PREGÃO ELETRÔNICO Nº 377/2026	
SECRETARIA ESPECIAL DE GESTÃO DAS CONTRATAÇÕES, LICITAÇÕES E LOGÍSTICA - SECLOG	
PROCESSO N° 174/2026-COMPRAS.GOV-SEPLAN	
TIPO	MENOR PREÇO POR LOTE.
BASE LEGAL	Lei nº 14.133/2021. LC nº 123/2006. Leis Estaduais nº: 9.1832023; 9.166/2023, 9.156/2023 e 8747/2020. Decretos Estaduais nº: 285/2023 e 342/2023.
OBJETO:	Registro de preço para Contratação de solução de software do tipo Plataforma Unificada de Operações de Cibersegurança operando em arquitetura centralizada, capaz de consolidar em um único console as funções de: Detecção e Resposta a Ameaças (XDR), Gestão de Vulnerabilidades, Inteligência de Ameaças, Simulação de Ataques (Segurança Ofensiva), Automação de Resposta a Incidentes (SOAR) e Governança, Risco e Conformidade (GRC), incluindo mecanismos de integridade de dados via Blockchain, na modalidade Software as a Service (SaaS), visando atender às necessidades dos órgãos e entidades do Estado de Sergipe.
PARTICIPAÇÃO:	AMPLA

	DIA	**HORÁRIO**
INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS	23/09/2026	09h00min

REFERÊNCIA DE TEMPO: Para todas as referências de tempo será observado o horário de Brasília /DF e, dessa forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.

FORMALIZAÇÃO DE CONSULTAS E EDITAL:

Secretaria de Especial das Contratações, Licitações e Logística - SECLOG

Endereço: Rua Duque de Caxias n° 346 – Bairro São José – CEP: 49.015-320 – Aracaju/SE – Secretaria Especial de Gestão das Contratações, Licitações e Logística – SECLOG.

-Horário de Expediente: 7h às 13h
- www.comprasnet.se.gov.br
- www.licitanet.com.br
-wellington.melo@seclog.se.gov.br

LOCAL: www.licitanet.com.br

EDITAL

PROCESSO Nº 174/2026-COMPRAS.GOV-SEPLAN

Pregão nº 377/2026.

1.0 - DISPOSIÇÕES PRELIMINARES:

1.1 – A SECLOG e este Pregoeiro, designado pela Portaria nº 14 de 2026, tornam público para conhecimento dos interessados que na data, horário e local já indicados anteriormente, realizar-se-á licitação na modalidade PREGÃO ELETRÔNICO, do tipo MENOR PREÇO POR LOTE.

OBSERVAÇÃO: Em caso de eventual diferença entre a(s) especificação(ões) do objeto descritas no Licitanet e as especificações constantes neste edital de pregão eletrônico, prevalecerão as últimas.

2.0 - DO OBJETO:

2.1 - O presente Pregão Eletrônico tem por objeto o Registro de preços para Contratação de solução de software do tipo Plataforma Unificada de Operações de Cibersegurança operando em arquitetura centralizada, capaz de consolidar em um único console as funções de: Detecção e Resposta a Ameaças (XDR), Gestão de Vulnerabilidades, Inteligência de Ameaças, Simulação de Ataques (Segurança Ofensiva), Automação de Resposta a Incidentes (SOAR) e Governança, Risco e Conformidade (GRC), incluindo mecanismos de integridade de dados via Blockchain, na modalidade Software as a Service (SaaS), visando atender às necessidades dos órgãos e entidades do Estado de Sergipe, conforme especificações técnicas constantes do Anexo I deste edital.

2.2 – O Sistema de Registro de Preços tem por finalidade o registro formal de preços, fornecedores, unidades participantes e condições de execução do objeto, aplicáveis a futuras contratações decorrentes da Ata de Registro de Preços.

2.3 - A existência de preços registrados não obriga a Administração Pública Estadual a firmar as contratações que dele poderão advir, ficando-lhe facultada a realização de licitações para aquisição de um ou mais itens, hipótese em que, em igualdade de condições, o beneficiário do registro terá preferência, nos termos do art. 195 do Decreto Estadual nº 342/2023.

3.0 - DOTAÇÃO ORÇAMENTÁRIA:

3.1 - As despesas decorrentes da contratação do objeto desta licitação correrão à conta dos recursos consignados no orçamento do Estado de Sergipe para os exercícios alcançados pelo prazo de validade da Ata de Registro de Preços, a cargo da unidade orçamentária contratante, cujos programas de trabalho e elementos de despesas específicos constarão no respectivo Contrato (Anexo III).

4.0 - DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO:

4.1- Até 03 (três) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este Edital mediante petição a ser enviada via sistema e/ou para o endereço de e-mail do pregoeiro indicado na primeira folha deste edital.

4.2- Caberá ao Pregoeiro decidir sobre a impugnação no prazo de até três dias úteis contados da data de recebimento da impugnação.

4.2.1 - O pregoeiro poderá ser auxiliado, em caso de dúvida, por aqueles que participaram da fase de planejamento da contratação ou por outros órgãos, para apoio

técnico, conforme art. 8º, §3º da Lei nº 14.133/2021, bem como pela PGE/SE, mediante consulta encaminhada pelo Secretário Especial da SECLOG, nos termos do §7º do art. 20 do Decreto Estadual nº 342/2023.

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

4.4- Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico via internet, no endereço indicado no Edital.

4.5- O pregoeiro responderá aos pedidos de esclarecimentos no prazo de até 03 (três) dias úteis, contado da data de recebimento do pedido, e poderá, em caso de dúvida, requisitar subsídios formais aos responsáveis pela elaboração do edital e dos anexos.

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

4.5.2- A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

4.6- As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a administração.
4.7- As impugnações ao Edital e os pedidos de esclarecimentos, somente serão considerados tempestivos se enviados até o último dia útil para apresentação.

5.0 - CONDIÇÕES PARA PARTICIPAÇÃO:

5.1 - Poderão participar do processo os interessados que atenderem a todas as exigências contidas neste Edital e seu Anexo.

5.2 - Estarão impedidos de participar, direta ou indiretamente, de qualquer fase deste processo licitatório os interessados que se enquadrem em uma ou mais das situações a seguir:

5.2.1 - estejam cumprindo a penalidade de suspensão temporária ou de impedimento de licitar e de contratar, impostas pelo Estado de Sergipe.

5.2.2 - sejam declaradas inidôneas em qualquer esfera de Governo;

5.2.3 - estejam sob falência, dissolução ou liquidação;

5.2.3.1 - as empresas em recuperação judicial poderão participar se comprovar a existência de plano de recuperação judicial homologado, aprovado ou autorizado pelo juízo competente.

5.2.4 - autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando estes forem os elementos técnicos fundamentais de licitação que versar sobre obra, serviços ou fornecimento de bens a ele relacionados;

5.2.5 - 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 obra, serviços ou fornecimento de bens a ela necessários;

5.2.6 - servidores ou dirigentes de órgão ou entidade contratante ou responsável pela licitação;

5.2.7 - empresas controladoras, controladas ou coligadas, nos termos da Lei (Federal) nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

5.2.8 - 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

5.3 - NÃO será concedido tratamento diferenciado e favorecido às microempresas e empresas de pequeno porte (ME/EPP) neste Pregão Eletrônico, uma vez que o objeto - Plataforma Unificada de Operações de Cibersegurança (SaaS), enquadra-se na hipótese de afastamento prevista na Lei Estadual nº 8.747/2020, por tratar-se de objeto de alta especificidade técnica incompatível com segmentação de cota reservada, conforme fundamentação constante do item 1.7 do Termo de Referência.

5.4 - É admitida a participação de empresas em consórcio, nos termos do art. 97 do Decreto Estadual nº 342/2023**.**

6.0 - REGULAMENTO OPERACIONAL DO CERTAME:

6.1 - O certame será conduzido pelo Pregoeiro, que terá, em especial, as seguintes atribuições:

6.1.1 - coordenar os trabalhos da equipe de apoio;

6.1.2 - receber, examinar e decidir as impugnações e os pedidos de esclarecimentos ao edital e aos anexos, além de poder requisitar subsídios formais aos responsáveis pela elaboração desses documentos;

6.1.3 - verificar a conformidade da proposta em relação aos requisitos estabelecidos, inclusive quanto às amostras;

6.1.4 - coordenar a sessão pública e o envio de lances;

6.1.5 - verificar e julgar as condições de habilitação;

6.1.6 - sanear erros ou falhas que não alterem a substância das propostas, dos documentos de habilitação e sua validade jurídica;

6.1.7 - receber, examinar os recursos, emitir relatório e encaminhá-los à autoridade competente quando mantiver sua decisão;

6.1.8 - declarar o vencedor;

6.1.9 - adjudicar o objeto, quando não houver recurso e quando o valor arrematado estiver dentro do valor de referência;

6.1.10 - conduzir os trabalhos da equipe de apoio; e

6.1.11 - encaminhar o processo à autoridade superior para homologação.

7.0 - PARTICIPAÇÃO:

7.1 – As propostas de preço deverão ser encaminhadas eletronicamente até data e horário definidos para a abertura das propostas, conforme indicação na primeira página deste Edital.

7.2 - Caberá ao fornecedor acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

7.3 - Caso haja desconexão com o Pregoeiro no decorrer da etapa competitiva do pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances, retornando o

Pregoeiro, quando possível, sua atuação no certame, sem prejuízo dos atos realizados.

7.3.1 - Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão do pregão poderá ser suspensa e terá reinício somente após comunicação expressa aos participantes na opção *chat* do sistema eletrônico, onde será designado dia e hora para a continuidade da sessão.

7.4 - Caso exista a necessidade de ser suspenso o Pregão, tendo em vista a quantidade de lotes/itens, o Pregoeiro designará novo dia e horário para a continuidade do certame.

7.5 – O andamento do procedimento de licitação entre a data de abertura das propostas e a adjudicação do objeto deve ser acompanhado diariamente pelos participantes por meio do portal "www.licitanet.com.br", que veiculará avisos, convocações, desclassificações de licitantes, justificativas e outras decisões referentes ao procedimento.

8.0 - DA APRESENTAÇÃO DA PROPOSTA

8.1 - Os licitantes encaminharão, exclusivamente por meio do sistema (licitanet), a proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

8.1.1- Para envio das documentações no sistema, seguir o manual de orientações para envio de proposta e documentos de habilitação, disponibilizado no sítio https://www.licitanet.com.br;
8.1.2- A(s) proposta(s) deverá(ão) ser enviada(s) em seu(s) respectivo(s) lote(s)/item (ns);
8.1.3- Após negociações, a proposta atualizada deverá ser anexada no sítio http://www.licitanet.com.br/ dentro do prazo estabelecido no item 9.25.2.

8.2 - O envio da proposta ocorrerá por meio de usuário e senha.

8.2.1 – Os documentos em meio físico não serão recebidos/reconhecidos pela SECLOG.

