado em sandbox.
- 11.2.18.30. As atualizações do módulo devem ser constantes ao longo da vigência do contrato;
- 11.2.18.31. Deve proteger e-mails com arquivos protegidos.
- 11.2.18.32. Deve proteger o fluxo de mensagens inbound e outbound.
- 11.2.18.33. Deve ser possível criar diferentes políticas de proteção para diferentes rotas de e-mail como inbound e outbound.
- 11.2.18.34. Deve ser capaz de analisar documentos protegidos por senha através da informação contextual do corpo do e-mail e sandbox.
- 11.2.18.35. Detecção de logins suspeitos do Microsoft 365 e Google.
- 11.2.18.36. Detectar e bloquear URLs para roubo de credenciais enviadas via e-mail
- 11.2.18.37. Detectar aplicações de terceiros.
- 11.2.18.38. Deve possuir ao menos um mecanismo proprietário de inteligência artificial para análise das mensagens.
- 11.2.18.39. A solução deve prover o serviço de Sandbox, baseado em cloud, para garantir a análise e bloqueio de ameaças conhecidas e desconhecidas incluindo bloqueio de ameaças do tipo zero-hour, variantes de malwares, phishing de roubo de credenciais, documentos com códigos maliciosos ocultos.
- 11.2.18.40. Deve realizar a análise do artefato em modo inline/tempo real.
- 11.2.18.41. Deve realizar a análise comportamental e a análise estática.
- 11.2.18.42. A solução deve analisar e bloquear possíveis ameaças que utilizam URLs e arquivos;
- 11.2.18.43. O serviço de Sandbox deve ser proprietário e do mesmo fabricante da solução de antispam.
- 11.2.18.44. O serviço de Sandbox deve ser integrado com a console de administração de antispam.
- 11.2.18.45. Quando um arquivo for enviado para análise, o e-mail deve ser retido e não deve ser entregue ao usuário final até que o processo de análise e categorização seja concluído.



- 11.2.18.46. Deve suportar a reescrita das URLs, contida nos e-mails, para todas as mensagens ou para uma determinada categoria de classificação como Phishing, Spam, Adult ou Bulk.
- 11.2.18.47. Mensagens contento arquivos anexos já previamente categorizadas como maliciosas devem ser bloqueadas e movidas para pasta de quarentena.
- 11.2.18.48. Deve suportar a adição de domínios confiáveis para que não seja realizado a reescrita da URL.
- 11.2.18.49. Caso o arquivo e/ou a URL contida no e-mail for considerada maliciosa, eles devem ser bloqueados.
- 11.2.18.50. O sistema deve ser capaz de identificar quando um website legítimo acessível por link em uma mensagem legítima enviada de um remetente também legítimo estiver comprometido, e entregar a mensagem ao usuário final com a URL bloqueada.
- 11.2.18.51. Deve ser capaz de analisar códigos QR (QR Code) via Sandbox antes da mensagem ser entregue na caixa postal do usuário.
- 11.2.18.52. Deve ser capaz de analisar códigos QR (QR Code) via Sandbox nas mensagens apontadas pelos usuários como suspeitas.
- 11.2.18.53. Deve possuir dashboard com dados dos ataques recebidos e com as seguintes informações:
- 11.2.18.53.1. Visualização de todas as ameaças recebidas;
 - 11.2.18.53.2. Classificação da ameaça (URL, Arquivo Anexo ou ambos);
 - 11.2.18.53.3. Informação se é um ataque direcionado ou se é um ataque já previamente detectado;
 - 11.2.18.53.4. Visualização dos endereços de e-mail a qual o ataque foi direcionado;
 - 11.2.18.53.5. Lista dos assuntos utilizados nos ataques com a URL ou arquivo malicioso;
 - 11.2.18.53.6. Quantidade de URLs maliciosas recebidas vs quantidade bloqueadas vs quantidades de URLs que usuário clicou;
 - 11.2.18.53.7. Principais Malwares recebidos vs bloqueados utilizados em URLs maliciosas;
 - 11.2.18.53.8. Visão dos principais usuários internos mais atacados;
 - 11.2.18.53.9. Visão dos usuários que mais clicaram em URL maliciosa;
 - 11.2.18.53.10. Visão dos usuários que estão em risco;
 - 11.2.18.53.11. Visão dos usuários VIPs da organização;
 - 11.2.18.53.12. Visão dos ataques que mais chegaram aos usuários VIP (importantes);
- 11.2.18.54. A solução deve possibilitar a extração das informações da Sandbox via API no formato REST API (Representational State Transfer API) e com possibilidade de configuração para métodos GET.



- 11.2.18.55. A Sandbox deve possuir integração com o Office 365 e Google G-Suite com o objetivo de trazer visibilidade de contas possivelmente comprometidas e o volume de arquivos compartilhados na cloud.
- 11.2.18.56. Deve ser possível adicionar lista de usuários VIP para uma melhor mitigação de ataques direcionados para estes usuários.
- 11.2.18.57. A Sandbox deve realizar integrações com provedores de inteligência de mercado para obter uma colaboração de inteligência e consequentemente, uma melhor taxa de detecção e bloqueio.
- 11.2.18.58. Deve permitir integração no mínimo com EDR/XDR líderes de mercado.
- 11.2.18.59. Deve ser possível visualizar taxas de usuários mais atacados versus quais tipos de ameaças mais recebem.
- 11.2.18.60. Deve informar o usuário sobre campanhas de malware existentes, incluindo os possíveis objetivos da campanha (ex.: acesso remoto, instalar Ransomware, roubar credenciais)
- 11.2.18.61. Deve possuir a opção de ajuste manual do tempo limite de análise do e-mail pelo Sandbox, além de definir a ação que será realizada caso esse tempo seja atingido, como quarentenar, liberar, rejeitar e descartar.
- 11.2.18.62. O tempo de retenção das mensagens em quarentena devem ser configuráveis para, no mínimo 30 dias.
- 11.2.18.63. A solução deve prover acesso a quarentena através de um portal HTTP/S e comunicação via e-mail.
- 11.2.18.64. O portal de quarentena e a comunicação via e-mail devem suportar múltiplas línguas e deve ser provido, no mínimo em português (Brasil), espanhol e inglês (Estados Unidos).
- 11.2.18.65. A comunicação via e-mail e o portal de quarentena devem ser configuráveis com o logo da empresa.
- 11.2.18.66. A solução deve possibilitar que o usuário final tenha sua própria "safe list" de e-mails, independente da lista geral da corporação.
- 11.2.18.67. Deve ser possível configurar a frequência que será enviado a comunicação via e-mail de quarentena.
- 11.2.18.68. Deve permitir a busca de e-mails nas quarentenas individuais dos usuários pelo administrador
- 11.2.18.69. No módulo de quarentena, a solução deve permitir aos usuários diferentes comandos/ações baseados nos módulos de bloqueio dos e-mails (SPAM, SPF, DKIM, DMARC, Low Priority E-mail, Anexos Maliciosos etc.). Dentre os comandos/ações devem ter pelo menos:
- 11.2.18.69.1. Block Sender;
 - 11.2.18.69.2. Allow Sender;
 - 11.2.18.69.3. View Message;
 - 11.2.18.69.4. Release Message;
 - 11.2.18.69.5. Delete Message;



- 11.2.18.69.6. Report Phishing;
- 11.2.18.69.7. Release and Allow Sender;
- 11.2.18.70. No portal de quarentena dos usuários, a solução deve possuir uma opção de localizar/buscar os e-mails, para que os próprios usuários possam realizar esta busca.
- 11.2.18.71. Deve suportar a integração com Active Directory ou com provedor de identidade em nuvem, por LDAP, LDAPS, SCIM ou API, admitindo-se o uso de conector de sincronização fornecido pelo fabricante quando este for o mecanismo padrão de integração da solução em nuvem, sem custo adicional e sem função de inspeção de tráfego;
- 11.2.18.72. Deve ser possível disponibilizar os seguintes "comandos" para a quarentena do usuário final, podendo removê-los ou adicioná-los:
 - 11.2.18.72.1. Liberar Mensagem;
 - 11.2.18.72.2. Liberar Mensagem e adicionar Sender na Whitelist;
 - 11.2.18.72.3. Ver Mensagem;
 - 11.2.18.72.4. Reportar um falso positivo;
 - 11.2.18.72.5. Reportar um falso negativo;
 - 11.2.18.72.6. Reportar um Phishing;
 - 11.2.18.72.7. Bloquear Sender;
 - 11.2.18.72.8. Deve ser possível obter a visualização, em tempo real, do processamento das filas de e-mail via GUI;
- 11.2.18.73. Deve possuir recurso para rastreamento de mensagens (Message Tracking) na própria console de gerenciamento com capacidade de pesquisa por subject, sender e recipient, verificando-se a ação tomada para específica mensagem, sem necessidade de integração com produtos de terceiros, "open source" ou serviço/servidor adicional.
- 11.2.18.74. Através do Message Tracking, a solução deve possibilitar a pesquisa com, no mínimo, os seguintes parâmetros:
 - 11.2.18.74.1. E-mail de envio;
 - 11.2.18.74.2. E-mail de destino;
 - 11.2.18.74.3. Assunto;
 - 11.2.18.74.4. Tempo (hora e data);
 - 11.2.18.74.5. Hostname;
 - 11.2.18.74.6. IP;
 - 11.2.18.74.7. Lista dos Arquivos Anexos;
 - 11.2.18.74.8. Tamanho da mensagem;
 - 11.2.18.74.9. Tempo de processamento da mensagem na solução;
 - 11.2.18.74.10. Score de Spam atribuído depois das filtragens;



- 11.2.18.75. Deve ser possível realizar notificação ao administrador por e-mail caso os filtros de AntiSpam ou antivírus não recebam atualizações por um determinado período.
- 11.2.18.76. Os relatórios devem ser acessíveis na própria console de gerenciamento sem necessidade de integração com produtos de terceiros, "open source" ou serviço/servidor adicional.
- 11.2.18.77. A solução deve suportar a integração com sistemas externos de syslogs, tanto para versão onpremises ou em cloud.
- 11.2.18.78. A solução deve mapear, gerar o incidente e responder de forma automatizada a incidentes relacionados a eventuais fraudes realizadas via e-mail que não tenham sido bloqueadas pela solução de antispam.
- 11.2.18.79. A solução deve ser capaz de remover qualquer e-mail da caixa postal do usuário independente da classificação como spam, e-mail marketing ou outros.
- 11.2.18.80. A interface de administração deve ser em HTTPS.
- 11.2.18.81. O incidente gerado deve fornecer, no mínimo, as seguintes informações:
- 11.2.18.81.1. Escore da ameaça;
 - 11.2.18.81.2. Lista de destinatários que receberam a fraude;
 - 11.2.18.81.3. IP e Hostname do enviado;
 - 11.2.18.81.4. URLs utilizada na fraude;
 - 11.2.18.81.5. Hash MD5 dos arquivos malwares utilizados na campanha;
- 11.2.18.82. Deve, uma vez identificado a ameaça, de forma automatizada remover a mensagem phishing da caixa de correio do usuário final e movê-la para uma pasta de quarentena. Este processo deve acontecer para todos os usuários afetados, previamente relacionados no incidente gerado.
- 11.2.18.83. Após realizar a resposta ao incidente, a solução deve ser capaz de alertar o time de monitoramento e o usuário final, caso este seja configurado.
- 11.2.18.84. Deve ser possível monitorar um mailbox abuse - caixa de correio configurada para o público externo e interno com o objetivo de receber notificações de fraudes ou qualquer abuso.
- 11.2.18.85. A solução deve analisar as mensagens contida no mailbox abuse e, se detectada uma fraude real, deve-se criar um incidente na plataforma e deve ser executado respostas de mover para a quarentena quaisquer mensagens que tenham passado internamente e/ou que estejam ativas nos mailboxes dos usuários corporativos.
- 11.2.18.86. Deve ser possível configurar plug-in para o cliente de e-mail possibilitando que o usuário corporativo possa reportar possíveis mensagens suspeitas.
- 11.2.18.87. O plug-in deve suportar:
- 11.2.18.87.1. Microsoft Outlook;
 - 11.2.18.87.2. Microsoft OWA - Outlook Web Access;



- 11.2.18.88. O plug-in deve possuir diferentes idiomas, com no mínimo: português (Brasil), inglês (Estados Unidos) e espanhol.
- 11.2.18.89. Deve ser possível a configuração de diferentes ícones para o plug-in.
- 11.2.18.90. Uma vez que o usuário reporte uma mensagem suspeita, a solução deve realizar a análise para identificar se é uma ameaça real e se for, a plataforma deve identificar e remover o e-mail de todos os mailboxes.
- 11.2.18.91. A plataforma deve prover um dashboard com estatísticas dos incidentes, criticidades etc. gerados em uma janela de tempo configurada.
- 11.2.18.92. A solução deve trazer uma visão centralizada da análise de riscos do ambiente, correlacionando eventos de incidentes coletados das soluções de segurança de e-mail, sandbox, plataforma de conscientização de segurança da informação, Microsoft Active Directory e outros.
- 11.2.18.93. A solução deve trazer os riscos associados aos usuários corporativos, com detalhamentos técnicos dos incidentes e seus motivos
- 11.2.18.94. Os riscos devem estar em uma escala de 0 a 10, possibilitando que seja analisado os motivos do risco, a origem, privilégios, e outros fatores que influenciaram para uma escala baixa ou alta.
- 11.2.18.95. Deve ser possível customizar o threshold da análise de riscos.
- 11.2.18.96. Deve trazer estatísticas de riscos por pessoas e por departamentos da organização.
- 11.2.18.97. Como resultado da análise de risco, deve ser possível:
- 11.2.18.97.1. Possuir uma visão dos usuários mais atacados;
 - 11.2.18.97.2. Possuir uma visão dos usuários mais atacados que são VIP;
 - 11.2.18.97.3. Possuir uma visão dos usuários mais atacados e que trazem maior risco;
 - 11.2.18.97.4. Possuir uma visão das principais vulnerabilidades da organização;
 - 11.2.18.97.5. Possuir uma visão dos departamentos mais atacados;
 - 11.2.18.97.6. Possuir uma visão dos departamentos mais atacados e que trazem maior risco;
 - 11.2.18.97.7. Possuir uma visão dos países mais atacados;
 - 11.2.18.97.8. Possuir uma visão dos países mais atacados e que trazem maior risco;
 - 11.2.18.97.9. Para cada risco, possuir controles de remediação, atividades e recomendações;
- 11.2.18.98. Para cada usuário, deve ser possível ter visibilidade do histórico de incidentes, relacionado com as técnicas da fraude - phishing, comprometimento de conta, backdoor, ransomware, outras;
- 11.2.18.99. O serviço de ativação e sustentação da solução integrada de Segurança de E-mail e Conscientização de Usuários deverá contemplar, no mínimo, as seguintes atividades:



- 11.2.18.99.1. Provisãoamento da Solução, com a Ativação da plataforma na nuvem do fabricante;
- 11.2.18.99.2. Configuração de integração com Active Directory ou LDAP;
- 11.2.18.99.3. Criação e habilitação de contas de usuários administradores;
- 11.2.18.99.4. Configurações Iniciais de Segurança de E-mail como as recomendações e ajustes de registros SPF, DKIM e DMARC;
- 11.2.18.99.5. Definição de políticas de bloqueio, filtragem e quarentena e conceber a parametrização de regras de notificação para administradores;
- 11.2.18.99.6. Adequação dos parâmetros de fluxo e roteamento de mensagens para pleno funcionamento, que deverá ser realizado com a orientação para a mudança do fluxo de e-mail, ou via API (por exemplo, Office 365) para a solução de segurança ofertada, tal como validação de envio e recebimento de e-mails após ajustes;
- 11.2.18.99.7. Realização de testes de conectividade e fine tuning das regras de proteção;

11.3. SOLUÇÃO DE CONSCIENTIZAÇÃO DE USUÁRIOS – SEC AWARENESS

11.3.1. A implementação da solução de conscientização de usuários, deverá obedecer, no mínimo, aos seguintes itens:

- 11.3.1.1. Identificação das pessoas-chave (TI, conformidade e áreas de negócio) e definição de objetivos.
- 11.3.1.2. Elaboração de cronograma para campanhas de phishing educativo, treinamentos e quizzes.
- 11.3.1.3. Realização de reuniões mensais de alinhamento, apresentação do plano de trabalho.
- 11.3.1.4. Configuração das campanhas iniciais e análise dos resultados preliminares;
- 11.3.1.5. Realização de cerca de doze campanhas por ano, para até 9.500 contas por campanha.

11.3.2. Ferramenta de Phishing Simulations, Treinamento e Conscientização:

- 11.3.2.1. A solução deverá ser fornecida nuvem, para prover simulações de phishing e treinamentos contínuos para funcionários da empresa.
- 11.3.2.2. A solução deve ser provida 100% em nuvem e não deve ser exigir nenhum servidor adicional, IP dedicado para disparos de e-mail, tão pouco registro de domínios para a sua plena execução.
- 11.3.2.3. Não serão aceitos qualquer software livre, OpenSource ou outros que não sejam do fabricante.
- 11.3.2.4. A plataforma deve suportar no mínimo, os idiomas: inglês (Estados Unidos), português (Brasil) e espanhol sendo que o conteúdo dos treinamentos deve ser provido também, nas mesmas línguas já citadas.
- 11.3.2.5. Deve suportar integração com Azure Active Directory, LDAP Active Directory e OKTA.



- 11.3.2.6. Deve suportar integração com SAML.
- 11.3.3. Deve prover os seguintes módulos/funcionalidades através da mesma console:
 - 11.3.3.1. Customização e Simulação de Phishing via e-mail;
 - 11.3.3.2. Customização e Simulação de Phishing via USB;
 - 11.3.3.3. Treinamentos;
 - 11.3.3.4. Exames e Testes;
 - 11.3.3.5. Relatórios e Indicadores;
 - 11.3.3.6. Materiais Adicionais como cartilhas, papel de paredes, videos etc;
- 11.3.4. Os Treinamentos deverão ter as seguintes características:
 - 11.3.4.1. Deverão ser disponibilizados através de vídeos e módulos Interativos;
 - 11.3.4.2. Deverão estar disponíveis ao menos nos idiomas inglês (Estados Unidos), português (Brasil) e espanhol;
- 11.3.5. Caso não haja integração SAML, deve ser possível implementar políticas de senhas complexas.
- 11.3.6. A plataforma deve possuir imagens customizadas para serem utilizadas em simulações de phishing e treinamentos customizados.
- 11.3.7. Deve ser possível customizar alertas de interação com o usuário final em caso de:
 - 11.3.7.1. Novo treinamento atribuído a um usuário;
 - 11.3.7.2. Novo exame atribuído a um usuário;
 - 11.3.7.3. Treinamento concluído com sucesso;
 - 11.3.7.4. Treinamento ainda pendente para ser realizado;
 - 11.3.7.5. Relatório de acompanhamento de colaboradores ainda pendentes para conclusão de treinamento;
- 11.3.8. Deve ser possível a customização de grupos de usuários, independente da estrutura de grupos do Active Directory.
- 11.3.9. Não deve haver restrição de volume de e-mail phishing enviados durante o contrato vigente
- 11.3.10. Deve ser possível criar campanhas de Phishing com as mínimas características:
- 11.3.11. Campanhas no formato texto e HTML
- 11.3.12. Campanhas com arquivos anexos (PDF, WORD, EXCEL, HTML no mínimo)
- 11.3.13. Campanhas com arquivos anexos comprimidos (formato ZIP) e com senha
- 11.3.14. A plataforma deve prover, no mínimo, 40 templates de e-mail phishing prontos para serem utilizados em Portugues-BR
- 11.3.15. A plataforma deve possibilitar a criação de novos templates e-mail phishing conforme a necessidade
- 11.3.16. Não deve haver restrição de quantidade de templates de e-mail phishing que podem ser criados ou utilizados na plataforma.



11.3.17. A customização de novos templates de e-mail phishing deve possuir as seguintes características:

11.3.17.1. Lista de domínios próprios providos pelo fabricante da solução que podem ser utilizados nas simulações, sem qualquer ônus adicional para a sua utilização;

11.3.17.2. Devem possuir domínios para serem utilizados no conceito de "impersonation";

11.3.18. Deve possuir domínios parecidos com grandes marcas no mínimo, nos seguintes segmentos de negócios:

11.3.18.1. Financeiro, no mínimo domínios parecidos com a Paypal;

11.3.18.2. Corporativo, no mínimo domínios parecidos com Onedrive, Sharepoint, Outlook e HP;

11.3.18.3. Tecnologia, no mínimo domínios parecidos com Microsoft;

11.3.18.4. Redes Sociais, no mínimo domínios parecidos com LinkedIn;

11.3.18.5. Comercial, no mínimo domínios parecidos com Adobe;

11.3.18.6. Serviços de Cloud, no mínimo domínios parecidos com Dropbox;

11.3.18.7. Consumo final, no mínimo domínios parecidos com Gmail;

11.3.18.8. Deve ser possível criar subdomínio no link da simulação de Phishing, como por exemplo, <https://subdominio.teste.com.br>;

11.3.18.9. Deve ser possível ajustar o endereço URL utilizado no e-mail Phishing, como por exemplo, www.urlphishing.com.br/login.php;

11.3.18.10. Deve ser possível ajustar os principais campos no e-mail como:

- a) Assunto;
- b) E-mail Origem (campo FROM);
- c) E-mail Retorno (campo Reply-To);
- d) URL Path;

11.3.18.11. Deve ser possível criar um e-mail através de texto ou HTML.

11.3.18.12. Deve ser possível trabalhar com, no mínimo, as seguintes variáveis de sistema para uma melhor automação:

- a) Nome;
- b) Sobrenome;
- c) Endereço de E-mail;

11.3.18.13. Deve ser possível trocar o protocolo utilizando no link da simulação do phishing para HTTPS://, HTTP://

11.3.18.14. Deve ser possível trocar o link da URL da simulação de phishing.

11.3.18.15. Deve ser possível testar o e-mail phishing antes de utilizar em produção.

11.3.18.16. A plataforma deve prover base de imagens para serem utilizados nas campanhas de phishing.



- 11.3.18.17. Deve suportar o envio randômico de uma ou mais campanhas de phishing levando em consideração a quantidade de usuários a ser enviado, dias e horas de disparos de e-mail.
- 11.3.18.18. Deve ser possível agendar o envio das campanhas de phishing conforme uma data pré-definida.
- 11.3.18.19. Deve ser possível definir o tempo que a URL utilizada na campanha de Phishing fique disponível e acessível.
- 11.3.18.20. Deve possibilitar a coleta do comportamento dos usuários internos de forma anônima para atender a quesitos legais como a Lei Geral de Proteção de Dados ou outra.
- 11.3.18.21. Deve ser possível coletar informações de geolocalização.
- 11.3.18.22. Deve ser possível coletar informações se usuário abriu e-mail de phishing.
- 11.3.18.23. Deve ser possível coletar informações se usuário clicar mais de uma vez no link utilizado na simulação de phishing.
- 11.3.18.24. As simulações de phishing devem ser compatíveis com os principais sistemas operacionais de mercado como Windows, Mac, Linux e dispositivos, como Android, IOS smartphone, tablet e outro.
- 11.3.18.25. Deve registrar o endereço IP de onde o usuário final abriu o phishing.
- 11.3.18.26. Deve registrar de qual dispositivo ou computador ou sistema operacional que o usuário final abriu o phishing.
- 11.3.18.27. Deve ser possível exportar os resultados via CSV, PNG, PDF e SVG.
- 11.3.18.28. Deve ser possível acompanhar o andamento da campanha via portal.
- 11.3.18.29. Deve ser possível a criação de arquivos para a simulação de phishing por USB, onde será possível analisar comportamento de usuários internos obtendo acesso a pen-drives desconhecidos.
- 11.3.18.30. Deve ser possível clonar uma campanha de phishing já existente.
- 11.3.18.31. Deve contemplar, no mínimo, os seguintes conteúdos de treinamento:
- a) Identificação de links fraudulentos;
 - b) Identificação de e-mail phishing;
 - c) Senha Seguras e Política de senhas;
 - d) GDPR e LGPD;
 - e) Segurança Física;
 - f) Protegendo dados Confidenciais;
 - g) Segurança em Redes Sociais;
 - h) Segurança física;
 - i) Ataques Business E-mail Compromise;
 - j) Proteção de dados;
 - k) Proteção em nuvem;



- l) PCI DSS;
- m) Engenharia Social
- n) Ataques de Ransomware;

11.3.18.32. Deve possibilitar a customização do conteúdo dos treinamentos conforme a necessidade.

11.3.18.33. Deve ser possível configurar data início e fim para a realização dos treinamentos.

11.3.18.34. Deve ser possível aplicar mais de um módulo de treinamento por grupo de usuários, sem haver restrições de quantidade de módulos de treinamentos vinculados.

11.3.18.35. Deve ser possível enviar notificações por e-mail, pré-agendadas, de alerta ao usuário de que existem treinamentos pendentes e/ou novos para serem realizados.

11.3.18.36. Deve ser possível a administração de execução dos módulos de treinamento, por ordem de execução.

11.3.18.37. Deve ser possível vincular os módulos de treinamentos para um usuário ou um grupo de usuários pre-configurado no Active Directory.

11.3.18.38. Deve ser possível disponibilizar para o administrador da plataforma e para o usuário final visualizar o tempo de cada módulo atribuído e o tempo total dos treinamentos vinculados.

11.3.18.39. Deve ser possível configurar um certificado virtual quando usuário final obtiver sucesso no término de um curso.

11.3.18.40. Deve suportar a exportação dos módulos de treinamento via SCORM, no mínimo, na versão 1.2.

11.3.18.41. A solução não deve ter restrições de quantidade de customizações devam ser realizadas.

11.3.18.42. Deve ser possível vincular o certificado de conclusão do curso após o término do treinamento.

11.3.19. Módulo de Testes / Exames

11.3.19.1. A solução deverá disponibilizar acervo próprio de questões de avaliação em quantidade e variedade suficientes para cobrir todos os temas da biblioteca de treinamentos contratada e para permitir avaliações sem repetição de questões para o mesmo usuário dentro de um mesmo ciclo anual, admitido que as questões estejam embarcadas nos próprios módulos de treinamento ou em conteúdo importado em padrão aberto.

11.3.19.2. A plataforma deve disponibilizar perguntas e respostas em inglês, português e espanhol.

11.3.19.3. Deve possibilitar criar questões novas, conforme a demanda sem custos adicionais.

11.3.19.4. Com relação às perguntas novas:

11.3.19.5. Deve ser configurável em verdadeiro/falso ou múltiplas escolhas;

11.3.19.6. Deve possibilitar importar imagens para uma melhor ilustração;



- 11.3.19.7. Deve ser possível criar categorias de perguntas e respostas;
- 11.3.19.8. Para cada categoria, deve possuir a opção de alternar as perguntas para nunca seguir uma sequência repetitiva de mesma questão;
- 11.3.19.9. Deve ser possível aplicar diferentes categorias de perguntas para diferentes grupos de usuários;
- 11.3.19.10. Deve ser possível a total customização das perguntas e respostas, com logo e conteúdo apropriados;
- 11.3.20. Relatórios e Indicadores
 - 11.3.20.1. Deve suportar exportar relatórios nos formatos CSV ou PDF;
 - 11.3.20.2. Deve prover Dashboard centralizado;
 - 11.3.20.3. Deve possuir filtros para uma dinâmica visualização;
 - 11.3.20.4. Deve possuir, no mínimo, os seguintes relatórios:
 - a) Detalhes das campanhas de phishing;
 - b) Taxa de falhas por campanha de Phishing e por usuário;
 - c) Comparação de efetividade entre campanhas de phishing;
 - d) Detalhes individuais de cada campanha como:
 - e) Nome do usuário;
 - f) Tipo de endpoint;
 - g) Localização Geográfica;
 - h) Comportamento individual;
 - i) Taxa de sucesso e falhas nos testes;
 - j) Tempo de execução do treinamento;
 - a) Usuários que não realização os treinamentos;
 - 11.3.20.5. Os relatórios devem ser acessados através da mesma console de administração da plataforma e não serão aceitos qualquer modulo ou serviço adicional que dependa de qualquer recurso adicional.
- 11.3.21. Funcionalidades Adicionais:
 - 11.3.21.1. Deve ser possível disponibilizar um plug-in para que o usuário final possa reportar mensagens que ele considere suspeitas para obter um melhor engajamento do conceito de educação.
 - 11.3.21.2. O plug-in deve suportar Microsoft Outlook, Microsoft Outlook Web Access.
 - 11.3.21.3. O plug-in deve ser provido em inglês, português e em espanhol
 - 11.3.21.4. Deve ser possível a customização do ícone utilizado no plug-in para outro de livre escolha.
 - 11.3.21.5. Deve ser possível trocar qualquer tradução no plug-in para outra de melhor escolha, sem nenhuma restrição. Por exemplo, "relatar phishing" para "Reportar Phishing".



11.3.21.6. Deve ser possível criar notificações customizadas para o usuário final como:

- a) Agradecimento ao usuário reportar um e-mail suspeito;
- b) Agradecimento ao usuário final fortalecendo a importância do conteúdo de conscientização;
- c) Enviar validação ao usuário final se e-mail é ou não uma ameaça real a corporação;

11.3.21.7. Mensagens reportadas pelo usuário final devem ser analisadas automaticamente por um centro de vacinas de ameaças globais, sendo parte da solução nativa do fabricante;

11.3.21.8. Se a mensagem analisada for categorizada como uma ameaça real, deve ser possível enviar alerta para uma lista de distribuição para rápida mitigação de novos casos;

11.3.21.9. Se a mensagem analisada for categorizada como uma ameaça real, deve ser possível realizar a integração com sistema de SOAR - Security Orchestration, Automation and Response;

12. FERRAMENTA DE PREVENÇÃO CONTRA PERDA DE DADOS – EMAIL - DLP

12.1. Requisitos Gerais

12.1.1. Deve ser 100% SaaS. Não será aceito soluções que necessitem hardware adicional on-premise

12.1.2. Deve suportar qualquer serviço de correio eletrônico, instalado em nuvem ou on-premises;

12.1.3. Deve suportar arquiteturas híbridas de e-mail, na qual coexistem e-mail on-premises e em nuvem;

12.1.4. Deve funcionar sem a necessidade de agentes instalados nos dispositivos;

12.1.5. O serviço SaaS deve:

12.1.5.1. O ambiente deve ser provido em modo dedicado, ou seja, IPs e servidores dedicados

12.1.5.2. Certificado SOC 2 Type II

12.1.5.3. Comprovação de mecanismo válido de transferência internacional de dados pessoais, mediante certificação no EU-U.S. Data Privacy Framework (incluindo as extensões Suíça e Reino Unido), ou adoção de Cláusulas Contratuais Padrão da União Europeia, ou outro mecanismo equivalente reconhecido, observado o disposto nos artigos 33 a 36 da Lei 13.709/2018 (LGPD);

12.1.5.4. Avaliação CSA STAR Level 1 Self-Assessment

12.1.5.5. SLA de disponibilidade de 99.999%

12.1.5.6. Suporte e monitoramento 24x7

12.1.6. A solução deve ser capaz de analisar e-mails de mais de um domínio de correio eletrônico na mesma console



- 12.1.7. Deve suportar nativamente e-mails no idioma Português
- 12.1.8. Deve permitir a integração com outras soluções para remediação ou resposta
- 12.1.9. Deve permitir a criação de diferentes políticas por grupos de usuários ou usuários individuais, e da mesma forma aplicar exceções para grupos ou usuários individuais
- 12.1.10. Deve ser capaz de redirecionar tráfego a outro sistema baseado no cabeçalho, assunto, conteúdo da mensagem e regras de compliance
- 12.1.11. Deve ser capaz de alterar a mensagem para os destinatários.
- 12.1.12. Deve permitir que modelos sejam criados por departamentos, atendendo a necessidades específicas
- 12.1.13. Deve ser capaz de armazenar os e-mails que violem as políticas em servidor próprio
- 12.1.14. Deve armazenar os seguintes meta dados de arquivos envolvidos em violações de política
 - 12.1.14.1. Tipo de arquivo
 - 12.1.14.2. Tamanho do arquivo
 - 12.1.14.3. Data de criação
 - 12.1.14.4. Data de alteração
 - 12.1.14.5. Código de classificação
 - 12.1.14.6. Regra violada
 - 12.1.14.7. ID (hash do conteúdo ou file fingerprint)
- 12.1.15. Deve possuir os seguintes mecanismos de detecção
- 12.1.16. Dicionários pré-configurados, permitindo a importação de novos dicionários
- 12.1.17. Dicionários personalizados
- 12.1.18. Proximidade
- 12.1.19. Exact Data Match (EDM) Single Column e Multiple-Column
- 12.1.20. Indexed Document Matching (IDM)
- 12.1.21. Dicionários negativos para redução de falso-positivos
- 12.1.22. Expressões regulares
- 12.1.23. Correlação
- 12.1.24. Deve permitir a criação de regras usando operadores "AND" e "OR"
- 12.1.25. Deve permitir as seguintes respostas para e-mails detectados
 - 12.1.25.1. Abrir incidente
 - 12.1.25.2. Copiar a mensagem para folder
 - 12.1.25.3. Descartar o e-mail
 - 12.1.25.4. Resposta personalizada ao remetente
 - 12.1.25.5. Enviar e-mail ao destinatário



- 12.1.25.6. Alterar o assunto ou conteúdo e enviar ao destinatário
- 12.1.25.7. Alterar o cabeçalho do e-mail
- 12.1.26. Deve permitir a criação de folders de armazenamento de mensagens pelo administrador
- 12.1.27. Deve possuir mecanismo de OCR (Optical character recognition) para leitura de documentos escaneados, imagens ou legendas/subtítulos em uma imagem
 - 12.1.27.1. Não deve haver limite de uso para a funcionalidade
 - 12.1.27.2. O reconhecimento óptico de caracteres deve suportar, no mínimo, os seguintes formatos: imagens JPEG, PNG, TIFF, BMP, GIF e JPEG 2000, e documentos PDF, DOC/DOCX, XLS/XLSX e PPT/PPTX, admitindo-se formatos adicionais como diferencial, conforme documentação oficial do fabricante;
 - 12.1.27.3. Deve suportar imagens rotacionadas a 90, 180 e 270 graus
 - 12.1.27.4. Deve ser capaz de processar imagens com resolução menor que 300 dpi
 - 12.1.27.5. Deve ser capaz de processar imagens incluídas em arquivos