8.3 – A proposta de preços do licitante deverá conter as seguintes informações, quando for o caso:

8.3.1 -Valor unitário e total do item;

8.3.2 – Marca;

8.3.3 - Fabricante;

8.3.4 - Descrição detalhada do objeto, contendo as informações similares à especificação do Termo de Referência.

8.4 - O licitante classificado em primeiro lugar terá o prazo de até 03 (três) horas para apresentação dos documentos de habilitação.

8.4.1 - convocado para apresentação dos documentos de habilitação, o licitante poderá entregá-los parcialmente, desde que constem os documentos ausentes no SICAF.

8.4.2 - Para tanto, deve informar esta condição imediatamente (via chat de mensagens do licitanet) após encerrada a sessão de disputa, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

8.5 -Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta anteriormente inserida no sistema;

8.6 -Os documentos que compõem a proposta somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

8.7 - As propostas encaminhadas terão prazo de validade de 90 (noventa) dias consecutivos, contados da data da sessão de abertura desta licitação, conforme disposição legal.

8.8 - Os preços deverão ser cotados em moeda corrente nacional e preenchidos no campo apropriado do sistema eletrônico e neles deverão estar inclusas todas e quaisquer despesas, tais como frete, encargos sociais, seguros, tributos diretos e indiretos incidentes sobre o fornecimento do objeto licitado.

8.9 O não cumprimento do item 8.0, e de seus subitens, ensejará desclassificação no certame, salvo motivo devidamente justificado e aceito pelo Pregoeiro.

8.10 - A proposta de preços deverá ser cotada de acordo com o detalhamento constante no Termo de Referência (Anexo I).

9.0 - <u>ABERTURA DAS PROPOSTAS E SESSÃO DE LANCES:</u>

9.1- A partir do horário previsto neste edital, terá início à sessão pública do Pregão Eletrônico, com a divulgação das propostas de preços recebidas pelo sítio já indicado no item 8.1, passando o Pregoeiro a avaliar a aceitabilidade das propostas.

9.2 - Aberta a etapa competitiva, os representantes dos licitantes deverão estar conectados ao sistema para participar da sessão de lances. A cada lance ofertado o participante será imediatamente informado de seu recebimento e respectivo horário de registro e valor.

9.2.1- Para efeito da disputa de preços, as propostas encaminhadas eletronicamente pelos licitantes serão consideradas lances.

9.2.2- Cada licitante poderá encaminhar lance com valor superior ao menor preço registrado, desde que seja inferior ao seu último lance e diferente de qualquer outro valor ofertado para o lote/item.

9.3 - Com o intuito de conferir celeridade à condução do processo licitatório, é permitido ao pregoeiro a abertura e gerenciamento simultâneo da disputa de até 10 lotes/itens da mesma licitação.

9.3.1- O pregoeiro comunicará aos licitantes, após a abertura da sala de disputa, a sua opção por realizar a disputa simultânea de lotes/itens, se for o caso.

9.3.2 - Em regra, a disputa simultânea de lotes/itens obedecerá à ordem sequencial dos mesmos. Entretanto, o pregoeiro poderá efetuar a abertura da disputa de lotes/itens selecionados fora da ordem sequencial.

9.4- O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis ou não apresentem as especificações técnicas exigidas no Termo de Referência.

9.4.1 - A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

9.4.2 - A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

9.5- O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

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

9.6.1- O lance deverá ser ofertado **PELO VALOR TOTAL DO LOTE.**

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

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

9.9 - O intervalo entre os lances enviados, tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta, não poderá ser inferior a 05 (cinco) segundos, sob pena de serem automaticamente descartados pelo sistema os respectivos lances.

9.10 - Será adotado para o envio de lances no pregão eletrônico o modo de disputa **"ABERTO E FECHADO"**, em que os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

9.11 - A etapa de lances da sessão pública terá duração inicial de 15 (quinze) minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de tempo de até 10 (dez) minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

9.12 - Encerrado o prazo previsto no item 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 05 (cinco) minutos, o qual será **sigiloso** até o encerramento deste prazo.

> 9.12.1- Não havendo pelo menos 03 (três) ofertas nas condições definidas neste item, poderão os autores dos melhores lances, na ordem de classificação, até o máximo de 03 (três), oferecer um lance final e fechado em até 05 (cinco) minutos, o qual será **sigiloso** até o encerramento deste prazo.

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

> 9.13.1- Não havendo lance final e fechado classificado na forma estabelecida nos itens anteriores, haverá o reinício da etapa fechada, para que os demais licitantes, até o máximo de 03 (três), na ordem de classificação, possam ofertar um lance final e fechado em até 05 (cinco) minutos, o qual será **sigiloso** até o encerramento deste prazo.

9.14- Poderá o pregoeiro, auxiliado pela equipe de apoio, justificadamente, admitir o reinício da etapa fechada, caso nenhum licitante classificado na etapa de lance fechado atender às exigências de habilitação.

9.15- Em caso de falha no sistema (em qualquer fase do certame) a ocorrência deverá ser comunicada imediatamente ao Licitanet, pelo licitante ou pelo pregoeiro. Os lances em desacordo com os subitens anteriores poderão ser desconsiderados pelo pregoeiro após manifestação do Licitanet acerca da ocorrência;

> 9.15.1- Na hipótese do subitem anterior, a ocorrência deverá ser registrada no chat de mensagens (licitanet).

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

9.17- 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.

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

9.19- Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.

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

9.19.2- O pregoeiro solicitará ao licitante melhor classificado que, **no prazo de 03 (três) horas,** envie a proposta adequada ao último lance ofertado após a negociação realizada, **acompanhada dos documentos de habilitação** exigidos neste Edital.

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

10.0 - JULGAMENTO DAS PROPOSTAS

10.1 - O Pregoeiro efetuará o julgamento das propostas pelo critério de "**MENOR PREÇO**", podendo encaminhar, pelo sistema eletrônico, contraproposta diretamente ao licitante que tenha apresentado o lance de menor valor por item/lote, para que seja obtido preço melhor, bem assim decidir sobre sua aceitação, observados os prazos para fornecimento, as especificações técnicas, parâmetros mínimos de desempenho e de qualidade e demais condições definidas neste edital.

10.2 - Após o encerramento da sessão de disputa e estando o valor da melhor proposta acima do valor de referência, o Pregoeiro negociará a redução do preço com o seu detentor.

10.2.1 – No caso em que o orçamento estimado da contratação tenha caráter sigiloso, ele será tornado público apenas e imediatamente após a classificação final e fase de negociação, sem prejuízo da divulgação no instrumento convocatório do detalhamento dos quantitativos e das demais informações necessárias para a elaboração das propostas (Art. 51 do Decreto Estadual n.º 342/2023 e art. 24 da Lei nº 14.133/2021).

10.3 - Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao valor de referência estipulado nos autos do processo administrativo que deu origem a este edital.

10.4 - Será desclassificada a proposta vencedora que:

10.4.1- contiver vícios insanáveis;

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

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

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

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

10.5- No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

10.5.1 - A inexequibilidade só será considerada após diligência do pregoeiro, que comprove:

a) que o custo do licitante ultrapassa o valor da proposta; e
b) inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

10.5.2 - Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita.

10.6 - Havendo lances no tempo de disputa da sessão pública, a proposta final de preços do licitante detentor da melhor oferta deverá ter seus valores unitários e totais ajustados de forma que os preços de cada um dos itens não resultem, após os ajustes, inexequíveis, superfaturados ou acima dos valores unitários de referência;

10.7 - Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, 24 (vinte e quatro) horas de antecedência, e a ocorrência será registrada em ata;

10.8 - O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, no prazo a ser definido pelo pregoeiro, sob pena de não aceitação da proposta.

10.8.1- O prazo estabelecido poderá ser prorrogado pelo Pregoeiro por solicitação escrita e justificada do licitante, formulada antes de findo o prazo, e formalmente aceita pelo Pregoeiro.

10.8.2- Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo Pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

10.9 - Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

10.10 - Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.

10.11 - Se o licitante desatender às exigências habilitatórias, abaixo definidas, o Pregoeiro examinará a proposta ou o lance subsequente, verificando a sua aceitabilidade, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta ou lance que atenda ao edital.

11.0 - DA HABILITAÇÃO:

11.1 - Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

11.1.1- Consolidada de Pessoa Jurídica do Tribunal de Contas da União (https://certidoes-apf.apps.tcu.gov.br/)

11.1.2- A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 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.

11.1.3 - Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

11.1.4 - A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

11.1.5 - O licitante será convocado para manifestação previamente à sua inabilitação.

11.1.6 - Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

11.2 - 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.

11.3 - Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

11.4 - Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

11.4.1- Serão aceitos registros de CNPJ de licitante matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

11.5- Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a anexá-los no sítio http://www.licitanet.com.br/ no prazo de 03 (três) horas, sob pena de inabilitação.

11.6- Ressalvado o disposto no item 7.3 (desconexão do sistema), os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação:

11.7 - **Habilitação jurídica:**

11.7.1- No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

11.7.2- Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

11.7.3- No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

11.7.4- Inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

11.7.5- No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

11.7.6- No caso de cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 1971;

11.7.7- No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização;

11.7.8- Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva;

11.7.9 - Além dos documentos acima arrolados, em cada caso, se permitido o consórcio de empresas, deverá haver comprovação do compromisso público ou particular de

constituição de consórcio, subscrito pelos consorciados, no qual conste cláusula de responsabilidade solidária e indicação da pessoa jurídica líder, responsável pelo consórcio, conforme art. 97 do Decreto Estadual nº 342/2023 e art. 15 da Lei nº 14.133/2021.

11.7.9.1 - As empresas que participem por meio de consórcio ficam impedidas de participar desta licitação de forma isolada ou por meio de outro consórcio.

11.7.9.2 - Todas as empresas que compõem o consórcio devem apresentar seus documentos para fins de habilitação jurídica.

11.8- Regularidade fiscal e trabalhista:

11.8.1- prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

11.8.2-prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

11.8.4- prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

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

11.8.6 - prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

11.8.7 - prova de regularidade com a Fazenda Estadual do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

11.8.8 -caso o licitante seja considerado isento dos tributos estaduais relacionados ao objeto licitatório, deverá comprovar tal condição mediante declaração da Fazenda Estadual do seu domicílio ou sede, ou outra equivalente, na forma da lei;

11.8.9 - Todas as empresas que compõem o consórcio devem apresentar regularidade fiscal e trabalhista.

11.9-Qualificação Econômico-Financeira.

11.9.1- Certidão negativa de feitos sobre falência, recuperação judicial ou recuperação extrajudicial, expedida pelo distribuidor da sede do licitante. Caso a empresa se encontre em processo de recuperação judicial, deverá ser apresentada certidão emitida pela instância judicial competente, que certifique que a interessada está apta econômica e financeiramente a participar de procedimento licitatório nos termos da Lei nº 14.133/2021;

11.9.2- Balanço patrimonial e demonstrações contábeis dos 2 (dois) últimos exercícios sociais, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

11.9.2.1 - As exigências contidas neste item podem ser comprovadas por meio de registro na junta comercial respectiva ou por intermédio do SPED – Sistema Público de Escrituração Digital, na forma da legislação que regula a matéria;

11.9.2.2- No caso de empresa constituída há menos de 02 (dois) anos, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

11.9.2.3 - É admissível o balanço intermediário, se decorrer de lei ou contrato social/estatuto social.

11.9.2.4 - Caso o licitante seja cooperativa, tais documentos deverão ser acompanhados da última auditoria contábil-financeira, conforme dispõe o artigo 112 da Lei nº 5.764, de 1971, ou de uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador;

11.9.2.6- A comprovação da situação financeira da empresa será constatada mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um) resultantes da aplicação das fórmulas:

$$LG = \frac{\text{Ativo Circulante} + \text{Realizável à Longo Prazo}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

11.9.2.5 - As empresas que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar, considerados os riscos para a Administração, e, a critério da autoridade competente, o capital social mínimo ou o patrimônio líquido mínimo de **10% (dez por cento)** do valor estimado da contratação ou do item pertinente.

11.9.3 - Em caso de consórcio, devem ser cumpridos os seguintes requisitos:

11.9.3.1 - apresentação do somatório dos valores de cada consorciado na proporção de sua respectiva participação;

11.9.3.2 - acréscimo de 20% (vinte por cento) sobre o valor, índice ou percentual exigido de licitante individual para a habilitação econômico-financeira;

11.9.3.3 - demonstração, por todos os consorciados, do atendimento aos requisitos contábeis definidos no instrumento convocatório.

11.10- Qualificação Técnica

11.10.1- **Comprovação de aptidão para o fornecimento de bens em características,** quantidades e prazos compatíveis com o objeto desta licitação, e com o item pertinente, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.

11.10.1.1 – Para efeito de comprovação da qualificação exigida no item 11.10.1, o licitante deverá seguir o detalhamento informado no Termo de Referência anexado a este edital.

11.11 - O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal

11.12 - Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a continuidade da mesma.

11.13 -Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.

11.14 - O licitante provisoriamente vencedor em um lote/item, que estiver concorrendo em outro lote/item, ficará obrigado a comprovar os requisitos de habilitação cumulativamente, isto é, somando as exigências do lote/item em que venceu às do lote/item em que estiver concorrendo, e assim sucessivamente, sob pena de inabilitação, além da aplicação das sanções cabíveis.

11.14.1- Não havendo a comprovação cumulativa dos requisitos de habilitação, a inabilitação recairá sobre o(s) lote (s)/ item(s) de menor(es) valor(es) cuja retirada(s) seja(m) suficiente(s) para a habilitação do licitante nos remanescentes.

11.15 - O Pregoeiro reserva-se o direito de solicitar da licitante, em qualquer tempo, no curso da licitação, quaisquer esclarecimentos sobre documentos já entregues, fixando-lhe prazo para atendimento.

11.16 - A falta de qualquer dos documentos de habilitação exigidos no edital implicará a inabilitação da licitante, situação em que poderá ser concedido prazo para complementação da documentação, mediante motivo devidamente justificado e aceito pelo pregoeiro.

11.17 - Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor.

12.0 - DOS RECURSOS:

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

12.2 - A intenção de recorrer deverá ser manifestada imediatamente, no prazo improrrogável de 10(dez) minutos, sob pena de preclusão, após julgamento da proposta e habilitação.

12.2.1 - A intenção de recurso deverá ser apresentada em campo específico do sistema e não suspenderá a sessão de licitação.

12.2.2 - A intenção de recurso só será analisada pelo pregoeiro no momento do recebimento das razões recursais.

12.3 - Declarado vencedor, fica aberto o prazo recursal de 03 (três) dias úteis para apresentação de suas razões.

12.3.1 - As razões recursais só serão recebidas pelo pregoeiro se constar no sistema a intenção de recurso apresentada no prazo correspondente.

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

12.5 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.

12.6 Os recursos interpostos fora do prazo não serão conhecidos.

12.7 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 vista imediata dos elementos indispensáveis à defesa de seus interesses.

12.8 O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida, somente em relação ao lote/item objeto da contestação, até que sobrevenha decisão final da autoridade competente.

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

12.10 Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico.

13.0 - DA ADJUDICAÇÃO E HOMOLOGAÇÃO

13.1- Em caso de recurso, ou quando houver apenas uma proposta habilitada, ou, ainda, quando não se realizarem lances durante a sessão de disputa, caberá ao Superintendente Geral de Compras Centralizadas a adjudicação do objeto ao licitante declarado vencedor.

13.2 - Nos demais casos, o pregoeiro fará a adjudicação do(s) lote(s)/ item(s) ao(s) licitante(s) vencedor (es).

13.3- Após a adjudicação, constatada a regularidade dos atos praticados, o secretário de Estado do órgão demandante homologará o procedimento licitatório, quando o processo de contratação for de sua competência.

13.4 - Os processos autorizados pelo Secretário Especial de Gestão das Contratações, Licitações e Logística serão por ele homologados.

14.0 - DA ASSINATURA DA ATA DE REGISTRO DE PREÇOS:

14.1 - Após a homologação do resultado da licitação, a(s) licitante(s) classificadas em primeiro lugar em cada lote/item serão convocadas para assinar a Ata de Registro de Preço, que também conterá a assinatura da autoridade competente da Unidade Gerenciadora.

14.1.1 – Os convocados selecionados deverão providenciar a assinatura da Ata de Registro de Preços em prazo não superior a 05 (cinco) dias úteis após convocação da UNIDADE GERENCIADORA.

14.1.2 - O prazo para assinatura poderá ser prorrogado apenas uma vez, por igual período, quando solicitado pelo convocado durante seu transcurso e desde que ocorra motivo justificável aceito pela UNIDADE GERENCIADORA.

14.1.3 – A assinatura da Ata de Registro de Preços realizar-se-á através de certificação digital no padrão ICP-Brasil e protocolado virtualmente, no sítio https://www.edocsergipe.se.gov.br/protocolo-externo/.

14.1.3.1 – O protocolo virtual deve ser endereçado ao setor de Registro de Preços da UNIDADE GERENCIADORA.

14.1.4 – Os fornecedores selecionados deverão indicar representantes, às suas expensas,

com poderes específicos para a assinatura da Ata de Registro de Preços.

14.2 – O fornecedor que não providenciar a assinatura da Ata de Registro de Preço no prazo acima perderá o direito a ter seus preços registrados, sem prejuízo das sanções previstas na legislação em vigor.

14.3 - É facultado à UNIDADE GERENCIADORA, quando o convocado não assinar a Ata de Registro de Preços no prazo e condições estabelecidas, convocar as licitantes remanescentes, na ordem de classificação, independentemente da aplicação das sanções previstas na legislação em vigor.

14.3.1 – Os licitantes remanescentes deverão comprovar previamente toda a documentação de habilitação exigida no edital, para a assinatura da Ata.

14.3.2 – Caso o licitante remanescente não comprovar a habilitação, convocar-se-ão os demais, observada a ordem de classificação.

15.0 - DA ATA DE REGISTRO DE PREÇOS:

15.1 – A Ata de Registro de Preços é o documento vinculativo, obrigacional, com característica de compromisso para futura contratação com a Administração Pública Estadual, na qual se registram os preços, fornecedores, unidades participantes e condições a serem praticadas.

15.2 – A Ata de Registro de Preços não obriga os órgãos e entidades do Estado de Sergipe a firmar contratações, podendo ocorrer licitações específicas para aquisição do objeto, obedecida a legislação; sendo assegurada ao detentor do registro a preferência de fornecimento em igualdade de condições.

15.3 – A Ata de Registro de Preços terá validade de 01 (um) ano, contado a partir da publicação do extrato, prorrogável, por igual período, desde que comprovado o preço vantajoso.

15.4 – O preço registrado e os respectivos fornecedores são divulgados no Diário Oficial do Estado e no Portal Nacional de Contratações Públicas - PNCP, e ficarão disponibilizados durante a vigência da Ata de Registro de Preços.

16.0 – DAS CONTRATAÇÕES:

16.1 - Após a publicação da Ata de Registro de Preços da UNIDADE GERENCIADORA no Diário Oficial do Estado de Sergipe e no Portal Nacional de Contratações Públicas - PNCP, poderão ser firmadas contratações dentro do prazo de validade do Registro.

16.2 - As Contratações decorrentes da Ata de Registro de Preços formalizar-se-ão mediante a assinatura de Instrumento - CONTRATO DE PRESTAÇÃO DE SERVIÇOS DE TIC (Anexo III) –, firmado entre as unidades participantes e os detentores do registro.

16.3 - As cláusulas contratuais observarão as especificações do objeto e condições definidas na legislação vigente, neste edital e anexos, na Ata de Registro de Preços, e nas propostas vencedoras, independentemente de transcrição.

16.4 - As contratações pelo sistema de Registro de Preços podem ser formalizadas enquanto vigente a Ata de Registro de Preços.

16.4.1 - O contrato firmado durante o prazo de validade da Ata de Registro de Preços tem vigência própria e produz efeitos até o total cumprimento das obrigações pelas partes, mesmo após o término da vigência da Ata.

16.5 Os contratos decorrentes da Ata serão reajustados anualmente pelo IPCA acumulado no período, após transcorrido 12 (doze) meses da data-base da proposta, conforme arts. 92, XVII e 124 da Lei nº 14.133/2021.

17.0 – DA REVISÃO DOS PREÇOS E DO CANCELAMENTO DOS REGISTROS:

17.1 – Os preços registrados poderão ser atualizados periodicamente, nos termos do art. 199 do

Decreto Estadual nº 342/2023, observadas as condições e os procedimentos estabelecidos na legislação aplicável.

17.2 Os preços registrados na Ata poderão ser revisados se tornarem-se superiores aos praticados no mercado, conforme disposições da cláusula Décima Primeira da Ata de Registro de Preços

17.3 – Se, por algum motivo superveniente, o fornecedor não puder manter o compromisso registrado na Ata, deverá apresentar à UNIDADE GERENCIADORA justificativa comprobatória da impossibilidade, antes de ser notificado para o fornecimento, caso em que, aceita a justificativa, poderá ser liberado do compromisso sem aplicação de penalidade, conforme disposições da cláusula Décima Primeira da Ata de Registro de Preços.

18.0 – DAS SANÇÕES ADMINISTRATIVAS:

18.1 - Os licitantes que cometerem qualquer das infrações previstas nos artigos 215, 216 e 217 do Decreto Estadual nº 342/2023 poderá sofrer as seguintes sanções:

18.1.1 - advertência;

18.1.2 – multa, observados os seguintes limites máximos:

a) multa de 0,3 % (três décimos por cento) por dia, até o trigésimo dia de atraso, sobre o valor do fornecimento ou serviço não realizado;

b) multa de 10 % (dez por cento) sobre o valor total ou parcial da obrigação não cumprida, com o conseqüente cancelamento da nota de empenho ou documento equivalente;

18.1.4 - impedimento de licitar e de contratar com o Estado de Sergipe, pelo prazo de até 3 (três) anos;

18.1.5 - declaração de inidoneidade para licitar ou contratar com a Administração Pública.