12.2. Gestão de incidentes

- 12.2.1. Para cada evento de DLP gerado deve ser possível o envio das informações para qualquer sistema externo desde que ele seja compatível com reports Webhook JSON
- 12.2.2. Para cada evento de DLP gerado deve ser possível o envio das informações para qualquer e-mail de sistema
- 12.2.3. Toda a console de gestão de incidentes, relatórios e regras de DLP deve ser gerenciada através da mesma interface. Não serão aceitos hardware adicionais ou sistemas de terceiros para realizar a gestão dos relatórios ou gestão dos incidentes
- 12.2.4. Retenção dos eventos gerados deve ser de responsabilidade do fabricante e não deve depender de solução terceira ou de outro fabricante
- 12.2.5. Retenção dos eventos deve ser durante todo o contrato vigente
- 12.2.6. Deve possuir um dashboard central com uma visão sumarizada de todos os incidentes gerados e níveis de riscos
- 12.2.7. Deve ser possível atribuir diferentes filtros para uma melhor mitigação de um incidente contemplando no mínimo os seguintes critérios:
 - 12.2.7.1. Dias, horas, Semanas, Anos, janela de tempo predefinido
 - 12.2.7.2. TAG
 - 12.2.7.3. Origem do evento (incidente gerado,
 - 12.2.7.4. User, email, grupo do Active Directory
 - 12.2.7.5. Host Name
 - 12.2.7.6. IP Address
 - 12.2.7.7. Sistema Operacional
 - 12.2.7.8. País origem de conexão
 - 12.2.7.9. Domínio que a estação de trabalho pertence



12.2.7.10. Nome da Aplicação

12.2.7.11. Nome do executável

12.2.7.12. Hash do arquivo

12.2.8. Deve ser capaz configurar tabela dinâmicas na interface para uma melhor gestão e visualização dos incidentes

12.2.9. Deve possuir no mínimo os seguintes reports pré-configurados:

12.2.9.1. Top usuários com maior incidente

12.2.9.2. Quantidade de alertas por dia

12.2.9.3. Maior quantidade de incidentes por tipo de arquivos

12.2.9.4. Incidentes de DLP por localização geográfica

12.2.10. A console de administração deve prover um sistema de workflow onde deva possibilitar atribuir, no mínimo, os seguintes status:

12.2.10.1. Assignar um incidente a um recurso

12.2.10.2. Escalar incidente a outro time

12.2.10.3. Fechar incidente

12.2.10.4. Adicionar incidente sendo investigado

12.2.10.5. Falso Positivo

12.2.11. Deve ser possível atribuir comentários de investigação para cada incidente

12.2.12. Deve ser possível observar os dados detectados no arquivo combinando com a regra de DLP para entender melhor quais dados estão sendo detectados

12.2.13. Deve ser possível exportar uma nova mitigação ou relatório via CSV, PDF ou JSON

12.2.14. Deve possuir APIs disponíveis para integração com qualquer SIEM que suporte JSON

12.3. Gerência

12.3.1. Deve suportar autenticação por SAML2

12.3.2. Deve possuir trilha de auditoria da console de administração

12.3.3. Deve fornecer relatório dos violadores (usuários que enviaram os e-mails detectados)

12.4. Ferramenta de endpoint e prevenção contra perda de dados

12.4.1. Deve ser 100% SaaS. Não será aceito soluções que necessitem hardware adicional onpremise.

12.4.2. Deve suportar agentes para Microsoft Windows e MacOS no mínimo nas seguintes versões:

12.4.2.1. Windows 11 - 64-bit

12.4.2.2. Microsoft supported versions of Windows 10

12.4.2.3. Windows Server 2016 - 64-bit



- 12.4.2.4. Windows Server 2019 -64-bit
- 12.4.2.5. Windows 8.1 - 64-bit
- 12.4.2.6. macOS Monterey R12
- 12.4.2.7. macOS Big Sur R11
- 12.4.2.8. macOS Catalina 10.15
- 12.4.3. Deve suportar os seguintes browser:
 - 12.4.3.1. Google Chrome
 - 12.4.3.2. Microsoft Internet Explorer
 - 12.4.3.3. Microsoft Edge for Windows
 - 12.4.3.4. Mozilla Firefox
 - 12.4.3.5. Apple Safari
 - 12.4.3.6. Opera
- 12.4.4. Deve suportar os seguintes requisitos mínimos de hardware
 - 12.4.4.1. 1.5 GHz Intel Core processor or Apple M1 Chip CPU
 - 12.4.4.2. 8 GB RAM ou mais
- 12.4.5. Plataforma SaaS deve possuir a certificação SOC2 type II
- 12.4.6. Comunicação do agente com a plataforma SaaS deve ocorrer através da porta HTTPS 443
- 12.4.7. Deve ser possível configurar senha para remoção do agente
- 12.4.8. O agente deve possuir funcionalidade de automático restart caso o agente seja parado
- 12.4.9. O pacote de instalação do agente deve ser provido em formato EXE e MSI
- 12.4.10. A instalação dos agentes deve ocorrer via script, via GPO ou prover suporte a utilização de qualquer software de terceiro para realizar a instalação de forma não assistida
- 12.4.11. Deve ser provido os scripts de instalação e remoção dos agentes
- 12.4.12. Deve ser possível configurar o tempo de retenção dos logs de eventos no computador do usuário em caso de falha de comunicação com a plataforma de gerenciamento
- 12.4.13. Os eventos armazenados localmente devem ser mantidos criptografados
- 12.4.14. Deve ser possível configurar políticas de update de versão dos agentes
- 12.4.15. Deve suportar RBAC para granularidade de permissionamento na console
- 12.4.16. Deve monitorar e aplicar política de controle de dados no endpoint (USB, impressora, compartilhamento de rede, Bluetooth, área de transferência, navegador), independentemente de o acesso à estação de trabalho ocorrer localmente ou por sessão remota, conforme suportado pela solução;
- 12.4.17. Deve possuir bloqueios nos seguintes protocolos ou canais



- 12.4.17.1. USB
- 12.4.17.2. Impressão
- 12.4.17.3. Aplicações de sincronismo com plataforma cloud
- 12.4.17.4. HTTP e HTTPS
- 12.4.17.5. Compartilhamento de Rede
- 12.4.17.6. Copia e Cola
- 12.4.17.7. Airdrop para dispositivos MAC
- 12.4.17.8. Prompt de IA
- 12.4.17.9. Upload
- 12.4.18. Para a análise de dados de DLP, deve ser possível configurar:
 - 12.4.18.1. Limite do tamanho do arquivo
 - 12.4.18.2. Limite do tempo de análise de um arquivo
- 12.4.19. Em caso de bloqueio, deve ser possível configurar as notificações de bloqueio para no mínimo em Português, Espanhol e Inglês.
- 12.4.20. Deve ser possível customizar justificações para serem apresentada ao usuário final, no caso de um possível vazamento de dados
- 12.4.21. Deve ser possível adicionar o logo da empresa nas notificações de bloqueio nas notificações de prompts, bloqueio e avisos.
- 12.4.22. Para todo o bloqueio de DLP, deve ser possível reter os arquivos em plataforma externa, provida pelo cliente, sendo elas no mínimo:
 - 12.4.22.1. AWS
 - 12.4.22.2. Azure
- 12.4.23. Deve ser possível adicionar o logo da empresa nas notificações de bloqueio
- 12.4.24. Deve ser possível adicionar diferentes TAGs para cada incidente
- 12.4.25. Deve ser possível criar novas TAG conforme a necessidade
- 12.4.26. Deve ser capaz de bloquear um possível vazamento de dados levando em consideração os seguintes critérios:
 - 12.4.26.1. Extensão de arquivos
 - 12.4.26.2. Mimetype
 - 12.4.26.3. Microsoft Information Protection (MIP) Label
 - 12.4.26.4. Identificação de onde o arquivo foi download para bloquear qualquer arquivo baixado de um sistema crítico
 - 12.4.26.5. Tipos de arquivos customizados
 - 12.4.26.6. Usuário específico
 - 12.4.26.7. Grupo do AD específico
 - 12.4.26.8. Fabricante do device USB



- 12.4.26.9. USB device ID
- 12.4.26.10. USB Serial number
- 12.4.26.11. Deve possuir detectores pre-configurados para diferentes tipos de dados
- 12.4.26.12. Importação de dados estruturados para ser analisado utilizando múltiplas colunas de informações.
- 12.4.26.13. Adição de termos - palavras chaves - como INTERNO. Adição de termos deve suportar:
 - 12.4.26.14. case sensitive
 - 12.4.26.15. case insensitive
 - 12.4.26.16. expressões regulares
 - 12.4.26.17. pesos diferentes por termo ou expressão regular
 - 12.4.26.18. Quantidade de ocorrência para o mesmo tempo ou expressão regular
- 12.4.27. Deve ser possível utilizar na mesma política de DLP, a combinação de smart IDs, termos, expressão regulares e dados estruturados sem qualquer restrição. Para a combinação de regras de DLP, deve suportar:
 - 12.4.27.1. Expressões lógicas como igual, menor que ou igual, maior que ou igual, maior, menor
 - 12.4.27.2. Operadores como "próximo" ou "não próximo"
 - (1) OR
 - (2) AND
 - (3) NOT
- 12.4.28. Deve ser possível configurar diferentes "gatilhos" de bloqueios, levando em consideração a soma do peso de um critério multiplicado pela quantidade ocorrências por termo
- 12.4.29. Deve funcionar em navegadores web sem necessidade de plugin
- 12.4.30. Deve ser capaz de monitorar abas anônimas dos navegadores web
- 12.4.31. Gestão de Incidentes
- 12.4.32. Para cada evento de DLP gerado deve ser possível o envio das informações para qualquer sistema externo desde que ele seja compatível com reports Webhook JSON
- 12.4.33. Para cada evento de DLP gerado deve ser possível o envio das informações para qualquer e-mail de sistema
- 12.4.34. Toda a console de gestão de incidentes, relatórios e regras de DLP deve ser gerenciada através da mesma interface. Não serão aceitos hardware adicionais ou sistemas de terceiros para realizar a gestão dos relatórios ou gestão dos incidentes
- 12.4.35. Retenção dos eventos gerados deve ser de responsabilidade do fabricante e não deve depender de solução terceira ou de outro fabricante
- 12.4.36. Retenção dos eventos deve ser durante todo o contrato vigente

12.4.37. Deve possuir um dashboard central com uma visão sumarizada de todos os incidentes gerados e níveis de riscos

12.4.38. Deve possível atribuir diferentes filtros para uma melhor mitigação de um incidente para no mínimo os seguintes critérios:

12.4.38.1. Dias, horas, Semanas, Anos, janela de tempo pré-definido

12.4.38.2. TAG

12.4.38.3. Origem do evento (incidente gerado,

12.4.38.4. User, e-mail, grupo do Active Directory

12.4.38.5. Host Name

12.4.38.6. IP Address

12.4.38.7. Sistema Operacional

12.4.38.8. Pais origem de conexão

12.4.38.9. Domínio que a estação de trabalho pertence

12.4.38.10. Nome da Aplicação

12.4.38.11. Nome do executável

12.4.38.12. Nome da impressora

12.4.38.13. Hash do arquivo

12.4.38.14. Deve ser capaz configurar tabelas dinâmicas na interface para uma melhor gestão e visualização dos incidentes

12.4.39. Deve possuir no mínimo os seguintes reports pré-configurados:

12.4.39.1. Top usuários com maiores incidentes

12.4.39.2. Quantidade de alertas por dia

12.4.39.3. Maior quantidade de incidentes por tipo de arquivos

12.4.39.4. Incidentes de DLP por localização geográfica

12.4.39.5. Tipo de dispositivos de USB mais utilizados

12.4.39.6. Top website utilizados para upload de arquivos sensíveis que geraram incidente

12.4.39.7. Uso de aplicações de inteligência artificial (sites, usuários, arquivos, atividades).

12.4.40. A console de administração deve prover um sistema de workflow onde deva possibilitar atribuir, no mínimo, os seguintes status:

12.4.40.1. Assignar um incidente a um recurso

12.4.40.2. Escalar incidente a outro time

12.4.40.3. Fechar incidente

12.4.40.4. Adicionar incidente sendo investigado

12.4.40.5. Falso Positivo



- 12.4.41. Deve ser possível atribuir comentários de investigação para cada incidente
- 12.4.42. Deve ser possível observar os dados detectados no arquivo combinando com a regra de DLP para entender melhor quais dados estão sendo detectados
- 12.4.43. Deve ser possível exportar uma nova mitigação ou relatório via CSV, PDF ou JSON
- 12.4.44. Deve possuir APIs disponíveis para integração com qualquer SIEM que suporte JSON
- 12.4.45. Deve possuir trilha de auditoria da console de administração
- 12.4.46. Deve possuir métricas de agentes instalados no ambiente
- 12.4.47. Deve possuir métricas da última conexão realizada por um agente
- 12.4.48. Deve possuir métricas de volume de dados enviados por um agente
- 12.4.49. Deve suportar "Single Sign One) via OAuth 2.0, SAML.
- 12.4.50. Funcionalidades de detecção e resposta a riscos internos (insider risk), compreendendo:
 - 12.4.50.1. o monitoramento do comportamento de usuários com privilégio,
 - 12.4.50.2. a correlação de eventos de Endpoint e de dados,
 - 12.4.50.3. a trilha de evidências, e
 - 12.4.50.4. o fluxo de investigação,
- 12.4.51. A funcionalidade de Insider Risk - IR deve ser contemplada no mesmo agente de DLP instalado. Não serão aceitos soluções que necessitem instalação de plug-in ou agentes adicionais
- 12.4.52. A solução deve ser 100% SaaS. Não serão aceitas soluções que necessitam hardware adicional para a função de IR.
- 12.4.53. A solução deve possuir no mínimo 200 regras de IR pré configuradas na console.
- 12.4.54. A solução deve monitorar atividades suspeitas e não suspeitas de um usuário.
- 12.4.55. Os dados coletados devem ser armazenados e geridos pela solução contratada.
- 12.4.56. O monitoramento e geração de incidentes devem permanecer ativos mesmo quando não tiver conectividade com a Internet ou com a Rede. Os logs devem ser retidos no desktop do usuário e sincronizado quando a conectividade com a Internet ou rede for reestabelecida.
- 12.4.57. Deve ser possível configurar diferentes níveis de retenção de logs localmente.
- 12.4.58. Logs e eventos armazenados localmente devem ser criptografados.
- 12.4.59. Deve ser possível tirar fotos da sessão do usuário conforme definições de políticas de IR.
- 12.4.60. Deve ser possível configurar as seguintes principais regras de IR.
- 12.4.61. Monitorar quando usuário realizar pesquisas suspeitas na Internet.
- 12.4.62. Monitorar quando o usuário iniciar uma conversa de Whatsapp Web e sua conversação.



- 12.4.63. Detectar e monitorar quando o usuário realizar a troca do nome de um arquivo que possa conter dados sensíveis.
- 12.4.64. Detectar e monitorar quando o usuário compactar um arquivo utilizando ferramentas como Winzip inserindo senhas.
- 12.4.65. Detectar e monitorar quando o usuário realizar download de um arquivo que possuir label Microsoft MIP.
- 12.4.66. Detectar e monitorar quando o usuário realizar upload de um arquivo que possuir label Microsoft MIP.
- 12.4.67. Detectar e monitorar quando o usuário conectar dispositivos externos. Deve catalogar informações como DeviceID, informações do Volume montado no sistema operacional, informações do fabricante, Serial Number, Class Name, e Interface Class Name.
- 12.4.68. Detectar e monitorar quando o usuário realizar uma conexão FTP externo.
- 12.4.69. Detectar e monitorar quando o usuário imprimir grande quantidade de folhas em determinado período de tempo.
- 12.4.70. Detectar e monitorar quando o usuário abrir a pasta de instalação dos binários do agente de IR.
- 12.4.71. Detectar e monitorar quando o usuário abrir sites de webmail
- 12.4.72. Detectar e monitorar qualquer atividade realizada pelo usuário quando abrir cliente de e-mail Microsoft Outlook
- a) Detectar e monitorar qualquer atividade realizada pelo usuário quando abrir cliente de e-mail genéricos
 - b) Detectar e monitorar quando o usuário abrir sistemas web de Chat/Instant Message
 - c) Deve ser possível configurar alertas para qualquer evento pré-configurado
 - d) Eventos devem ser explorados/investigados na mesma interface do Endpoint DLP
 - e) Gestão de Incidentes
 - f) Para cada evento de DLP gerado deve ser possível o envio das informações para qualquer sistema externo desde que ele seja compatível com reports Webhook JSON
 - g) Para cada evento de DLP gerado deve ser possível o envio das informações para qualquer e-mail de sistema
 - h) Toda a console de gestão de incidentes, relatórios e regras de DLP deve ser gerenciada através da mesma interface. Não serão aceitos hardware adicionais ou sistemas de terceiros para realizar a gestão dos relatórios ou gestão dos incidentes
 - i) Retenção dos eventos gerados deve ser de responsabilidade do fabricante e não deve depender de solução terceira ou de outro fabricante
 - j) Retenção dos eventos deve ser durante todo o contrato vigente



- k) Deve possuir um dashboard central com uma visão sumarizada de todos os incidentes gerados e níveis de riscos
- l) Deve possível atribuir diferentes filtros para uma melhor mitigação de uma incidente para no mínimo os seguintes critérios:
 - m) Dias, horas, Semanas, Anos, janela de tempo pré-definido
 - n) TAG
 - o) Origem do evento (incidente gerado,
 - p) User, email, grupo do Active Directory
 - q) Host Name
 - r) IP Address
 - s) Sistema Operacional
 - t) Pais origem de conexão
 - u) Domínio que a estação de trabalho pertence
 - v) Nome da Aplicação
 - w) Nome do executável
 - x) Hash do arquivo
- y) Deve ser capaz configurar tabelas dinâmicas na interface para uma melhor gestão e visualização dos incidentes
- z) Deve possuir no mínimo os seguintes reports pre-configurados:
 - aa) Top usuários com maior incidentes
 - bb) Quantidade de alertas por dia
 - cc) Maior quantidade de incidentes por tipo de arquivos
 - dd) Incidentes de DLP por localização geográfica
 - ee) Tipo de dispositivos de USB mais utilizados
 - ff) Top website utilizados para upload de arquivos sensíveis que geraram incidente
 - gg) A console de administração deve prover um sistema de workflow onde deva possibilitar atribuir, no mínimo, os seguintes status:
 - hh) Assignar um incidente a um recurso
 - ii) Escalar incidente a outro time
 - jj) Fechar incidente
 - kk) Adicionar incidente sendo investigado
 - ll) Falso Positivo
 - mm) Deve ser possível atribuir comentários de investigação para cada incidente
 - nn) Deve ser possível observar os dados detectados no arquivo combinando com a regra de DLP para entender melhor quais dados estão sendo



detectados

- oo) Deve ser possível exportar uma nova mitigação ou relatório via CSV, PDF ou JSON
- pp) Deve possuir APIs disponíveis para integração com qualquer SIEM que suporte JSON
- qq) Deve possuir trilha de auditoria da console de administração
- rr) Deve possuir métricas de agentes instalados no ambiente
- ss) Deve possuir métricas da última conexão realizada por um agente
- tt) Deve possuir métricas de volume de dados enviados por um agente

12.5. Ferramenta de casb

12.5.1. A solução de CASB deve ser fornecida como SaaS (Software-as-a-Service)

12.5.2. A solução deve ser licenciada por usuários, não limitado a integrações de aplicações SaaS. Ou seja, uma vez contratado a solução, o contratante pode realizar a integrações com outras aplicações SaaS sem quaisquer custos adicionais.

12.5.3. A solução deve ter disponibilidade de pelo menos 99.9%

12.5.4. Deve possuir integração via ICAP com Zscaler e/ou Citrix

12.5.5. Deve ser possuir integrações via RestAPI

12.5.6. Funcionalidades

12.5.7. A solução deve permitir integração via API, no mínimo, nas seguintes aplicações SaaS:

- 12.5.7.1. Microsoft Office 365
- 12.5.7.2. Google Workspace
- 12.5.7.3. Box
- 12.5.7.4. Dropbox
- 12.5.7.5. Egnyte
- 12.5.7.6. Salesforce
- 12.5.7.7. Okta
- 12.5.7.8. ServiceNow
- 12.5.7.9. Slack
- 12.5.7.10. Workday
- 12.5.7.11. Workplace
- 12.5.7.12. Jira Software
- 12.5.7.13. Confluence
- 12.5.7.14. Github

12.5.8. A solução deve permitir a integração via API, no mínimo, nas seguintes soluções de IaaS



- 12.5.8.1. Azure
- 12.5.8.2. AWS
- 12.5.9. A solução deve possuir mecanismo de controle de acesso que permite ou não o login em aplicações federadas/suportadas através de máquinas gerenciadas ou não gerenciadas
- 12.5.10. A solução deve monitorar os aplicativos de terceiros utilizados pelos usuários através de autenticação via O365 e GSuite, informando o risco associado ao uso dessa aplicação, no mínimo, as seguintes informações
 - 12.5.10.1. Application ID
 - 12.5.10.2. Permissões requeridas pela aplicação
 - 12.5.10.3. Informações do fabricante
 - 12.5.10.4. Dados forenses caso exista
 - 12.5.10.5. Usuários que possuem a aplicação autorizada
- 12.5.11. A solução deve monitorar contas comprometidas, com a possibilidade de notificar os responsáveis e suspender o login em questão
- 12.5.12. Deve ser possível restringir acessos a aplicação SaaS através dos seguintes critérios, no mínimo:
 - 12.5.12.1. País origem do acesso
 - 12.5.12.2. Segmento de rede
 - 12.5.12.3. Endereço IP
 - 12.5.12.4. Grupo de Active Directory
 - 12.5.12.5. Usuário
 - 12.5.12.6. Agente de conexão. Por exemplo, Ipad, Firefox Browser, Linux, etc
 - 12.5.12.7. Redes TOR
 - 12.5.12.8. Redes Públicas de VPN
 - 12.5.12.9. Redes Públicas de Proxy
- 12.5.13. A solução deve trazer informações relacionadas a phishing/spearphishing, quando uma conta for comprometida
- 12.5.14. A solução deve realizar análise comportamental de uma conta comprometida, utilizando informações do centro de inteligência do fabricante para classificar se o nível do risco do ataque e nível crítico, alto, médio ou baixo. Para cada um dos níveis, deve ser possível realizar diferentes remediações
- 12.5.15. Para a classificação suspeita, a solução deve utilizar informações do centro de inteligência do fabricante e inteligência artificial para identificar se o suspeito possa ser alguém de um departamento suspeito, uma pessoa suspeita ou alguém externamente da organização.
- 12.5.16. A solução deve identificar e alertar manipulação suspeitas de arquivos confidenciais. Deve ser possível gerar alertas e remediações para as seguintes ações:
 - 12.5.16.1. Arquivo Removido



- 12.5.16.2. Download
- 12.5.16.3. Conteúdo Compartilhado
- 12.5.16.4. Conteúdo Atualizado
- 12.5.16.5. Deve ser possível analisar e categorizar dados com os seguintes critérios:
- 12.5.16.6. Extensões de Arquivos
- 12.5.16.7. Label Microsoft (MIP)
- 12.5.16.8. Regex
- 12.5.16.9. SmartIDs
- 12.5.16.10. EDM
- 12.5.16.11. IDM
- 12.5.16.12. OCR
- 12.5.16.13. Palavras Chaves
- 12.5.16.14. Validações por Multi-column
- 12.5.16.15. Identificadores que cobrem regulamentações como PCI, GDPR, dados brasileiros
- 12.5.16.16. Dicionários e correspondência de proximidade
- 12.5.17. A solução deve remediar violações nas políticas por compartilhamento removendo, modificando permissões de compartilhamento e colocando arquivos em quarentena
- 12.5.18. A solução deve suportar ao menos as seguintes ações ao ter uma política violada:
 - 12.5.18.1. Alertar
 - 12.5.18.2. Mover para interno
 - 12.5.18.3. Quarentenar
 - 12.5.18.4. Mover para privado
 - 12.5.18.5. Remover Arquivo
 - 12.5.18.6. Trocar Label Microsoft MIP para outra
- 12.5.19. A solução deve identificar arquivos malware verificados através de uma estrutura de sandbox
- 12.5.20. A solução deve prover remediações se o usuário compartilhar dados sensíveis para um usuário fora da organização.
- 12.5.21. A solução deve prover remediações se o usuário compartilhar dados sensíveis com um link anônimo
- 12.5.22. A solução deve prover remediações caso ocorra elevações de permissionamento em uma conta sem o devido consentimento do mesmo
- 12.5.23. A solução deve permitir políticas aplicadas por grupos de usuários específicos. Com a possibilidade de incluir e excluir usuários/grupos
- 12.5.24. A solução deve permitir respostas diferentes baseadas no risco da política criada



- 12.5.25. A solução deve expor dados de IP e geolocalização (cidade, região, país) dos eventos
- 12.5.26. A solução deve possuir pelo menos filtros por cloud service, período, nome da atividade, categoria da atividade, nome do usuário, IP
- 12.5.27. A solução deve possuir logs referente a inspeção de dados em arquivos utilizando o motor DLP que armazenem e mostrem o nome do usuário e o arquivo registrado na violação
- 12.5.28. A solução deve mostrar um trecho com o conteúdo que acionou a violação da política de DLP
- 12.5.29. A solução deve permitir que dados sensíveis violados possam ser anonimizados de acordo com o perfil de acesso às logs, ou seja, somente usuários específicos podem ter acesso ao dado sensível completo
- 12.5.30. A solução deve fornecer funcionalidade de análise comportamental do usuário
- 12.5.31. A solução não deve exigir a instalação de um agente instalado no endpoint
- 12.5.32. A solução deve possuir integração com qualquer fornecedor de SIEM
- 12.5.33. A solução deve possuir integração com qualquer fornecedor de SOAR
- 12.5.34. A solução deve possuir recurso de ShadowIT, com risco e categoria de aplicações, sem qualquer custo adicional
- 12.5.35. A solução deve oferecer a capacidade de personalizar os critérios de pontuação de risco de alertas e atividades com base nas prioridades individuais da empresa
- 12.5.36. Os dados de registro para fornecer visibilidade e análise devem ser mantidos por pelo menos um (1) ano
- 12.5.37. A solução deve possuir um painel para fornecer informações sobre ameaças e gerenciar o fluxo de trabalho de incidentes
- 12.5.38. A solução pode impor controles contextuais no acesso móvel e desktop
- 12.5.39. Sua solução pode impor políticas para restringir o acesso a aplicações específicas (suportadas) apenas de dispositivos gerenciados
- 12.5.40. A solução deve permitir o envio por e-mail de relatórios agendados
- 12.5.41. Gerência
- 12.5.42. A solução deve fornecer interface de gerenciamento HTTPS
- 12.5.43. A solução deve disponibilizar diferentes perfis de acessos a console
- 12.5.44. O modelo de autenticação API deve ser via OAuth2
- 12.5.45. Gestão de Incidentes
- 12.5.46. Para cada evento de DLP gerado deve ser possível o envio das informações para qualquer sistema externo desde que ele seja compatível com reports Webhook JSON
- 12.5.47. Para cada evento de DLP gerado deve ser possível o envio das informações para qualquer e-mail de sistema



- 12.5.48. Toda a console de gestão de incidentes, relatórios e regras de DLP deve ser gerenciada através da mesma interface. Não serão aceitos hardware adicionais ou sistemas de terceiros para realizar a gestão dos relatórios ou gestão dos incidentes
- 12.5.49. Retenção dos eventos gerados deve ser de responsabilidade do fabricante e não deve depender de solução terceira ou de outro fabricante
- 12.5.50. Retenção dos eventos deve ser durante todo o contrato vigente
- 12.5.51. Deve possuir um dashboard central com uma visão sumarizada de todos os incidentes gerados e níveis de riscos
- 12.5.52. Deve possível atribuir diferentes filtros para uma melhor mitigação de um incidente para no mínimo os seguintes critérios:
- 12.5.53. Dias, horas, Semanas, Anos, janela de tempo pré-definido
- 12.5.53.1. TAG
 - 12.5.53.2. Origem do evento (incidente gerado,
 - 12.5.53.3. User, e-mail, grupo do Active Directory
 - 12.5.53.4. Host Name
 - 12.5.53.5. IP Address
 - 12.5.53.6. Sistema Operacional
 - 12.5.53.7. Pais origem de conexão
 - 12.5.53.8. Domínio que a estação de trabalho pertence
 - 12.5.53.9. Nome da Aplicação
 - 12.5.53.10. Nome do executável
 - 12.5.53.11. Hash do arquivo
- 12.5.54. Deve ser capaz configurar tabelas dinâmicas na interface para uma melhor gestão e visualização dos incidentes
- 12.5.55. Deve possuir no mínimo os seguintes reports pre-configurados:
- 12.5.55.1. Top usuários com maior incidentes
 - 12.5.55.2. Quantidade de alertas por dia
 - 12.5.55.3. Maior quantidade de incidentes por tipo de arquivos
 - 12.5.55.4. Incidentes de DLP por localizacao geográfica
 - 12.5.55.5. A console de administração deve prover um sistema de workflow onde deva possibilitar atribuir, no mínimo, os seguintes status:
 - 12.5.55.6. Assignar um incidente a um recurso
 - 12.5.55.7. Escalar incidente a outro time
 - 12.5.55.8. Fechar incidente
 - 12.5.55.9. Adicionar incidente sendo investigado
 - 12.5.55.10. Falso Positivo
 - 12.5.55.11. Deve ser possível atribuir comentários de investigação para cada incidente



12.5.55.12. Deve ser possível observar os dados detectados no arquivo combinando com a regra de DLP para entender melhor quais dados estão sendo detectados

12.5.55.13. Deve ser possível exportar uma nova mitigação ou relatório via CSV, PDF ou JSON

12.5.55.14. Deve possuir APIs disponíveis para integração com qualquer SIEM que suporte JSON.

12.6. Módulo de exploração do Risco Humano – correlação.

12.6.1. A solução deve consolidar sinais de risco humano (exposição a ameaças, comportamentos do usuário, interações com dados e identidade em uma visão unificada

12.6.2. A solução deve priorizar usuários com base em probabilidade de comprometimento, volume/tipo de ataques por e-mail e impacto potencial

12.6.3. A solução deve sugerir automaticamente ações de mitigação com base em sinais correlacionados

12.6.4. A solução deve apresentar tendências de risco ao longo do tempo e relatórios executivos

12.6.5. A solução deve expor risco humano via APIs/connector para plataformas de governança de identidade (ex.: SailPoint)

12.6.6. A solução deve integrar com módulos de e-mail security, DLP e colaboração para fechar o ciclo de mitigação

12.6.7. A solução deve utilizar modelos avançados (AI/ML) e inteligência de ameaças em tempo real para alimentar o scoring de risco

12.6.8. A solução deve fornecer explicabilidade do score de risco por fator (ataques, comportamento, impacto)

12.6.9. A solução deve permitir exportar métricas/risco para BI (CSV/API) para análises personalizadas

13. SERVIÇO DE IMPLANTAÇÃO DAS SOLUÇÕES DE SEGURANÇA

13.1. Os serviços de implantação das soluções de segurança compreendem o conjunto estruturado de atividades técnicas, operacionais e de governança necessárias para a disponibilização, configuração, integração e entrada em produção das ferramentas que compõem o ecossistema de segurança da informação da SEFAZ/ES.

13.2. A implantação deverá ser executada de forma planejada, coordenada e orientada a resultados, observando o cronograma aprovado, os critérios de aceite definidos e as melhores práticas de mercado, com o objetivo de estabelecer uma base sólida para a operação contínua do Security Operation Center (SOC).

13.3. Planejamento e Iniciação da Implantação

13.3.1. A fase inicial compreende:

13.3.1.1. Realização de reunião de kick-off com as equipes técnicas e de gestão;

13.3.1.2. Levantamento detalhado do ambiente tecnológico (inventário de ativos, arquitetura, integrações e fluxos);



- 13.3.1.3. Identificação de requisitos técnicos, operacionais e de segurança;
- 13.3.1.4. Elaboração e apresentação do plano de implantação contendo:
- 13.3.1.5. cronograma detalhado;
- 13.3.1.6. definição de marcos de entrega;
- 13.3.1.7. plano de comunicação;
- 13.3.1.8. matriz de responsabilidades;
- 13.3.1.9. Definição dos critérios de priorização por criticidade de ativos e serviços.

13.4. Preparação do Ambiente e Provisionamento

13.4.1. Nesta fase deverão ser executadas as seguintes atividades:

- 13.4.1.1. Provisionamento das licenças e ativação das soluções contratadas;
- 13.4.1.2. Configuração inicial das plataformas (cloud, on-premises ou híbridas);
- 13.4.1.3. Preparação de ambientes (produção, homologação e testes);
- 13.4.1.4. Configuração de conectividade segura (VPN, APIs, agentes, coletores de logs);
- 13.4.1.5. Instalação de componentes necessários (sensores, agentes, scanners, conectores);
- 13.4.1.6. Validação de requisitos de infraestrutura e desempenho.

13.5. Integração das Soluções e Coleta de Dados

13.5.1. A integração constitui etapa crítica da implantação e envolve:

- 13.5.1.1. Integração com fontes de dados;
- 13.5.1.2. Active Directory e sistemas de identidade;
- 13.5.1.3. firewalls, proxies e dispositivos de rede;
- 13.5.1.4. servidores, endpoints e aplicações;
- 13.5.1.5. serviços em nuvem e APIs;
- 13.5.1.6. Configuração de ingestão e normalização de logs (SIEM);
- 13.5.1.7. Integração entre ferramentas (SIEM, XDR, NDR, DLP, E-mail, Vulnerabilidade, BAS);
- 13.5.1.8. Implementação de pipelines de coleta e correlação de eventos;
- 13.5.1.9. Garantia da integridade, rastreabilidade e retenção dos dados.