18.2 - O valor da multa aplicada será descontado do valor da garantia prestada, retido dos pagamentos devidos pela Administração ou cobrado judicialmente, sendo corrigida monetariamente, de conformidade com a variação do IPCA, a partir do termo inicial, até a data do efetivo recolhimento.

18.3 - A contagem do período de atraso na execução dos ajustes será realizada a partir do primeiro dia útil subsequente ao do encerramento do prazo estabelecido para o cumprimento da obrigação.

19.0 - DO PROGRAMA DE INTEGRIDADE (Lei Estadual nº 8.866/21 e Decreto estadual nº 41.008/21)

19.1 - Na hipótese de contrato administrativo, cujo valor, global ou estimado, se enquadre nos parâmetros estabelecidos pelo art. 1º da Lei (Estadual) nº 8.866/2021, será exigida, no momento da celebração do contrato, apresentação de:

19.1.1 - Relatório de Perfil e Relatório de Conformidade do Programa, nos termos dos Anexos do Decreto (Estadual) nº 41.008/21.

19.2 - O Programa de Integridade consiste, no âmbito de uma pessoa jurídica, no conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidade e na aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes com o objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a Administração Pública do Estado de Sergipe.

19.3 - Aplica-se a exigência do Programa de Integridade às sociedades empresárias e às sociedades simples, personificadas ou não, independente da forma de organização ou modelo societário adotado, bem como a quaisquer fundações, associações civis, ou sociedades estrangeiras, que tenham sede, filial ou representação no território brasileiro, constituídas de fato ou de direito, ainda que temporariamente.

19.4 - A implantação do Programa de Integridade, no âmbito da pessoa jurídica, deve ocorrer no prazo de 180 (cento e oitenta) dias corridos, a partir da data de celebração do contrato.

> 19.4.1 - O Programa de Integridade meramente formal e que se mostre absolutamente ineficaz para mitigar o risco de ocorrência de atos lesivos dispostos na Lei (Federal) nº 12.846, de 1º de agosto de 2013, não deve ser considerado para fim de cumprimento desta Lei.

19.5 - Para efetiva implantação do Programa de Integridade, os custos/despesas resultantes devem correr à conta da empresa contratada, não cabendo ao órgão contratante o seu ressarcimento.

19.6 - A empresa que possuir o Programa de Integridade implantado deve apresentar, no momento da contratação, declaração informando a sua existência.

19.7 - A não implantação do programa de integridade no prazo definido pode implicar em sanção de multa de até 10% (dez por cento) do valor atualizado do contrato, além de, sem prejuízo da multa aplicada, impossibilidade de aditamento contratual, rescisão unilateral do contrato e impossibilidade de licitar e contratar com a Administração Pública do Estado, pelo período de 02 (dois) anos ou até efetiva comprovação de implantação e aplicação do Programa de Integridade.

20.0 - DAS DISPOSIÇÕES FINAIS:

20.1 - A presente licitação não importa necessariamente em contratação, podendo a UNIDADE GERENCIADORA revogá-la, no todo ou em parte, por razões de interesse público, derivado de fato superveniente comprovado ou anulá-la por ilegalidade, de ofício ou por provocação mediante ato escrito e fundamentado disponibilizado no sistema para conhecimento dos participantes da licitação.

20.2 - Os proponentes assumem todos os custos de preparação e apresentação de suas propostas e o Estado de Sergipe não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

20.4 - Após apresentação da proposta, não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceito pelo Pregoeiro.

20.5 - Da 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 expedientes na Secretaria Especial das Contratações, Licitações e Logística.

20.6 - É facultado ao Pregoeiro ou à Autoridade Superior, em qualquer fase da licitação, promover diligências com vistas a esclarecer ou a complementar a instrução do processo.

20.7 - O desatendimento de exigências formais, não essenciais, não importará no afastamento do proponente, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta.

20.8 - As normas que disciplinam este Pregão serão sempre interpretadas em favor da ampliação da disputa entre os proponentes, desde que não comprometam o interesse da Administração, a finalidade e a segurança da contratação.

20.9 - As decisões referentes a este processo licitatório poderão ser comunicadas aos proponentes por qualquer meio de comunicação que comprove o recebimento ou, ainda, mediante publicação no Diário Oficial do Estado.

20.10 - A participação do proponente nesta licitação implica a aceitação de todos os termos deste edital.

20.11 - Havendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será transferida para dia e horário definidos pelo pregoeiro, comunicando devidamente aos licitantes do pregão eletrônico.

20.12 - Os casos omissos serão decididos pelo Pregoeiro em conformidade com as disposições constantes dos Decretos e Leis citadas no preâmbulo deste edital.

20.13 - O foro designado para julgamento de quaisquer questões judiciais resultantes deste edital será o da Comarca de Aracaju/SE.

21.0 - SÃO PARTES INTEGRANTES DESTE EDITAL:

21.1 - Anexo I - Termo de Referência;

21.2 - Anexo II - Minuta da Ata de Registro de Preços;

21.3 - Anexo III - Minuta de Contrato de Prestação de Serviços;

21.4 - Anexo IV – Relação de Unidades Participantes;

21.5 - Anexo V - Modelo do Termo de Adesão;

21.6 - Anexo VI - Modelos de Declarações:

21.6.1 - Declaração de Microempresa, Empresa de Pequeno Porte, nos termos da Lei Complementar nº 123, de 2006;

21.6.2 - Declaração de que está ciente e concorda com as condições contidas no ato convocatório e seus anexos, bem como de que cumpre plenamente os requisitos de habilitação;

21.6.3 - Declaração para fins do disposto no inciso VI do art. 68 da Lei nº 14.133, de 2021, que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos, salvo menor a partir de 14 (quatorze) anos, na condição de aprendiz, nos termos do inciso XXXIII do art. 7º da Constituição Federal;

21.6.4 - Declaração de que a proposta apresentada para essa licitação foi elaborada de maneira independente;

21.6.5 - Declaração de que não possui, em sua cadeia produtiva, 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;

21.6.6 Declaração informando se os serviços são produzidos ou prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24

de julho de 1991;

21.6.7 - Declaração de contratos firmados com a iniciativa privada e a Administração Pública.

Aracaju, 09 de setembro de 2026.

Wellington Melo
Pregoeiro/SECLOG

# ANEXO I
{

TERMO DE REFERÊNCIA

1. DO OBJETO

1.1. Contratação de solução de software do tipo **Plataforma Unificada de Operações de Cibersegurança** operando em **arquitetura centralizada**, capaz de **consolidar em um único console** as funções de: Detecção e Resposta a Ameaças (XDR), Gestão de Vulnerabilidades, Inteligência de Ameaças, Simulação de Ataques (Segurança Ofensiva), Automação de Resposta a Incidentes (SOAR) e Governança, Risco e Conformidade (GRC), incluindo mecanismos de integridade de dados via Blockchain, na modalidade *Software as a Service* (SaaS).

1.2. O escopo inclui o licenciamento de uso de plataforma unificada, serviços de implantação, operação de Centro de Operações de Segurança (SOC), suporte técnico especializado e fornecimento de dispositivos de autenticação segura (chaves FIDO2), por meio do Sistema de Registro de Preços, em Grupo Único, conforme condições, quantidades e exigências estabelecidas neste instrumento.

Item	Especificação	CÓDIGO I-GESP	Métrica/ Unidade de Medida	Qtd
1	SUBSCRIÇÃO DE PLATAFORMA UNIFICADA DE GESTÃO DE EXPOSIÇÃO, VISIBILIDADE E SEGURANÇA OFENSIVA Licenciamento do módulo central por 12 meses, responsável por: Inventário contínuo de ativos; Análise de Tráfego de Rede; Motor de Vulnerabilidades; Campanhas de Phishing; Automação de resposta; Pentests Automatizados; Monitoramento DDoS e Web; Monitoramento de ativos na Deep e Dark Web.	468473-7	Subscrição Anual (Domínios + Endpoints+ Containers)	
2	SUBSCRIÇÃO DE PLATAFORMA INTEGRADA DE DEFESA ATIVA Licenciamento do módulo de proteção ativa por 12 meses: NAC (Definição de políticas de acesso e isolamento) e IPS (Prevenção de intrusão com assinatura e comportamento).	468476-1	Subscrição Anual (Por IPs)	
3	SUBSCRIÇÃO DE PLATAFORMA INTEGRADA DE PROTEÇÃO DE DADOS E IDENTIDADE Licenciamento do módulo de governança de dados por 12 meses: DLP (Data Loss Prevention – monitoramento da exfiltração	468477-0	Subscrição Anual (Por Endpoints)	

	de dados).			
4	IMPLANTAÇÃO E INTEGRAÇÃO (SETUP) – PLATAFORMA UNIFICADA Instalação, ativação, configuração e integração da PLATAFORMA UNIFICADA DE GESTÃO DE EXPOSIÇÃO (Item 1).	468502-4	Serviço Global	
5	IMPLANTAÇÃO E INTEGRAÇÃO (SETUP) – PLATAFORMA DE DEFESA ATIVA Instalação, ativação, configuração e integração da PLATAFORMA INTEGRADA DE DEFESA ATIVA (Item 2).	468501-6	Serviço Global	
6	IMPLANTAÇÃO E INTEGRAÇÃO (SETUP) – PLATAFORMA DE PROTEÇÃO DE DADOS Instalação, ativação, configuração e integração da PLATAFORMA INTEGRADA DE PROTEÇÃO DE DADOS (Item 3).	468503-2	Serviço Global	
7	SERVIÇO CONTINUADO DE GESTÃO DE VULNERABILIDADES E OFENSIVA Incluindo análise de tráfego, execução de pentests, triagem de riscos e relatórios personalizados de exposição.	468481-8	Mensal	
8	SERVIÇO CONTINUADO DE OPERAÇÃO DE DEFESA ATIVA E RESPOSTA A INCIDENTES (SOC) Monitoramento integrado das plataformas; gestão de incidentes; governança cibernética; curadoria de Playbooks de automação; resposta a incidentes.	468482-6	Mensal	
9	SERVIÇO TÉCNICO ESPECIALIZADO PARA CUSTOMIZAÇÃO (SOB DEMANDA) Horas de serviços técnicos para demandas de engenharia de segurança e ajustes arquitetônicos.	468485-0	Hora de Serviço Técnico (HST)	

1.3. Em se tratando de Sistema de Registro de Preços, os quantitativos acima representam a estimativa máxima de consumo para o período de vigência da Ata, não havendo obrigatoriedade de contratação da totalidade dos itens.

1.4. O(s) serviço(s) objeto desta contratação são caracterizados como comum(ns), uma vez que seus padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado (art. 6º, inciso XIII, da Lei nº 14.133/2021).