13.6. Configuração das Soluções por Domínio de Segurança

13.6.1. Gestão de Vulnerabilidades e Riscos

- 13.6.1.1. Implantação de scanners ativos e passivos;
- 13.6.1.2. Descoberta e inventário automatizado de ativos;
- 13.6.1.3. Configuração de políticas de varredura;
- 13.6.1.4. Classificação de vulnerabilidades com base em risco;



13.6.1.5. Integração com sistemas de identidade e análise de exposição;

13.6.1.6. Geração de relatórios iniciais de risco e baseline de segurança.

13.6.2. Monitoramento, SIEM, SOAR e Resposta a Incidentes

13.6.2.1. Implantação e configuração da plataforma SIEM;

13.6.2.2. Criação e ajuste de casos de uso (use cases);

13.6.2.3. Configuração de regras de correlação baseadas em MITRE ATT&CK;

13.6.2.4. Implementação de playbooks automatizados (SOAR);

13.6.2.5. Integração com firewall, BAS e demais soluções;

13.6.2.6. Configuração de alertas, dashboards e painéis operacionais;

13.6.2.7. Implantação de simulação de ataques (BAS) e validação de controles.

13.6.3. Proteção de Endpoints

13.6.3.1. Instalação de agentes em endpoints e servidores;

13.6.3.2. Configuração de políticas de proteção contra ransomware;

13.6.3.3. Ativação de monitoramento comportamental;

13.6.3.4. Configuração de respostas automáticas (isolamento, bloqueio, quarentena);

13.6.3.5. Integração com SIEM para enriquecimento de eventos.

13.6.4. Gestão de Disponibilidade

13.6.4.1. Configuração de monitoramento de hosts, APIs e URLs;

13.6.4.2. Definição de métricas de disponibilidade e desempenho;

13.6.4.3. Implantação de dashboards operacionais;

13.6.4.4. Configuração de alertas de indisponibilidade e degradação;

13.6.4.5. Integração com SOC para resposta a incidentes operacionais.

13.6.5. Segurança de E-mail, DLP e Conscientização

13.6.5.1. Configuração de políticas de proteção de e-mail (anti-phishing, anti-spam, sandbox);

13.6.5.2. Implementação de controles de DLP (prevenção de vazamento);

13.6.5.3. Criação de políticas baseadas em classificação de dados;

13.6.5.4. Execução de campanhas de conscientização (Security Awareness);

13.6.5.5. Realização de simulações de phishing;

13.6.5.6. Integração com SIEM e ferramentas de resposta.

13.6.6. Microsegmentação de Rede

13.6.6.1. Mapeamento de fluxos de comunicação entre ativos;

13.6.6.2. Definição de políticas de segmentação por zona e criticidade;

13.6.6.3. Implantação de controles de isolamento lógico;



13.6.6.4. Configuração de regras de acesso e contenção;

13.6.6.5. Testes de movimentação lateral e validação de políticas.

13.7. Automação, Orquestração e Playbooks

13.7.1. Definição de fluxos de resposta a incidentes;

13.7.2. Criação de playbooks automatizados para:

13.7.3. phishing;

13.7.4. ransomware;

13.7.5. vazamento de dados;

13.7.6. comprometimento de credenciais;

13.7.7. Integração entre ferramentas para resposta coordenada;

13.7.8. Testes de automação e validação de eficácia.

13.8. Testes, Validação e Ajustes

13.8.1. Execução de testes funcionais e de integração;

13.8.2. Simulação de ataques controlados (BAS);

13.8.3. Validação de detecção e resposta;

13.8.4. Ajustes finos em regras, políticas e automações;

13.8.5. Garantia de aderência aos critérios de aceite definidos no TR.

13.9. Estabelecimento do Baseline e Operação Assistida

13.9.1. Definição do baseline de comportamento do ambiente;

13.9.2. Redução de falsos positivos;

13.9.3. Ajuste de thresholds e parâmetros de detecção;

13.9.4. Acompanhamento assistido da operação inicial;

13.9.5. Transferência gradual para operação contínua (SOC).

13.10. Documentação e Entregáveis (As-Built)

13.10.1. Ao final da implantação, a CONTRATADA deverá entregar:

13.10.2. Documentação técnica completa (As-Built);

13.10.3. Arquitetura da solução implantada;

13.10.4. Inventário de ativos monitorados;

13.10.5. Catálogo de casos de uso e playbooks;

13.10.6. Relatórios de configuração e integração;

13.10.7. Procedimentos operacionais;

13.10.8. Evidências de testes e validações realizadas.

13.11. Transferência de Conhecimento

13.11.1. Repasse de conhecimento das configurações para a equipes da SEFAZ/ES;



- 13.11.2. Apresentação dos fluxos operacionais do SOC;
- 13.11.3. Repasse de conhecimento do uso das ferramentas;
- 13.11.4. Orientações sobre governança e resposta a incidentes.

13.12. Governança da Implantação

- 13.12.1. Durante toda a execução deverão ser realizadas:
- 13.12.2. Reuniões periódicas de acompanhamento;
- 13.12.3. Relatórios de progresso;
- 13.12.4. Gestão de riscos e impedimentos;
- 13.12.5. Controle de mudanças;
- 13.12.6. Alinhamento contínuo com a CONTRATANTE.

13.13. Resultado Esperado da Implantação

- 13.13.1. Ao final dos serviços, a SEFAZ/ES deverá dispor de um ambiente:
 - 13.13.1.1. totalmente integrado e monitorado;
 - 13.13.1.2. com visibilidade centralizada de eventos de segurança;
 - 13.13.1.3. com capacidade de detecção e resposta automatizada;
 - 13.13.1.4. aderente às melhores práticas (NIST, ISO 27001, MITRE ATT&CK);
 - 13.13.1.5. preparado para operação contínua do SOC (24x7x365).

14. SERVIÇOS DE OPERAÇÃO DO SECURITY OPERATION CENTER

14.1. Dos requisitos gerais para todos os serviços:

- 14.1.1. Para todos os componentes fornecidos, como: servidores, coletores, appliance virtual e softwares, a CONTRATADA deverá fornecer serviço de backup dos dados com no mínimo as seguintes características:
 - 14.1.1.1. Armazenamento em ambiente off-site, ou seja, fora do ambiente da CONTRATANTE;
 - 14.1.1.2. Para o armazenamento off-site, deverá ser considerado datacenter no Brasil que possua no mínimo a seguinte certificação:
 - 14.1.1.3. ISO 27001;
 - 14.1.1.4. A comunicação entre o serviço de backup dos servidores, banco de dados e softwares internos e o ambiente de cloud deverá ter o protocolo de segurança TLS tanto para os tráfegos de entrada quanto para os tráfegos de saída;
 - 14.1.1.5. Deverá permitir a restauração granular de arquivos, repositórios e banco de dados;
 - 14.1.1.6. Deverá ter a capacidade de realizar proteção (backup) e replicação incremental;
 - 14.1.1.7. Deverá ter capacidade de configurar políticas de retenção dos dados;
 - 14.1.1.8. Sobre a retenção das cópias de segurança (backup) em ambiente off-site,



deverá considerar a seguinte política:

- 14.1.1.8.1. 1 (uma) copia diária de cada servidor, banco de dados e software;
- 14.1.1.8.2. Retenção de até 7 dias;
- 14.1.2. Este requisito se restringe aos componentes e softwares das soluções de segurança ofertados pela CONTRATADA.
- 14.1.3. A CONTRATADA deve executar a caça de ameaças de forma PROATIVA e REATIVA conforme SUBPROCESSO DE THREAT HUNTING:
 - 14.1.3.1. Threat Hunting Proativo: Essencial para detectar ameaças avançadas que passam despercebidas por sistemas automáticos, antecipando ataques e mitigando riscos de segurança. Contribui para uma defesa adaptativa contra ameaças emergentes e reduz a superfície de ataque;
 - 14.1.3.2. Threat Hunting Reativo: Fundamental para uma resposta rápida e eficaz a incidentes de segurança, permitindo investigar profundamente ameaças identificadas, reduzir o tempo de permanência do atacante e melhorar continuamente as defesas com base nos TTPs observados.
- 14.1.4. **Sub-Subprocesso De Resposta A Incidente De Segurança Da Informação**
 - 14.1.4.1. Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação da SEFAZ-ES, levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade. Logo o início do processo de resposta a incidente de segurança se dará, sempre que um evento adverso for submetido pelo SERVIÇOS DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS descrito no presente Termo de Referência, porém não se limitando a este. Poderá o corpo técnico de segurança da SEFAZ-ES a qualquer tempo, abrir um incidente de segurança.
 - 14.1.4.2. Após o incidente de segurança de exceção aberto, será de responsabilidade do grupo de resposta a incidente de segurança da CONTRATADA, analisar os logs e artefatos enviados, a fim de no primeiro instante identificar as fontes geradoras de tais logs.
 - 14.1.4.3. Como próximo passo o grupo de resposta a incidente de segurança da CONTRATADA, deverá comunicar ao time de segurança da informação da SEFAZ-ES as informações iniciais sobre o incidente de segurança gerado, e quais serão as linhas de atuação para solução do incidente
 - 14.1.4.4. Juntamente com a SEFAZ-ES, o grupo de resposta a incidentes de segurança da CONTRATADA, deverá definir a severidade do incidente de segurança. A severidade do incidente de segurança da informação será definida através da combinação de urgência e impacto, onde impacto é definido como a medida de criticidade do negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente.
 - 14.1.4.5. Todo o processo de análise e resultados obtidos, devem ser documentados a todo tempo na ferramenta de gestão de incidentes da segurança da informação, para que a SEFAZ-ES acompanhe todos os passos para a solução do incidente.
 - 14.1.4.6. Uma vez identificado o comportamento suspeito e os principais vetores de



ataque, o grupo de resposta a incidentes de segurança da CONTRATADA deverá acionar os responsáveis pela mitigação, que executarão os procedimentos de contenção necessários. Caso as ferramentas envolvidas estejam sob a gestão da CONTRATADA, esta deverá estabelecer processo interno de acionamento para que a contenção seja realizada no menor tempo possível. Quando a ação de contenção depender de autorização prévia do corpo técnico de segurança da SEFAZ-ES, a contagem dos indicadores de tempo de contenção e de resposta ficará suspensa desde a solicitação formal até o recebimento da autorização.

14.1.4.7. O grupo de resposta a incidente de segurança da CONTRATADA, deve documentar na ferramenta de incidente de segurança, as lições aprendidas do incidente de segurança em questão, formando durante todo o período de vigência do contrato uma grande base de conhecimento sobre ataques adversos.

14.1.5. Sub-Subprocesso De Forense Digital Para Resposta A Incidentes

14.1.5.1. As atividades do DFIR serão acionadas em caso de inoperância parcial ou total do ambiente da SEFAZ-ES, no contexto de incidente de cibersegurança, nessas situações especiais poderão ser executadas as atividades abaixo descritas, mas não se limitando apenas a estas;

14.1.5.1.1. Análise Forense de Dispositivos de Armazenamento

14.1.5.1.2. Exame detalhado de discos rígidos e outros dispositivos para identificar sinais de comprometimento.

14.1.5.1.3. Análise de Logs do Sistema

14.1.5.1.4. Análise aprofundada de logs de sistema e segurança para traçar o comportamento e a linha do tempo de um ataque.

14.1.5.2. Investigação de Malware

14.1.5.2.1. Análise de amostras de malware, identificação de seu comportamento e vetores de ataque;

14.1.5.2.2. Análise de Tráfego de Rede Forense

14.1.5.2.3. Inspeção detalhada de pacotes de rede para identificar atividades maliciosas ou invasões;

14.1.5.3. Análise de Memória Volátil (RAM)

14.1.5.3.1. Investigação de dados temporários em memória para capturar processos maliciosos em execução;

14.1.5.4. Investigação de Ataques de Ransomware

14.1.5.4.1. Determinação do vetor de infecção, análise da criptografia e desenvolvimento de estratégias de mitigação;

14.1.5.5. Análise de Backdoors

14.1.5.5.1. Investigação de portas dos fundos instaladas por invasores para acesso persistente ao sistema;

14.1.5.6. Recuperação de Dados Forense

14.1.5.6.1. Tentativa de recuperação de dados comprometidos ou destruídos durante um ataque cibernético;



14.1.5.7. Análise de Ataques de Phishing

- 14.1.5.7.1. Investigação de incidentes de phishing que resultaram no comprometimento de credenciais ou sistemas;

14.1.5.8. Análise de Artefatos Persistentes

- 14.1.5.8.1. Identificação de artefatos, como scripts maliciosos ou executáveis, deixados por invasores;

14.1.5.9. Identificação de Acessos Não Autorizados

- 14.1.5.9.1. Investigação e documentação de acessos indevidos ou tentativas de escalonamento de privilégios;
- 14.1.5.9.2. Análise de Logs de Autenticação
- 14.1.5.9.3. Revisão de logs de autenticação para identificar tentativas de login fraudulentas;
- 14.1.5.9.4. Análise de Comandos Executados no Sistema
- 14.1.5.9.5. Revisão dos comandos executados por invasores durante o ataque;
- 14.1.5.9.6. Análise de Códigos Maliciosos em Aplicações Web
- 14.1.5.9.7. Inspeção de código injetado em aplicações web para exploração de vulnerabilidades;

14.1.5.10. Análise de Exfiltração de Dados

- 14.1.5.10.1. Investigação de atividades de extração não autorizada de dados sensíveis;
- 14.1.5.10.2. Identificação de Técnicas de Evasão de Defesas
- 14.1.5.10.3. Análise dos métodos usados por invasores para evitar a detecção por sistemas de segurança;
- 14.1.5.10.4. Investigação de Exploração de Vulnerabilidades
- 14.1.5.10.5. Identificação das vulnerabilidades exploradas pelos atacantes para comprometer o sistema;

14.1.5.11. Análise Forense de Sistemas Operacionais

- 14.1.5.11.1. Investigação detalhada dos arquivos de sistema, registros e logs do sistema operacional comprometido;
- 14.1.5.11.2. Investigação de Incidentes de Espionagem Cibernética
- 14.1.5.11.3. Análise detalhada de incidentes envolvendo espionagem cibernética, com foco na identificação dos métodos e atores;

14.1.5.12. Análise de Tentativas de Escalabilidade de Privilégios

- 14.1.5.12.1. Investigação de tentativas de invasores de obter privilégios administrativos em um sistema;
- 14.1.5.12.2. Investigação de Incidentes em Dispositivos Móveis
- 14.1.5.12.3. Análise forense de dispositivos móveis comprometidos para determinar o vetor de ataque;



14.1.5.13. Análise de Registros de Firewall

14.1.5.13.1. Revisão de registros de firewall para rastrear tentativas de invasão e identificar padrões de ataque;

14.1.5.13.2. Investigação de Modificação de Arquivos de Sistema

14.1.5.13.3. Identificação de alterações maliciosas nos arquivos e configurações do sistema;

14.1.5.14. Investigação de Exploração de Serviços de Rede

14.1.5.14.1. Análise de ataques que exploram serviços de rede vulneráveis, como DNS, SMTP, entre outros;

14.1.5.14.2. Análise de Comportamento de Processos Maliciosos

14.1.5.14.3. Identificação do comportamento de processos maliciosos em execução, como coleta de dados ou comunicação com servidores de comando e controle;

14.1.5.15. Investigação de Ataques Persistentes Avançados (APTs)

14.1.5.15.1. Análise detalhada de ataques sofisticados e persistentes visando a infiltração prolongada em sistemas;

14.1.5.16. Recuperação e Preservação de Metadados Forenses

14.1.5.16.1. Aquisição de metadados relevantes para auxiliar na reconstrução da linha do tempo de um incidente;

14.1.5.17. Análise de Indicadores de Comprometimento (IOCs)

14.1.5.17.1. Identificação e correlação de indicadores de comprometimento para traçar as atividades dos invasores;

14.1.6. Sub-Processo De Threat Hunting

14.1.6.1. A CONTRATADA deverá implementar um processo de Threat Hunting, atuando de forma proativa e buscando ameaças e atividades maliciosas na rede ou nos sistemas, monitorando de forma contínua todos os eventos correlacionados.

14.1.6.2. O SUBPROCESSO DE THREAT HUNTING deverá seguir as recomendações do HMM – Threat Hunting Maturity Model:

14.1.6.2.1. Coleta de dados (o volume e a qualidade dos dados que uma empresa extrai de seu ambiente);

14.1.6.2.2. Criação de hipóteses (o que é levado em consideração na criação de hipóteses);

14.1.6.2.3. Ferramentas e técnicas para testes de hipóteses;

14.1.6.2.4. Detecção de padrões e táticas, técnicas e procedimentos (TTPs);

14.1.6.2.5. Automação analítica (até que ponto os procedimentos de caça a ameaças são automatizados);

14.1.6.3. Ao incorporar este modelo no serviço Gerenciado de Segurança, a SEFAZ-ES garante que a empresa escolhida esteja alinhada com as melhores práticas de Threat Hunting, proporcionando uma defesa robusta e adaptável contra ameaças emergentes;



- 14.1.6.4. Definir uma hipótese e uma declaração de uma possibilidade de ameaça, tal hipótese deve ser elaborada utilizando como referência novos vetores de ameaças e novas tendências baseadas em inteligência de ameaças e fontes de riscos digitais, informações relevantes coletadas por processos de aprendizagem de máquina e inteligência artificial e investigações de táticas, técnicas e procedimentos criando desta forma uma hipótese de como ameaças podem existir dentro do ambiente e de como encontrá-las;
- 14.1.6.5. Uma vez que a hipótese tenha sido definida a CONTRATADA deverá realizar um plano de coleta dos eventos dentro das plataformas relevantes de acordo com a hipótese definida;
- 14.1.6.6. Uma vez que os eventos relevantes estejam disponíveis, a CONTRATADA deverá avaliar a massa de eventos para buscar anomalias associadas a hipótese definida;
- 14.1.6.7. Caso sejam encontrados eventos maliciosos, estes entram no processo de resposta a incidentes de segurança da informação, conforme descrito neste documento;
- 14.1.6.8. Caso não sejam encontrados eventos maliciosos, o processo de caçada é finalizado, sendo repetido no dia seguinte com uma nova hipótese;
- 14.1.6.9. Todo processo deve ser documentado através da plataforma de gerenciamento de chamados, incluindo qual hipótese foi utilizada, quais dados foram analisados e o resultado da análise;
- 14.1.6.10. Todas as regras que forem criadas pela equipe de Threat Hunting deverão ser validadas por meio da realização de simulações de ataques, utilizando ferramenta específica de gerenciamento contínuo de exposição a ameaças com o objetivo de testar a eficácia das detecções, ajustar os controles existentes e gerar novos casos de uso a serem incorporados ao processo de monitoramento e resposta a incidentes da CONTRATANTE.
- 14.1.6.11. A CONTRATADA deverá executar serviços contínuos de Threat Hunting, com foco na identificação de comunicações anômalas, análise de fluxos de rede e validação de indicadores de comprometimento (IoCs), de modo a antecipar ameaças e gerar novos casos de uso aplicáveis ao processo de monitoramento e resposta a incidentes da CONTRATANTE.
- 14.1.6.12. A CONTRATADA deverá disponibilizar relatórios detalhados de conexões suspeitas e persistentes com domínios, endereços IP e serviços potencialmente maliciosos, priorizando eventos por grau de risco e criticidade.
- 14.1.6.13. Integração dos resultados do Threat Hunting ao processo de Detecção e Resposta a Incidentes da CONTRATANTE, garantindo que eventos anômalos gerem automaticamente novos alertas ou ajustes nas regras do SIEM/XDR/SOAR.
- 14.1.6.14. Esse processo deverá ampliar a visibilidade sobre ameaças emergentes, identificar falhas de cobertura nos controles existentes e contribuir diretamente para o amadurecimento das regras de detecção e mitigação, incorporando mecanismos de automação no processo de resposta para acelerar a contenção e a erradicação de ameaças.
- 14.1.6.15. Com o aumento do volume e complexidade das ameaças será exigido que



a CONTRATADA execute processos manuais e automáticos de busca de ameaças (threat hunting) para atender o CONTRATANTE. A fim de balizar todo o processo de caçada de ameaças e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem.

14.1.6.16. A CONTRATADA deve possuir mecanismos próprios que realizem a monitoração das principais Redes Sociais (Facebook, Twitter, LinkedIn, Instagram, YouTube, etc.), lojas de aplicativos para Smartphones (Google Play Store e Apple Store) e lojas não oficiais.

14.1.6.17. A CONTRATADA deve prover serviço de monitoramento de domínios nacionais e internacionais, incluindo TLDs e gTLDs, que verifique a utilização do uso indevido da marca do CONTRATANTE no nome do domínio ou na URL cadastrada, contendo o domínio/URL cadastrado, a CONTRATANTE que administra o registro do domínio, e os dados proprietário do domínio.

14.1.6.18. Monitorar ameaças virtuais emergentes externas ao ambiente e avaliar a aplicabilidade especificamente as políticas de segurança do CONTRATANTE, propondo proativamente a realização de contramedidas com o objetivo de prevenir a exploração de alguma brecha de segurança.

14.1.7. Equipe De Inteligência De Ameaças

14.1.7.1. A contratada deverá contar com uma equipe de Inteligência de ameaças, dedicada a identificar as intenções, capacidades e, prioritariamente, as oportunidades usadas pelos criminosos através da coleta, normalização, correlação e análise de dados, transformando-os em inteligência e entregando ao CONTRATANTE relatórios periódicos, apresentando dados de mercado e o atual cenário do ambiente do CLIENTE.

14.1.7.2. Esses dados poderão ser utilizados para melhora na proteção, seja na atuação direta com a equipe de Hunting em novos casos de uso ou mantendo os times da CONTRATANTE informados, através de Boletins de Ameaças.

14.1.7.3. A CONTRATADA deverá possuir plataforma de inteligência que informe IoCs (Indicadores de comprometimento) contendo, no mínimo, hashes de binários maliciosos nos formatos MD5, SHA1, SHA256, filename, domínios maliciosos, URLs maliciosas, bem como IPs maliciosos com geolocalização e pontuação de risco, reduzindo a possibilidade de falso positivo;

14.1.7.4. Deve possuir equipe de Threat Intelligence que execute Análise de Superfície, um trabalho que avalia o ambiente na perspectiva de um agente malicioso em busca de eventuais brechas utilizando o framework OSINT (Inteligência de Fontes Abertas) com foco na identificação de superfície de ataque e as possíveis oportunidades na perspectiva de um agente malicioso.

14.1.7.5. Deve executar de forma recorrente a Análise de Superfície, no mínimo semestralmente, utilizando especialistas de Cyber Threat Intelligence na execução de um Assessment interno e análise externa utilizando técnicas de OSINT, apresentando informações dos perímetros com objetivo de entregar relatório, apontando de forma prática como tratar cada ponto identificado e apresentar um score qualitativo de maturidade para o CONTRATANTE.

14.1.8. Grupo Técnico Do Monitoramento E Resposta A Incidentes



14.1.8.1. A CONTRATADA deverá manter o GRUPO TÉCNICO DO MONITORAMENTO E RESPOSTA A INCIDENTES com objetivo e foco de trabalhar no processo de monitoramento de ataques cibernéticos.

14.1.8.2. Este grupo deverá ser exclusivo para trabalhar no serviço em questão, não podem os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem, com os demais serviços descritos no objeto do presente termo de referência.

14.1.8.3. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no IMR – INSTRUMENTO DE MEDIÇÃO DE RESULTADOS e CATÁLOGO DE SERVIÇO do presente termo de referência.

14.1.8.4. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para executar o processo de monitoramento de ataques cibernéticos da SEFAZ-ES, a CONTRATADA deverá, obrigatoriamente, compor os GRUPO DE MONITORAMENTO E RESPOSTA A INCIDENTES, com 01 (um) profissional para cada perfil que segue descrito abaixo:

Perfis	Certificações	Descrição
Analista de Segurança I	Certified in Cybersecurity – (ISC)	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.
Analista de Segurança II	Certified Ethical Hacker	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM. Experiência comprovada de no mínimo 24 (vinte e quatro) meses em segurança da informação.
Analista III	Certificação da solução a ser utilizada no serviço	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.

14.1.8.5. Todos os profissionais deverão possuir diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

14.1.8.6. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO TÉCNICO DO MONITORAMENTO E RESPOSTA A INCIDENTES, porém, conforme já foi mencionado neste termo de referência, este(s) deve(m) compor única e exclusivamente o time denominado GRUPO TÉCNICO DO MONITORAMENTO E RESPOSTA A INCIDENTES.

14.1.9. Entregas A Serem Realizadas

14.1.9.1. Para acompanhamento do serviço a ser ofertado pela CONTRATADA, os entregáveis abaixo deverão compor o relatório mensal a ser entregue pela CONTRATADA para acompanhamento da execução contratual:

INDICADOR	AGRUPADOR	DESCRIÇÃO
-----------	-----------	-----------



KPI-1	MDR	Número total de eventos correlacionados
KPI-2	MDR	Número total de incidentes abertos
KPI-3	MDR	TOP do número de eventos correlacionados por IP de destino
KPI-4	MDR	TOP do número de eventos correlacionados por país de origem
KPI-5	MDR	Número total de regras de correlacionamento
KPI-6	MDR	TOP 10 do número de eventos correlacionados por regra de correlacionamento

14.1.9.2. Tais entregáveis, relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring). Nesse contexto, o profissional deve apresentá-lo de forma virtual, por meio de solução de videoconferência;

14.2. Processo do serviço de gerenciamento contínuo de exposição a ameaças

14.2.1. Requisitos gerais

14.2.1.1. Este processo abrange todos os dispositivos com serviço de GERENCIAMENTO CONTÍNUO DE EXPOSIÇÃO A AMEAÇAS, incluindo IPs e URLs por amostragem deverá ser executado em regime de 8 (oito) horas por dia, 07 (sete) dias por semana. As ações envolvem desde a gestão da solução. A CONTRATADA deverá executar minimamente as ações abaixo:

14.2.1.2. Definição do escopo e objetivos dos testes de penetração automatizados, considerando IPs e Aplicações WEB de críticas e de amostragem;

14.2.1.3. Parametrização das soluções de penetração automatizadas, para que estejam devidamente configuradas;

14.2.1.4. Revisar as permissões e acessos à infraestrutura-alvo para evitar falhas na execução dos testes;

14.2.1.5. Atualização anual do inventário de ativos críticos a serem testados;

14.2.1.6. Executar a automação de varredura de vulnerabilidades que podem ser exploradas pela solução;

14.2.1.7. Avaliação de possíveis exploits automatizados com base nas vulnerabilidades encontradas;

14.2.1.8. Simulação automatizada de acessos não autorizados;

14.2.1.9. Avaliar a capacidade de escalar privilégios de usuários normais para administradores;

14.2.1.10. Simular a exploração de vulnerabilidades em redes internas;

14.2.1.11. Avaliar se as medidas de controle (firewall, EDR) estão efetivas contra ataques automatizados;

14.2.1.12. Verificar vulnerabilidades em aplicações web críticas designadas;

14.2.1.13. Simulação de Exfiltração de Dados;

14.2.1.14. Testar a capacidade de evitar a exfiltração de dados de sistemas sensíveis;

14.2.1.15. Revisar os logs de segurança e eventos capturados durante os testes



automatizados;

14.2.1.16. Avaliar a eficácia dos controles de detecção contra tentativas de evasão automatizadas;

14.2.1.17. Gerar relatório automatizado das vulnerabilidades encontradas;

14.2.1.18. Reavaliação dos resultados para garantir a qualidade e precisão dos testes;

14.2.1.19. Revisão das técnicas usadas nos testes automatizados para garantir sua adequação;

14.2.2. Grupo técnico do gerenciamento contínuo de exposição a ameaças

14.2.2.1. A CONTRATADA deverá manter o GRUPO TÉCNICO DO GERENCIAMENTO CONTÍNUO DE EXPOSIÇÃO A AMEAÇAS com objetivo e foco de trabalhar no processo de gestão e identificação de ameaças por amostragem.

14.2.2.2. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no CATÁLOGO DE SERVIÇO e IMR – INSTRUMENTO DE MEDIÇÃO DE RESULTADOS do presente termo de referência.

14.2.2.3. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade, a CONTRATADA deverá, obrigatoriamente, compor os GRUPO TÉCNICO DO GERENCIAMENTO CONTÍNUO DE EXPOSIÇÃO A AMEAÇAS, com 01 (um) profissional para cada perfil que segue descrito abaixo:

Perfis	Certificações	Descrição
Analista de Segurança I	Certificação na solução ofertada	Conhecimento avançado em segurança da informação, com experiência em testes de penetração de segurança da informação. Experiência comprovada de no mínimo 2 (dois) anos em segurança da informação.
Analista de Segurança II	Certified Ethical Hacker	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.

14.2.2.4. Todos os profissionais deverão possuir diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

14.2.2.5. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO TÉCNICO DO GERENCIAMENTO CONTÍNUO DE EXPOSIÇÃO A AMEAÇAS, porém, conforme já foi mencionado neste termo de referência, este(s) deve(m) compor única e exclusivamente o time denominado GRUPO TÉCNICO DO GERENCIAMENTO CONTÍNUO DE EXPOSIÇÃO A AMEAÇAS.



14.2.3. Entregas A Serem Realizadas

14.2.3.1. Para acompanhamento do serviço a ser ofertado pela CONTRATADA, os entregáveis abaixo deverão compor o relatório mensal a ser entregue pela CONTRATADA para acompanhamento da execução contratual:

INDICADOR	AGRUPADOR	DESCRIÇÃO
KPI-1	PTA	Vulnerabilidades Exploráveis Confirmadas
KPI-2	PTA	Cadeias de Ataque Identificadas
KPI-3	PTA	Quantidade de Explorações Bem-Sucedidas
KPI-4	PTA	Score de Exposição ao Ataque
KPI-5	PTA	Exposições por Tipo de Técnica

14.2.3.2. Tais entregáveis, relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring). Nesse contexto, o profissional deve apresentá-lo de forma virtual, por meio de solução de videoconferência;

14.3. Processo de serviço gerenciado de inteligência aplicado à segurança

14.3.1. Requisitos gerais

14.3.1.1. O serviço visa o monitoramento contínuo e ininterrupto de termos e ativos digitais acessíveis e públicos na internet em níveis de superfície (surface), profunda (deep) e oculta (dark) web, como canais de fóruns, redes de compartilhamento de textos e códigos-fontes, aplicativos de mensagens, lojas de aplicativos, feeds, phishing, typosquatting, redes sociais, vídeo streaming, vítimas de malwares e páginas de comércio eletrônico, gerando identificadores através de eventos relevantes ao negócio, aos quais devem ser analisados, processados, organizados e enriquecidos, obedecendo um processo cíclico de refinamento e enriquecimento de inteligência de dados de riscos digitais, com equipe especializada no processo investigativo (threat hunting), de inteligência de ameaças cibernéticas (threat intelligence) e serviços de remoção de conteúdos infratores (takedown services).

14.3.1.2. A CONTRATADA deve realizar o monitoramento contínuo de fontes externas nacionais e internacionais, como fóruns, Redes Sociais, Internet Relay Chat (IRC), mídias sociais, nuvens públicas e grupos hackers para identificação de motivações, intenções e atividades de possíveis adversários que possam causar impactos à CONTRATANTE.

14.3.1.3. Os Serviços de Proteção de Riscos Digitais, doravante SPRD, devem suportar quatro grandes pilares: mapeamento, monitoramento, curadoria e mitigação.

14.3.1.4. Mapeamento, tem por objetivo identificar e entender os ativos digitais sob risco.

14.3.1.5. Monitoramento, visa o monitoramento contínuo e ininterrupto dos ativos digitais, com o objetivo de documentar, contextualizar, enriquecer e priorizar os riscos e alertas com capacidade de reportar detalhes de incidentes permitindo a tomada de decisão inteligente em relação a tais riscos.

14.3.1.6. Mitigação, visa a reduzir o risco dos ativos digitais, através dos alertas enviados aos clientes, procedimentos de take down, ou sugestão de configurações do



ambiente para mitigar riscos identificados pela plataforma durante a fase de monitoramento

14.3.2. Mapeamento

14.3.2.1. A CONTRATADA entregará a CONTRATANTE a lista dos ativos digitais a serem monitorados, que devem ser cadastrados dentro da plataforma.

14.3.2.2. O SPRD deve ser capaz de contextualizar o tipo de ativo, afim de que seja possível criar regras específicas para cada caso ou tipo de ativo.

14.3.2.3. O SPRD deve possuir capacidade para entender no mínimo as seguintes classes de ativos:

14.3.2.3.1. Domínios: é um nome que serve para localizar e identificar conjuntos de computadores na internet. O nome de domínio foi concebido com o objetivo de facilitar a memorização dos endereços de computadores na Internet.

14.3.2.3.2. Marcas: é a marca registrada, nome fantasia, nome do produto, nome de fachada, razão social, termo ou expressão que identifique o CONTRATANTE.

14.3.2.3.3. BIN: Números do cartão de crédito para identificar o banco emissor e a conta do cliente. Os primeiros seis dígitos, liderados pelo primeiro dígito que identifica a bandeira do cartão, são coletivamente conhecidos como o número de identificação do emissor e denominados números de identificação bancária.

14.3.2.3.4. Endereço IP: Endereço de Protocolo da Internet, do inglês Internet Protocol address, é um rótulo numérico atribuído a cada dispositivo conectado a uma rede de computadores que utiliza o Protocolo de Internet para comunicação.

14.3.2.3.5. Pessoa: Informação de identificação pessoal de empregado ou pessoa de interesse para monitoramento de riscos digitais dirigidos a pessoa física.