1.5. O serviço é enquadrado como continuado, tendo em vista que a segurança da informação, o monitoramento de ameaças e a proteção de dados sensíveis custodiados pelo Estado constituem necessidades permanentes da Administração, cuja interrupção pode comprometer a integridade dos dados públicos e o funcionamento dos serviços essenciais, sendo a vigência plurianual mais vantajosa considerando a diluição dos custos de implantação (setup) e a curva de aprendizado da solução.

1.6. A aglutinação dos itens 1 a 9 em Lote (Grupo) Único fundamenta-se na indissociabilidade técnica e operacional da solução de cibersegurança demandada, conforme Item 8 do Estudo Técnico Preliminar. A contratação fragmentada acarretaria grave prejuízo ao Estado, pois inviabilizaria a correlação nativa de eventos entre os módulos de Defesa Ativa, Gestão de Vulnerabilidades e o Centro de Operações (SOC). O fracionamento geraria silos de dados intransponíveis, graves conflitos de responsabilidade (SLA) na cadeia de resposta a incidentes críticos e inviabilizaria a automação imediata, demonstrando que o lote único é a única via técnica e economicamente segura para garantir a proteção integral da infraestrutura tecnológica.

1.6.1. A relação funcional entre os nove itens confirma a indissociabilidade da solução: os Itens 1 a 3 (subscrições das plataformas de Gestão de Exposição/Segurança Ofensiva, de Defesa Ativa e de Proteção de Dados e Identidade) constituem o núcleo tecnológico que gera a telemetria correlacionada; os Itens 4 a 6 (implantação e integração – setup) são pré-condição de funcionamento das respectivas subscrições, sem utilidade autônoma; os Itens 7 e 8 (serviços continuados de gestão de vulnerabilidades/ofensiva e de operação de SOC e resposta a incidentes) dependem da ingestão unificada dos dados das plataformas dos Itens 1 a 3; e o Item 9 (horas técnicas sob demanda) instrumentaliza ajustes de engenharia sobre o mesmo ambiente integrado.

1.6.2. A adjudicação por item ou o parcelamento em lotes distintos foi avaliada e revelou-se técnica e economicamente inviável: a contratação de subscrições, setup e operação continuada de fornecedores distintos romperia a correlação nativa de eventos entre os módulos, geraria silos de dados, conflitos de responsabilização (SLA) na cadeia de resposta a incidentes e impossibilitaria a automação (SOAR) imediata, além de elevar o Custo Total de Propriedade (TCO) pela perda de economia de escala e de integração.

1.6.3. Demonstra-se, assim, a vantagem técnica e econômica da modelagem em Grupo Único, em consonância com o art. 82, § 1º, da Lei nº 14.133/2021 e o art. 187, § 1º, do Decreto Estadual nº 342/2023, sem prejuízo de que a contratação isolada de item integrante do grupo, quando cabível, seja precedida de pesquisa de mercado e demonstração de sua vantajosidade, nos termos do art. 82, § 2º, da Lei nº 14.133/2021.

1.7. Do afastamento do tratamento diferenciado às microempresas e empresas de pequeno porte. Deixa-se de adotar a cota reservada e o tratamento favorecido previstos na Lei Estadual nº 8.747/2020, com fundamento na exceção do art. 6º, II, do referido diploma, uma vez que o objeto é indivisível e reunido em Grupo Único, de modo que o tratamento diferenciado, ao pressupor a divisão do objeto, representaria prejuízo ao conjunto ou complexo a ser contratado, comprometendo a integração nativa, a correlação de eventos e a unicidade de responsabilização técnica que constituem a essência da solução, restando justificado o afastamento nos termos do art. 6º, II, da Lei Estadual nº 8.747/2020.

2. JUSTIFICATIVA DA CONTRATAÇÃO

2.1. A presente contratação justifica-se pela imperiosa necessidade de modernizar a infraestrutura de segurança da informação e garantir a conformidade do Estado de Sergipe com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD). O cenário atual de TIC apresenta desafios críticos, tais como o aumento exponencial de incidentes cibernéticos (mais de 8.600 registrados no Brasil no primeiro semestre de 2024), a sofisticação de ataques (ex: Ransomware com uso de IA) e a exposição jurídica decorrente do tratamento massivo de dados sensíveis dos cidadãos. A solução integrada de Cibersegurança e LGPD visa mitigar riscos de vazamento de dados, interrupção de serviços essenciais e sanções administrativas, fornecendo:

2.1.1 **Visibilidade e Controle:** Inventário contínuo de ativos e análise de vulnerabilidades em tempo real.

2.1.2 Defesa Ativa: Bloqueio automatizado de ameaças via IPS e políticas Zero Trust.

2.1.3 Governança Cibernética: Classificação técnica de ativos, gestão de privilégios de acesso e monitoramento de conformidade técnica com frameworks de segurança (ex: ISO 27001 e NIST).
2.1.4 **Resposta a Incidentes:** Capacidade de orquestração (SOAR) e suporte técnico especializado de Resposta a Incidentes (CSIRT) para atuação imediata frente a violações e tentativas de invasão.

A adoção do Sistema de Registro de Preços (SRP) é motivada pela necessidade de padronização da solução em nível governamental e pela impossibilidade de prever com exatidão o quantitativo de incidentes que demandam horas técnicas de suporte ou a expansão exata do parque tecnológico (novos servidores/endpoints) ao longo do exercício, permitindo aquisições sob demanda e otimização dos recursos públicos. A permissão para adesões (caronas) fundamenta-se na economia de escala e na uniformização dos protocolos de segurança no Estado.

2.2. **Necessidade:** O Governo do Estado de Sergipe necessita elevar sua maturidade em segurança da informação frente ao aumento de ataques cibernéticos (Ransomware, Phishing) e cumprir as obrigações legais da Lei nº 13.709/2018 (LGPD).

2.3. Integração: A contratação de uma solução unificada (Cibersegurança + LGPD) justifica-se pela necessidade de correlação de eventos: vazamentos de dados (LGPD) geralmente decorrem de falhas de segurança (Vulnerabilidades). A gestão centralizada reduz o Custo Total de Propriedade (TCO) e otimiza a equipe técnica reduzida.

2.4. Soberania e Segurança: A exigência de auditoria de logs com integridade criptográfica visa garantir a validade jurídica das evidências em caso de incidentes, assegurando a responsabilização e a defesa do ente público.

2.5. O objeto da contratação também está alinhado com a Estratégia de Governo Digital, conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
OE-0X	Elevar o nível de maturidade em segurança da informação e privacidade de dados (Estratégia de Governo Digital).
OE-0X	Garantir a disponibilidade, integridade e confidencialidade dos serviços públicos digitais.
OE-0X	Assegurar a proteção técnica dos dados sensíveis e críticos, atendendo aos requisitos de segurança do Art. 46 da LGPD.

3. ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

A solução contratada deverá consistir em uma **Plataforma Unificada de Operações de Segurança e Governança**, operando em regime de *Software as a Service* (SaaS), desenvolvida preferencialmente em arquitetura de microsserviços ou *containers*, garantindo escalabilidade horizontal e alta disponibilidade. Tal solução de TIC consiste na **prestação de serviços continuados de Segurança Cibernética Gerenciada** (MSSP/SOC), suportada por uma plataforma de Defesa Ativa, Visibilidade e Segurança Ofensiva. A finalidade é garantir a proteção da infraestrutura tecnológica, a detecção proativa de ameaças, a resposta rápida a incidentes e o monitoramento contínuo de vulnerabilidades e vazamentos de dados na rede estadual. Abrangendo o licenciamento de software na modalidade Software as a Service (SaaS), implantação, operação assistida, suporte técnico especializado e fornecimento de dispositivos de autenticação. A solução tem como finalidade garantir a proteção de dados pessoais, conformidade legal e segurança digital da Administração.

A plataforma deverá consolidar, em um único console de gerenciamento, os seguintes módulos e funcionalidades:

3.1. Plataforma Unificada/Integrada de Segurança da Informação

3.1.1. Requisitos de Interface do Usuário

3.1.1.1. As interfaces do usuário, incluindo orientações de uso da solução e todos os manuais, devem estar no idioma português do Brasil (PT-BR).

3.1.1.2. A aplicação/interface web deve rodar nas versões atuais dos principais navegadores de Internet existentes no mercado à época da instalação da solução e deve garantir compatibilidade com as suas novas versões.

3.2. Solução de Gerenciamento de Vulnerabilidades

3.2.1 A solução de segurança cibernética deverá ser capaz de realizar monitoramento ativo para abranger os endereços IP públicos, endpoints e Nomes de domínio totalmente qualificados Externos e internos (FQDNs) simultaneamente.

3.2.2 Essa capacidade permitirá que toda a infraestrutura de TIC seja analisada de forma contínua, proporcionando uma visão completa e detalhada do ambiente digital.

3.2.3 A solução deverá realizar escaneamentos periódicos e automatizados, buscando identificar não apenas vulnerabilidades conhecidas, mas também possíveis falhas de configuração que possam representar riscos à segurança.

3.2.4 O processo de análise de vulnerabilidades deverá ser complementado pela utilização de Inteligência Artificial (IA). Onde a IA permitirá uma análise preditiva, capaz de identificar padrões anormais e possíveis brechas de segurança antes mesmo que se tornem uma ameaça real.

3.2.5 Além disso, a IA deverá contribuir para a priorização das vulnerabilidades encontradas, classificando-as de acordo com a criticidade baseada no padrão CVSS (Common Vulnerability Scoring System), de forma a facilitar a tomada de decisões rápidas e assertivas pela equipe de segurança da informação.

3.2.6 Entre as funcionalidades oferecidas, a solução deverá também ter a capacidade de detectar vulnerabilidades Zero-Day, ou seja, falhas ainda não divulgadas publicamente e que podem ser exploradas por atacantes antes que correções sejam disponibilizadas. Essa detecção em tempo real é essencial para manter um alto nível de proteção, especialmente em ambientes onde a segurança da informação é crítica.

3.2.7 Os testes de intrusão, também conhecidos como Pentests, são uma peça-chave na estratégia de segurança proposta. A solução deverá de forma automatizada realizar testes de penetração utilizando ferramentas modernas e eficientes. Os testes devem ser conduzidos em três diferentes modalidades:

3.2.8 **Black-box:** onde o executor do teste não possui qualquer conhecimento prévio sobre a infraestrutura ou sistemas da organização, simulando um ataque externo real.

3.2.9 **Gray-box:** onde o teste é realizado com informações limitadas, proporcionando uma visão equilibrada entre o desconhecimento completo e o acesso total ao ambiente.

3.2.10 **White-box:** onde o executor do teste tem pleno acesso a informações detalhadas sobre o ambiente tecnológico e a arquitetura da rede, permitindo uma análise profunda e minuciosa.

3.2.11 A solução deverá integrar um painel de prevenção de Phishing, onde será possível criar campanhas específicas para treinar e conscientizar os usuários finais sobre os riscos do Phishing.

3.2.12 Essas campanhas permitirão o envio automatizado de e-mails simulados de Phishing, monitorando em tempo real a quantidade de e-mails disparados, o número de cliques realizados e, consequentemente, quantos usuários foram "capturados" pela tentativa de Phishing.

3.2.13 O painel administrativo oferecerá funcionalidades para edição, reenvio de campanhas e geração de relatórios detalhados, proporcionando insights valiosos para reforçar políticas de segurança e promover treinamentos mais eficazes.

3.2.14 Os testes de intrusão deverão incluir simulações de diferentes tipos de ataques cibernéticos, como SQL Injection, Cross-Site Scripting (XSS), ataques de negação de serviço (DDoS), tentativas de força bruta e testes de phishing. Essas simulações permitem avaliar a robustez das defesas do sistema, identificar possíveis pontos fracos e sugerir soluções específicas para cada tipo de vulnerabilidade detectada.

3.2.15 Gerenciamento e análise da exposição a ameaças e da superfície de ataque (interna e externa).

3.2.16 Utilização de ferramenta especializada para:
- Gerenciamento de vulnerabilidades.
- Varredura e avaliação de vulnerabilidades e configuração segura.
- Análise e priorização de risco cibernético.

3.3. Painel de Prevenção de Phishing

3.3.1 O módulo de prevenção de phishing será um componente fundamental da solução, devendo oferecer uma plataforma completa para a criação e gerenciamento de campanhas de conscientização de segurança. Através do painel administrativo, o usuário administrador deverá conseguir configurar campanhas simuladas de phishing, enviando e-mails personalizados para grupos específicos de colaboradores.

3.3.2 Dessa forma a interface do painel deverá permitir:

3.3.2.1. O administrador poderá criar campanhas de prevenção, definir o modelo de e-mail e o público-alvo.

3.3.2.2. Acompanhar o envio dos e-mails e o progresso da campanha, como quantidade de e-mails enviados, cliques nos links suspeitos e identificação dos usuários que caíram na simulação.

3.3.3 A solução deverá gerar relatórios abrangentes, exibindo métricas como taxa de cliques, percentual de usuários suscetíveis ao phishing e insights para aprimoramento das práticas de segurança.

3.3.4 Caso necessário, deverá ser possível reenviar campanhas para reforçar o treinamento dos usuários que demonstraram vulnerabilidades.

3.4. Simulação de Ataques DDoS

3.4.1 O módulo de simulação de ataques DDoS (Distributed Denial of Service) deverá oferecer uma abordagem prática para testar a resiliência da infraestrutura da organização. Com uma interface intuitiva, o painel deverá permitir:

3.4.2 O administrador poderá definir o tipo de ataque DDoS, o volume de requisições e o alvo específico (IP ou URL).
3.4.3 Acompanhar métricas como o número de solicitações por segundo, latência de resposta e taxa de erro durante o ataque simulado.
3.4.4 O painel deverá também exibir gráficos detalhados sobre o tempo de resposta e o impacto na disponibilidade do sistema, permitindo identificar gargalos e possíveis melhorias na infraestrutura.

3.5. Testes de Invasão e Segurança

3.5.1 A solução deverá incluir uma variedade de testes de invasão (Pentest) para identificar vulnerabilidades e fortalecer a segurança do ambiente digital. Entre os testes disponíveis, destacar-se-ão:
3.5.2 Avaliação da segurança a partir da rede interna da organização, simulando um ataque de um colaborador mal-intencionado ou de uma máquina comprometida.
3.5.3 Simulação de ataques vindos de fora da organização, avaliando a robustez de firewalls, sistemas de detecção de intrusão (IDS) e a exposição de serviços públicos.
3.5.4 Verificação da segurança de sites e sistemas web, utilizando técnicas como injeção de SQL, Cross-Site Scripting (XSS) e análise de vulnerabilidades em APIs.

3.6. Monitoramento e Análise de Vulnerabilidades

3.6.1 O sistema de monitoramento contínuo deverá utilizar ferramentas avançadas de análise para detectar vulnerabilidades conhecidas e novos vetores de ataque. As principais funcionalidades incluirão:
3.6.1.1 Varredura automatizada em sistemas, servidores e dispositivos conectados à rede, identificando falhas de configuração, softwares desatualizados e possíveis pontos de entrada para invasores.
3.6.1.2 Integração com sistemas de coleta de logs, permitindo identificar padrões anômalos e atividades suspeitas em tempo real.
3.6.1.3 Utilização de bases de dados atualizadas sobre ameaças conhecidas, aplicando correlações entre eventos monitorados e possíveis ataques.
3.6.1.4 Realização de varreduras automatizadas completas em ativos internos e externos.
3.6.1.5 Varreduras autenticadas e não autenticadas.
3.6.1.6 Compatibilidade mínima com o protocolo SCAP (Security Content Automation Protocol).

3.7. Monitoramento de Vazamento de Dados

3.7.1 Realizar o monitoramento, análise e busca inteligente por dados vazados ou expostos, incluindo o monitoramento deles na DarkWeb.
3.7.2 Relatórios e Indicadores de Desempenho
3.7.3 A solução deverá oferecer uma ampla variedade de relatórios gerenciais e técnicos, fornecendo insights valiosos para a tomada de decisão:
3.7.4 Com uma linguagem acessível, ideal para apresentações a gestores, destacando os principais riscos e as ações tomadas para mitigar vulnerabilidades.
3.7.5 Detalhamento das vulnerabilidades encontradas, incluindo evidências, métodos utilizados nos testes e sugestões práticas para correção.
3.7.6 A solução deverá permitir ao usuário configurar o painel de controle, escolhendo os indicadores mais relevantes para o seu ambiente. Camada de Segurança, Autenticidade e Validade Jurídica
3.7.7 Possuir mecanismo de armazenamento e coleta de documentos digitais auditáveis com validade jurídica, baseada em blockchain.
3.7.8 Assegurar a autenticidade de documentos digitais.
3.7.9 Gerar relatórios técnicos com informações registradas, com validade jurídica conforme o artigo 369 do CPC/2015.
3.7.10 Possuir método de autenticação robusto com chave física USB (Chave de Hardware) para acesso à interface de gerenciamento, além de usuário e senha.
3.7.11 A Contratada deverá fornecer o quantitativo de chaves compatível com o número de licenças de administradores da plataforma (Item 1), conforme o quantitativo de dispositivos de autenticação FIDO2 previsto na estimativa deste Termo de Referência.
3.7.12 Possuir módulo para identificar e mitigar domínios semelhantes que possam ser usados em ataques de phishing.

3.8. Testes de Segurança Automatizados (BAS)

3.8.1 Implementação de testes de segurança automatizados para simular ataques e validar a eficácia dos controles de segurança.
3.8.2 Processo de Testes Automatizados
3.8.3 Planejamento, execução, análise e geração de relatórios de testes automatizados contínuos de segurança.
3.8.4 Utilização de ferramenta de simulação de brechas e ataques (Breach and Attack Simulation - BAS).
3.8.5 Capacidades da Ferramenta BAS
3.8.6 Realização de baterias de testes de simulação de ataques com base em bibliotecas atualizadas de ameaças e exploits.
3.8.7 Execução imediata ou agendada.
3.8.8 Abrangência:
3.8.9 Infiltração de rede e aplicações web (ator malicioso externo para ativo-alvo interno).
3.8.10 Endpoint (comprometimento e exfiltração em ativo-alvo interno, estação de trabalho ou servidor, com cobertura mínima do sistema operacional Microsoft Windows).
3.8.11 Bases de Conhecimento de Segurança
3.8.12 A solução deverá ter integração as seguintes bases de conhecimento de segurança:
3.8.13 NIST National Vulnerability Database (NVD).
3.8.14 MITRE Common Vulnerabilities and Exposures (CVE).
3.8.15 NIST Official Common Platform Enumeration (CPE).
3.8.16 MITRE Common Weakness Enumeration (CWE).
3.8.17 OWASP Top 10.
3.8.18 CIS Benchmarks.
3.8.19 A solução deve demonstrar alinhamento técnico com a matriz MITRE ATT&CK, permitindo o mapeamento das detecções e incidentes às táticas e técnicas conhecidas de adversários, facilitando a análise de Threat Hunting.
3.8.20 Abrangência dos Ativos de TIC
3.8.21 A solução deve abranger uma ampla gama de ativos de TIC, incluindo:
3.8.22 Dispositivos de usuário final (estações de trabalho, notebooks, dispositivos móveis e periféricos).
3.8.23 Dispositivos de rede.
3.8.24 Dispositivos inteligentes conectados à rede (IoT).
3.8.25 Servidores.
3.8.26 Contêineres.
3.8.27 Sistemas operacionais.
3.8.28 Serviços e aplicações em rede.
3.8.29 Ativos e postura de segurança em nuvem.
3.8.30 A solução deve possuir motor de análise cognitiva baseado em Inteligência Artificial,
3.8.31 Utilizar modelos de linguagem grande (LLMs - Large Language Models) ou tecnologia equivalente para interpretação de logs e eventos de segurança em linguagem natural, auxiliando na contextualização de alertas;
3.8.32 Empregar algoritmos de aprendizado de máquina não supervisionado para detecção de anomalias comportamentais que desviem do padrão base (baseline), sem dependência exclusiva de assinaturas estáticas;
3.8.33 Realizar a correlação de eventos utilizando estrutura de dados em grafos ou topologia relacional avançada, permitindo identificar conexões complexas entre usuários, IPs, arquivos e processos em tempo hábil;
3.8.34 Possuir capacidade de 'consciência contextual', avaliando o risco não apenas pelo evento isolado, mas pelo histórico e comportamento tático da entidade monitorada.
3.8.35 A solução deve atuar como uma plataforma unificada de detecção e resposta, integrando nativamente ou via conectores:

3.8.36 Ingestão e normalização de dados provenientes de múltiplas fontes, incluindo, mas não se limitando a: EDR (Endpoint Detection and Response), NDR (Network Detection and Response), WAF (Web Application Firewall) e provedores de nuvem (ex: AWS, Azure, Google Cloud);
3.8.37 Capacidade de enriquecimento automático de dados (Data Enrichment) utilizando fontes de inteligência de ameaças (Threat Intel), geolocalização e dados de identidade (IAM/AD);
3.8.38 Criação de uma camada de abstração que permita a consulta unificada aos dados, independentemente da fonte de origem.
3.8.39 Considerando a sensibilidade dos dados governamentais processados:
3.8.40 Os modelos de Inteligência Artificial Generativa (LLMs) utilizados para análise de incidentes devem, preferencialmente, possuir capacidade de execução local (On-Premise) ou em nuvem privada no Brasil (Private Cloud), garantindo que dados sensíveis ou logs da infraestrutura não sejam enviados para treinamento de modelos públicos de terceiros;
3.8.41 O tempo de inferência e resposta do motor cognitivo para alertas críticos deve ser compatível com a necessidade de bloqueio de ameaças em tempo real (baixa latência).