14.3.2.4. Seguindo um processo de monitoramento contínuo em regime 24x7 a CONTRATADA deve entregar à CONTRATADA em forma de relatórios e notificações:

14.3.2.4.1. Identificar, reconhecer, coletar, analisar, processar, organizar e apresentar informações disponíveis e acessíveis, de forma automatizada e personalizada, em conversas, mídias e redes sociais, demais páginas da internet de superfície, profunda e oculta, fóruns, redes de compartilhamento de textos e códigos-fonte, aplicativos de mensageria, lojas de aplicativos, feeds RSS, páginas de comércio eletrônico, bem como monitorar outros serviços de descoberta e monitoração e quaisquer outras fontes de informação disponíveis e acessíveis

14.3.3. Grupo técnico de serviço gerenciado de inteligência aplicado à segurança

14.3.3.1. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no CATÁLOGO DE SERVIÇO e IMR – INSTRUMENTO DE MEDIÇÃO DE RESULTADOS do presente termo de referência.

14.3.3.2. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para executar o processo de monitoramento de ataques cibernéticos do CLIENTE, a CONTRATADA deverá, obrigatoriamente, compor o GRUPO TÉCNICO GERENCIADO DE INTELIGÊNCIA APLICADO À SEGURANÇA, com ao menos 01 (um) perfil de cada profissional que segue descrito abaixo:



Perfil	Conhecimentos / Papeis / Responsabilidades
Analista de Threat Intelligence	Revisão de Eventos Criação de Regras de Baseline OSINT de novas fontes Criação de Regras de Automação Criação de Regras Regex e Yara Criação de Personas e Interação com Fraudadores Identificação de novas Fontes
Gerente do Serviço de Proteção de Riscos Digitais	Liderança/Gerenciamento do Time Responsável pela Qualidade do Serviço/Plataforma Dono do Produto, responsável por novos recursos, novas soluções e funcionalidades dentro da plataforma. Apresentação Executiva / Técnica Gerenciamento de Custo, Precificação e Parthenbers. Especialista em Cibersegurança com ênfase em inteligência de riscos digitais.

14.3.4. Entregas A Serem Realizadas

14.3.4.1. Para acompanhamento do serviço a ser ofertado pela CONTRATADA, os entregáveis abaixo deverão compor o relatório mensal a ser entregue pela CONTRATADA para acompanhamento da execução contratual:

INDICADOR	AGRUPADOR	DESCRIÇÃO
KPI-1	INTELIGÊNCIA	Quantidade total de menções detectadas em fontes abertas, profundas e ocultas
KPI-2	INTELIGÊNCIA	Quantidade de incidentes abertos a partir de detecções em surface, deep e dark web
KPI-3	INTELIGÊNCIA	Quantidade de solicitações de takedown encaminhadas aos provedores e autoridades
KPI-4	INTELIGÊNCIA	Quantidade de takedowns concluídos com sucesso
KPI-5	INTELIGÊNCIA	Tempo médio de resposta entre a detecção da ameaça e a abertura do incidente
KPI-6	INTELIGÊNCIA	Quantidade de eventos classificados por tipologia (phishing, malware, typosquatting etc.)
KPI-7	INTELIGÊNCIA	Percentual de incidentes enriquecidos com dados de contexto (atores, TTPs, IOC)

14.3.4.2. Tais entregáveis, relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring). Nesse contexto, o profissional deve apresentá-lo de forma virtual, por meio de solução de videoconferência;

14.4. Processo de hiperautomação para detecção e resposta a ameaças

14.4.1. Requisitos gerais

14.4.1.1. Este processo abrange todos os componentes da solução de hiperautomação para detecção e resposta a ameaças, devendo operar de forma contínua, em regime 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano.

14.4.1.2. O processo deverá estar integrado ao Processo de Detecção e Resposta a Incidentes da CONTRATANTE, de forma a assegurar uma atuação orquestrada, ágil e eficiente diante de ameaças cibernéticas.

14.4.1.3. A CONTRATADA deverá executar, minimamente, as seguintes atividades:

14.4.1.3.1. Validar o ambiente após a ativação da solução, garantindo que



todos os componentes estejam devidamente configurados e operacionais;

- 14.4.1.3.2. Configurar Virtual Appliances adicionais e assegurando a integração com os demais elementos do ambiente;
- 14.4.1.3.3. Configurar Script Hosts adicionais, com validação de conectividade e comunicação com os sistemas de detecção;
- 14.4.1.3.4. Configurar Coletores adicionais, alinhados às políticas de segurança e limites contratuais, para ampliar a abrangência de visibilidade do ambiente;
- 14.4.1.3.5. Monitorar continuamente os Virtual Appliances, Script Hosts e Coletores, garantindo sua disponibilidade, desempenho e correta integração ao processo de detecção e resposta;
- 14.4.1.3.6. Executar troubleshooting em Coletores, Virtual Appliances ou Script Hosts em caso de falha, com registro detalhado das ações corretivas adotadas;
- 14.4.1.4. Gerar relatório executivo mensal consolidando métricas, indicadores e status do serviço, evidenciando:
 - 14.4.1.4.1. Volume de eventos analisados;
 - 14.4.1.4.2. Tempo médio de resposta;
 - 14.4.1.4.3. Incidentes tratados automaticamente;
 - 14.4.1.4.4. Integrações realizadas com o processo de resposta a incidentes;
- 14.4.1.5. Implementar mecanismos de automação de resposta para contenção, erradicação e recuperação de incidentes, sempre em alinhamento com o processo de resposta a incidentes da CONTRATANTE;
- 14.4.1.6. Revisar periodicamente a eficácia das ações automatizadas, recomendando ajustes para melhoria contínua, considerando novas ameaças ou vetores identificados;
- 14.4.1.7. Garantir que todas as atividades de automação estejam registradas em trilhas de auditoria, com rastreabilidade de execução para fins de conformidade;
- 14.4.1.8. Realizar integração nativa ou via APIs com outras soluções de segurança do ambiente da CONTRATANTE, incluindo SIEM, SOAR, EDR/XDR, Firewalls e soluções de proteção de e-mail, assegurando a centralização e correlação dos eventos;
- 14.4.1.9. Atualizar periodicamente os playbooks de automação, de forma a incorporar novas técnicas de ataque, indicadores de comprometimento e boas práticas recomendadas por órgãos reguladores e entidades de referência em cibersegurança.

14.4.2. Grupo técnico de hiperautomação para detecção e resposta a ameaças

- 14.4.2.1. A CONTRATADA deverá manter o GRUPO TÉCNICO DE HIPERAUTOMAÇÃO PARA DETECÇÃO E RESPOSTA A AMEAÇAS com objetivo e foco de trabalhar no processo de gestão e resposta a incidentes.
- 14.4.2.2. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no CATÁLOGO DE SERVIÇO e IMR –



INSTRUMENTO DE MEDIÇÃO DE RESULTADOS do presente termo de referência.

14.4.2.3. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade, a CONTRATADA deverá, obrigatoriamente, compor os GRUPO TÉCNICO DE HIPERAUTOMAÇÃO PARA DETECÇÃO E RESPOSTA A AMEAÇAS, com 01 (um) profissionais para cada perfil que segue descrito abaixo:

Perfis	Certificações	Descrição
Analista de Segurança I	Certified in Cybersecurity – CC (ISC)	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de EDR. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.
Analista de Segurança II	Certified Ethical Hacker	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de EDR. Experiência comprovada de no mínimo 24 (vinte e quatro) meses em segurança da informação.
Analista III	Certificação da solução a ser utilizada no serviço	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de EDR. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.

14.4.2.4. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO TÉCNICO DE HIPERAUTOMAÇÃO PARA DETECÇÃO E RESPOSTA A AMEAÇAS, porém, conforme já foi mencionado neste termo de referência, este(s) deve(m) compor única e exclusivamente o time denominado GRUPO TÉCNICO DE HIPERAUTOMAÇÃO PARA DETECÇÃO E RESPOSTA A AMEAÇAS.

14.4.3. Entregas A Serem Realizadas

14.4.3.1. Para acompanhamento do serviço a ser ofertado pela CONTRATADA, os entregáveis abaixo deverão compor o relatório mensal a ser entregue pela CONTRATADA para acompanhamento da execução contratual:

INDICADOR	AGRUPADOR	DESCRIÇÃO
KPI-1	HIPERAUTOMAÇÃO PARA DETECÇÃO E RESPOSTA A AMEAÇAS	Quantidade de incidentes detectados em tempo real no período
KPI-2	HIPERAUTOMAÇÃO PARA DETECÇÃO E RESPOSTA A AMEAÇAS	Quantidade de ameaças classificadas por tipo (Malware, Phishing, C&C, Spam, Mining, etc.)
KPI-3	HIPERAUTOMAÇÃO PARA DETECÇÃO E RESPOSTA A AMEAÇAS	Percentual de incidentes correlacionados com múltiplas fontes de Threat Intelligence
KPI-4	HIPERAUTOMAÇÃO PARA DETECÇÃO E RESPOSTA A AMEAÇAS	Quantidade de consultas DNS maliciosas detectadas
KPI-5	HIPERAUTOMAÇÃO PARA DETECÇÃO E RESPOSTA A AMEAÇAS	Quantidade de conexões suspeitas detectadas em endpoints remotos e servidores
KPI-6	HIPERAUTOMAÇÃO PARA DETECÇÃO E RESPOSTA A AMEAÇAS	Quantidade de incidentes resolvidos automaticamente pela plataforma



KPI-7	HIPERAUTOMAÇÃO PARA DETECÇÃO E RESPOSTA A AMEAÇAS	Percentual de incidentes escalados para intervenção humana
KPI-8	HIPERAUTOMAÇÃO PARA DETECÇÃO E RESPOSTA A AMEAÇAS	Percentual de bloqueios automáticos bem-sucedidos por integração com fabricantes homologados
KPI-9	HIPERAUTOMAÇÃO PARA DETECÇÃO E RESPOSTA A AMEAÇAS	Percentual de incidentes enriquecidos com contexto (atores, TTPs, MITRE ATT&CK)
KPI-10	HIPERAUTOMAÇÃO PARA DETECÇÃO E RESPOSTA A AMEAÇAS	Quantidade de ativos monitorados (estações, servidores, IoT)
KPI-11	HIPERAUTOMAÇÃO PARA DETECÇÃO E RESPOSTA A AMEAÇAS	Percentual de agentes/coletores instalados em funcionamento e atualizados

14.4.3.2. Tais entregáveis, relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring). Nesse contexto, o profissional deve apresentá-lo de forma virtual, por meio de solução de videoconferência;

14.5. Processo de serviços gerenciados de firewall

14.5.1. Requisitos Gerais

14.5.1.1. O processo de administração dos firewalls deverá garantir a operação contínua, segura e eficiente da solução de segurança perimetral, abrangendo as atividades de configuração, monitoramento, atualização, suporte, gestão de mudanças e produção de relatórios, em conformidade com as melhores práticas de mercado e recomendações do fabricante.

14.5.1.2. O suporte técnico/operação deverá ser prestado 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, durante todo o período de vigência do contrato e o atendimento deverá ocorrer imediatamente após a abertura do chamado técnico, no qual deverá ser fornecido um número de registro de chamado técnico;

14.5.1.3. Consiste na operação das soluções ofertadas, a validação de configurações, aplicação de novas configurações, realização de atualizações de segurança, monitoramento proativo das soluções, atendimento das soluções, Health Check anuais;

14.5.1.4. Antes do início da operação, deverá ser conduzido um assessment detalhado do ambiente, contemplando, no mínimo:

14.5.1.4.1. Levantamento das informações técnicas dos firewalls e suas integrações;

14.5.1.4.2. Análise de políticas de segurança existentes, regras de acesso e rotas configuradas;

14.5.1.4.3. Identificação de vulnerabilidades, falhas de configuração e riscos associados;

14.5.1.4.4. Definição de matriz de compatibilidade e requisitos para continuidade da operação;



- 14.5.1.4.5. Elaboração de relatório diagnóstico com recomendações técnicas e plano de ação;
- 14.5.1.4.6. Homologação do planejamento junto à CONTRATANTE.
- 14.5.1.5. O serviço de operação deverá ser composto de um monitoramento 24x7 de todos os appliances e modelos que compõem a oferta do serviço, monitorando no mínimo os seguintes parâmetros:
 - 14.5.1.5.1. Disponibilidade de cada appliance;
 - 14.5.1.5.2. Performance dos appliances;
 - 14.5.1.5.3. Memória;
 - 14.5.1.5.4. CPU;
 - 14.5.1.5.5. Uptime;
 - 14.5.1.5.6. Data e horário dos alarmes.
- 14.5.1.6. O monitoramento deve enviar e-mail em regime 24x7 para ocorrência de alarmes de severidade crítica e alta;
- 14.5.1.7. Administrar os firewalls seguindo as melhores práticas do fabricante, assegurando o pleno funcionamento da solução e seus componentes;
- 14.5.1.8. Monitorar continuamente todos os dispositivos de firewall, incluindo logs, eventos de segurança e disponibilidade;
- 14.5.1.9. Manter os firewalls atualizados com a versão mais estável e homologada pelo fabricante;
- 14.5.1.10. Realizar health check mensal da plataforma, visando identificar falhas de configuração, vulnerabilidades ou ajustes necessários para elevação do nível de maturidade de segurança;
- 14.5.1.11. Executar a gestão de mudanças de forma estruturada, incluindo registro, análise, homologação e implementação aprovada em janelas de manutenção;
- 14.5.1.12. Apoiar na criação de rotinas de backup e restore da solução, incluindo cenários de recuperação de desastres;
- 14.5.1.13. Registrar e acompanhar chamados técnicos junto ao fabricante sempre que necessário;
- 14.5.1.14. Manter procedimentos operacionais atualizados relacionados à administração da solução;
- 14.5.1.15. Comunicar e solicitar apoio da equipe de segurança da CONTRATANTE em incidentes que demandem ações conjuntas;
- 14.5.1.16. Definir e aplicar políticas de segurança, NAT, QoS, VPN (client-to-site e site-to-site), PBF (Policy Based Forwarding) e integração com diretórios de usuários;
- 14.5.1.17. Tratar incidentes relacionados à solução de firewall, em alinhamento com o processo de resposta a incidentes da CONTRATANTE;
- 14.5.1.18. Monitorar periodicamente tendências de novas ameaças e vulnerabilidades aplicáveis aos firewalls, com recomendações de mitigação;
- 14.5.1.19. Enviar relatórios periódicos de ameaças identificadas, indicadores de



desempenho, SLA e plano de ação;

14.5.2. Grupo técnico de serviços gerenciados de firewall

14.5.2.1. A CONTRATADA deverá manter o GRUPO TÉCNICO DE GERENCIADOS DE FIREWALL com objetivo e foco de trabalhar no processo de gestão e resposta a incidentes.

14.5.2.2. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no CATÁLOGO DE SERVIÇO e IMR – INSTRUMENTO DE MEDIÇÃO DE RESULTADOS do presente termo de referência.

14.5.2.3. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade, a CONTRATADA deverá, obrigatoriamente, compor os GRUPO TÉCNICO DE GERENCIADOS DE FIREWALL, com 01 (um) profissionais para cada perfil que segue descrito abaixo:

Perfis	Certificações	Descrição
Analista de Segurança I	CCSA – CheckPoint Certified Security <u>ou</u> CCSE - CheckPoint Certified Security Expert <u>ou</u> Certified Forcepoint NGFW Administrator ITIL Foundation v4	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de NGFW – Next Generation Firewall. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.
Analista II	Certificação da solução a ser utilizada no serviço	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de NGFW – Next Generation Firewall. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.

14.5.2.4. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO TÉCNICO DE GERENCIADOS DE FIREWALL, porém, conforme já foi mencionado neste termo de referência, este(s) deve(m) compor única e exclusivamente o time denominado GRUPO TÉCNICO DE GERENCIADOS DE FIREWALL.

14.5.3. Entregas A Serem Realizadas

14.5.3.1. Para acompanhamento do serviço a ser ofertado pela CONTRATADA, os entregáveis abaixo deverão compor o relatório mensal a ser entregue pela CONTRATADA para acompanhamento da execução contratual:

INDICADOR	AGRUPADOR	DESCRIÇÃO
KPI-1	GESTÃO DE FIREWALLS	Configuração de política de segurança (L4/L7)
KPI-2	GESTÃO DE FIREWALLS	Aplicação de política de Threat Prevention (antivírus, anti-spyware/bot ou IPS)
KPI-3	GESTÃO DE FIREWALLS	Configurar integração com base de usuários (auth)
KPI-4	GESTÃO DE FIREWALLS	Aplicar controle de uso de aplicação por usuário/grupo de usuário
KPI-5	GESTÃO DE FIREWALLS	Configurar VPN client-to-site/site-to-site
KPI-6	GESTÃO DE FIREWALLS	Criação de rota ou correção de tráfego assimétrico
KPI-7	GESTÃO DE FIREWALLS	Configuração de PBF (Policy Based Forwarding)
KPI-8	GESTÃO DE FIREWALLS	Configuração de política de NAT
KPI-9	GESTÃO DE FIREWALLS	Aplicação de política de SSL Decryption



KPI-10	GESTÃO DE FIREWALLS	Aplicação de categoria de URL filtering baseada em usuário/grupo de usuário
KPI-11	GESTÃO DE FIREWALLS	Análise/criação de IOC (Indicator of Compromise)
KPI-12	GESTÃO DE FIREWALLS	Criação de assinatura customizada para identificação e controle de aplicação
KPI-13	GESTÃO DE FIREWALLS	Aplicação de políticas de QoS
KPI-14	GESTÃO DE FIREWALLS	Health Check (relatório de adoção de uso de boas práticas de config)

14.5.3.2. Tais entregáveis, relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring). Nesse contexto, o profissional deve apresentá-lo de forma virtual, por meio de solução de videoconferência;

14.6. Processo a serem executados serviço de proteção avançada contra ransomware

14.6.1. Requisitos gerais

14.6.1.1. Este processo abrange todos os dispositivos com XDR, incluindo estações de trabalho e servidores, e deverá ser executado em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano. As ações envolvem desde a gestão da solução até a resposta e remediação contínua de incidentes. A CONTRATADA deverá executar minimamente as ações abaixo:

14.6.1.2. Atuar em conjunto com o GRUPO DE SERVIÇO DE RESPOSTA A INCIDENTES para executar ações de contenção, erradicação e recuperação conforme necessário;

14.6.1.3. Identificar endpoints sem comunicação e notificar a CONTRATANTE para atuação;

14.6.1.4. Realizar a instalação de Agentes para que todos os novos endpoints, para essa atividade poderá ser utilizado GPOs;

14.6.1.5. Verificar se todos os agentes XDR estão com a versão mais estável;

14.6.1.6. Revisar alertas e eventos de segurança capturados pelo XDR;

14.6.1.7. Realizar o isolamento de endpoints infectados, se necessário, para evitar propagação de ameaças;

14.6.1.8. Remover endpoint do isolamento depois das tratativas de contenção e limpeza;

14.6.1.9. Realizar varreduras completas em endpoints sempre que necessário;

14.6.1.10. Revisar e atualizar mensalmente as políticas de detecção e resposta baseadas em novas ameaças;

14.6.1.11. Garantir a integração contínua entre o XDR e o sistema de SIEM, alimentando os dados de eventos de segurança;

14.6.1.12. Realizar auditoria dos logs gerados pelo XDR mensalmente, verificando consistência e integridade;



- 14.6.1.13. Configurar alertas para incidentes críticos e monitorar o tempo de resposta;
- 14.6.1.14. Monitorar atividades de zero-day e aplicar mitigação quando necessário;
- 14.6.1.15. Revisar a taxa de falsos positivos e ajustar as regras de detecção para minimizar interrupções;
- 14.6.1.16. Gerar relatórios mensais para a alta gestão sobre o status de segurança dos endpoints;
- 14.6.1.17. Rever acessos à console administrativa do XDR, garantindo que apenas pessoal autorizado tenha permissão;
- 14.6.1.18. Revisar incidentes passados e garantir que lições aprendidas sejam aplicadas em futuras respostas;
- 14.6.1.19. Avaliar mensalmente a eficácia do processo de gestão do XDR e propor melhorias.

14.6.2. Grupo técnico Extended Detection and Response

- 14.6.2.1. A CONTRATADA deverá manter o GRUPO TÉCNICO ENDPOINT DETECTION AND RESPONSE com objetivo e foco de trabalhar no processo de gestão e resposta a incidentes.
- 14.6.2.2. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no CATÁLOGO DE SERVIÇO e IMR – INSTRUMENTO DE MEDIÇÃO DE RESULTADOS do presente termo de referência.
- 14.6.2.3. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade, a CONTRATADA deverá, obrigatoriamente, compor os GRUPO TÉCNICO ENDPOINT DETECTION AND RESPONSE, com 01 (um) profissional para cada perfil que segue descrito abaixo:

Perfis	Certificações	Descrição
Analista de Segurança I	Certified in Cybersecurity – CC (ISC)	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de EDR. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.
Analista de Segurança II	Certified Ethical Hacker	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de EDR. Experiência comprovada de no mínimo 24 (vinte e quatro) meses em segurança da informação.
Analista III	Certificação da solução a ser utilizada no serviço	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de EDR. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.

- 14.6.2.4. Todos os profissionais deverão possuir diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);



14.6.2.5. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO TÉCNICO ENDPOINT DETECTION AND RESPONSE, porém, conforme já foi mencionado neste termo de referência, este(s) deve(m) compor única e exclusivamente o time denominado GRUPO TÉCNICO ENDPOINT DETECTION AND RESPONSE.

14.6.3. Entregas A Serem Realizadas

14.6.3.1. Para acompanhamento do serviço a ser ofertado pela CONTRATADA, os entregáveis abaixo deverão compor o relatório mensal a ser entregue pela CONTRATADA para acompanhamento da execução contratual:

INDICADOR	AGRUPADOR	DESCRIÇÃO
KPI-1	XDR	Soma endpoints infectados
KPI-2	XDR	Soma ameaças por mecanismo de detecção
KPI-3	XDR	Soma das ameaças por tipo
KPI-4	XDR	Quantidade de Agentes Instalados
KPI-5	XDR	Quantidade de Agentes por versão
KPI-6	XDR	Quantidade de dispositivos por Sistema Operacional
KPI-7	XDR	Quantidade de aplicações potencialmente vulneráveis por criticidade
KPI-8	XDR	Quantidade de ameaças detectadas nos últimos 7 dias
KPI-9	XDR	Quantidade de ameaças por nível de severidade

14.6.3.2. Tais entregáveis, relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring). Nesse contexto, o profissional deve apresentá-lo de forma virtual, por meio de solução de videoconferência;

14.7. Processo a serem executados serviço de proteção de e-mail, conscientização e proteção contra vazamento de informações

14.7.1. Requisitos gerais

14.7.1.1. A solução de segurança de e-mail deverá oferecer monitoramento e gerenciamento contínuos, em regime 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, abrangendo todas as caixas de correio corporativas. Isso inclui o acompanhamento do correto funcionamento da plataforma (console, serviços, componentes e licenças).

14.7.1.2. O prestador deverá executar configurações na solução, incluindo ajuste de console, autenticação, integrações, backups, módulos de filtragem e atualização de componentes.

14.7.1.3. Deverá ser fornecida análise de mensagens sob demanda, com classificação de e-mails suspeitos (spam, phishing, malware, falsos positivos) e tratamento de incidentes relacionados.

14.7.1.4. A administração de acessos deverá contemplar a criação e alteração de perfis de usuários, papéis e permissões, conforme solicitação da CONTRATANTE.

14.7.1.5. A CONTRATADA deverá criar, revisar e ajustar políticas de segurança de e-mail (antispam, phishing, DLP, reputação de IPs e URLs) em conjunto com a



CONTRATANTE, alinhadas às melhores práticas do mercado.

- 14.7.1.6. O serviço deverá realizar a aprovação ou liberação de mensagens retidas em quarentena e o bloqueio de remetentes ou domínios maliciosos conforme necessidade.
- 14.7.1.7. Deverá ser realizada a implantação de novos componentes ou módulos da solução sempre que houver expansão ou atualização, garantindo que todos os servidores, gateways ou serviços de e-mail estejam cobertos.
- 14.7.1.8. O processo deverá incluir Health Check da plataforma três vezes por semana, abrangendo a análise de mensagens entregues via log de auditoria, verificação de bloqueios (DNS, fila de SMTP), análise de phishing, spam e falso positivo, bloqueio de mensagens maliciosas e revisão de protocolos (Good Sender, Bad Sender, Transparent User), reputação de IPs e URLs, cabeçalhos, DKIM, PTR, SPF e destinatários inválidos.
- 14.7.1.9. A cada trimestre deverá ser realizado Health Check completo da plataforma, com avaliação das configurações e elaboração de relatórios contendo recomendações de melhoria.
- 14.7.1.10. A CONTRATADA deverá atuar em conjunto com o Grupo de Resposta a Incidentes para executar ações de contenção, erradicação e recuperação de incidentes de e-mail, integrando a solução de e-mail à plataforma XDR e SIEM para correlação de eventos e resposta orquestrada.
- 14.7.1.11. Deverá identificar caixas de correio ou servidores de e-mail sem comunicação com a solução e notificar a CONTRATANTE para correção imediata.
- 14.7.1.12. A CONTRATADA deverá verificar periodicamente se todos os componentes da solução de segurança de e-mail (módulos de filtragem, assinaturas de ameaças, licenças e firmware) estão atualizados e na versão mais estável.
- 14.7.1.13. A revisão de alertas e eventos gerados pela solução deverá ser contínua, contemplando investigações de e-mails classificados como spam, phishing ou malware e outras violações de políticas. Os eventos suspeitos deverão ser escalados ao time de resposta à incidentes quando necessário.
- 14.7.1.14. Quando detectadas ameaças, a solução deverá permitir o isolamento ou bloqueio de remetentes, domínios ou fluxos de mensagens para evitar a propagação de ataques; após a remediação, a CONTRATADA deverá restaurar o fluxo normal de e-mails.
- 14.7.1.15. Deverão ser realizadas varreduras completas de mensagens e logs, assim como avaliações de reputação de IP e URL, sempre que surgirem alertas de ameaças ou por solicitação da CONTRATANTE.
- 14.7.1.16. A ferramenta de segurança de e-mail deverá possibilitar integração nativa com as soluções de XDR e SIEM que vierem a ser selecionadas pela CONTRATANTE no certame, garantindo correlação de dados entre e-mail, rede e endpoints. Essa integração deverá ocorrer de forma oficial entre os fabricantes, assegurando visibilidade centralizada, bem como respostas automatizadas e coordenadas a incidentes.

14.7.2. Grupo técnico de segurança avançada de e-mail e conscientização



14.7.2.1. A CONTRATADA deverá manter o GRUPO TÉCNICO DE SEGURANÇA AVANÇADA DE E-MAIL E CONSCIENTIZAÇÃO com objetivo e foco de trabalhar no processo de gestão e resposta a incidentes.

14.7.2.2. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no CATÁLOGO DE SERVIÇO e IMR – INSTRUMENTO DE MEDIÇÃO DE RESULTADOS do presente termo de referência.

14.7.2.3. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade, a CONTRATADA deverá, obrigatoriamente, compor os GRUPO TÉCNICO DE PREVENÇÃO CONTRA PERDA DE DADOS, com 01 (um) profissional para cada perfil que segue descrito abaixo:

Perfis	Certificações	Descrição
Analista I	Certificação da solução a ser utilizada no serviço de segurança de E-MAIL	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de E-MAIL. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.
Analista II	Certificação da solução a ser utilizada no serviço de CONSCIENTIZAÇÃO	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de CONSCIENTIZAÇÃO. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.

14.7.2.4. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO TÉCNICO DE SEGURANÇA AVANÇADA DE E-MAIL E CONSCIENTIZAÇÃO, porém, conforme já foi mencionado neste termo de referência, este(s) deve(m) compor única e exclusivamente o time denominado GRUPO TÉCNICO DE SEGURANÇA AVANÇADA DE E-MAIL E CONSCIENTIZAÇÃO.

14.8. Processo do serviço prevenção contra perda de dados

14.8.1. Requisitos gerais

14.8.1.1. Este processo abrange todos os dispositivos com serviço de DLP, incluindo estações de trabalho e notebooks e deverá ser executado em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano. As ações envolvem desde a gestão da solução até a resposta e remediação contínua de incidentes. A CONTRATADA deverá executar minimamente as ações abaixo:

14.8.1.1.1. Atuar em conjunto com o GRUPO DE SERVIÇO DE RESPOSTA A INCIDENTES para executar ações de contenção conforme necessário;

14.8.1.1.2. Revisar e definir as políticas de proteção a serem aplicadas com base nos dados sensíveis identificados;

14.8.1.1.3. Monitorar e restringir a movimentação de arquivos críticos por canais não autorizados;

14.8.1.1.4. Definir alertas automáticos para violações das políticas de DLP;

14.8.1.1.5. Configurar ações automáticas de bloqueio para violações críticas de políticas de DLP;



- 14.8.1.1.6. Realizar auditoria dos logs na gerência do DLP;
- 14.8.1.1.7. Emitir relatórios sobre incidentes detectados;
- 14.8.1.1.8. Realizar testes de efetividade das políticas DLP implantadas;
- 14.8.1.1.9. Verificar a integração do DLP com soluções complementares SIEM;
- 14.8.1.1.10. Ajustar políticas com base em novos tipos de ameaças ou regras de negócio da SEFAZ-ES;
- 14.8.1.1.11. Validar que as políticas DLP estejam em conformidade com LGPD;
- 14.8.1.1.12. Configurar e revisar mensalmente lista de exceções de dados que não precisam seguir as políticas padrão;
- 14.8.1.1.13. Implementar monitoramento contínuo de tentativas de acesso não autorizadas;
- 14.8.1.1.14. Revisar mensalmente as permissões e privilégios de acesso de usuários na gerência;
- 14.8.1.1.15. Atualizar periodicamente a solução DLP com a última versão estável;
- 14.8.1.1.16. Estabelecer fluxos de escalonamento de incidentes graves para a alta gestão;
- 14.8.1.1.17. Verificar se as regras de contenção e bloqueio estão atuando conforme planejado;
- 14.8.1.1.18. Elaborar relatórios para a alta administração, sempre que solicitado.

14.8.2. Grupo técnico de prevenção contra perda de dados

- 14.8.2.1. A CONTRATADA deverá manter o GRUPO TÉCNICO DE PREVENÇÃO CONTRA PERDA DE DADOS com objetivo e foco de trabalhar no processo de gestão e resposta a incidentes.
- 14.8.2.2. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no CATÁLOGO DE SERVIÇO e IMR – INSTRUMENTO DE MEDIÇÃO DE RESULTADOS do presente termo de referência.
- 14.8.2.3. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade, a CONTRATADA deverá, obrigatoriamente, compor os GRUPO TÉCNICO DE PREVENÇÃO CONTRA PERDA DE DADOS, com 01 (um) profissional para cada perfil que segue descrito abaixo:

Perfis	Certificações	Descrição
Analista I	Certificação da solução a ser utilizada no serviço	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de DLP. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.

- 14.8.2.4. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO TÉCNICO DE PREVENÇÃO



CONTRA PERDA DE DADOS, porém, conforme já foi mencionado neste termo de referência, este(s) deve(m) compor única e exclusivamente o time denominado GRUPO TÉCNICO DE PREVENÇÃO CONTRA PERDA DE DADOS.

14.8.3. Entregas A Serem Realizadas

14.8.3.1. Para acompanhamento do serviço a ser ofertado pela CONTRATADA, os entregáveis abaixo deverão compor o relatório mensal a ser entregue pela CONTRATADA para acompanhamento da execução contratual;

INDICADOR	AGRUPADOR	DESCRIÇÃO
KPI-1	DLP	Quantidade de Endpoints Instalados
KPI-2	DLP	Quantidade de incidentes de DLP monitorados
KPI-3	DLP	Quantidade de incidentes de DLP bloqueados
KPI-4	DLP	Quantidade de tentativas de acesso ou envio a dados não autorizados
KPI-5	DLP	Quantidade de Incidentes por tipo e/ou regra
KPI-6	E-MAIL	Quantidade de mensagens classificadas como spam bloqueadas pela solução
KPI-7	E-MAIL	Quantidade de mensagens de phishing detectadas e bloqueadas
KPI-8	E-MAIL	Taxa de falsos positivos identificados e tratados
KPI-9	E-MAIL	Quantidade de mensagens liberadas da quarentena após revisão
KPI-10	E-MAIL	Quantidade de incidentes de malware identificado em anexos
KPI-11	E-MAIL	Percentual de mensagens analisadas em relação ao total de mensagens recebidas
KPI-12	E-MAIL	Quantidade de Health Checks realizados e relatórios entregues
KPI-13	CONSCIENTIZAÇÃO	Quantidade de campanhas de phishing simulado realizadas
KPI-14	CONSCIENTIZAÇÃO	Percentual de usuários que clicaram em links de phishing simulado
KPI-15	CONSCIENTIZAÇÃO	Percentual de usuários que reportaram corretamente tentativas de phishing
KPI-16	CONSCIENTIZAÇÃO	Evolução do índice de maturidade de conscientização em segurança (antes x depois das campanhas)

14.8.3.2. Tais entregáveis, relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring). Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências da SEFAZ-ES ou de forma virtual, por meio de solução de videoconferência;

14.9. Processo a serem executados serviço de microssegmentação de rede

14.9.1. Requisitos Gerais

14.9.1.1. A CONTRATADA deverá configurar a solução para fornecer visibilidade completa do tráfego de rede em tempo real, mostrando todas as comunicações entre os ativos protegidos.

14.9.1.2. Deverá implementar o mapeamento automático de dependências de aplicações, identificando quais processos do sistema operacional são responsáveis por cada comunicação de rede.

14.9.1.3. A CONTRATADA deverá criar e implementar políticas de microssegmentação baseadas em rótulos e atributos dos ativos (origem, destino, porta, protocolo, aplicação e processos).

14.9.1.4. Deverá configurar políticas utilizando os templates nativos da solução para serviços como Active Directory, SQL Server, SharePoint, Exchange e outros.



- 14.9.1.5. Deverá configurar políticas de isolamento para ativos comprometidos, restringindo sua comunicação apenas ao previamente definido.
- 14.9.1.6. Deverá realizar análise de impacto antes da aplicação de modificações nas políticas, garantindo que não haverá interrupção de serviços críticos.
- 14.9.1.7. A CONTRATADA deverá configurar o enforcement de políticas através da orquestração dos firewalls nativos dos sistemas operacionais, sem criar camadas adicionais.
- 14.9.1.8. Deverá implementar a orquestração do Windows Filtering Platform para dispositivos Windows e do IP Tables para dispositivos Linux.
- 14.9.1.9. Deverá configurar regras de inbound e outbound nos firewalls dos ativos protegidos.
- 14.9.1.10. A CONTRATADA deverá realizar a integração nativa com o scanner de vulnerabilidade presente neste edital para controle contextual baseado em vulnerabilidades.
- 14.9.1.11. Deverá integrar a solução com o Active Directory para controle de regras baseado em grupos do AD.
- 14.9.1.12. A CONTRATADA deverá configurar o sistema de sugestões inteligentes para criação de regras baseadas nos fluxos detectados.
- 14.9.1.13. Deverá configurar proteção por senha para prevenir remoção acidental ou proposital dos agentes.
- 14.9.1.14. Deverá implementar o monitoramento contínuo das regras aplicadas com proteção anti-tampering.
- 14.9.1.15. Deverá configurar a retenção de políticas para permitir rollback quando necessário.

14.9.2. Grupo técnico de microssegmentação de rede

- 14.9.2.1. A CONTRATADA deverá manter o GRUPO TÉCNICO DE MICROSSEGMENTAÇÃO DE REDE com objetivo e foco de trabalhar no processo de gestão e resposta a incidentes.
- 14.9.2.2. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no CATÁLOGO DE SERVIÇO e IMR – INSTRUMENTO DE MEDIÇÃO DE RESULTADOS do presente termo de referência.
- 14.9.2.3. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade, a CONTRATADA deverá, obrigatoriamente, compor os GRUPO TÉCNICO DE MICROSSEGMENTAÇÃO DE REDE, com 01 (um) profissional para cada perfil que segue descrito abaixo:

Perfis	Certificações	Descrição
Analista de Segurança I	ISO27001	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de NAC – Network Access Control. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.
Analista II	Certificação da solução a	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de



	ser utilizada no serviço	NAC – Network Access Control. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.
--	--------------------------	--

14.9.2.4. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO TÉCNICO CONTROLE DE ACESSO A REDE, porém, conforme já foi mencionado neste termo de referência, este(s) deve(m) compor única e exclusivamente o time denominado GRUPO TÉCNICO CONTROLE DE ACESSO À REDE.

14.9.3. Entregas A Serem Realizadas

14.9.3.1. Para acompanhamento do serviço a ser ofertado pela CONTRATADA, os entregáveis abaixo deverão compor o relatório mensal a ser entregue pela CONTRATADA para acompanhamento da execução contratual:

INDICADOR	AGRUPADOR	DESCRIÇÃO
KPI-1	MICROSEGMENTAÇÃO	Quantidade de workloads/ativos descobertos e inventariados pela solução
KPI-2	MICROSEGMENTAÇÃO	Percentual de workloads protegidos em relação ao total descoberto
KPI-3	MICROSEGMENTAÇÃO	Quantidade de aplicações críticas mapeadas com dependências visíveis
KPI-4	MICROSEGMENTAÇÃO	Quantidade de políticas de segmentação aplicadas com sucesso
KPI-5	MICROSEGMENTAÇÃO	Percentual de políticas aplicadas sem erros em relação ao total publicado
KPI-6	MICROSEGMENTAÇÃO	Quantidade de tentativas de comunicação lateral (East-West) bloqueadas
KPI-7	MICROSEGMENTAÇÃO	Quantidade de conexões de tráfego não autorizado detectadas
KPI-8	MICROSEGMENTAÇÃO	Percentual de tráfego permitido vs. tráfego bloqueado por políticas
KPI-9	MICROSEGMENTAÇÃO	Quantidade de incidentes mitigados por contenção automática
KPI-10	MICROSEGMENTAÇÃO	Quantidade de workloads isolados em incidentes de segurança
KPI-11	MICROSEGMENTAÇÃO	Quantidade de workloads com agentes instalados e em comunicação
KPI-12	MICROSEGMENTAÇÃO	Percentual de workloads com agentes atualizados na versão mais estável

14.9.3.2. Tais entregáveis, relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring). Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências da SEFAZ-ES ou de forma virtual, por meio de solução de videoconferência;

14.10. Processo a serem executados no serviço operação e resposta a requisição

14.10.1. Requisitos Gerais

14.10.1.1. A fim de balizar todo o processo de cumprimento de requisição de serviço da SEFAZ-ES, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir *ipsis litteris*.

14.10.1.2. Ao receber uma solicitação de requisição de serviço via e-mail, telefone ou Whatsapp, de funcionários autorizados da SEFAZ-ES, o analista da central de serviços



deve registrar ou complementar as informações da requisição.

- 14.10.1.3. Para requisições de serviços abertas via web, o sistema de ITSM do inglês Information Technology Service Management, deve automaticamente realizar o registro da requisição de serviço.
- 14.10.1.4. Quando o requisitante realiza a requisição através de e-mail ou telefone, o analista da central de serviços, deve após registrar ou complementar a requisição, fazer a categorização e priorização da requisição de serviços.
- 14.10.1.5. A categorização deve ser realizada pelo analista da central de serviços relacionado o item de configuração, com o seu grupo definido no CATÁLOGO DE SERVIÇO do presente termo. As demais informações levantadas devem ser documentadas na requisição de serviço.
- 14.10.1.6. Quando o meio de solicitação for via web o sistema de ITSM deve realizar a categorização e priorização da requisição de serviço automaticamente, obedecendo às mesmas regras seguidas pelo processo de registro via e-mail ou telefone.
- 14.10.1.7. A priorização deve ser realizada de acordo com as regras de negócio estabelecidas no presente termo.
- 14.10.1.8. Caso o analista da central de serviços não identifique o serviço solicitado como um item do catálogo de serviço, deverá este informar ao solicitante sobre sua inexistência. Na sequência o analista deve registrar uma solicitação de novo serviço ou modificação em serviço existente, que deve ser tratada pelo processo de gerenciamento de portfólio da CONTRATADA.
- 14.10.1.9. Uma vez identificado que o serviço requisitado consta no catálogo de serviços, e está disponível, o analista da central de serviços deve verificar se o serviço precisa ou não de aprovação para ser executado. Caso seja necessário, o analista deve submeter a requisição a um grupo aprovador.
- 14.10.1.10. O sistema de ITSM deve identificar automaticamente se o serviço é ou não elegível em primeiro nível, conforme configurado no catálogo de serviços.
- 14.10.1.11. Caso o serviço seja elegível para primeiro nível, o analista da central de serviço deverá atuar, desde que exista procedimento pré-estabelecido e aprovado pela SEFAZ-ES.
- 14.10.1.12. É de responsabilidade da CONTRATADA manter uma base de conhecimento, como todos os procedimentos pré-estabelecidos e aprovados pela SEFAZ-ES. Tal base de conhecimento deve fazer parte do sistema de ITSM, e a qualquer tempo está acessível à SEFAZ-ES para consultas e aprovações de novos procedimentos.
- 14.10.1.13. Também é de responsabilidade da CONTRATADA a criação, revisão, manutenção, de tais procedimentos operacionais, sendo de responsabilidade da SEFAZ-ES apenas participar como aprovador sempre que um procedimento for criado, e/ou sofre algum tipo de alteração.
- 14.10.1.14. Caso a solução da requisição de serviço dependa da atuação de um terceiro fornecedor da SEFAZ-ES, o analista deve comunicar ao requisitante o status da requisição de serviço (pendente fornecedor), e o prazo previsto para o seu cumprimento. Nesse caso, a contagem do acordo de nível de serviço (SLA) é interrompido.



- 14.10.1.15. O analista da central de serviços que atuou no cumprimento da requisição deve fazer o registro da sua atuação, descrevendo informações relevantes para o cumprimento daquele serviço em particular.
- 14.10.1.16. Em caso de solução, o analista da central de serviços que atuou no cumprimento da requisição deve registrar no sistema de ITSM que a requisição de serviço foi resolvida, devendo: Informar o(s) item(ns) de configuração envolvido(s) com a requisição; e corrigir a categorização da requisição de serviços, se necessário.
- 14.10.1.17. O analista da central de serviços, ao identificar que a requisição não é elegível em primeiro nível, deve encaminhá-la para o grupo solucionador indicado. Esse encaminhamento poderá ser automático, quando o grupo solucionador e a elegibilidade do serviço estiverem determinados no catálogo de serviços. Ao receber uma requisição de serviço, o grupo solucionador deve analisá-la para verificar se compete ao grupo ou se deve ser encaminhada a outro grupo solucionador e, se para atendê-la, será necessária uma mudança.
- 14.10.1.18. Ao identificar que uma requisição de serviços encaminhada para a fila do grupo não faz parte do seu escopo, o analista do grupo solucionador deve direcioná-la ao grupo mais indicado para atender a requisição. Se compete ao grupo solucionador, esse atua no cumprimento da requisição.
- 14.10.1.19. Caso seja necessária uma mudança para executar o serviço requisitado, o fluxo segue para o processo gerenciar mudanças. A governança sobre processo de gestão de mudança não pertence ao objeto deste termo, a CONTRATADA apenas participa quando convocada do processo gestão de mudança já estabelecido pela SEFAZ-ES.
- 14.10.1.20. Se ao buscar atender à requisição de serviço o grupo solucionador identificar que para seu atendimento é necessário direcionar a solicitação a um fornecedor externo (de serviços ou de infraestrutura), deve acionar o fornecedor conforme as regras que serão estabelecidas pela SEFAZ-ES.
- 14.10.1.21. Nesse ponto, o status do chamado no sistema de ITSM deve ser atualizado para "encaminhado para fornecedor" e ficará aguardando seu retorno.
- 14.10.1.22. O registro da requisição de serviço na ferramenta do fornecedor, quando for o caso, deve ser documentado no registro da requisição no sistema de ITSM da CONTRATADA. Caberá ao grupo solucionador acompanhar e monitorar o fornecedor no atendimento da solicitação.
- 14.10.1.23. Cabe ao grupo solucionador avaliar e validar a entrega efetuada pelo fornecedor. São elementos de controle de qualidade e desempenho dessa atividade os níveis mínimos de serviço ou as regras definidas no instrumento contratual, edital de licitação e termo de referência.
- 14.10.1.24. O grupo que atuou no cumprimento da requisição de serviço deve fazer o registro da sua atuação no sistema de ITSM, descrevendo as informações relevantes para o cumprimento daquele serviço em particular.
- 14.10.1.25. Em caso de solução o grupo que atuou no cumprimento da requisição deve registrar no sistema de ITSM que a requisição de serviço foi resolvida, devendo: Informar o(s) item(ns) de configuração envolvido(s) com a requisição; e corrigir a categorização da requisição de serviços, se necessário.



14.10.1.26. Após ser resolvida, a requisição de serviço deve ficar por 3 (três) dias corridos com status igual a resolvido, podendo ser reaberta pela SEFAZ-ES no determinado período, caso este entenda que tal requisição não foi resolvida de fato. Ao final de 3 (três) dias corridos, caso não haja nenhuma intervenção da SEFAZ-ES, a requisição deverá ser alterada para o status fechado.

14.10.1.27. A CONTRATANTE poderá se entender como melhor prática utilizar a ferramenta de ITSM da SEFAZ-ES.

14.10.1.28. Os serviços serão executados em regime 24x7 por equipe da CONTRATADA de maneira remota.

14.10.2. Grupo técnico de operações e resposta a requisições

14.10.2.1. A CONTRATADA deverá manter uma torre de operação denominada GRUPO TÉCNICO DE OPERAÇÕES E RESPOSTA A REQUISIÇÕES.

14.10.2.2. A fim de garantir que os profissionais envolvidos têm conhecimento e habilidade, para executar o processo de resposta a requisições da SEFAZ-ES, a CONTRATADA obrigatoriamente deverá compor o GRUPO TÉCNICO DE OPERAÇÕES E RESPOSTA A REQUISIÇÕES, com os perfis descritos abaixo:

Perfil	Certificações	Descrição
Analista I	CCSA – CheckPoint Certified Security <u>ou</u> CCSE - CheckPoint Certified Security Expert <u>ou</u> Certified Forcepoint NGFW Administrator ITIL Foundation v4	Conhecimento avançado em segurança da informação, e infraestrutura com experiência em operação, sustentação e suporte a ambientes similares ao supracitado. Experiência comprovada de no mínimo 3 (três) ano em segurança da informação.
Analista II	CompTIA Security+ CompTIA Cysa+	Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.

14.10.3. Entregas A Serem Realizadas

14.10.3.1. Para acompanhamento do serviço a ser ofertado pela CONTRATADA, os entregáveis abaixo deverão compor o relatório mensal a ser entregue pela CONTRATADA para acompanhamento da execução contratual:

INDICADOR	AGRUPADOR	DESCRIÇÃO
KPI-1	Grupo técnico de operações e resposta a requisições	Número total de requisições abertas
KPI-2	Grupo técnico de operações e resposta a requisições	Número total de requisições por função
KPI-3	Grupo técnico de operações e resposta a requisições	Número total de requisições concluídas
KPI-4	Grupo técnico de operações e resposta a requisições	TOP do número de requisições por ativo
KPI-5	Grupo técnico de operações e resposta a requisições	TOP do número de requisições por origem
KPI-6	Grupo técnico de operações e resposta a requisições	TOP 10 requisições por aplicações

14.10.3.2. Tais entregáveis, relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring). Nesse contexto, o profissional deve apresentá-lo de forma virtual, por meio de solução de videoconferência;



14.11. Processo a serem executados no serviço gestão de disponibilidade

14.11.1. Requisitos gerais

14.11.1.1. O serviço de gestão de disponibilidade deverá ser executado em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano e contemplar, no mínimo, as seguintes atividades:

14.11.1.1.1. Ativação do monitoramento dos ativos constantes na relação de ativos críticos da SEFAZ-ES;

14.11.1.1.2. Como primeiro e importante passo do processo em questão, se dará na inclusão de todos os itens de configuração e seus devidos componentes (CPU, memória, interfaces de redes, disco) nas soluções de monitoramento. Será de responsabilidade da CONTRATADA tal inclusão, e as configurações necessárias nos itens de configurações para o perfeito monitoramento.

14.11.1.1.3. A SEFAZ-ES informará quais são os ativos críticos que devem ser monitorados pela CONTRATADA.

14.11.1.1.4. Após a inclusão dos itens de configuração nas soluções de monitoramento, a CONTRATADA deverá manter o monitoramento contínuo durante 60 (sessenta) dias, a fim de construir uma linha de base de tal ambiente.

14.11.1.1.5. Após os 60 (sessenta) dias de monitoramento contínuo e ininterrupto, entende-se que será possível identificar comportamentos anômalos do ambiente. Baseado em tal monitoramento deverá a CONTRATADA construir uma linha de base de alertas a serem gerados, quando alguma anomalia relacionada a disponibilidade, performance ou capacidade, for detectada pelas soluções de monitoramento.

14.11.1.1.6. A linha de base deve relacionar cada alerta, com um procedimento denominado Instrução de Trabalho. A instrução de trabalho deve conter o procedimento a ser realizado para solucionar o problema informado pelo alerta em questão. Tais instruções de trabalho devem pertencer ao processo de gestão de conhecimento da CONTRATADA, logo deverão ser geridas através do sistema de ITSM relacionado no tópico SOBRE O SISTEMA DE ITSM A SER UTILIZADO do presente termo de referência. Deverá tais instruções de trabalho estarem acessíveis à SEFAZ-ES a qualquer tempo, a fim de participar consultivamente na criação e no processo de aprovação de tais instruções de trabalho.

14.11.1.1.7. Cada alerta deverá ser classificado com uma das severidades, a saber:

- P1: Interrupção total do funcionamento do item de configuração.
- P2: Baixa performance do item de configuração.

14.12. Grupo técnico de gestão de disponibilidade

14.12.1. A CONTRATADA deverá manter uma torre de operação denominada GRUPO DE GESTÃO DE DISPONIBILIDADE, com objetivo e foco de trabalhar no processo de gestão de disponibilidade.

14.12.2. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo



de nível de serviço estabelecido no item Gestão de disponibilidade do presente termo de referência.

- 14.12.3. A fim de garantir que os profissionais envolvidos têm conhecimento e habilidade, para executar o processo de gestão de disponibilidade da SEFAZ-ES, a CONTRATADA obrigatoriamente deverá compor o GRUPO DE GESTÃO DE DISPONIBILIDADE, com ao menos 1 (um) perfil descrito abaixo:

Certificações	Descrição
ISO 27001	Conhecimento avançado em segurança da informação, com experiência em operação, sustentação e suporte a ambientes similares ao supracitado. Experiência comprovada de no mínimo 1 (um) ano em segurança da informação.

14.13. Entregas A Serem Realizadas

- 14.13.1. Os entregáveis devem ser do tipo dashboard em tempo real;

- 14.13.2. Para acompanhamento do serviço a ser ofertado, a CONTRATADA deverá disponibilizar dashboard com no mínimo os seguintes KPIs abaixo listados:

INDICADOR	AGRUPADOR	DESCRIÇÃO
KPI-1	Gestão de Disponibilidade	Dashboard para dispositivos de Firewall, contendo: Disponibilidade ping, Consumo de memória, Consumo de CPU, Consumo de link, Perda de Pacote, Tempo de resposta, Picos de UPLOAD e DOWNLOAD.
KPI-2	Gestão de Disponibilidade	Dashboard para links de dados: Qtd. de links monitorados, Qtd. Link UP, Qtd Link DOW, porcentagem de uso de cada link, UPLOAD E DOWNLOAD por link.
KPI-3	Gestão de Disponibilidade	Dashboard para URLs: Tempo de resposta da URL, Disponibilidade, Indisponibilidade.
KPI-4	Gestão de Disponibilidade	Dashboard para Servidores: Disponibilidade Ping, Tempo de Uptime, gráfico de entrada e saída de tráfego de rede, Porcentagem de uso CPU, Porcentagem de uso memória, porcentagem de uso Disco.
KPI-5	Gestão de Disponibilidade	Dashboard de alarmes: Nome do Host, Severidade do alarme, descrição do problema, e hora do alarme.
KPI-6	Gestão de Disponibilidade	Dashboard geral: TOP 10 Consumo de memória, TOP 10 Consumo de disco, TOP consumo de CPU, TOP tempo de resposta, TOP perda de pacotes, Mapa com o estado de cada localidade, Alerta para dispositivos fora de serviço ou sem comunicação.
KPI-7	Gestão de Disponibilidade	Dashboard Monitoramento Nutanix – Parâmetros de informação da saúde e disponibilidade do ambiente Nutanix.

- 14.13.3. Tais entregáveis e indicadores devem ser discutidos em reunião mensal, com presença de profissional que conheça todos os serviços e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring). Nesse contexto, o profissional deve apresentá-lo de forma virtual, por meio de solução de videoconferência;

SERVIÇOS DE MONITORAMENTO DA ADOÇÃO ÀS MELHORES PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

15. ELABORAÇÃO DO RELATÓRIO DE GESTÃO DE VULNERABILIDADE - PGV

15.1. Requisitos gerais

- 15.1.1. O Serviço de Monitoramento de Vulnerabilidades deverá ser executado obrigatoriamente em duas fases distintas e complementares:



- 15.1.1.1. Fase Pontual - que consiste na estruturação inicial completa do programa, incluindo a elaboração do Relatório de Gestão de Vulnerabilidades (PGV), realização da Análise de Impacto nos Negócios (BIA) e elaboração do Relatório de Respostas à Incidentes (PRI), avaliação de maturidade e assessment do ambiente atual, desenvolvimento do roadmap estratégico e projeto de transformação dos processos e ferramentas;
- 15.1.1.2. Fase Continuada - que compreende a operacionalização do programa estabelecido, para monitoramento contínuo, gestão do ciclo de vida das vulnerabilidades, atualização periódica dos processos e indicadores.
- 15.1.2. A Fase Pontual estabelecerá as bases fundamentais, processos, políticas e procedimentos que serão operacionalizados e mantidos durante a Fase Continuada, garantindo assim a evolução constante da maturidade em segurança cibernética e a proteção efetiva contra ameaças emergentes.
- 15.1.3. O serviço deverá contemplar, como fase inicial e obrigatória, a elaboração de um Relatório de Gestão de Vulnerabilidades abrangente, que será desenvolvido através de etapas estruturadas incluindo:
 - 15.1.3.1. Elaboração de uma análise de impacto nos negócios (BIA) para identificação de processos e ativos críticos;
 - 15.1.3.2. avaliação de maturidade e assessment do ambiente atual de segurança e das ferramentas existentes;
 - 15.1.3.3. desenvolvimento de roadmap estratégico com ações priorizadas e cronograma de implementação;
 - 15.1.3.4. elaboração de um Relatório de Resposta a Incidentes;
 - 15.1.3.5. projeto de transformação dos processos operacionais e configuração das plataformas de gestão de vulnerabilidades;
 - 15.1.3.6. estabelecimento de políticas, procedimentos, SLAs e métricas de desempenho.

15.2. RELATÓRIO DE GESTÃO DE VULNERABILIDADES - RGV

- 15.2.1. Esta fase inicial deverá ser executada em prazo máximo de 12 semanas, com entregas parciais documentadas e validadas pela CONTRATANTE, servindo como base fundamental para a operacionalização contínua e efetiva do monitoramento de vulnerabilidades, garantindo que todas as atividades subsequentes estejam alinhadas com os objetivos de negócio e requisitos de conformidade regulatória da organização.
- 15.2.2. O serviço deverá estabelecer um monitoramento robusto de vulnerabilidades que contemple a identificação, avaliação, priorização, remediação e mitigação de vulnerabilidades de forma contínua e estruturada;
- 15.2.3. O serviço deverá implementar um framework baseado no Ciclo de Vida de Gestão de Vulnerabilidades (VM Lifecycle), abrangendo as fases de descoberta de ativos, avaliação de vulnerabilidades, priorização de riscos, remediação/mitigação e reavaliação;
- 15.2.4. O serviço deverá adotar metodologia alinhada com as normas internacionais ISO/IEC 27001, ISO/IEC 27002, ISO 22301:2020 e frameworks NIST SP 800-53 e NIST Cybersecurity Framework;
- 15.2.5. O serviço deverá garantir a operação contínua e adaptativa do monitoramento



permitindo que a organização responda proativamente às ameaças emergentes e evolução do cenário de riscos cibernéticos;

15.2.6. O serviço deverá estabelecer processos estruturados para monitoramento contínuo das ferramentas de gestão de vulnerabilidades, incluindo a detecção de novas ameaças e categorização adequada;

15.2.7. O RGV deverá ser atualizado semestralmente, considerando as alterações e evoluções ocorridas no ambiente em decorrência das medidas adotadas no âmbito deste contrato ou de quaisquer outros fatores que modifiquem o cenário existente, de modo a mantê-lo aderente às necessidades atuais da SEFAZ.

16. BUSINESS IMPACT ANALYSIS - BIA

16.1. O serviço deverá realizar a elaboração completa da Análise de Impacto nos Negócios (BIA) para até 15 (quinze) áreas de negócios da CONTRATANTE, visando o levantamento sistemático dos sistemas e recursos que suportam os processos críticos para a organização;

16.2. O serviço deverá executar workshops estruturados com gestores de negócios para instruções sobre o preenchimento da Matriz BIA e coleta de informações essenciais sobre processos e atividades críticas;

16.3. O serviço deverá conduzir entrevistas detalhadas com stakeholders-chave, tanto do ponto de vista técnico (TI) quanto de gestão de riscos e conformidade, para validação e alinhamento dos dados coletados;

16.4. O serviço deverá identificar e documentar os potenciais impactos de perda financeira, reputacional, regulatória e operacional frente às possíveis disrupções dos processos críticos de negócio;

16.5. O serviço deverá definir e documentar os indicadores críticos de continuidade: MTPD (Período Máximo de Disrupção Tolerada), RTO (Recovery Time Objective) e RPO (Recovery Point Objective) para cada processo identificado como crítico;

16.6. O serviço deverá mapear e documentar todos os recursos tecnológicos, suas dependências e respectivos fornecedores relacionados aos processos e atividades críticas identificadas;

16.7. O serviço deverá documentar as janelas de manutenção, mitigação de riscos e janelas críticas de mudança para cada processo crítico;

16.8. O serviço deverá selecionar e priorizar os processos/atividades críticos aos negócios para tratamento adequado no programa de gestão de vulnerabilidades;

16.9. O serviço deverá entregar a Matriz BIA completa e validada, contendo todos os dados complementares dos processos críticos e suas respectivas análises de impacto;

16.10. O serviço deverá fornecer documentação detalhada incluindo prazos toleráveis de disrupções dos processos e respectivos impactos à organização, servindo como base para priorização das ações de segurança.

16.11. O BIA deverá ser atualizado semestralmente, considerando as alterações e evoluções ocorridas no ambiente em decorrência das medidas adotadas no âmbito deste contrato ou de quaisquer outros fatores que modifiquem o cenário existente, de modo a mantê-lo aderente às necessidades atuais da SEFAZ.



17. RELATÓRIO DE RESPOSTA A INCIDENTES - RRI

17.1. O presente escopo tem como finalidade estabelecer as diretrizes e atividades necessárias para a elaboração e implementação de um Relatório de Resposta a Incidentes (RRI), de forma a garantir que a CONTRATANTE esteja preparada para detectar, responder e recuperar-se eficazmente de incidentes de segurança cibernética, em alinhamento ao NIST Cybersecurity Framework (NIST CSF) e às melhores práticas internacionais.

17.2. Objetivos Estratégicos

- 17.2.1. Desenvolver um Relatório de Resposta a Incidentes formal e aderente ao NIST CSF;
- 17.2.2. Melhorar a capacidade de detecção precoce de incidentes de segurança;
- 17.2.3. Definir processos claros e documentados para resposta a incidentes;
- 17.2.4. Garantir a rápida recuperação após incidentes, assegurando a continuidade do negócio;
- 17.2.5. Assegurar conformidade com regulamentações e normas aplicáveis (ex.: LGPD, ISO 27001, BACEN, ANPD).

17.3. Escopo do Relatório de Resposta a Incidentes

17.3.1. O RRI deverá ser um documento formal contendo procedimentos, ferramentas e fluxos de trabalho para lidar com incidentes cibernéticos.

17.3.2. O relatório deverá contemplar:

- a) Prevenção – definição de controles e medidas proativas para redução de riscos;
- b) Detecção – mecanismos de identificação precoce de anomalias e incidentes;
- c) Resposta – protocolos de contenção, erradicação e recuperação;
- d) Recuperação – restabelecimento seguro de serviços e continuidade operacional;
- e) Aprimoramento – lições aprendidas e ajustes contínuos do documento.

17.3.3. Planejamento

- a) Realização de reuniões iniciais de alinhamento, apresentação do plano de trabalho, definição de cronograma e reunião de kick-off;
- b) Levantamento dos processos e ferramentas de Segurança da Informação e áreas de negócio envolvidas (Tecnologia, Infraestrutura, Segurança da Informação);
- c) Mapeamento de até 20 (vinte) processos com apoio da CONTRATANTE;
- d) Definição da equipe responsável, organograma de papéis e responsabilidades.

17.3.4. Execução

- a) Elaboração do Relatório de Ação Detalhado (RRI), contendo processos, fluxos de escalonamento e responsabilidades;



- b) Estruturação de Playbooks de Incidentes para cenários críticos (1 playbook);
- c) Definição dos seguintes estágios principais:
 - i.Preparação;
 - ii.Detecção;
 - iii.Análise;
 - iv.Contenção (curto e longo prazo);
 - v.Eradicação;
 - vi.Recuperação;
 - vii.Lições aprendidas.

17.3.5. Definição de papéis e responsabilidades através de Matriz RACI (mínimo de 1 matriz), contemplando áreas internas e prestadores de serviços;

17.3.6. Estruturação de mecanismos de integração com processos de SIEM, XDR e SOC da CONTRATANTE.

17.3.7. Análise de Prestadores de Serviços de TI

- a) Verificação dos SLAs de fornecedores internos e externos;
- b) Definição de responsabilidades conjuntas em incidentes (Matriz RACI).
- c) Elaboração do Playbook
- d) Construção de playbooks específicos para incidentes de alta criticidade (1 playbook obrigatório: Ransomware);
- e) Cada playbook deverá conter atividades pré-definidas para garantir padronização da resposta;
- f) As atividades deverão contemplar tratamento pós-incidente, incluindo investigação avançada e consolidação de lições aprendidas.

17.3.8. Entregáveis Mínimos

- a) Documento formal do Relatório de Resposta a Incidentes (RRI);
- b) Cronograma detalhado de execução;
- c) Relatório de levantamento de processos e organograma funcional;
- d) Matriz RACI de responsabilidades internas e de terceiros (mínimo 1);
- e) Relatório de Ação estruturado com fluxos de escalonamento;
- f) Playbook mínimo de Ransomware;
- g) Relatório de lições aprendidas e recomendações de melhoria contínua.

17.3.9. O RRI deverá ser atualizado semestralmente, considerando as alterações e evoluções ocorridas no ambiente em decorrência das medidas adotadas no âmbito deste contrato ou de quaisquer outros fatores que modifiquem o cenário existente, de modo a mantê-lo aderente às necessidades atuais da SEFAZ.



17.4. Implantação Do Serviço de Monitoramento De Vulnerabilidade

17.4.1. Serviço continuado de gestão de vulnerabilidades

- 17.4.1.1. Preparação e realização de varreduras para análise de vulnerabilidades de ativos de infraestrutura de TI e aplicações Web e elaboração de relatório da análise;
- 17.4.1.2. Instalação, configuração e documentação das ferramentas fornecidas, inclusive suas integrações;
- 17.4.1.3. Apoio na manutenção preventiva, corretiva e atualizações das ferramentas fornecidas;
- 17.4.1.4. Gerar mensalmente relatório com serviços realizados no mês, vulnerabilidades não corrigidas e tempos de atendimento. O relatório mensal poderá ser customizado de acordo com a necessidade da SEFAZ-ES;
- 17.4.1.5. Identificar possíveis vulnerabilidades de segurança da informação, a fim de apoiar a definição de plano de ação mensal e evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas;
- 17.4.1.6. A solicitação dos serviços será realizada por meio de chamado aberto pela SEFAZ-ES;
- 17.4.1.7. A CONTRATADA deve apresentar relatório das principais remediações para o tratamento das vulnerabilidades mais comuns, das vulnerabilidades mais críticas e dos exploits conhecidos.
- 17.4.1.8. A fim de balizar todo o processo de gestão de vulnerabilidade da SEFAZ-ES, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir *ipsis litteris*.
- 17.4.1.9. A CONTRATADA deverá levantar junto à SEFAZ uma lista de ativos e recursos que deverão fazer parte do processo de gestão de vulnerabilidade. Tal lista poderá ser revisitada e atualizada durante todo o período de vigência de contrato, e deverá conter as seguintes informações mínimas, a saber:
 - 17.4.1.9.1. Nome do ativo e/ou serviço;
 - 17.4.1.9.2. Grupo de serviço;
 - 17.4.1.9.3. IP
 - 17.4.1.9.4. Janela de análise (Horário permitido para análise);
 - 17.4.1.9.5. Prioridade.
- 17.4.1.10. A CONTRATADA deverá realizar de forma contínua uma avaliação prévia no ambiente computacional da SEFAZ-ES, a fim de, consultivamente sugerir e complementar a lista de ativos e recursos disponibilizados à SEFAZ-ES.
- 17.4.1.11. De acordo com as variáveis e critérios estabelecidos no catálogo de serviços, na lista de ativos e recursos da SEFAZ-ES, a CONTRATADA deverá realizar checagens (scans) e varreduras, buscando encontrar vulnerabilidades de segurança no ambiente da SEFAZ-ES, utilizando as ferramentas e soluções definidas no presente termo de referência.
- 17.4.1.12. Após o término das rotinas de checagens (scans) e varreduras no



ambiente, deverá a CONTRATADA realizar uma análise de falso positivo das vulnerabilidades descobertas, isso quer dizer, que devem ser informadas à SEFAZ-ES apenas vulnerabilidades que existam de fato em seu ambiente.

17.4.1.13. Após análise de falso positivo, a CONTRATADA deverá informar à SEFAZ-ES as vulnerabilidades encontradas, obedecendo os critérios e requisitos estabelecidos no tópico ENTREGAS A SEREM REALIZADAS do presente termo de referência.

17.4.2. Serviços de avaliação de maturidade de segurança

17.4.2.1. Os serviços deverão contemplar a realização de avaliações periódicas de maturidade dos controles de segurança da informação em toda a organização CONTRATANTE.

17.4.2.1.1. O intervalo entre as avaliações não deverá exceder 90 (noventa) dias.

17.4.2.2. Deverão ser realizado o levantamento de todos os controles implementados e conduzidas entrevistas estruturadas com os responsáveis pelas áreas de tecnologia e segurança para coleta de informações e apresentação de indicadores de avanço da maturidade em segurança da SEFAZ.

17.4.2.3. O serviço deverá incluir a avaliação de conformidade com os principais frameworks e normas de mercado, incluindo ISO 27001/27002, NIST CSF, CIS Controls, PCI-DSS, GDPR e legislações de privacidade locais.

17.4.2.4. Deverão ser realizadas verificações passivas da infraestrutura externa da organização, examinando a segurança de sistemas operacionais, navegadores, servidores de e-mail e websites corporativos.

17.4.3. Serviços de análise e validação

17.4.3.1. Os serviços deverão incluir a coleta e análise de arquivos de configuração dos principais ativos de tecnologia da CONTRATANTE.

17.4.3.2. Deverá ser realizada a validação cruzada entre as informações coletadas via questionários e as configurações técnicas reais dos sistemas.

17.4.3.3. Os profissionais deverão executar verificações interativas e integradas da infraestrutura de rede, servidor, aplicação, banco de dados e segurança.

17.4.3.4. O serviço deverá identificar gaps entre a percepção de maturidade reportada pela organização e o estado real verificado tecnicamente.

17.4.4. Serviços de quantificação de impacto financeiro

17.4.4.1. Os profissionais deverão realizar a modelagem e quantificação do impacto financeiro potencial de incidentes de segurança cibernética.