3.9. Requisitos de Interface do Usuário

3.9.1 Todas as funcionalidades da solução que dependam de interação com o usuário devem ser disponibilizadas via interface/aplicação web sem necessidade de instalação de agentes ou conectores nas máquinas dos usuários ou em servidores da CONTRATANTE (Banco de Dados, File Server, etc).
3.9.2 As interfaces do usuário, incluindo orientações de uso da solução e todos os manuais, devem estar no idioma português do Brasil (PT-BR).
3.9.3 A aplicação/interface web deve rodar nas versões atuais dos principais navegadores de Internet existentes no mercado à época da instalação da solução e deve garantir compatibilidade com as suas novas versões.
3.9.4 Deve ser compatível com os navegadores de dispositivos móveis: Android e iOS - web adaptativo/responsivo ou possuir aplicativo móvel.
3.9.5 Deve permitir ao usuário visualizar e adicionar anexos em qualquer formulário da solução.

3.10. Requisitos de Integração e Interoperabilidade

3.10.1 Deverá suportar as seguintes características e funcionalidades:

3.10.1.1. Integração nativa entre seus módulos.
3.10.1.2. Recurso de integração por meio de API e toda documentação em português do Brasil (PT-BR).
3.10.1.3. Integração síncrona e assíncrona com aplicações da CONTRATANTE incluindo RESTful e SOAP APIs, assim como requisições de API GET, PUSH, PULL.
3.10.1.4. Integração de sistemas de terceiros e recursos de migração de dados, por meio de uma variedade de técnicas de integração, incluindo: Webservices; JDBC; LDAP; Excel; CSV; e e-mail.
3.10.1.5. Tecnologias padrão da indústria, como SOAP, REST ou WSDL.
3.10.1.6. Integrações de API e de linha de comando também via MID Server (Middleware/Barramento), onde todo o tráfego de Webservices deve ser encriptado com TLS.
3.10.1.7. Arquitetura orientada a serviços (SOA), na qual todos os objetos de dados podem usar os Webservices para acessar a integração bidirecional de nível de dados.
3.10.1.8. Interface rica (Rich interface) para carregar dados externos usando conjuntos de importação de várias fontes de dados, como HTTPS, FTPS e SCP usando formatos de arquivo, como XML, CSV e Microsoft Excel XLS.

3.11. Requisitos de Avaliação de Maturidade de TI

3.11.1 Deve permitir avaliar o nível de maturidade da governança de TI da organização, identificando lacunas e sugerindo melhorias nas práticas de segurança e conformidade.
3.11.1.1. Suas principais funcionalidades devem incluir:
3.11.1.1.1. Avaliação de controles de segurança e governança.
3.11.1.1.2. Relatório de maturidade de TI com recomendações de melhoria.
3.11.1.1.3. Interface para planejamento de evolução de conformidade.
3.11.1.1.4. Classificação das Ações por Gravidade, Urgência e Tendência.

3.11.1.1.5. Classificação das Ações por Impacto ao Negócio.
3.11.1.1.6. Classificação e Acompanhamento dos Planos de Ação.
3.11.1.1.7. Enumeração dos Impactos e Classificação dos Riscos existentes.
3.11.1.1.8. Enumeração de Melhorias Indicadas.

3.12. Requisitos de Gestão de Conformidade e Ética no Uso de IA

3.12.1 Deve apoiar o CONTRATANTE na governança e conformidade no uso de Inteligência Artificial (IA), assegurando transparência, ética, segurança e aderência à LGPD e às normas vigentes. Assim, deve permitir a realização de auditorias, análise e tratamento dos riscos identificados de forma autônoma, bem como a recomendação de melhorias nos sistemas de IA adotados.

3.12.2 Deve possuir mecanismo de entrevista assistida por IA para coleta estruturada de informações sobre o sistema de Inteligência Artificial, incluindo:

3.12.3 Identificação do sistema (nome, finalidade, responsáveis).

3.12.4 Questionário baseado em diretrizes legais e éticas pré-definidas.

3.12.5 Suporte para esclarecimento de dúvidas em tempo real durante o processo

3.12.6 Deve possuir classificação automática do sistema de IA conforme critérios legais, visando mitigar riscos de violações à ética e implementar ações de adequação.

3.12.7 Deve realizar a avaliação de conformidade com:

3.12.8 Transparência na tomada de decisão algorítmica.

3.12.9 Proteção de dados e privacidade; e

3.12.10 Governança e responsabilidade técnica.

3.12.11 Deve permitir a emissão de relatórios estruturados contendo:

3.12.12 Resumo da entrevista e classificação do sistema;

3.12.13 Pontos de conformidade e não conformidade com referência a artigos legais;

3.12.14 Recomendações técnicas e operacionais para adequação; e

3.12.15 Opção de exportação em formato PDF.

3.12.16 Deve possuir funcionalidade para atualização dinâmica das análises, conforme mudanças na legislação ou no próprio sistema de IA auditado.

3.12.17 Deve utilizar banco de dados vetorial para armazenamento eficiente e recuperação contextualizada de informações.

3.12.18 Deve suportar técnicas de Recuperação Aumentada por Geração (RAG) para garantir respostas contextualizadas e fundamentadas juridicamente às consultas dos usuários e às bases de conhecimento.

3.12.19 Deve utilizar modelos de linguagem avançados para interpretação de questionários, sumarização de dados e geração de relatórios.

3.12.20 Deve realizar a orquestração e customização de agentes de IA especializados em extração de texto, análise de risco e conformidade regulatória.

3.12.21 Deve realizar o mapeamento automático de requisitos legais da LGPD, bem como do Projeto de Lei 2338/2023 e normativos correlatos.

3.12.22 Deve realizar a identificação de artigos aplicáveis e justificativas para eventuais não conformidades.

3.12.23 Deve permitir garantia de transparência algorítmica (explicabilidade das decisões de IA).

3.12.24 Deve possuir mecanismos para mitigação de vieses discriminatórios em modelos de IA.

3.12.25 Deve possuir auditoria de impactos sociais e ambientais do sistema.

3.13. Requisitos de Gestão de Capacitação

3.13.1 Deverá suportar as seguintes características e funcionalidades:

3.13.2 Planejamento e monitoramento de atividades como cursos, workshops e treinamentos periódicos, alinhados às políticas de segurança e privacidade da organização.

3.13.3 Agendamento de eventos com notificações automáticas e registro de participantes, garantindo que o Encarregado de Dados acompanhe o cronograma de capacitações.

3.13.4 Integração com o componente de conscientização e treinamento, possibilitando a sincronização de dados de participação dos usuários nos treinamentos e o acompanhamento centralizado pelo Encarregado de Dados.

3.13.5 Painel centralizado com uma visão completa da gestão de eventos de capacitação, para facilitar a governança dos processos de treinamento, com foco em promover a conformidade com a LGPD e práticas de cibersegurança.

3.13.6. Serviço Técnico Especializado para Implantação, Parametrização e Customização da Solução, incluindo Apoio ao Diagnóstico, Adequação e Governança em Privacidade e Proteção de Dados Pessoais (Sob Demanda)

3.14. Requisitos Arquiteturais e de Integração

- **Ambiente Híbrido:** Capacidade de monitoramento simultâneo e centralizado de ativos localizados em infraestrutura local (*On-Premises* física ou virtualizada) e em Nuvem Pública/Privada.
- **Arquitetura Modular:** Ser desenvolvida em arquitetura de microsserviços ou containers, permitindo escalabilidade horizontal e atualização independente de módulos.
- **Ingestão de Dados:** Capacidade nativa de ingestão, normalização e correlação de *logs* provenientes de fontes heterogêneas, incluindo *Syslog*, Agentes de *Endpoint*, APIs de terceiros e *NetFlow*.
- **Interoperabilidade (API):** Disponibilização de Interface de Programação de Aplicações (API) do tipo *RESTful*, documentada, permitindo integração bidirecional com outros sistemas de segurança e gestão de TI.

3.15. FUNCIONALIDADES DE DEFESA E VISIBILIDADE (BLUE TEAM)

A solução deve incluir módulo de proteção de infraestrutura com as seguintes capacidades:

- **Agentes de Endpoint (EDR):** Fornecer agentes leves para sistemas operacionais Windows e Linux, capazes de:
    - Coletar telemetria de processos, conexões de rede e alterações no registro.

  - Realizar Monitoramento de Integridade de Arquivos (FIM) em tempo real.
  - Detectar anomalias comportamentais (heurística) além de assinaturas de malware.
- **Prevenção de Intrusão (HIDS/NIDS):** Capacidade de analisar tráfego e logs para identificar tentativas de exploração, força bruta e varreduras de porta, com capacidade de bloqueio ativo.
- **Mapeamento MITRE ATT&CK:** Correlacionar automaticamente os alertas de segurança com as táticas e técnicas da matriz MITRE ATT&CK, facilitando a análise de contexto.
- **Análise de Fluxo de Rede:** Monitorar fluxos de comunicação para identificar movimentação lateral, comunicações com servidores de Comando e Controle (C2) e exfiltração de dados.

3.16. Módulo de Gestão de Vulnerabilidades e Segurança Ofensiva

A solução deve possuir motor de varredura integrado (não sendo aceita ferramenta de terceiros desconexa), capaz de:

- **Varredura Contínua:** Capacidade de *scan* de ativos (IPs, servidores, aplicações web) para detecção de CVEs (Vulnerabilidades e Exposições Comuns).
- **Varreduras Híbridas:** Executar scans autenticados (com credenciais) e não autenticados (visão do atacante externo).
- **Priorização de Risco:** Classificação automática de vulnerabilidades baseada em criticidade e *Threat Intelligence* (inteligência de ameaças).
- **Pentest Automatizado:** Funcionalidade para execução de testes de intrusão automatizados e recorrentes.
- **Simulação de Ataques (BAS):** Capacidade de executar simulações de vetores de ataque reais para validar a eficácia dos controles de perímetro (Firewall, IPS, Antivírus).
- **Campanhas de Engenharia Social:** Ferramenta para criação e gestão de testes de *phishing* simulado, visando a educação e conscientização dos usuários.
- **Base de Conhecimento:** Possuir repositório atualizado de testes de vulnerabilidade de rede (NVTs), cobrindo CVEs (Common Vulnerabilities and Exposures) conhecidos.
- **Enriquecimento com Threat Intelligence:** Integrar nativamente com feeds de inteligência de ameaças para identificar se uma vulnerabilidade detectada possui exploits públicos ou está sendo explorada ativamente (IoCs).