17.4.4.2. O serviço deverá considerar variáveis específicas da CONTRATANTE, incluindo faturamento anual, média salarial, investimentos em segurança, setor de atuação e localização geográfica.

17.4.4.3. Deverão ser desenvolvidos cenários de risco considerando diferentes tipos de atacantes, métodos de ataque e objetivos maliciosos.



17.4.4.4. Os serviços deverão calcular a probabilidade de materialização de riscos com base na atratividade dos ativos e nas capacidades necessárias para comprometê-los.

17.4.4.5. Deverá ser prestado serviço contínuo de análise do cenário de ameaças relevante para o setor e região de atuação da CONTRATANTE.

17.4.4.6. Os profissionais deverão fornecer análises sobre grupos de atacantes ativos, suas técnicas, táticas e procedimentos (TTPs).

17.4.4.7. O serviço deverá incluir o monitoramento de indicadores de comprometimento e tendências de ataques cibernéticos globais e setoriais.

17.4.4.8. Deverão ser produzidos relatórios periódicos correlacionando as ameaças identificadas com as vulnerabilidades e controles da organização.

17.4.5. Serviços de orçamento e planejamento estratégico

17.4.5.1. Os profissionais deverão elaborar simulações e análises hipotéticas de retorno sobre investimento (ROI) para melhorias de segurança propostas.

17.4.5.2. Deverá ser prestado apoio na priorização de investimentos em segurança, baseando-se na criticidade dos riscos e importância para os processos de negócio.

17.4.5.3. Os serviços deverão incluir a elaboração de roadmap de segurança com recomendações priorizadas de implementação.

17.4.5.4. Deverão ser realizadas sessões de apresentação executiva para comunicar os riscos cibernéticos em termos financeiros e de negócio.

17.4.6. Entregáveis do Serviço de Monitoramento de Vulnerabilidades

17.4.6.1. Para acompanhamento do serviço a ser ofertado pela CONTRATADA, os entregáveis abaixo deverão compor o relatório mensal a ser entregue pela CONTRATADA para acompanhamento da execução contratual:

INDICADOR	AGRUPADOR	DESCRIÇÃO
KPI-1	Solução de Gestão de Vulnerabilidades	Disponibilidade da solução
KPI-2	Solução de Gestão de Vulnerabilidades	Quantidade de vulnerabilidades INFRA
KPI-3	Solução de Gestão de Vulnerabilidades	Quantidade de Vulnerabilidades WEB
KPI-4	Solução de Gestão de Vulnerabilidades	Quantidade de Vulnerabilidades container
KPI-5	Solução de Gestão de Vulnerabilidades	Quantidade de Vulnerabilidades corrigidas
KPI-6	Solução de Gestão de Vulnerabilidades	TOP 10 – Ativos mais vulneráveis
KPI-7	Solução de Gestão de Vulnerabilidades	TOP 10 – Vulnerabilidades mais comuns em ativos
KPI-8	Solução de Gestão de Vulnerabilidades	TOP 10 – Aplicações WEB mais vulneráveis
KPI-9	Gestão de Vulnerabilidades no Active Directory	Quantidade de contas com privilégios administrativos ou permissões excessivas.
KPI-10	Gestão de Vulnerabilidades no Active Directory	Número de caminhos de ataque identificados que permitem elevação de privilégios ou movimento lateral.



KPI-11	Gestão de Vulnerabilidades no Active Directory	Quantidade de configurações inseguras em GPOs, trusts, ACLs e Kerberos.
KPI-12	Gestão de Vulnerabilidades no Active Directory	Número de contas expiradas, inativas ou desabilitadas que ainda permanecem ativas.
KPI-13	Gestão de Vulnerabilidades no Active Directory	Quantidade de delegações inseguras ou mal configuradas detectadas em objetos do AD.
KPI-14	Gestão de Vulnerabilidades no Active Directory	Top 10 exposições mais críticas em controladores de domínio e usuários privilegiados.
KPI-15	Gestão de Vulnerabilidades no Active Directory	Quantidade de alertas abertos, resolvidos e pendentes, categorizados por nível de risco.
KPI-16	Gestão de Vulnerabilidades no Active Directory	Tempo médio de resolução entre a identificação de uma exposição crítica e sua mitigação.
KPI-17	Gestão de Vulnerabilidades no Active Directory	Número de tickets de correção abertos automaticamente a partir das descobertas.
KPI-18	Gestão de Vulnerabilidades no Active Directory	Evolução do risco ao longo do tempo (redução ou aumento de exposições críticas).
KPI-19	Gestão de Vulnerabilidades no Active Directory	Score consolidado de segurança do AD, dividido por categorias (usuários, DCs, trusts, GPOs).
KPI-20	Maturidade de Controles	Score médio de maturidade dos controles avaliados
KPI-21	Maturidade de Controles	Quantidade de controles com maturidade adequada vs total de controles
KPI-22	Maturidade de Controles	Percentual de aderência ao NIST CSF
KPI-23	Maturidade de Controles	Percentual de aderência ao ISO 27001
KPI-24	Maturidade de Controles	Valor do impacto financeiro potencial identificado
KPI-25	Maturidade de Controles	ROI projetado dos investimentos em segurança
KPI-26	Maturidade de Controles	Quantidade de controles críticos identificados para investimento
KPI-27	Maturidade de Controles	Valor total de investimento recomendado vs orçamento disponível
KPI-28	Maturidade de Controles	Percentual de conformidade entre questionários e análises técnicas
KPI-29	Maturidade de Controles	Quantidade de gaps identificados entre percepção e realidade técnica
KPI-30	Maturidade de Controles	Quantidade de ambientes avaliados no período
KPI-31	Maturidade de Controles	Percentual de ativos críticos cobertos pela avaliação
KPI-32	Maturidade de Controles	Quantidade de cenários de ameaças simulados
KPI-33	Maturidade de Controles	Score de probabilidade de sucesso de ataques (PoS) médio da organização
KPI-34	Maturidade de Controles	Quantidade de controles por categoria avaliados
KPI-35	Maturidade de Controles	Percentual de controles com evidências coletadas
KPI-36	Maturidade de Controles	Taxa de evolução da maturidade período a período
KPI-37	Maturidade de Controles	Quantidade de recomendações implementadas vs total de recomendações
KPI-38	Maturidade de Controles	Quantidade de relatórios executivos gerados mensalmente
KPI-39	Maturidade de Controles	Tempo médio de geração de relatórios via plataforma
KPI-40	Maturidade de Controles	Quantidade de ativos com análise de configuração realizada
KPI-41	Maturidade de Controles	Percentual de conformidade com CIS Benchmarks (Relatório de Maturidade de Padrões)
KPI-42	Maturidade de Controles	Frequência de atualização dos dashboards de risco
KPI-43	Maturidade de Controles	Quantidade de visualizações dos painéis pelos stakeholders
KPI-44	Maturidade de Controles	Taxa de completude dos questionários de avaliação
KPI-45	Maturidade de Controles	Tempo médio de resposta aos questionários compartilhados
KPI-46	Maturidade de Controles	Quantidade de indicadores de ameaças monitorados
KPI-47	Maturidade de Controles	Relevância das ameaças para o setor/região (score de contextualização)



17.4.6.2. Tais entregáveis, relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring). Nesse contexto, o profissional deve apresentá-lo de forma virtual, por meio de solução de videoconferência;

18. DOS REQUISITOS GERAIS PARA A EXECUÇÃO DOS SERVIÇOS

18.1. Processo a serem executados serviço de monitoramento de ataque e resposta a incidentes

- 18.1.1. A fim de balizar todo o processo de monitoramento de ataques cibernéticos da SEFAZ-ES, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir *ipsis litteris*.
- 18.1.2. Este serviço deverá ser executado em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- 18.1.3. É sabido que para o sucesso de um monitoramento de ataques cibernético, a primeira definição se deve a que tipo de ocorrência de eventos de segurança, se deseja detectar e tomar algum tipo de ação, logo será de responsabilidade da CONTRATADA como primeiro passo deste processo, a definição de linha de base de eventos monitorados.
- 18.1.4. Tal definição de linha de base de eventos de segurança monitorados, não deve ser tomada de forma unilateral pela CONTRATADA, a SEFAZ-ES deverá participar ativamente no processo de construção de forma consultiva, porém se ratifica que é de responsabilidade da CONTRATADA a definição e colocar em operação tal linha de base.
- 18.1.5. Espera-se que a linha de base de eventos de segurança monitorados, seja revista de forma contínua, contudo não se limitando a este tempo, pois todos os dias novos ataques são projetados no mundo, e se espera que a CONTRATADA tome ciência destes ataques, e por sua vez atualize a linha de base, para que em um cenário onde estes novos ataques sejam direcionados à SEFAZ-ES sejam detectados através dos serviços em questão.
- 18.1.6. O produto de um evento é a correlação dos insumos: logs e rede, gerados pelos itens de configurações do parque da SEFAZ-ES. Uma vez definida a linha de base de eventos, será também de responsabilidade da CONTRATADA avaliar se todos os insumos para a correta geração do evento, estão sendo enviados corretamente para a ferramenta definida.
- 18.1.7. Caso a CONTRATADA identifique a ausência dos insumos a ser gerado por um item de configuração, será de responsabilidade da CONTRATADA avisar e solicitar à SEFAZ-ES para que seja corrigido a configuração e normalizado o recebimento de logs, respeitando a quantidade de GB/DIA contratado.



18.1.8. Dar-se-á então o passo de classificação do evento, também de responsabilidade da CONTRATADA. O grupo de monitoramento de ataques da CONTRATADA deve focar as ações nos eventos que são significativos, logo tal grupo deve analisar todos os eventos apresentados, classificando-os nos seguintes grupos, a saber:

18.1.8.1. Eventos de Informação: Estes eventos não requerem qualquer ação. São usados para fazer verificação de funcionalidade dos itens de configuração de segurança. Ou seja, tem por objetivo identificar se as ferramentas e soluções estão funcionando dentro do esperado. Estes eventos são também úteis para gerar estatísticas como por exemplo, porcentagem de hosts com a última vacina de antivírus do dia;

18.1.8.2. Eventos de Aviso: Este grupo de eventos deve ser utilizado, quando existe algum comportamento anômalo se comparado a linha de base de operação padrão do ambiente (serviço, tráfego e/ou solução), porém ainda não gerou algum tipo de impacto ao ambiente (serviço, tráfego e/ou solução) da SEFAZ-ES, como por exemplo fictício: Por exemplo, é esperado que exista 1000 (mil) ataques do tipo port scan bloqueados pelo firewall, porém na última hora este número passou para 10000 (dez mil) ataques, todavia o firewall ainda continua bloqueando sem que haja degradação da performance do ambiente (serviço, tráfego e/ou solução);

18.1.8.3. Eventos de Exceção: Estes eventos são aqueles que sugere que os pilares de segurança da informação (confidencialidade, integridade e confidencialidade), foram impactados, como por exemplo: Uma infecção gerada por um malware do tipo ransomware que não tenha sido bloqueada pela solução de antivírus da SEFAZ-ES;

18.1.8.4. Eventos de Críticos: Esses eventos ocorrem quando uma ameaça foi detectada e já existem indícios claros de comprometimento significativo do ambiente, como violação de dados sensíveis, presença confirmada de malware avançado, ou evidências de ataque em andamento. Exemplos incluem a descoberta de um acesso não autorizado a dados confidenciais ou um comprometimento ativo de uma conta privilegiada que está sendo utilizada para movimentos laterais dentro da rede da SEFAZ-ES neste momento;

18.1.9. Uma vez classificado o evento se inicia o passo de resposta ao mesmo, que também é de responsabilidade da CONTRATADA. As respostas são baseadas nos grupos de classificação de eventos, a saber:

18.1.9.1. Para eventos do tipo Informação, não é requerido qualquer tipo de ação, porém como já mencionado no presente termo de referência, tais eventos são utilizados para verificação do perfeito funcionamento das soluções de segurança, portanto se espera que a CONTRATADA os utilize para tal;

18.1.9.2. Para eventos do tipo Aviso, deve existir a garantia por parte da CONTRATADA que uma interface humana, ou seja, uma analista que pertence ao grupo de monitoramento de ataques, esteja validando se tal evento pode se transformar em um evento do tipo exceção, e obviamente tomando as ações cabíveis para identificar a causar raiz da mudança de comportamento do ambiente;

18.1.9.3. Para eventos do tipo Exceção, deverá a CONTRATADA transformar tal evento em um incidente de segurança, realizando, portanto, a sua abertura na ferramenta de incidente de segurança da informação, definida no SUBPROCESSO DE RESPOSTA A INCIDENTE DE SEGURANÇA DA INFORMAÇÃO. Após a abertura do



incidente de segurança obedecendo os critérios estabelecidos para tal, se encerra a participação do grupo de monitoramento de ataques;

18.1.9.4. Para eventos classificados como Críticos, deverá ser acionado imediatamente o grupo responsável por Digital Forensics and Incident Response (DFIR). O acionamento do DFIR ocorre quando há indícios claros de comprometimento significativo do ambiente, como violação de dados sensíveis, presença confirmada de malware avançado, ou evidências de ataque em andamento. O grupo DFIR será responsável por conduzir uma investigação detalhada, realizar coleta de evidências, preservação de dados, análise forense e elaborar um relatório técnico que auxilie na mitigação sua atuação está definida no SUBPROCESSO DE FORENSE DIGITAL PARA RESPOSTA A INCIDENTES.

18.1.10. Como último passo do processo, a CONTRATADA deve encerrar os eventos após as devidas ações tomadas, conforme definido no parágrafo acima. Eventos podem ter apenas dois tipos de status “aberto” ou “encerrado”, ou seja, após o correto tratamento o evento deverá ter seu status alterado na ferramenta de “aberto” para “encerrado”.

18.1.11. Importante ressaltar que todo processo de tratamento do evento, independente de qual fase e/ou status, deve ser registrado. Também é responsabilidade da CONTRATADA a segurança dos eventos, e fica expressamente proibido a remoção de qualquer evento, independentemente de sua classificação e fase de tratamento.

18.2. Sobre O Sistema De ITSM a Ser Utilizado

18.2.1. Todas as requisições devem ser registradas, controladas, coordenadas, promovidas e gerenciadas por todo o seu ciclo de vida por meio de um único sistema. Isso garante uma abordagem consistente e reproduzível para o tratamento das requisições e reduz o potencial conflito, e a quantidade de requisições perdidas que possam surgir durante o tratamento.

18.2.2. O sistema de ITSM do inglês Information Technology Service Management (Gerenciamento de Serviços de TI), deve ser obrigatoriamente de propriedade da CONTRATADA, ter suporte e garantia ativo com o fabricante, ser instalado em infraestrutura de propriedade da CONTRATADA, não sendo permitido a utilização de sistemas de ITSM do tipo open source.

18.2.3. Para que em qualquer tempo independentemente do local, funcionários autorizados do corpo técnico da SEFAZ-ES, tenham a possibilidade de abrir requisições para o SOC do inglês Cyber Operations Center da CONTRATADA, o sistema de ITSM do inglês Information Technology Service Management (Gerenciamento de Serviços de TI) utilizado pela CONTRATADA, deverá ser acessível via internet utilizando protocolo SSL do inglês Secure Socket Layer, com certificado digital emitido em nome da CONTRATADA.

18.2.4. Uma das origens de requisição de serviço poderá ser via interface humana, e a fim de evitar possíveis alterações anômalas e indesejadas no ambiente de segurança da informação, apenas funcionários autorizados do corpo técnico da SEFAZ-ES, poderão realizar abertura de requisições de serviços.

18.2.5. Sempre que uma nova requisição de serviço for solicitada, pelo corpo técnico da SEFAZ-ES, a CONTRATADA deverá previamente observar se tal contato está autorizado a solicitar tais serviços, antes de iniciar o atendimento. Caso tal contato não seja autorizado, o atendimento não deverá ser iniciado, e um comunicado de tentativa de



abertura de atendimento não autorizado, deve ser enviado ao gestor de contrato por parte da SEFAZ-ES.

18.2.6. A CONTRATADA deverá manter uma plataforma para gerir tais contatos autorizados, constando ao menos as seguintes informações dos contatos: nome, telefone, e-mail, cargo. O gerenciamento (criar, atualizar, desativar e remover) desta plataforma deve estar disponível via internet para a SEFAZ-ES, seguindo os critérios de segurança estabelecido para o sistema de ITSM do inglês Information Technology Service Management (Gerenciamento de Serviços de TI), ou seja, acessível via internet utilizando protocolo SSL do inglês Secure Socket Layer, com certificado digital emitido em nome da CONTRATADA.

18.2.7. Em tal plataforma de gestão de contatos autorizados, deve ter a capacidade de relacionar os contatos autorizados, com os itens de configuração de sua responsabilidade do ambiente de segurança da informação da SEFAZ-ES.

18.2.8. Nos primeiros 30 (trinta) dias iniciais do contrato, a SEFAZ-ES informará através de ofício destinado a CONTRATADA, sobre quem e quantos são os contatos autorizados, bem como uma matriz de responsabilidade relacionado aos itens de configuração que compõem a arquitetura de segurança da informação da SEFAZ-ES.

18.2.9. Após o recebimento do ofício a CONTRATADA deverá em até 15 (quinze) dias disponibilizar os acessos aos canais de comunicação, a todos os contatos autorizados. A CONTRATADA ainda deve enviar o comunicado de boas-vindas para cada contato, com manual de acesso a cada canal de comunicação, bem como também suas devidas credenciais.

18.2.10. O acesso aos canais de comunicação relacionados no presente termo, de qualquer tipo (telefonia, sistemas, e-mails, Whatsapp) devem estar disponíveis para todos os contatos autorizados, a serem relacionados pela SEFAZ-ES.

18.3. Canais De Comunicações

18.3.1. A CONTRATADA deverá disponibilizar acesso a requisições, no mínimo, pelos seguintes meios, por ordem de prioridade:

GRUPO DE TECNOLOGIA	CLASSIFICAÇÃO
Linha de telefone gratuita (0800)	Tipo 1
E-mail com domínio registrado e de propriedade da CONTRATADA.	Tipo 2
Sistema de ITSM do inglês Information Technology Service Management (Gerenciamento de serviços de TI)	Tipo 3
Suporte via WhatsApp para usuário com número celular cadastrado no sistema.	Tipo 4

18.3.2. Deverá constar na proposta técnica todos os meios de comunicação, este item será diligenciado e validado pela equipe técnica.

18.4. Central De Serviços

18.4.1. Para atender as requisições proativas e reativas do presente termo, a CONTRATADA deverá possuir uma central de serviço, com o objetivo de proporcionar um único ponto de contato para todos os funcionários da SEFAZ-ES, autorizados a realizar uma requisição de serviço.

18.4.2. Tal central de serviço deve ser do tipo virtual, ou seja, deve ser instalada em ao menos dois locais distintos com distância geográfica de no mínimo 50 km (cinquenta quilômetros), e funcionar como uma única central de atendimento, ou seja, ambas devem



utilizar e estarem acessíveis através dos mesmos canais de comunicações, obedecendo os requisitos estabelecidos no tópico CANAIS DE COMUNICAÇÃO, do presente termo, bem como também utilizar do mesmo sistema de ITSM do inglês Information Technology Service Management, obedecendo os requisitos estabelecidos no tópico SOBRE O SISTEMA DE ITSM A SER UTILIZADO.

18.4.3. A indisponibilidade física e/ou virtual de uma das centrais de serviços, não pode afetar o funcionamento de sua oferta de serviço.

18.4.4. Tal central terá acesso a dados e informações referente a arquitetura de segurança da informação da SEFAZ-ES, e com o objetivo de manter tais acessos aos dados e informações sobre a governança e legislação brasileira, ambas as centrais de serviço devem obrigatoriamente serem instaladas fisicamente no Brasil.

18.4.5. Todas as requisições de serviços restringem-se aos itens de configuração do presente termo. Todos os itens de configurações fazem parte única e exclusivamente do ambiente de segurança da informação da SEFAZ-ES, sendo assim toda e qualquer requisição de serviço estará ligada a tal ambiente, logo a central de serviço deve ser parte de um SOC do inglês Security Operations Center.

18.4.6. A Comprovação deve ser enviada juntamente com toda a documentação e proposta comercial na fase de comprovação e avaliação da documentação;

18.4.7. A CONTRATADA a qualquer tempo pode ser auditada via questionários ou visitas in-loco, pela SEFAZ-ES, e/ou instituição independente CONTRATADA pela SEFAZ-ES, referente aos itens de controle e normas estabelecidos na ABNT NBR ISO/IEC 20001, portanto se espera que a CONTRATADA tenha evidências e experiência de execução da norma, mesmo antes de ter o contrato assinado com a SEFAZ-ES, referente a tal objeto do presente termo.

18.4.8. A Comprovação deve ser enviada juntamente com toda a documentação e proposta comercial na fase de comprovação e avaliação da documentação;

18.5. Do IMR – Nível Mínimo de Serviços

18.5.1. O IMR aplica-se exclusivamente aos serviços continuados de operação do SOC descritos no item 14 do objeto, não incidindo sobre os itens de fornecimento de licenças ou implantação, que possuem critérios próprios de aceite e pagamento.

18.5.2. Para chamados de severidade Crítica/Urgente, Alta, Normal ou Baixa, o início dos atendimentos realizados e os prazos de solução estão especificados na tabela a seguir:

REFERÊNCIA	SEVERIDADE	DESCRIÇÃO	PRAZO MÁXIMO PARA PRIMEIRO ATENDIMENTO	PRAZO MÁXIMO DA SOLUÇÃO
SEVERIDADE-01	Urgente/ Crítica	O serviço está totalmente parado ou inoperante;	Até 1 (uma) hora após a abertura do chamado remoto.	Até 24 (vinte e quatro) horas após abertura do chamado remoto.
SEVERIDADE-02	Alta	O serviço está ativo, mas com inoperância da maioria de suas funcionalidades, causando um impacto	Até 4 (quatro) horas após a abertura do chamado remoto	Até 2 (dois) dias corridos após abertura do chamado remoto;



		negativo no ambiente de produção		
SEVERIDADE-03	Normal	O serviço está em operação, mas suas funcionalidades são executadas com restrições	Até 8 (oito) horas após a abertura do chamado remoto.	Até 4 (quatro) dias corridos após abertura do chamado remoto.
SEVERIDADE-04	Baixa	O serviço está em operação e a falha não compromete suas funcionalidades ou questões não tratadas pela documentação	Até 12 (doze) horas após a abertura do chamado remoto.	Até 6 (seis) dias úteis após a abertura do chamado remoto.

18.6. Acordo De Nível De Serviço

18.6.1. Os níveis mínimos de serviço contratados serão registrados, monitorados e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade, condição fundamental para realização dos pagamentos.

18.6.2. O pagamento mensal estará condicionado ao desempenho apurado, podendo sofrer glosas proporcionais em caso de descumprimento dos níveis mínimos estabelecidos, conforme tabela de faixas de desempenho.

18.6.3. As glosas serão aplicadas automaticamente sobre o valor mensal da fatura, independentes de eventual aplicação de penalidades administrativas e não afastam a obrigação de correção das falhas.

18.6.4. Caso a CONTRATADA apresente IDG < 80% por 2 meses consecutivos, ou IDG < 90% por 3 meses consecutivos, poderá ser caracterizada inexecução parcial do contrato, sujeitando-se às sanções previstas.

18.6.5. Os indicadores poderão ser revisados periodicamente conforme evolução da maturidade do SOC desde que pactuados entre as partes mediante justificativa técnica.

18.6.6. A CONTRATADA deverá disponibilizar evidências e logs para auditoria, permitir rastreabilidade completa das medições e garantir integridade dos dados apresentados.

18.6.7. Haverá na fase inicial de estabilização um período de 90 (noventa) dias sem aplicação de glosa integral.

18.6.8. O desempenho mensal da CONTRATADA será aferido por meio do Índice de Desempenho Global (IDG), calculado a partir da média ponderada dos KPI's definidos:

$$IDG = \sum (Nota do Indicador \times Peso)$$

Onde:

Cada indicador recebe nota de 0 a 100.

O peso é proporcional à criticidade do indicador.

O resultado será expresso em percentual (%).

#	Indicador	Descrição	Fórmula de Apuração	Meta (SLO)	Peso (%)	Critério de Medição
1	MTTD	Tempo médio de detecção	Soma dos tempos / nº de incidentes	De acordo com a severidade	15%	Mensal



2	MTTR	Tempo médio de resposta	Soma dos tempos / nº de incidentes	De acordo com a severidade	15%	Mensal
3	Cumprimento de SLA	% de incidentes atendidos no prazo	(Incidentes no prazo / total) x 100	≥ 95%	15%	Mensal
4	Falsos Positivos	% de alertas incorretos	(FP / total de alertas) x 100	≤ 10%	10%	Mensal
5	Taxa de Detecção	% de incidentes corretamente identificados	(Incidentes true positive detectados / total de detecções) x 100	≥ 95%	10%	Mensal
6	Tempo de Contenção	Tempo médio de mitigação	Soma dos tempos / nº incidentes	De acordo com a severidade	10%	Mensal
7	Disponibilidade SOC	Disponibilidade da plataforma	(Tempo disponível / total) x 100	≥ 99,5%	10%	Mensal
8	Evolução de Use Cases	Novos casos implementados	Nº mensal entregue	≥ 5/mês	5%	Mensal
9	Qualidade dos Relatórios	Entregas no prazo e completas	(Entregas conformes / total) x 100	100%	5%	Mensal
10	Aderência a Playbooks	Execução conforme padrão	(Execuções conformes / total) x 100	≥ 98%	5%	Mensal

18.6.9. Metodologia de Pontuação por Indicador

SEC. AWAR Cada KPI será convertido em nota de 0 a 100 conforme o desempenho:

- 100 pontos → Meta atingida ou superada
- 80 pontos → Até 10% de desvio
- 60 pontos → Até 20% de desvio
- 40 pontos → Até 30% de desvio
- 0 pontos → Acima de 30% de desvio

18.6.10. A pontuação de cada indicador deverá ser multiplicada pelo seu peso, obtendo-se assim a nota ponderada de cada indicador. Todas elas somadas comporão o IDG da CONTRATADA.

18.6.11. Faixas de Desempenho e Glosa

IDG (%)	Nível de Serviço	Consequência
≥ 95%	Excelente	Pagamento integral
90% – 94,9%	Adequado	Glosa de 5%
80% – 89,9%	Regular	Glosa de 10%
< 80%	Insatisfatório	Glosa de até 20%

18.7. Catálogo De Serviço

18.7.1. Na tabela abaixo são especificados os serviços que devem ser seguidos, porém não se limitando a esses serviços, considerando a contagem de tempo em 24x7;

Referência	Serviço	Descrição
IMR-1	GESTÃO DE VULNERABILIDADE	checagem (scan) e varredura diária
IMR-2	GESTÃO DE VULNERABILIDADE	checagem (scan) e varredura semanal
IMR-3	GESTÃO DE VULNERABILIDADE	checagem (scan) e varredura mensal



IMR-4	MDR	busca continua por padrões e ameaças através da ferramenta de monitoramento e correlacionamento de logs
IMR-5	MDR	criação de casos de uso para ameaças identificadas
IMR-6	MDR	criação de regras e alertas a partir de casos de uso descobertos pelo processo de threat hunting
IMR-7	MDR	resposta a incidente crítico - sistema totalmente inoperante com impacto nas operações críticas de negócio
IMR-8	MDR	resposta a incidente alto - sistema parcialmente inoperante com impacto nas operações críticas de negócio
IMR-9	MDR	resposta a incidente médio - sistema parcialmente inoperante sem impacto nas operações críticas de negócio
IMR-10	MDR	resposta a incidente baixo - informacional, ajustes na configuração, dúvidas e/ou esclarecimentos
IMR-11	XDR	suporte técnico em casos de problemas relacionados a plataforma (console e componentes)
IMR-12	XDR	aplicar configurações da solução de seguindo as melhores práticas do fabricante
IMR-13	XDR	criar/alterar políticas
IMR-14	XDR	instalar e configurar componentes do produto
IMR-15	XDR	atender a casos que tratem de dúvida dos usuários
IMR-16	XDR	fornece orientações para execução da rotina de backup
IMR-17	XDR	apoiar consultivamente no processo de restore do backup da solução
IMR-18	XDR	monitorar os servidores (on premisses) que compõem a solução
IMR-19	XDR	apoiar de forma consultiva na distribuição do agent
IMR-20	XDR	identificar de forma proativa problemas na eficácia do endpoint gerenciado e reportar: endpoints que estão com as definições desatualizadas a mais de 7 dias
IMR-21	XDR	identificar de forma proativa problemas na eficácia do endpoint gerenciado e reportar: endpoints que não se comunicam a mais de 7 dias com a console
IMR-22	XDR	identificar de forma proativa problemas na eficácia do endpoint gerenciado e reportar: endpoints desatualizados (build)
IMR-23	DLP	relatórios periódicos sobre o status da criptografia e conformidade
IMR-24	DLP	criação e configuração de políticas para proteção de dados sensíveis
IMR-25	DLP	apoio a resposta a incidentes relacionados à violação de políticas de dlp
IMR-26	DLP	integração da solução de dlp com outras ferramentas de segurança da organização
IMR-27	DLP	relatórios de auditoria para verificar conformidade com as políticas de dlp
IMR-28	DLP	suporte técnico especializado e manutenção da solução
IMR-29	DLP	revisão periódica das políticas de dlp para garantir a eficácia contínua
IMR-30	DLP	auditoria de dlp



IMR-31	SIMULAÇÃO	instalação e configuração inicial da solução de gerenciamento de riscos de ameaças
IMR-32	SIMULAÇÃO	criação e configuração de cenários específicos para execução de testes automatizados
IMR-33	SIMULAÇÃO	realização periódica de testes automatizados no siem e no xdr
IMR-34	SIMULAÇÃO	suporte técnico especializado e manutenção da solução de pta
IMR-35	SIMULAÇÃO	revisão periódica dos cenários de teste para garantir a eficácia dos testes automatizados
IMR-36	SIMULAÇÃO	elaboração de relatórios sobre as vulnerabilidades e recomendações de mitigação
IMR-37	DISPONIBILIDADE	cadastramento dos ativos
IMR-38	DISPONIBILIDADE	configuração de threshold de alertas por cada tipo de ativo monitorado
IMR-39	DISPONIBILIDADE	configuração de dashboards customizadas por tipo de ativo
IMR-40	DISPONIBILIDADE	monitoramento dos alertas
IMR-41	DISPONIBILIDADE	notificação dos alertas via matriz de escalation através da central de serviços da contratada
IMR-42	FIREWALL	configuração de política de segurança
IMR-43	FIREWALL	aplicação de política de threat prevention (antivírus, antispware/bot ou ips)
IMR-44	FIREWALL	configurar integração com base de usuários (auth)
IMR-45	FIREWALL	aplicar controle de uso de aplicação por usuário/grupo de usuário
IMR-46	FIREWALL	configurar vpn client-to-site/site-to-site
IMR-47	FIREWALL	atualização firmware (so)
IMR-48	FIREWALL	configuração de pbf (policy based forwarding)
IMR-49	FIREWALL	configuração de política de nat
IMR-50	FIREWALL	aplicação de categoria de url filtering baseada em usuário/grupo de usuário
IMR-51	FIREWALL	aplicação de políticas de qos
IMR-52	FIREWALL	health check (relatório de adoção de uso de boas práticas de config)
IMR-53	RISCO DE IDENTIDADES	mapeamento periódico de vulnerabilidades críticas em contas privilegiadas do active directory
IMR-54	RISCO DE IDENTIDADES	integração de alertas de risco de identidade com o processo de resposta a incidentes
IMR-55	INTELIGÊNCIA DE AMEAÇAS	cadastro, atualização e remoção de marcas, domínios, ips, perfis sociais, vips, apps a serem monitorados na plataforma.
IMR-56	INTELIGÊNCIA DE AMEAÇAS	criação e ajuste de regras de alerta com base nos critérios específicos do negócio (ex: palavras-chave, geolocalização, tipos de ameaça).
IMR-57	INTELIGÊNCIA DE AMEAÇAS	abertura e análise de páginas suspeitas, para confirmação de ataque e prosseguir com solicitação de takedown.
IMR-58	MICROSEGMENTAÇÃO	mapeamento do tráfego leste-oeste entre workloads, servidores e aplicações críticas
IMR-62	MICROSEGMENTAÇÃO	criação e revisão periódica de políticas de segmentação zero trust
IMR-64	MICROSEGMENTAÇÃO	integração da microsegmentação com siem/soar para contenção automática de incidentes



IMR-65	GESTÃO ESTRATÉGICA DE RISCO	avaliação da postura de cibersegurança com base em modelos quantitativos
IMR-68	GESTÃO ESTRATÉGICA DE RISCO	recomendações estratégicas para mitigação de riscos e alinhamento às normas regulatórias (lgpd, iso 27001, bacen)
IMR-69	E-MAIL SECURITY	análise por demanda de mensagens com falhas (classificação, incidente na falhas (classificação, incidente na ferramenta)
IMR-70	E-MAIL SECURITY	relatórios periódicos sobre volume de e-mails analisados, bloqueados e liberados
IMR-72	E-MAIL SECURITY	Realizar a criação de acessos de usuários ou alterações nas roles de acesso
IMR-73	E-MAIL SECURITY	Integração com o processo de resposta a incidentes para reportar tentativas de phishing direcionado
IMR-74	E-MAIL SECURITY	Liberação de mensagens retidas na quarentena
IMR-75	CONSCIENTIZAÇÃO DE USUÁRIOS	Realização de campanhas periódicas de conscientização em segurança da informação com foco em phishing, engenharia social e boas práticas
IMR-76	CONSCIENTIZAÇÃO DE USUÁRIOS	Execução de simulações de phishing controladas, com métricas de usuários que clicaram, reportaram ou ignoraram
IMR-77	CONSCIENTIZAÇÃO DE USUÁRIOS	Emissão de relatórios executivos sobre engajamento, riscos de comportamento e evolução de maturidade dos usuários
IMR-78	CONSCIENTIZAÇÃO DE USUÁRIOS	Suporte consultivo para definição de políticas internas de boas práticas de segurança junto aos usuários
IMR-79	HIPERAUTOMAÇÃO	Configurar Virtual Appliance adicional
IMR-80	HIPERAUTOMAÇÃO	Configurar Script Host adicional
IMR-81	HIPERAUTOMAÇÃO	Configurar Coletor adicional
IMR-82	HIPERAUTOMAÇÃO	Gerar relatório executivo mensal consolidando métricas, indicadores e status do serviço
IMR-83	HIPERAUTOMAÇÃO	Revisar periodicamente a eficácia dos fluxos automatizados de resposta, recomendando ajustes de melhoria contínua
IMR-84	HIPERAUTOMAÇÃO	Integrar os mecanismos de automação ao processo formal de detecção e resposta a incidentes da CONTRATANTE
IMR-85	HIPERAUTOMAÇÃO	Garantir a rastreabilidade de todas as atividades automatizadas, com registro em trilhas de auditoria para conformidade



ANEXO III DO TR - MODELO DE PLANILHA DE PREÇOS – PROPOSTA COMERCIAL

LOTE	ITEM	DESCRIÇÃO	TECNOLOGIA	MÉTRICA	QTD	VLR. UNIT	VLR. MENSAL	VLR. TOTAL
1	1	EMS E5 SU EMS E3 Per User	EMS	Usuários	800			

LOTE	ITEM	DESCRIÇÃO	TECNOLOGIA	MÉTRICA	QTD	VLR. UNIT	VLR. MENSAL	VLR. TOTAL
2	2	Solução de Microsegmentação de rede	MICROSEG.	Workloads	1.000		N/A	

LOTE	ITEM	DESCRIÇÃO	TECNOLOGIA	MÉTRICA	QTD	VLR. UNIT	VLR. MENSAL	VLR. TOTAL
3	3	Solução de Gestão de Vulnerabilidades com foco em Risco e Identidade	GV	Ativos	1800		N/A	
	4		GVAD	Usuários	1000		N/A	
	5		RISK	Solução	1		N/A	
	6	Solução de Monitoramento Avançado, Resposta a Incidentes Automatizada, Hiperautomação, Soluções aplicadas a Firewall e teste automatizado	SIEM	GB/dia	200		N/A	
	7		DRPs	CNPJ	1		N/A	
	8		PTA	Solução	1		N/A	
	9		SecOps	Ativos	2500		N/A	
	10	Solução de Gestão de disponibilidade	Host/URL/API	Workloads	500		N/A	
	11	Solução Integrado de Proteção de E-mail, Conscientização de Usuários e Prevenção de Vazamento de Informações	SMG/ SEC. AWAR	Usuários	1000		N/A	
	12		DLP	Usuários	1000		N/A	
	13	Serviços de implantação das Soluções descritas nos Itens 3 a 12	SERVIÇOS	Escopo Fechado	1		N/A	
	14	Serviços de Operação do Security Operation Center	SERVIÇOS	Meses	24	N/A		
	15	Serviços de Monitoramento da adoção às melhores práticas de Segurança da Informação	PGV	CNPJ	1	N/A		
	16		BIA	CNPJ	1	N/A		
	17		PRI	CNPJ	1	N/A		

DADOS CADASTRAIS DA EMPRESA

CNPJ:

Razão Social:

Natureza:

Nome Fantasia:

Endereço:

Bairro:

Município:

UF:

CEP:

Telefone: ()

Responsável pela proposta:

e-mail:

Data do orçamento:

Carimbo com razão Social da Empresa ou assinatura digital

VALIDADE DA PROPOSTA

O prazo de validade da proposta deverá ser de 90 (noventa dias).

....., ... de de 2026

Atenciosamente.

Nome e assinatura do representante legal

CPF nº



ANEXO IV DO TR – MODELO DE TERMO DE RECEBIMENTO

TERMO DE RECEBIMENTO

☐ PROVISÓRIO

☐ COM RESSALVAS

☐ DEFINITIVO

☒ SEM RESSALVAS

DADOS DO CONTRATO

PROCESSO Nº:		DATA:	
CONTRATO Nº:		UNIDADE GESTORA:	
CONTRATADO:			
CNPJ:		VALOR DO CONTRATO:	
VIGÊNCIA:		A	
OBJETO:			

DADOS DO GESTOR/COMISSÃO DO CONTRATO

NOME:			
CPF:		MATRÍCULA:	
UNIDADE DE LOTAÇÃO	DE		

DADOS DO FISCAL DO CONTRATO

NOME/RAZÃO SOCIAL:	SECRETARIA DE ESTADO DA FAZENDA – SEFAZ		
CPF/CNPJ:		MATRÍCULA:	
UNIDADE DE LOTAÇÃO:			
RESPONSÁVEL TÉCNICO:			
CPF:		REGISTRO DE CLASSE:	
ENDEREÇO:			



RECIBO

CONDIÇÕES DE RECEBIMENTO

1 – A obrigação foi cumprida: ☒ No prazo ☐ Fora do prazo (Data: ____/____/____) ☐ Integralmente ☐ Parcialmente, tendo em vista o seguinte: _____ — _____ — _____ —	1 – O objeto foi entregue: ☒ Na quantidade exigida ☐ Em quantidade irregular ☐ Outras observações: _____ — _____ — _____ —
--	---

RESSALVAS

Fiscal do Contrato



ANEXO V DO TR - TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO

O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da Contratante em decorrência de relação contratual, vigente ou não.

Referência: Art. 18, Inciso V, alínea “a” da IN SGD/ME Nº 94/2022.

Pelo presente instrumento a Secretaria de Estado da Fazenda do Espírito Santo, sediada na Av. João Batista Parra, nº 600 – Enseada do Suá em Vitória-ES - CEP: 29050-375, doravante denominado CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ nº <Nº do CNPJ>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º <nº do contrato> doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da CONTRATANTE; Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições abaixo discriminadas.

1 – OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas disponibilizadas pela CONTRATANTE e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

2 – CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua



imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

3 – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

4 – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

- I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;
- II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;
- III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

5 – DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento prévio e expresso da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem



como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

6 – VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

7 – PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas



e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme previsto nos arts. 155 a 163 da Lei nº. 14.133, de 2021.

8 – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.



9 – FORO

A CONTRATANTE elege o foro da cidade de Vitória-ES, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

10 – ASSINATURAS

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

CONTRATADA	CONTRATANTE
<Nome> <Qualificação>	<Nome> <Qualificação>
TESTEMUNHAS	
<Nome> <Qualificação>	<Nome> <Qualificação>

<Local>, <dia> de <mês> de <ano>.



ANEXO VI DO TR - TERMO DE CIÊNCIA

INTRODUÇÃO

O Termo de Ciência visa obter o comprometimento formal dos empregados da Contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no órgão/entidade.

No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados.

Referência: Art. 18, Inciso V, alínea "b" da IN SGD/ME Nº 94/2022.

1 – IDENTIFICAÇÃO

CONTRATO Nº	xxxx/aaaa		
OBJETO	<objeto do contrato>		
CONTRATADA	<nome da contratada>	CNPJ	xxxxxxxxxxxxx
PREPOSTO	<Nome do Preposto da Contratada>		
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>	MATR.	xxxxxxxxxxxxx

2 – CIÊNCIA

Por este instrumento, os funcionários abaixo identificados declaram ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes da Contratante.

Funcionários da Contratada		
Nome	Matrícula	Assinatura
<Nome do(a) Funcionário(a)>	<xxxxxxxxxx>	
<Nome do(a) Funcionário(a)>	<xxxxxxxxxx>	
...	...	...

<Local>, <dia> de <mês> de <ano>.



**ANEXO VII DO TR - DECLARAÇÃO DE CIÊNCIA E CONSENTIMENTO QUANTO AO
CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS - LEI Nº 13.709/2018**

Processo Administrativo nº	Nº do Contrato	Data de Assinatura
Objeto		
Identificação da Empresa Contratada		
Nome da Empresa		
CNPJ	Inscrição Estadual	
Endereço		
Cidade	Estado	
CEP	Telefone	E-mail institucional

por meio de seu representante legal, ____, portador da Carteira de Identidade nº ____, expedida pela ____, e inscrito no CPF sob o nº ____, DECLARA QUE:

- Os eventuais dados pessoais relacionados à LICITANTE/CONTRATADA disponibilizados à SEFAZ para efeito de participação no presente certame e que possam ser exigidos para a execução contratual, serão tratados para finalidade específica, em conformidade com os termos do artigo 7º da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).
- É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.
- As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei nº 13.709/2018, sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do edital/instrumento contratual.
- As partes responderão administrativa e judicialmente, em caso de causarem danos patrimoniais, morais, individuais ou coletivos aos titulares de dados pessoais repassados em decorrência da participação no certame e eventual execução contratual, por inobservância à LGPD.

<Local>, <dia> de <mês> de <ano>.



ANEXO VIII - TERMO DE VISITA TÉCNICA

Identificação da Empresa Contratada		
Nome da Empresa		
CNPJ	Inscrição Estadual	
Endereço		
Cidade	Estado	
CEP	Telefone	E-mail institucional

Declaro para fins de participação no certame licitatório para a aquisição de serviços de Security Operation Center - SOC da SEFAZ/ES que a empresa acima, através de seu representante, _____, inscrito no CPF sob o número: _____, esteve presente na SEFAZ, à Av. João Batista Parra, nº 600, Enseada do Suá, em Vitória-ES no dia _____ para a visita técnica referente ao pregão nº _____ e foi cientificada de todos os detalhes do objeto, sendo orientada a encaminhar todos os seus questionamentos por escrito para publicação e divulgação para todos os licitantes no portal de compras Compras.gov.

Vitória, ____ de _____ de 2026.

Responsável pela condução da Visita



ANEXO IX DO TR - MODELO DE DECLARAÇÃO DE PLENO CONHECIMENTO DO OBJETO

(Timbre ou dados da empresa)

À

Secretaria de Fazenda do Estado do Espírito Santo – SEFAZ/ES

Ref.: Pregão Eletrônico nº:

DECLARAÇÃO DE PLENO CONHECIMENTO DO OBJETO

_____(razão social da licitante),
CNPJ nº _____, estabelecida no endereço

_____, neste ato
representada pelo(a) Sr(a).
_____(representant

e da empresa e qualificação do mesmo, constando inclusive qual a função/cargo na empresa), portador(a) do CPF nº _____, **DECLARA**, sob as penas da Lei, que possui pleno conhecimento do objeto do Pregão Eletrônico nº _____ e concorda com todas as exigências contidas no Edital e anexos, que **OPTOU** por não realizar a visita/vistoria ao(s) local(is) de execução dos serviços, que **ASSUME** todo e qualquer risco por esta decisão e **SE COMPROMETE** a prestar fielmente os serviços nos termos do Edital, do Termo de Referência e dos demais anexos que compõem o processo da presente licitação.

(Local e data)

Assinatura e carimbo
(Responsável da empresa)



ANEXO II – MODELOS DO EDITAL

ANEXO II.A - MODELO DE PROPOSTA COMERCIAL

____ de _____ de ____.

PREGÃO Nº 012/2026

Empresa: (Nome da Empresa)

À (Nome do Órgão)

Prezados Senhores,

1 - Compõem nossa Proposta os seguintes anexos:

1.1 - Proposta Comercial Detalhada, com a indicação do preço unitário de cada item e do preço global.

1.2 - Documentos exigidos para Habilitação.

1.3 - Dados Complementares para Assinatura do Contrato.

2 - O prazo de validade da proposta não será inferior a 90 (noventa) dias, a contar da data de sua apresentação.

3 - Os preços ora propostos incluem todas as despesas diretas, indiretas, benefícios, tributos, contribuições, seguros e licenças, além de compreender a integralidade dos custos de direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, normas infralegais, nas convenções coletivas e nos termos de ajuste de conduta vigentes, de modo a se constituírem à única e total contraprestação pelo fornecimento dos itens.

4 - Indicamos a seguinte modalidade de garantia do contrato, conforme art. 96 da Lei nº 14.133/2021: _____

Atenciosamente,

(Nome do representante e assinatura)



ANEXO III – MINUTA DE TERMO DE CONTRATO

Contrato nº ____/_____
Pregão nº 012/2026
Processo nº 2025-GN6G7
ID CiudadES nº _____

TERMO DE CONTRATO QUE ENTRE SI FAZEM
O ESTADO DO ESPÍRITO SANTO, POR
INTERMÉDIO DA SECRETARIA DE ESTADO DA
FAZENDA E A EMPRESA

PARA
CONTRATAÇÃO DE SECURITY OPERATION
CENTER – SOC.

O ESTADO DO ESPÍRITO SANTO, por intermédio da **SECRETARIA DE ESTADO DA FAZENDA – SEFAZ**, doravante denominada **CONTRATANTE**, órgão da Administração Direta do Poder Executivo, inscrita no CNPJ/MF sob o nº 27.080.571/0001-30, com sede na Avenida João Batista Parra, nº 600, Enseada do Suá, Vitória/ES, representada legalmente pelo seu **Subsecretário de Estado para Assuntos Administrativos**, Sr. **Alex dos Santos Favalessa**, servidor público, NF 3692710, nomeado(a) pelo Decreto nº 1101 S, de 10 de junho de 2024, portador da Matrícula Funcional nº 3692710 e a Empresa (**nome completo**), doravante denominada **CONTRATADA**, com sede (**endereço completo**), inscrita no CNPJ sob o nº _____ (preencher) neste ato representado(a) por (**nome e função no contratado**), conforme atos constitutivos da empresa ou procuração apresentada nos autos, ajustam o presente CONTRATO de prestação de serviços de Security Operation Center – SOC, nos termos da Lei Federal nº 14.133/2021 e Decreto Estadual nº 5.545-R/2023, de acordo com os termos do processo acima mencionado, parte integrante deste instrumento independente de transcrição, juntamente com a Proposta apresentada pela CONTRATADA, ficando, porém, ressalvadas como não transcritas as condições nela estipuladas que contrariem as disposições deste CONTRATO, que se regerá pelas Cláusulas Seguintes.

1 - CLÁUSULA PRIMEIRA: DO OBJETO

1.1 - O objeto do presente instrumento é a contratação de serviços de Security Operation Center – SOC da SEFAZ/ES, nas condições estabelecidas no Termo de Referência, Anexo I do Edital, e itens a seguir:

Lote	ITEM	DESCRIÇÃO	TECNOLOGIA	MÉTRICA	QTD	VLR. UNIT	VLR. MENSAL	VLR. TOTAL
1	1	EMS E5 SU EMS E3 Per User	SEM	Usuários	19200 (800 x 24 meses)			

Lote	ITEM	DESCRIÇÃO	TECNOLOGIA	MÉTRICA	QTD	VLR. UNIT	VLR. MENSAL	VLR. TOTAL
2	2	Solução de Microsegmentação de rede	MICROSEG	Workloads	1.000		N/A	



Lote	ITEM	DESCRIÇÃO	TECNOLOGIA	MÉTRICA	QTD	VLR. UNIT	VLR. MENSAL	VLR. TOTAL
3	3	Solução de Gestão de Vulnerabilidades com foco em Risco e Identidade	GV	Ativos	1800		N/A	
	4		GVAD	Usuários	1000		N/A	
	5		RISK	Solução	1		N/A	
	6	Solução de Monitoramento Avançado, Resposta a Incidentes Automatizada, Hiperautomação, Soluções aplicadas a Firewall e teste automatizado	SIEM	GB/dia	200		N/A	
	7		DRPs	CNPJ	1		N/A	
	8		PTA	Solução	1		N/A	
	9		SecOps	Ativos	2500		N/A	
	10	Solução de Gestão de disponibilidade	Host/URL/API	Workloads	500		N/A	
	11	Solução Integrado de Proteção de E-mail, Conscientização de Usuários e Prevenção de Vazamento de Informações	SMG/ SEC. AWAR	Usuários	1000		N/A	
	12		DLP	Usuários	1000		N/A	
	13	Serviços de implantação das Soluções descritas nos Itens 3 a 12	SERVIÇOS	Escopo Fechado	1		N/A	
	14	Serviços de Operação do Security Operation Center	SERVIÇOS	Meses	24	N/A		
	15	Serviços de Monitoramento da adoção às melhores práticas de Segurança da Informação	PGV	CNPJ	1	N/A		
	16		BIA	CNPJ	1	N/A		
	17		PRI	CNPJ	1	N/A		

1.2 - Integram este Contrato, como partes indissociáveis e independentemente de transcrição, os seguintes anexos:

- (a) o Edital e todos os seus Anexos;
- (b) a Proposta Comercial da Contratada;
- (c) Das Práticas Proibidas – GN2349-15

2 - CLÁUSULA SEGUNDA: DO PREÇO

2.1 - O valor total da contratação é de R\$ _____ (_____), para os 24 (vinte e quatro) meses de vigência contratual, realizado conforme quadro abaixo:

Lote	Item	Descrição	Forma de Pagamento	Quantidade	Valor Unitário	Valor Total
1	1	EMS E5 SU EMS E3 Per User EMS	Pagamento anual	2		R\$ -
Total Lote 1						R\$ -
2	2	Solução de Microsegmentação de rede - MICROSEG.	Pagamento anual	2		R\$ -
Total Lote 2						R\$ -
	3	Solução de Gestão de Vulnerabilidades com foco em Risco e Identidade – GV	Pagamento anual	2		R\$ -
	4	Solução de Gestão de Vulnerabilidades com foco em Risco e Identidade – GVAD	Pagamento anual	2		R\$ -
	5	Solução de Gestão de Vulnerabilidades com foco em Risco e Identidade – RISK	Pagamento anual	2		R\$ -



3	6	Solução de Monitoramento Avançado, Resposta a Incidentes Automatizada, Hiperautomação, Soluções aplicadas a Firewall e teste automatizado – SIEM	Pagamento anual	2		R\$	-
	7	Solução de Monitoramento Avançado, Resposta a Incidentes Automatizada, Hiperautomação, Soluções aplicadas a Firewall e teste automatizado – DRPs	Pagamento anual	2		R\$	-
	8	Solução de Monitoramento Avançado, Resposta a Incidentes Automatizada, Hiperautomação, Soluções aplicadas a Firewall e teste automatizado – PTA	Pagamento anual	2		R\$	-
	9	Solução de Monitoramento Avançado, Resposta a Incidentes Automatizada, Hiperautomação, Soluções aplicadas a Firewall e teste automatizado – SecOps	Pagamento anual	2		R\$	-
	10	Solução de Gestão de disponibilidade - Host/URL/API	Pagamento anual	2		R\$	-
	11	Solução Integrado de Proteção de E-mail, Conscientização de Usuários, Prevenção a Vazamento de Informações SMG/ SEC.AWAR	Pagamento anual	2		R\$	-
	12	Solução Integrado de Proteção de E-mail, Conscientização de Usuários e Prevenção de Vazamento de Informações – DLP	Pagamento anual	2		R\$	-
	13*	Serviços de implantação das Soluções descritas nos Itens 3 a 12	Pagamento parcelado, proporcional à evolução da implementação dos serviços	-	-	R\$	-
	14**	Serviços de Operação do Security Operation Center	Pagamento mensal	24		R\$	-
	15	Serviços de Monitoramento da adoção às melhores práticas de Segurança da Informação – PGV	Primeira Parcela	1		R\$	-
			Pagamento Mensal	20		R\$	-
	16	Serviços de Monitoramento da adoção às melhores práticas de Segurança da Informação - BIA	Primeira Parcela	1		R\$	-
			Pagamento Mensal	20		R\$	-
	17	Serviços de Monitoramento da adoção às melhores práticas de Segurança da Informação - PRI	Primeira Parcela	1		R\$	-
			Pagamento Mensal	20		R\$	-
Total Lote 3						R\$	-
Total Geral						R\$	-

2.2 - No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos (impostos etc.), encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

2.3 - O valor acima é meramente estimativo, de forma que os pagamentos devidos ao contratado dependerão dos quantitativos efetivamente fornecidos, e aceitos pela fiscalização/gestão do contrato

2.4 - Os preços inicialmente contratados são fixos e irrevogáveis pelo prazo de 1 (um) ano, contado da data-base vinculada à data do último orçamento estimado da contratação.

2.5 - Após o interregno de 1 (um) ano, contado da data-base estabelecida no item anterior, os preços iniciais poderão ser reajustados, mediante requerimento da CONTRATADA, pela aplicação do **Índice de Custo da Tecnologia da Informação (ICTI/IPEA)**, exclusivamente em relação às obrigações executadas após o implemento da anualidade, observada a seguinte fórmula:

$$VR = \frac{V(I - I^0)}{I^0} \quad \text{onde:}$$

VR = Valor do reajuste;

V = Valor atual do contrato ou da parcela a ser reajustada;

I⁰ = índice inicial - refere-se ao índice de custos ou de preços correspondente ao mês-base;

I = Índice relativo ao mês de reajuste.



2.6 - Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

2.7 - No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

2.8 - Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

2.9 - Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor. Na ausência de previsão legal quanto ao índice substituto, será adotado o novo índice definido para a Administração Estadual na contratação de serviços semelhantes.

2.10 - O reajuste de preços será formalizado por apostilamento.

2.11 - Os reajustes não interferem no direito das partes de solicitar, a qualquer momento, a manutenção do equilíbrio econômico dos contratos com base no disposto no art. 124, inciso II, alínea "d", da Lei 14.133/2021.

2.12 - O contratado deverá complementar a garantia contratual anteriormente prestada, de modo que se mantenha a proporção inicial em relação ao valor contratado.

2.13 - O reequilíbrio econômico e financeiro, em qualquer de suas espécies, observará, conforme a natureza do objeto contratual, as regras previstas nos arts. 45 a 53 do Decreto Estadual nº 5545-R/2023 e na Lei nº 14.133/2021, inclusive quanto à renúncia irrevogável por ausência de requerimento formal durante a vigência do contrato e antes de eventual prorrogação (art. 46 do Decreto).

3 - CLÁUSULA TERCEIRA: DAS CONDIÇÕES DE PAGAMENTO

3.1 - O pagamento será realizado de acordo com a natureza, a forma de fornecimento, os critérios de medição e aceite e o regime de execução aplicáveis a cada grupo de itens, observadas as condições estabelecidas no Termo de Referência, especialmente em seu **item 8**, e o respectivo cronograma de desembolso, nos seguintes termos:

I – Itens 1 a 12: o pagamento será realizado de forma anualizada, após a disponibilização e ativação integral do quantitativo de licenças contratado para o respectivo ciclo de subscrição, mediante comprovação de sua efetiva disponibilidade no ambiente indicado pela CONTRATANTE e emissão do correspondente Termo de Recebimento Definitivo;

II – Item 13: o pagamento será realizado de forma parcelada, proporcionalmente aos marcos físicos de implantação efetivamente concluídos e formalmente aceitos pela CONTRATANTE, conforme os percentuais, entregas e critérios de recebimento definidos no Termo de Referência, até a implementação integral das soluções;

III – Item 14: o pagamento será realizado mensalmente, no mês subsequente ao da prestação dos serviços, após a apresentação do relatório de medição, a aferição dos níveis de serviço e dos resultados alcançados e o aceite da CONTRATANTE,



observadas as eventuais glosas decorrentes do Instrumento de Medição de Resultado – IMR. Durante a fase de implantação, o valor mensal devido será proporcional à quantidade de soluções efetivamente implantadas, integradas, aceitas e transferidas para a operação, nos termos do Termo de Referência; e

IV – Itens 15 a 17: o pagamento será realizado em duas parcelas econômicas, sendo 50% (cinquenta por cento) do valor de cada item após a entrega e o aceite dos respectivos documentos de referência – RGV, BIA e RRI – e os 50% (cinquenta por cento) restantes mediante pagamentos mensais, vinculados à apresentação de relatórios, conforme o cronograma e os critérios de medição e aceite estabelecidos no Termo de Referência.

3.1.1 - A tabela abaixo resume a metodologia de pagamento a ser adotada para cada grupo de itens:

Itens	Forma de fornecimento	Medição e aceite	Pagamento
1 a 12	Disponibilização integral do quantitativo contratado em cada ciclo de subscrição.	Comprovação da ativação integral das licenças e de sua disponibilidade durante o ciclo.	Pagamento condicionado à comprovação da disponibilização e ativação do quantitativo contratado no respectivo ciclo.
13	Execução parcelada por marcos físicos de implantação.	Aceite progressivo dos marcos concluídos, conforme os critérios do Termo de Referência.	Pagamento por marco físico efetivamente executado e aceite, até a implementação completa.
14	Prestação continuada da operação do SOC.	Medição mensal dos serviços, níveis de serviço e resultados alcançados.	Pagamento mensal após aferição e aceite da medição, observadas eventuais glosas.
15 a 17	Entrega inicial por produto, seguida de acompanhamento continuado.	Aceite da entrega inicial e medições mensais da evolução das atividades.	Pagamento da entrega inicial correspondente à 50% do valor total do item e pagamentos mensais subsequentes dos 50% restantes.

3.2 - Somente poderão ser faturados os itens, parcelas, marcos físicos ou serviços efetivamente fornecidos, executados, medidos e aceitos pela CONTRATANTE, sem prejuízo da aplicação de glosas, retenções e demais ajustes previstos no Termo de Referência e neste Contrato.

3.3 - Após a autorização do Gestor do Contrato, a CONTRATADA deverá emitir a correspondente Nota Fiscal ou instrumento de cobrança equivalente, com a identificação do contrato, do grupo de itens, do período ou ciclo de referência, das parcelas executadas e dos valores eventualmente glosados.

3.4 - O pagamento será efetuado no prazo máximo de 10 (dez) dias úteis, contados do recebimento da Nota Fiscal ou do instrumento de cobrança equivalente devidamente atestado, mediante ordem bancária para crédito na conta indicada pela CONTRATADA, observadas as retenções tributárias e demais condições previstas na legislação aplicável.

3.5 - Demais condições de pagamento devem seguir as disposições constantes do Termo de Referência, anexo deste contrato.



4 - CLÁUSULA QUARTA: DO PRAZO DE VIGÊNCIA CONTRATUAL

4.1 - O prazo de vigência deste Contrato será de 24 (vinte e quatro) meses, contado da data de sua publicação no Portal Nacional de Contratações Públicas – PNCP, podendo ser prorrogado, a critério da CONTRATANTE, observadas as condições estabelecidas no Termo de Referência, os limites e requisitos previstos na Lei Federal nº 14.133/2021.

4.2 - Os prazos de execução, implantação, disponibilização de licenças, início da operação, entrega de produtos, acompanhamento e demais obrigações observarão os marcos e cronogramas específicos definidos no Termo de Referência, sem prejuízo do prazo de vigência estabelecido no item 4.1.

4.3 - Considerando a natureza das prestações abrangidas pelo objeto contratual, a possibilidade e as condições de prorrogação da vigência observarão o enquadramento específico de cada grupo de itens, nos termos da Lei Federal nº 14.133/2021 e das disposições do Termo de Referência, conforme quadro-resumo a seguir:

Itens	Classificação do Item quanto a possibilidade de Prorrogação	Prorrogação
1 a 12	Serviços contínuos. Prorrogável por até 10 (dez) anos, na forma dos artigos 106 e 107 da Lei nº 14.133/2021.	Admitida conforme o ciclo contratual e o ciclo de vida do projeto.
13	Escopo. Prazo de vigência será automaticamente prorrogado, nos termos do art. 111, da Lei nº 14.133/2021, quando o objeto não for concluído no período firmado acima, ressalvadas as providências cabíveis no caso de culpa do contratado.	Prorrogável apenas no caso de não entrega do serviço, sem reflexo financeiro adicional.
14	Serviços contínuos. Prorrogável por até 10 (dez) anos, na forma dos artigos 106 e 107 da Lei nº 14.133/2021.	Admitida conforme o ciclo contratual e o ciclo de vida do projeto.
15 a 17	Escopo. Prazo de vigência será automaticamente prorrogado, nos termos do art. 111, da Lei nº 14.133/2021, quando o objeto não for concluído no período firmado acima, ressalvadas as providências cabíveis no caso de culpa do contratado.	Prorrogável apenas no caso de não entrega do serviço, sem reflexo financeiro adicional

4.4 - Para os itens 1 a 12 e 14, caracterizados como serviços contínuos, eventual prorrogação dependerá do atendimento aos requisitos legais aplicáveis, da compatibilidade com o respectivo ciclo contratual e, quando couber, com o ciclo de vida do projeto, não gerando direito subjetivo à prorrogação em favor da CONTRATADA.

4.5 - Para os itens 13 e 15 a 17, caracterizados como prestações por escopo, a prorrogação do prazo observará o disposto no art. 111 da Lei Federal nº 14.133/2021, nas hipóteses em que o objeto não seja concluído no período contratualmente estabelecido, ressalvadas as providências cabíveis quando a não conclusão decorrer de culpa da CONTRATADA.

4.6 - A eventual prorrogação da vigência contratual dependerá de prévia manifestação da CONTRATANTE quanto à sua conveniência e oportunidade, bem como da verificação do cumprimento das condições legais e contratuais aplicáveis, inclusive quanto à manutenção da vantajosidade da contratação.



4.7 - A gestão do contrato, inclusive quanto à prorrogação, deve observar o que disposto no art. 22 do Decreto Estadual nº 5545-R/2023 e em orientações complementares da Administração Estadual.

4.8 - Não obstante o prazo estipulado nesta Cláusula, aplica-se a este Contrato as hipóteses de extinção previstas no art. 106, III, da Lei 14.133/2021, mediante justificativa da medida excepcional e prévia oitiva da Procuradoria-Geral do Estado, constituindo condições resolutivas do contrato:

4.8.1 - a inexistência ou insuficiência de dotações orçamentárias nas respectivas Leis Orçamentárias de cada exercício para atender as respectivas despesas, acarretando a extinção do contrato a partir de sua ocorrência; ou

4.8.2 - a ausência de vantagem para a Administração 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.

4.9 - Ocorrendo a resolução do contrato, com base em uma das condições resolutivas estipuladas acima, o Contratado não terá direito a qualquer espécie de indenização.

5 - CLÁUSULA QUINTA: DA DOTAÇÃO ORÇAMENTÁRIA

5.1 - As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento.

5.2 - A contratação será atendida pela seguinte dotação:

Gestão/Unidade: 220101;
Fonte de Recursos: 500 e 754;
Programa de Trabalho: 10.22.101.04.122.0050.1106;
Elemento de Despesa: 4.4.90.40 e 3.3.90.40;
Plano Interno: 2151 - GESTÃO FISCAL, CONTÁBIL E FINANCEIRA DO ESTADO.

5.3 - A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

6 - CLÁUSULA SEXTA: DA GARANTIA DE EXECUÇÃO

6.1 - A CONTRATADA prestará garantia de execução contratual no valor de R\$ _____ (preencher), na modalidade de _____ (preencher), correspondente a 5% (cinco por cento) do valor do contrato.

6.2 - O prazo de garantia de execução contratual e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

6.3 - Ocorrendo prorrogação de prazo ou aumento no valor contratual decorrente de acréscimos ou do reequilíbrio econômico-financeiro, por ocasião da assinatura do Termo



Aditivo, deverá a CONTRATADA proceder a renovação e/ou ao reforço da garantia inicial, proporcionalmente ao aumento de valor.

6.4 - A garantia deverá ser apresentada no prazo máximo de 10 (dez) dias, inclusive nos casos de Termo Aditivo.

6.4.1 - A inobservância do prazo fixado para apresentação ou renovação da garantia acarretará a aplicação de multa de 0,2% (dois décimos por cento) do valor do contrato por dia de atraso, até o máximo de 5% (cinco por cento), o qual poderá ser glosado de pagamentos devidos.

6.4.2 - O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover o bloqueio dos pagamentos devidos à CONTRATADA, até o limite de 5% (cinco por cento) do valor anual do contrato, a título de garantia.

6.4.3 - A CONTRATADA, a qualquer tempo, poderá substituir o bloqueio efetuado com base nesta cláusula por quaisquer das modalidades de garantia previstas em lei, sem prejuízo da manutenção da multa aplicada.

6.5 - Quando se tratar de consórcio, será permitido que seja apresentada a garantia integralmente pela empresa líder ou por qualquer das empresas consorciadas, ou, ainda, por cada uma das empresas consorciadas com os valores proporcionais à sua participação no consórcio.

7 - CLÁUSULA SÉTIMA: DA ENTREGA E RECEBIMENTO

7.1 - O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

8 - CLÁUSULA OITAVA: DAS RESPONSABILIDADES DAS PARTES

8.1 - Compete à Contratada:

8.1.1 - Cumprir todas as obrigações, as condições e os prazos relativos a entrega do(s) produto(s) adquirido(s) e/ou da execução do(s) serviço(s) contratado(s), conforme definido no Termo de Referência;

8.1.2 - providenciar a imediata correção das deficiências apontadas pelo setor competente do Contratante;

8.1.3 - manter, durante toda a execução do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação, conforme dispõe o inciso XVI do art. 92 da Lei Federal 14.133/2021;

8.1.4 - garantir a execução qualificada do contrato durante o período de garantia e/ou vigência, conforme definido no Termo de Referência;

8.1.5 - Visando ao regular cumprimento do contrato firmado com a Administração Pública, a CONTRATADA, nos termos do Decreto nº 4.251-R, de 21 de maio de 2018, se obriga a efetivar a contratação de mão-de-obra necessária à execução da obra ou



serviço advinda do sistema penitenciário estadual, no percentual de 6% (seis por cento) da mão-de-obra total para a execução do objeto contratual, nos termos da Lei complementar nº 879/2017;

8.1.6 - Atender demais disposições previstas no Termo de Referência.

8.2 - Compete à Contratante:

8.2.1 - efetuar o pagamento do preço previsto nos termos deste contrato;

8.2.2 - definir o local para entrega dos produtos adquiridos e/ou da execução dos serviços contratados, conforme definido no Termo de Referência;

8.2.3 - designar servidor(es) responsável(eis) pelo acompanhamento e fiscalização da entrega dos produtos adquiridos e/ou da execução do(s) serviço(s) contratado(s), conforme definido no Termo de Referência;

8.2.4 - Emitir decisão sobre eventuais solicitações ou reclamações relacionadas à execução dos contratos no prazo máximo de 1 (um) mês, a contar da data do protocolo do requerimento, admitida a prorrogação motivada, por igual período.

8.2.5 - Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 1 (um) mês, admitida a prorrogação motivada, por igual período.

8.2.6 - Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

8.3 - Da Proteção de Dados Pessoais.

8.3.1 - Proteção de dados, coleta e tratamento. Sempre que tiverem acesso ou realizarem qualquer tipo de tratamento de dados pessoais, as partes comprometem-se a envidar todos os esforços para resguardar e proteger a intimidade, vida privada, honra e imagem dos respectivos titulares, observando as normas e políticas internas relacionadas a coleta, guarda, tratamento, transmissão e eliminação de dados pessoais, especialmente as previstas na Lei Federal nº 13.709/2018 ("Lei Geral de Proteção de Dados Pessoais"), no Decreto Estadual nº 4922-R, de 09 de julho de 2021, e demais normas legais e regulamentares aplicáveis.

8.3.2 - Caso o objeto envolva o tratamento de dados pessoais com fundamento no consentimento do titular, a CONTRATADA deverá observar, ao longo de toda a vigência do Contrato, todas as obrigações legais e regulamentares específicas vinculadas a essa hipótese legal de tratamento.

8.3.3 - Ao receber o requerimento de um titular de dados, na forma prevista nos artigos 16 e 18 da Lei Federal nº 13.709/2018, a CONTRATADA deverá:

8.3.3.1 - Notificar imediatamente a CONTRATANTE;

8.3.3.2 - Auxiliá-la, quando for o caso, na elaboração da resposta ao requerimento;
e



8.3.3.3 - Eliminar todos os dados pessoais tratados com base no consentimento em até 30 (trinta) dias corridos, contados a partir do requerimento do titular.

8.3.4 - As partes armazenarão dados pessoais apenas pelo período necessário ao cumprimento da finalidade para a qual foram originalmente coletados e em conformidade com as hipóteses legais que autorizam o tratamento.

8.3.5 - As partes devem assegurar que o acesso a dados pessoais seja limitado aos empregados, prepostos ou colaboradores e eventuais subcontratados que necessitem acessar os dados pertinentes, na medida em que sejam estritamente necessários para o cumprimento deste Contrato e da legislação aplicável, assegurando que todos esses indivíduos estejam sujeitos a obrigações de sigilo e confidencialidade.

8.3.6 - A CONTRATADA deve, enquanto operadora de dados pessoais, implementar medidas técnicas e organizacionais apropriadas para o cumprimento das obrigações da CONTRATANTE previstas na Lei Federal nº 13.709/2018.

8.3.7 - Proteção de dados e incidentes de segurança. Considerando as características específicas do tratamento de dados pessoais e o estado atual da tecnologia, a CONTRATADA deverá adotar 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.

8.3.8 - A CONTRATADA deverá notificar a CONTRATANTE imediatamente sobre a ocorrência de incidentes de segurança relacionados a dados pessoais, fornecendo informações suficientes para que a CONTRATANTE cumpra quaisquer deveres de comunicação, dirigidos à Autoridade Nacional de Proteção de Dados e/ou aos titulares dos dados, acerca do incidente de segurança.

8.3.9 - As partes deverão adotar as medidas cabíveis para auxiliar na investigação e na mitigação das consequências de cada incidente de segurança.

8.3.10 - **Transferência internacional.** É vedada a transferência de dados pessoais pela CONTRATADA para fora do território do Brasil sem o prévio consentimento, por escrito, da CONTRATANTE, e demonstração da observância da adequada proteção desses dados, cabendo à CONTRATADA a responsabilidade pelo cumprimento da legislação de proteção de dados ou de privacidade de outro(s) país(es) que for aplicável.

8.3.11 - **Responsabilidade.** A CONTRATADA responderá por quaisquer danos, perdas ou prejuízos causados a CONTRATANTE ou a terceiros decorrentes do descumprimento da Lei Federal nº 13.709/2018, no Decreto Estadual nº 4922-R, de 09 de julho de 2021 e outras normas legais ou regulamentares relacionadas a este Contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização da CONTRATANTE em seu acompanhamento.

8.3.12 - Eventual subcontratação, mesmo quando autorizada pela CONTRATANTE, não exime a CONTRATADA das obrigações decorrentes deste Contrato, permanecendo integralmente responsável perante a CONTRATANTE mesmo na hipótese de descumprimento dessas obrigações por subcontratada.

8.3.13 - A CONTRATADA deve colocar à disposição da CONTRATANTE, quando solicitado, toda informação necessária para demonstrar o cumprimento do disposto



nestas cláusulas, permitindo a realização de auditorias e inspeções, diretamente pela CONTRATANTE ou por terceiros por ela indicados, com relação ao tratamento de dados pessoais.

8.3.14 - A CONTRATADA deve auxiliar a CONTRATANTE na elaboração de relatórios de impacto à proteção de dados pessoais, observado o disposto no artigo 38 da Lei Federal nº 13.709/2018, relativo ao objeto deste Contrato.

8.3.15 - Se a CONTRATANTE constatar que dados pessoais foram utilizados pela CONTRATADA para fins ilegais, ilícitos, contrários à moralidade ou mesmo para fins diversos daqueles necessários ao cumprimento deste Contrato, a CONTRATADA será notificada para promover a cessação imediata desse uso, sem prejuízo da rescisão do Contrato e de sua responsabilização pela integralidade dos danos causados.

8.3.16 - **Eliminação.** Extinto o Contrato, independentemente do motivo, a CONTRATADA deverá em, até 10 (dez) dias úteis, contados da data de seu encerramento, devolver todos os dados pessoais a CONTRATANTE ou eliminá-los, inclusive eventuais cópias, certificando a CONTRATANTE, por escrito, do cumprimento desta obrigação.

9 - CLÁUSULA NONA: DOS ADITAMENTOS

9.1 - O presente contrato poderá ser aditado, estritamente, nos termos previstos na Lei 14.133/2021, mediante manifestação formal da Procuradoria-Geral do Estado ou em conformidade com norma editada pela Procuradoria que dispense a análise jurídica.

10 - CLÁUSULA DÉCIMA: DAS SANÇÕES ADMINISTRATIVAS

10.1 - Comete infração administrativa, nos termos da Lei 14.133/2021, 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 12.846/2013.

10.2 - Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:



10.2.1 - 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 14.133/2021);

10.2.2 - Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei 14.133/2021);

10.2.3 - Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave (art. 156, § 5º, da Lei 14.133/2021);

10.2.4 - Multas (art. 156, II, e § 3º, da Lei 14.133/2021), observados os seguintes parâmetros:

10.2.4.1 - Multa moratória de 0,5% (cinco décimos por cento) por dia útil de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

10.2.4.2 - Multa compensatória de 0,5% (cinco décimos por cento) a 2% (dois por cento) incidente sobre o valor do contrato, para a infração descrita na alínea “a” do subitem 10.1;

10.2.4.3 - Multa compensatória de 0,5% (cinco décimos por cento) a 20% (vinte por cento) incidente sobre o valor do contrato, para as infrações descritas nas alíneas “b” a “h” do subitem 10.1.

10.3 - O atraso superior a 30 (trinta) dias autoriza a Administração a promover a extinção unilateral do contrato por descumprimento ou cumprimento irregular, convertendo a multa moratória em multa compensatória (art. 162, parágrafo único, da Lei 14.133/2021).

10.4 - Em caso de reincidência, o valor total das multas aplicadas não poderá exceder o limite de 30% (trinta por cento) sobre o valor total do Contrato.

10.5 - 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 14.133/2021).

10.6 - A penalidade de multa pode ser aplicada cumulativamente com as demais sanções, na forma do art. 156, § 7º, da Lei nº 14.133/2021.

10.7 - Na aplicação das sanções serão considerados (art. 156, § 1º, da Lei 14.133/2021):

(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.



10.8 - 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 14.133/2021).

10.9 - 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 14.133/2021 para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar, assim como as seguintes regras:

10.9.1 - Antes da aplicação de qualquer sanção administrativa, a Administração deverá notificar o contratado, facultando-lhe a apresentação de defesa prévia;

10.9.2 - A notificação deverá ocorrer pessoalmente, eletronicamente, com confirmação de recebimento, ou por correspondência com aviso de recebimento, indicando, no mínimo: a conduta reputada como infratora, a motivação para aplicação da penalidade, a sanção que se pretende aplicar, o prazo e o local de entrega das razões de defesa;

10.9.3 - O prazo para apresentação de defesa prévia para a penalidade de advertência será de 05 (cinco) dias úteis e de 15 (quinze) dias úteis para as demais penalidades, e serão contados na forma do art. 183 da Lei 14.133/2021;

10.9.4 - O contratado comunicará ao órgão promotor do certame as mudanças de endereço ocorridas no curso do processo licitatório e da vigência do contrato, considerando-se eficazes as notificações enviadas ao local anteriormente indicado, na ausência da comunicação;

10.9.5 - Ofertada a defesa prévia ou expirado o prazo sem que ocorra a sua apresentação, a Administração proferirá decisão fundamentada e adotará as medidas legais cabíveis, resguardado o direito de recurso, que deverá ser exercido nos termos da Lei 14.133/2021;

10.10 - Os atos previstos como infrações administrativas na Lei 14.133/2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei 12.846/2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159 da Lei 14.133/2021).

10.11 - 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 neste Contrato 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, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160 da Lei 14.133/2021).

10.12 - 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 ela 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 14.133/2021).



10.13 - 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 14.133/2021.

10.14 - Os débitos relativos a multas moratória e compensatória e as indenizações cabíveis poderão ser descontados dos valores devidos pela Administração ao contratado e, se insuficientes, a diferença poderá ser descontada da garantia prestada ou ser objeto de cobrança judicial (art. 156, § 8º, da Lei 14.133/2021).

10.14.1 - Os débitos do contratado para com a Administração contratante poderão ser compensados, total ou parcialmente, com os créditos decorrentes de outros contratos administrativos que o contratado possua com o Estado do Espírito Santo.

10.15 - Sem prejuízo da aplicação das sanções acima descritas, a prática de quaisquer atos lesivos à administração pública na licitação ou na execução do contrato, nos termos da Lei 12.846/2013, será objeto de imediata apuração observando-se o devido processo legal estabelecido no marco regulatório estadual anticorrupção.

11 - CLÁUSULA DÉCIMA PRIMEIRA: DA SUPERVENIENTE IRREGULARIDADE FISCAL, SOCIAL OU TRABALHISTA

11.1 - Constatado que o Contratado não se encontra em situação de regularidade fiscal, social ou trabalhista, o mesmo será notificado para no prazo de 10 (dez) dias úteis regularizar tal situação ou, no mesmo prazo, apresentar defesa, observando-se o procedimento de aplicação de sanções.

11.2 - Transcorrido esse prazo, ainda que não comprovada a regularidade e que não seja aceita a defesa apresentada, o pagamento será efetuado, sem prejuízo da tramitação do procedimento de aplicação de sanções.

11.3 - Em não sendo aceitas as justificativas apresentadas pelo Contratado, será imposta multa de 2% (dois por cento) sobre o saldo contratual não executado.

11.4 - Depois de transcorridos 30 (trinta) dias úteis da notificação da multa, se a empresa não regularizar a pendência fiscal ou trabalhista, deverá a Administração decidir sobre iniciar ou não procedimento de rescisão do contrato, podendo deixar de fazê-lo se reputar que a extinção antecipada do contrato ocasionará expressivos prejuízos ao interesse público.

11.5 - Em se tratando de irregularidade fiscal decorrente de crédito estadual, o Contratante informará à Procuradoria Fiscal da Procuradoria Geral do Estado sobre os créditos em favor da empresa, antes mesmo da notificação à empresa.

12 - CLÁUSULA DÉCIMA SEGUNDA: DA RESCISÃO

12.1 - A rescisão do Contrato poderá ocorrer nas hipóteses e condições previstas nos arts. 137 a 139 da Lei 14.133/2021.

13 - CLÁUSULA DÉCIMA TERCEIRA: DOS RECURSOS



13.1 - Os recursos, representação e pedido de reconsideração, somente serão acolhidos nos termos do arts. 165 a 168 da Lei 14.133/2021.

14 - CLÁUSULA DÉCIMA QUARTA: DO ACOMPANHAMENTO E FISCALIZAÇÃO

14.1 - A execução do contrato será acompanhada pelo gestor e pelo fiscal designados pela autoridade competente do órgão ou entidade, os quais representarão a Administração e confirmarão o recebimento do objeto contratado, observadas as disposições deste contrato. Sem esse recebimento, não será permitido qualquer pagamento.

15 - CLÁUSULA DÉCIMA QUINTA: DO REPRESENTANTE DA CONTRATADA

15.1 - Representará a Contratada na execução do ajuste, como preposto, (preencher no momento de assinatura do contrato, com nome completo, nacionalidade, profissão e estado civil do representante da empresa).

15.2 - O representante da CONTRATADA deverá realizar o cadastro no Sistema Corporativo de Gestão de Documentos Arquivísticos Digitais - EDOCS do Governo do Estado do Espírito Santo para envio e recebimento de documentos oficiais.

16 - CLÁUSULA DÉCIMA SEXTA: DOS CASOS OMISSOS

16.1 - Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei 14.133/2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078/1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

16.2 - Na ausência de prazo previamente estabelecido para o cumprimento de determinações emitidas pelo Contratante, será aplicado o prazo de 5 (cinco) dias úteis, contados a partir da data de ciência formal da determinação pela Contratada. Esse prazo poderá ser prorrogado, a critério exclusivo do Contratante, mediante solicitação formal e devidamente justificada pela Contratada.

17 - CLÁUSULA DÉCIMA SÉTIMA: DO FORO

17.1 - Fica eleito o foro de Vitória, Comarca da Capital do Estado do Espírito Santo, para dirimir qualquer dúvida ou contestação oriunda direta ou indiretamente deste instrumento, renunciando-se expressamente a qualquer outro, por mais privilegiado que seja.

17.2 - Antes de qualquer providência jurisdicional visando solucionar dúvida quanto à interpretação do presente instrumento, as partes deverão buscar solução administrativa, com a participação da Procuradoria Geral do Estado, por intermédio de um ou mais meios de solução consensual de conflitos previstos na Lei Complementar Estadual nº 1.011/2022.



E, por estarem justos e contratados, assinam o presente em três vias de igual teor e forma, para igual distribuição, para que produza seus efeitos legais.

Local, __ de _____ de _____ (preencher).

Nome da Contratante
Representante (nome completo)
Documento de Identificação

Nome da Contratada
Representante (nome completo)
Documento de Identificação



ANEXO I DO CONTRATO – TERMO DE REFERÊNCIA

(a ser anexado na fase de celebração do contrato, conforme Anexo I deste Edital)

ANEXO II - A PROPOSTA COMERCIAL DA CONTRATADA



ANEXO III - DAS PRÁTICAS PROIBIDAS, ELEGIBILIDADE E PAÍSES ELEGÍVEIS – GN2349-15

DAS PRÁTICAS PROIBIDAS

1. O Banco requer que todos os Mutuários (inclusive beneficiários de doações), órgãos executores e órgãos contratantes, bem como todas as empresas, entidades ou indivíduos que estejam atuando como proponentes ou participando de atividades financiadas pelo Banco, inclusive, entre outros, requerentes, licitantes, fornecedores de bens, empreiteiros, consultores, membros do pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionários (inclusive seus respectivos funcionários, empregados e representantes, sejam suas atribuições expressas ou implícitas) observem os mais altos padrões éticos e denunciem ao Banco¹ todos os atos suspeitos de constituir Prática Proibida sobre os quais tenham conhecimento ou venham a tomar conhecimento durante o processo de seleção, negociação ou execução de um contrato. As Práticas Proibidas compreendem (i) práticas corruptas, (ii) práticas fraudulentas, (iii) práticas coercitivas, (iv) práticas colusivas, (v) práticas obstrutivas e (vi) apropriação indébita. O Banco estabeleceu mecanismos para a denúncia de suspeitas de Práticas Proibidas. Qualquer denúncia deverá ser apresentada ao Escritório de Integridade Institucional (OII) do Banco para que se realize a devida investigação. O Banco também adotou procedimentos de sanção para a resolução de casos. Além disso, o Banco celebrou acordos com outras instituições financeiras internacionais visando ao reconhecimento recíproco das sanções aplicadas pelos respectivos órgãos de sanção.

(a) Para o cumprimento desta Política, o Banco define os termos indicados a seguir:

(i) *Uma prática corrupta* consiste em oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer coisa de valor para influenciar indevidamente as ações de outra parte;

(ii) *Uma prática fraudulenta* é qualquer ato ou omissão, inclusive a tergiversação de fatos ou circunstâncias que deliberada ou imprudentemente engane ou tente enganar

¹ No site do Banco (www.iadb.org/integrity) pode-se encontrar informações sobre denúncia de supostas Práticas Proibidas, as normas aplicáveis ao processo de investigação e sanção e o acordo que rege o reconhecimento recíproco de sanções entre instituições financeiras internacionais.



uma parte para obter benefício financeiro ou de outra natureza ou para evadir uma obrigação;

(iii) *Uma prática coercitiva* consiste em prejudicar ou causar danos ou ameaçar prejudicar ou causar danos, direta ou indiretamente, a qualquer parte ou a seus bens para influenciar indevidamente as ações de uma parte;

(iv) *Uma prática colusiva* é um acordo efetuado entre duas ou mais partes com o intuito de alcançar um propósito impróprio, inclusive influenciar inapropriadamente as ações de outra parte;

(v) *Uma prática obstrutiva* consiste em:

(i) destruir, falsificar, alterar ou ocultar evidência significativa para uma investigação do Grupo BID, ou prestar declarações falsas aos investigadores com a intenção de obstruir uma investigação do Grupo BID;

(ii) ameaçar, assediar ou intimidar qualquer parte para impedir a divulgação de seu conhecimento de assuntos que são importantes para a investigação do Grupo BID ou a continuação da investigação; ou

(iii) todo ato realizado com a intenção de impedir o exercício dos direitos contratuais de auditoria e inspeção do Grupo BID previstos no parágrafo 1 (f) ou seus direitos de acesso à informação; e

(vi) A “*apropriação indébita*” consiste no uso de fundos ou recursos do Grupo BID para um propósito indevido ou para um propósito não autorizado, cometido de forma intencional ou por negligência grave.

(b) Se o Banco determinar que, em qualquer etapa da aquisição ou execução de um contrato, uma empresa, entidade ou indivíduo atuando como proponente ou participando em uma atividade financiada pelo Banco, inclusive, entre outros, requerentes, licitantes, fornecedores de bens, empreiteiros, consultores, membros do pessoal, subempreiteiros, subconsultores, prestadores de serviços, concessionários, Mutuários (inclusive beneficiários de doações), órgãos executores ou órgãos contratantes (inclusive seus respectivos funcionários, empregados e representantes, sejam suas atribuições expressas ou implícitas) cometeu uma Prática Proibida, o Banco poderá:



(i) Não financiar nenhuma proposta de adjudicação de um contrato para a aquisição de bens ou a contratação de obras financiadas pelo Banco;

(ii) Suspender os desembolsos da operação se for determinado, em qualquer etapa, que um funcionário, agente ou representante do Mutuário, do órgão executor ou do órgão contratante cometeu uma Prática Proibida;

(iii) Declarar que houve aquisição viciada e cancelar e/ou declarar vencido antecipadamente o pagamento da parte do empréstimo ou doação relacionada inequivocamente com um contrato, se houver evidências de que o representante do Mutuário ou Beneficiário de uma doação não tomou as medidas corretivas adequadas (inclusive, entre outras medidas, a notificação adequada ao Banco após tomar conhecimento da Prática Proibida) dentro de um período que o Banco considere razoável;

(iv) Emitir advertência à empresa, entidade ou indivíduo com uma carta formal censurando sua conduta;

(v) Declarar que uma empresa, entidade ou indivíduo é inelegível, permanentemente ou por um período determinado, para: (i) ser adjudicada ou para participar em atividades financiadas pelo Banco; (ii) ser designado² como subconsultor, subempreiteiro, fornecedor de bens ou provedor de serviços de uma empresa elegível à qual tenha sido adjudicado um contrato financiado pelo Banco;

(vi) Encaminhar o assunto às autoridades competentes, encarregadas de fazer cumprir as leis; e/ou

(vii) Impor outras sanções que julgar apropriadas às circunstâncias, inclusive multas que representem para o Banco o reembolso dos custos referentes às investigações e processo. Essas sanções podem ser impostas adicionalmente ou em substituição às sanções acima referidas.

(c) O disposto nos incisos (i) e (ii) do parágrafo 1(b) se aplicará também aos casos em que as partes tenham sido temporariamente declaradas inelegíveis para a adjudicação

² Um subconsultor, subempreiteiro ou fornecedor de bens e serviços designado (utilizam-se diferentes expressões dependendo do documento de licitação) é aquele que cumpra uma das seguintes condições: (i) foi incluído pelo proponente em sua proposta ou proposta de pré-qualificação porque aporta experiência e conhecimentos específicos e essenciais que permitem ao proponente satisfazer os requisitos de elegibilidade da licitação; ou (ii) foi indicado pelo Mutuário.



de novos contratos, na pendência da adoção de uma decisão definitiva num processo de sanção ou qualquer outra decisão.

(d) A imposição de qualquer medida tomada pelo Banco conforme as disposições anteriormente referidas será de caráter público.

(e) Além disso, qualquer empresa, entidade ou indivíduo atuando como proponente ou participando de uma atividade financiada pelo Banco, inclusive, entre outros, requerentes, licitantes, fornecedores de bens, empreiteiros, consultores, membros do pessoal, subempreiteiros, subconsultores, prestadores de serviços, concessionários, Mutuários (inclusive beneficiários de doações), órgãos executores ou órgãos contratantes (inclusive seus respectivos funcionários, empregados e representantes, sejam suas atribuições expressas ou implícitas), poderá ser sujeito a sanções, em conformidade com o disposto nos acordos que o Banco tenha celebrado com outras instituições financeiras internacionais com respeito ao reconhecimento recíproco de decisões de inelegibilidade permanente. Para fins do disposto neste parágrafo, o termo “sanção” refere-se a toda inelegibilidade permanente, imposição de condições para a participação em futuros contratos ou adoção pública de medidas em resposta a uma contravenção às regras de uma instituição financeira internacional aplicáveis a denúncias de Práticas Proibidas.

(f) Deve constar dos documentos de licitação e dos contratos financiados com um empréstimo ou uma doação do Banco uma disposição que exija que os requerentes, licitantes, fornecedores de bens e seus representantes, empreiteiros, consultores, membros do pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionários permitam que o Banco inspecione quaisquer contas, registros e outros documentos relativos à apresentação de ofertas e ao cumprimento do contrato e os submeta a uma auditoria por auditores designados pelo Banco. De acordo com esta política, os requerentes, licitantes, fornecedores de bens e seus representantes, empreiteiros, consultores, membros do pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionários deverão prestar plena assistência ao Banco em sua investigação. O Banco requererá ainda que os contratos por ele financiados com um empréstimo ou doação incluam uma disposição que obrigue os requerentes, licitantes, fornecedores de bens e seus representantes, empreiteiros, consultores, membros do pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionários a: (i) manter todos os documentos e registros referentes às atividades



financiadas pelo Banco por um período de sete (7) anos após a conclusão do trabalho contemplado no respectivo contrato; (ii) fornecer qualquer documento necessário à investigação de denúncias de Práticas Proibidas e assegurar-se de que os empregados ou representantes dos requerentes, licitantes, fornecedores de bens e seus representantes, empreiteiros, consultores, subempreiteiros, subconsultores, prestadores de serviços e concessionários que tenham conhecimento das atividades financiadas pelo Banco estejam disponíveis para responder às consultas relacionadas com a investigação provenientes de funcionários do Banco ou de qualquer investigador, representante, auditor ou consultor devidamente designado. Caso o requerente, licitante, fornecedor de bens e seu representante, empreiteiro, consultor, membro do pessoal, subempreiteiro, subconsultor, prestador de serviços ou concessionário se negue a cooperar ou descumpra o exigido pelo Banco, ou de qualquer outra forma crie obstáculos à investigação do Banco, o Banco, a seu critério, poderá tomar medidas apropriadas contra o requerente, licitante, fornecedor de bens e seu representante, empreiteiro, consultor, membro do pessoal, subempreiteiro, subconsultor, prestador de serviços ou concessionário.

(g) O Banco exigirá que, quando um Mutuário adquirir bens, e contratar obras ou serviços (exceto os de consultoria diretamente de uma agência especializada de acordo com o parágrafo 3.10 da GN 2349-15, no âmbito de um acordo entre o Mutuário e a respectiva agência especializada, todas as disposições do parágrafo 1 relativas às sanções e Práticas Proibidas sejam aplicadas integralmente aos requerentes, licitantes, fornecedores de bens e seus representantes, empreiteiros, consultores, funcionários, subempreiteiros, subconsultores, prestadores de serviços e concessionários (inclusive seus respectivos funcionários, empregados e representantes, sejam suas atribuições expressas ou implícitas), ou qualquer outra entidade que tenha assinado contratos com essa agência especializada para fornecer os bens, obras e serviços (exceto os de consultoria), em conexão com as atividades financiadas pelo Banco. O Banco se reserva o direito de obrigar o Mutuário a lançar mão de recursos tais como a suspensão ou a rescisão. As agências especializadas deverão consultar a lista de empresas ou indivíduos declarados temporária ou permanentemente inelegíveis pelo Banco. Caso alguma agência especializada celebre um contrato ou uma ordem de compra com uma empresa ou um indivíduo declarado temporária ou permanentemente inelegível pelo Banco, o Banco não financiará os gastos correlatos e poderá tomar as demais medidas que considere apropriadas.



2. Com a concordância específica do Banco, além da Lista de Empresas e Indivíduos Sancionados, o Mutuário poderá introduzir nos formulários de licitação para contratos financiados pelo Banco o compromisso do licitante no sentido de observar, no decorrer do processo de seleção ou durante a execução do contrato, a legislação do país relativa a práticas proibidas (inclusive suborno) e as normas e sanções de uma agência de desenvolvimento multilateral/bilateral ou organização internacional que atue como cofinanciador relacionadas a práticas proibidas, conforme contido nos documentos de licitação.³ O Banco aceitará a inclusão desse compromisso, a pedido do país Mutuário, desde que as disposições que regem tal declaração lhe sejam satisfatórias.

ELEGIBILIDADE

1. O Fornecedor/Contratado e seus Subcontratados devem ser originários de países membros do Banco. Um Fornecedor ou Subcontratado é considerado nacional de um país elegível se atender aos seguintes requisitos:

- (a) Um indivíduo tem a nacionalidade de um país membro do Banco se atender a um dos seguintes requisitos:
 - (i) você é cidadão de um país membro; ou
 - (ii) Você estabeleceu seu domicílio em um país membro como residente "de boa-fé" e está legalmente autorizado a trabalhar nesse país.
- (b) Uma empresa tem a nacionalidade de um país membro se atender a ambos os seguintes requisitos:
 - (i) está legalmente constituído ou constituído sob as leis de um país membro do Banco; e
 - (ii) mais de cinquenta por cento (50%) do capital da empresa é de propriedade de pessoas físicas ou jurídicas dos países membros do Banco.

³ Por exemplo, tal compromisso pode ser redigido da seguinte forma: "Comprometemo-nos, no decorrer do processo licitatório (e durante a execução do contrato, caso nos seja adjudicado), a observar estritamente a legislação contra práticas proibidas (inclusive suborno) em vigor no país de [órgão contratante], e as normas e sanções de um organismo de desenvolvimento multilateral/bilateral ou organização internacional, atuando como cofinanciador, conforme essas leis e normas tenham sido incluídas por [órgão contratante] nos documentos de licitação para este contrato e, sem prejuízo dos procedimentos do Banco para lidar com casos de fraude e corrupção, cumprir as normas administrativas estabelecidas por [autoridade local] para receber e resolver todas as reclamações relativas aos procedimentos de licitação."



2. Todos os membros de uma joint venture, consórcio ou parceria (APCA) com responsabilidade solidária e todos os subcontratados devem cumprir os requisitos estabelecidos acima.

3. Todos os Bens e Serviços Relacionados a serem fornecidos nos termos do contrato e financiados pelo Banco devem ser originários de qualquer país membro do Banco. As mercadorias são originárias de um país membro do Banco se tiverem sido extraídas, cultivadas, colhidas ou produzidas em um país membro do Banco. Um bem é produzido quando, por meio de fabricação, processamento ou montagem, o resultado é um artigo comercialmente reconhecido cujas características básicas, função ou finalidade de uso são substancialmente diferentes de suas peças ou componentes. No caso de um bem que consiste em vários componentes individuais que requerem interconexão (que pode ser executada pelo fornecedor, pelo comprador ou por um terceiro) para tornar o bem operacional, e independentemente da complexidade da interconexão, o Banco considera esse bem elegível para financiamento se a montagem dos componentes individuais tiver sido feita em um país membro. Quando o bem é uma combinação de vários bens individuais que normalmente são embalados e vendidos comercialmente como uma única unidade, considera-se que o bem provém do país onde foi embalado e enviado ao comprador. Para efeitos de determinação da origem dos produtos identificados como "made in the European Union", estes serão elegíveis sem necessidade de identificar o país específico correspondente da União Europeia. A origem dos materiais, partes ou componentes das mercadorias ou a nacionalidade da empresa que produz, monta, distribui ou vende as mercadorias não determinam a origem das mercadorias.

PAÍSES ELEGÍVEIS

1. Países:

Alemanha, Argentina, Áustria, Bahamas, Barbados, Bélgica, Belize, Bolívia, Brasil, Canadá, Colômbia, Costa Rica, Chile, Croácia, Dinamarca, Eslovênia, Equador, El Salvador, Espanha, Estados Unidos, Finlândia, França, Guatemala, Guiana, Haiti, Holanda, Honduras, Israel, Itália, Jamaica, Japão, México, Nicarágua, Noruega, Panamá, Paraguai, Peru, Portugal, Reino Unido, República da Coreia, República



Dominicana, República Popular da China, Suécia, Suíça, Suriname, Trinidad e Tobago, Uruguai e Venezuela.

Territórios elegíveis

- (a) Guadalupe, Guiana Francesa, Martinica, Reunião – por ser Departamento da França.
- (b) Ilhas Virgens Americanas, Porto Rico, Guam - como Território dos Estados Unidos da América.
- (c) Aruba – como país constituinte do Reino dos Países Baixos; e Bonaire, Curaçao, Sint Maarten, Sint Eustatius - por serem Departamentos do Reino dos Países Baixos.
- (d) Hong Kong – Região Administrativa Especial da República Popular da China.

2) Critérios para determinar a nacionalidade e o país de origem dos bens e serviços

Os seguintes critérios serão usados para determinar: (a) a nacionalidade das empresas e indivíduos elegíveis para propor ou participar de contratos financiados pelo Banco e (b) o país de origem dos bens e serviços:

(A) Nacionalidade

(a) **Um indivíduo** é considerado nacional de um país membro do Banco se satisfaz um dos seguintes requisitos:

- (i) é cidadão de um país membro; ou
- (ii) estabeleceu seu domicílio em um país membro como residente "de boa-fé" e está legalmente autorizado a trabalhar nesse país.

(b) **Uma empresa** tem a nacionalidade de um país membro se satisfazer a dois requisitos a seguir:

- i. estar legalmente constituída ou estabelecida conforme as leis de um país membro do Banco; e
- ii. mais de cinquenta por cento (50%) do capital da empresa é de propriedade de indivíduos ou empresas de países membros do Banco.

Todos os sócios de uma associação em participação, consórcio ou associação (ACS) com responsabilidade conjunta e solidária e todos os subconsultores devem cumprir os requisitos estabelecidos acima



C) Origem dos Bens / Ativos

Os bens têm origem em um país membro do Banco se foram extraídos, cultivados, colhidos ou produzidos em um país membro do Banco. Considera-se que um bem é produzido quando, mediante manufatura, processamento ou montagem, o resultado é um artigo comercialmente reconhecido cujas características, funções ou finalidades de uso são substancialmente diferentes de suas partes ou componentes.

No caso de um bem que consiste em vários componentes individuais que devem ser interconectados (pelo fornecedor, comprador ou um terceiro) para que o bem possa ser utilizado, e sem importar a complexidade da interconexão, o Banco considera que este bem é elegível para o financiamento se a montagem dos componentes tiver sido feita em um país membro. Quando o bem é uma combinação de vários bens individuais que normalmente são empacotados e vendidos comercialmente como uma só unidade, o bem é considerado proveniente do país onde este foi empacotado e embarcado com destino ao comprador.

Para fins de determinação da origem dos bens identificados como “feito na União Europeia”, estes serão elegíveis sem necessidade de identificar o correspondente país específico da União Europeia.

A origem dos materiais, partes ou componentes dos bens ou a nacionalidade da empresa produtora, montadora, distribuidora ou vendedora dos bens não determina a origem deles.

C) Origem dos Serviços

O país de origem dos serviços é o mesmo do indivíduo ou empresa que presta os serviços, conforme os critérios de nacionalidade acima estabelecidos. Este critério é aplicado aos serviços conexos ao fornecimento de bens (tais como transporte, seguro, instalação, montagem etc.), aos serviços de construção e aos serviços de consultoria.

Documento original assinado eletronicamente, conforme MP 2200-2/2001, art. 10, § 2º, por:

ANGÉLICA TONEL ABRANTES COELHO
AGENTE DE CONTRATAÇÃO
SUBSAD - SEFAZ - GOVES
assinado em 26/10/2026 16:46:30 -03:00



INFORMAÇÕES DO DOCUMENTO

Documento capturado em 26/10/2026 16:46:30 (HORÁRIO DE BRASÍLIA - UTC-3)
por ANGÉLICA TONEL ABRANTES COELHO (AGENTE DE CONTRATAÇÃO - SUBSAD - SEFAZ - GOVES)
Valor Legal: ORIGINAL | Natureza: DOCUMENTO NATO-DIGITAL

A disponibilidade do documento pode ser conferida pelo link: <https://e-docs.es.gov.br/d/2026-N7HHFL>