3.17. FUNCIONALIDADES DE SEGURANÇA OFENSIVA E SIMULAÇÃO (RED TEAM)

Diferencialmente, a solução deve incorporar ferramentas de validação de segurança ativa:

- Simulador de Phishing: Módulo integrado para criação, envio e gestão de campanhas simuladas de phishing por e-mail, permitindo:
  - Uso de templates customizáveis.
  - Rastreamento de taxas de abertura, clique e inserção de credenciais.
  - Redirecionamento automático de usuários comprometidos para pílulas de treinamento/conscientização.
- **Simulador de Ataques de Negação de Serviço (DDoS):** Ferramenta controlada para testes de estresse de infraestrutura, permitindo configurar volume de tráfego, duração e tipos de protocolo (HTTP, UDP, SYN), com mecanismos de parada imediata (Kill Switch).
- **Monitoramento de Vazamentos (Dark Web):** Capacidade de monitorar proativamente domínios corporativos e e-mails institucionais em repositórios de vazamento de dados, fóruns clandestinos e redes Tor.

3.18. Módulo de Orquestração e Automação (SOAR) e Integração ITSM

A solução deve prover mecanismos para operacionalizar a resposta a incidentes:

- **Gestão de Incidentes (DFIR):** *Workflow* integrado para documentação e gestão do ciclo de vida de incidentes de segurança (Digital Forensics and Incident Response).
- **Automação de Resposta (Playbooks):** Capacidade de criar fluxos de trabalho automatizados baseados em gatilhos (ex: "Se malware detectado -> Isolar host da rede automaticamente").
- **Ações de Contenção:** Permitir execução remota de comandos de resposta nos agentes, como bloqueio de IPs, encerramento de processos e isolamento lógico de interface de rede.

- **Integração com Service Desk (ITSM):** A solução deve possuir conectores ou capacidade de integração via API para sincronização bidirecional com ferramentas de ITSM (ex: GLPI, ServiceNow, Jira, OTRS).
    - *Sincronização:* Abertura automática de tickets no ITSM a partir de incidentes críticos detectados na plataforma.
    - *Bidirecionalidade:* Alterações de status no ITSM (ex: encerramento de chamado) devem refletir na plataforma de segurança em tempo real (atraso máximo aceitável de 15 minutos), evitando retrabalho das equipes.

3.19. Módulo de Governança, Risco e Conformidade (GRC/LGPD)

A solução deve atender aos requisitos de GRC e validade jurídica:

- **Painel de Risco Unificado:** Apresentar um indicador numérico consolidado (Risk Score) da postura de segurança da organização, calculado com base em vulnerabilidades, incidentes e exposição de ativos.
- **Privacidade de Dados:** Ferramentas para inventário de dados pessoais (*Data Mapping*), gestão de solicitações de titulares (DSAR) e gestão de consentimento de cookies.
- **Relatórios Legais:** Geração automatizada de Relatórios de Impacto à Proteção de Dados (RIPD/DPIA) e ROPA.
- **Registro em Blockchain (Requisito Crítico):** Possuir funcionalidade nativa de registro de hashes de relatórios técnicos e trilhas de auditoria em tecnologia de livro-razão distribuído (Blockchain), garantindo imutabilidade, tempestividade e autenticidade das evidências para fins de conformidade legal e pericial.

3.20. Requisitos de Segurança, Auditoria e Validade Jurídica

- **Imutabilidade via Blockchain:** A solução deve possuir mecanismo de registro de logs e relatórios baseado em tecnologia de **livro-razão distribuído (Blockchain) ou encadeamento de hash (Merkle Tree)**.
    - *Abrangência:* Este mecanismo deve garantir a integridade não apenas dos relatórios de conformidade, mas também do **histórico de resposta a incidentes e investigações**, assegurando que as evidências forenses e os registros de ações da equipe técnica sejam inalteráveis e auditáveis juridicamente
- **Autenticação Segura:** Suporte obrigatório ao Múltiplo Fator de Autenticação (MFA) e compatibilidade com chaves de segurança físicas de hardware (padrão FIDO2/U2F) para acesso administrativo.
- **Relatórios de Conformidade:** Geração automática de relatórios mapeados para controles da LGPD (Lei Geral de Proteção de Dados) e ISO 27001.
- **Prevenção de Perda de Dados (DLP):** Capacidade de monitoramento de transferência de dados sensíveis em endpoints e mídias removíveis.
- **Gestão Granular de Acesso (RBAC):** Permitir a criação de perfis de acesso personalizados (ex: Administrador, Analista N1/N2, Auditor, Visualizador), segregando funções de leitura e escrita.
- **Auditoria Imutável:** Registrar todas as ações realizadas pelos operadores dentro da plataforma em logs protegidos contra exclusão.
- Fornecimento de Chaves de Segurança Físicas (Hardware Keys) compatíveis com o padrão **FIDO2/U2F**, para autenticação resistente a *phishing* dos administradores da plataforma.
    - Esclarece-se que o fornecimento das chaves de segurança físicas de hardware (padrão FIDO2/U2F) listadas nestes requisitos não constitui aquisição de equipamentos de informática autônomos por parte da Administração. Trata-se do fornecimento de dispositivos de autenticação indissociáveis e obrigatórios, atrelados à subscrição da plataforma (Item 1) durante a vigência do contrato, visando garantir o cumprimento do alto nível de segurança exigido para o acesso dos administradores.

3.21.ESPECIFICAÇÃO TÉCNICA: PLATAFORMA DE GESTÃO E VISUALIZAÇÃO UNIFICADA (CONSOLE CENTRAL)

3.21.1. A solução ofertada deverá dispor, obrigatoriamente, de uma interface de gerenciamento centralizada, operando sob o conceito de "Painel Único de Vidro" (Single Pane of Glass), desenvolvida em tecnologia web moderna e responsiva, capaz de atuar como o ponto focal de toda a operação de segurança cibernética da contratante. Este console não poderá se limitar a ser um mero agregador de links para ferramentas distintas; ele deve constituir uma plataforma integrada onde os dados provenientes de diferentes camadas de defesa, incluindo proteção de endpoints, varreduras de vulnerabilidade, inteligência de ameaças externas, simulações de ataques e conformidade regulatória, de forma que sejam normalizados, correlacionados e apresentados de forma coesa e inteligível. É imprescindível que o painel possua capacidade de processamento em tempo real, permitindo a visualização instantânea do estado de segurança da infraestrutura monitorada, sem a necessidade de recarregamento manual de páginas ou processos de sincronização em lote (batch) que gerem latência na informação.

3.21.2. Fundamentalmente, o painel unificado deverá incorporar um mecanismo algorítmico avançado de quantificação de risco cibernético, preferencialmente com correlações de dados utilização de inteligência avançada para todo o processamento e análise de comportamento, este mecanismo deve ser capaz de analisar o volume de vulnerabilidades detectadas, a severidade das mesmas (baseada em padrões internacionais como CVSS e o ambiente da contratada), a criticidade dos ativos afetados e a existência de incidentes ativos, consolidando todas essas variáveis em uma pontuação numérica de risco dinâmica e de fácil interpretação. Esta métrica de risco deve ser apresentada de forma segmentada, permitindo que os gestores visualizem, em widgets gráficos distintos, o nível de exposição específico de grupos de servidores, estações de trabalho e sistemas operacionais, facilitando a tomada de decisão sobre onde alocar recursos de remediação prioritariamente. O sistema deve permitir o "drill-down" (aprofundamento) a partir destes indicadores gráficos, possibilitando que o operador clique em uma métrica de risco e seja direcionado imediatamente para a lista detalhada dos ativos ou vulnerabilidades que compõem aquele indicador.

3.21.3. Além das métricas defensivas tradicionais, o painel unificado deve possuir a capacidade distinta de integrar e exibir, na mesma interface visual, os resultados de operações de segurança ofensiva e validação contínua. Isso implica que o console deve apresentar dados referentes a testes de simulação de ataques, como campanhas de conscientização contra phishing (taxas de abertura e comprometimento de usuários) e testes de estresse de negação de serviço (DDoS), lado a lado com os alertas de intrusão e integridade de sistemas. Esta característica é mandatória para prover uma visão holística que contemple tanto a eficácia das proteções técnicas quanto a resiliência do fator humano e da infraestrutura de rede, eliminando a necessidade de alternância entre múltiplos softwares para obter um panorama completo da segurança.

3.21.4. No que tange à usabilidade e ergonomia operacional, a interface deve suportar nativamente a personalização de visualizações baseada no perfil do usuário logado, garantindo a segregação de deveres e a relevância da informação apresentada. O sistema deve oferecer suporte a temas visuais adaptativos, incluindo obrigatoriamente um "Modo Escuro" (Dark Mode) para reduzir a fadiga visual dos operadores em ambientes de monitoramento contínuo (SOC 24x7). A navegação deve ser intuitiva, organizada por pilares funcionais (como Detecção, Vulnerabilidades, Incidentes e Relatórios), e deve incluir mecanismos de busca global que permitam localizar rapidamente ativos, endereços IP, usuários ou hashes de arquivos em toda a base de dados histórica e em tempo real da plataforma. Por fim, o painel deve evidenciar a conformidade e integridade das operações, exibindo de forma clara o status dos agentes de monitoramento e alertas sobre quaisquer dispositivos que deixem de reportar ao console central, garantindo que não existam pontos cegos silenciosos na infraestrutura de defesa.

3.22. ESPECIFICAÇÃO TÉCNICA: MOTOR DE ANÁLISE DE VULNERABILIDADES E VARREDURA DE REDE

3.22.1. A solução contratada deverá integrar nativamente, sem a necessidade de aquisição de módulos externos ou hardwares proprietários adicionais, um robusto motor de gerenciamento de vulnerabilidades (Vulnerability Management Engine), capaz de realizar a detecção, identificação e avaliação de falhas de segurança em ativos de TI, OT e/ou IoT conectados à rede da contratante. Este componente deve operar de forma totalmente integrada ao console central de gerenciamento, permitindo que os dados coletados nas varreduras sejam imediatamente correlacionados com outras camadas de segurança da plataforma. É imperativo que o motor de análise seja alimentado por um repositório de Testes de Vulnerabilidade de Rede (NVTs - Network Vulnerability Tests) dinâmico e abrangente, contendo um acervo superior a cem mil scripts de verificação distintos, com atualizações diárias automáticas via feed de dados criptografado, garantindo a detecção das Ameaças e Exposições Comuns (CVEs) mais recentes publicadas pela comunidade de segurança global.

3.22.2. O sistema deve oferecer flexibilidade total na configuração das metodologias de varredura, suportando obrigatoriamente a execução de testes em múltiplas modalidades de profundidade e intrusão. O mecanismo deve ser capaz de executar desde varreduras leves de descoberta de ativos (Asset Discovery), utilizando protocolos como ICMP e ARP para mapeamento de topologia, até varreduras exaustivas de portas e serviços. No que tange à varredura de portas, a solução deve suportar técnicas avançadas como TCP SYN Scan (half-open) para maior discrição e velocidade, TCP Connect Scan para validação completa de handshake, e varreduras UDP para identificação de serviços sem conexão, permitindo a customização das faixas de portas a serem analisadas (de portas conhecidas até o range completo 1-65535) e o ajuste de parâmetros de timing para evitar a sobrecarga dos ativos alvo ou o bloqueio por dispositivos de segurança perimetral.

3.22.3. A solução deve ter a capacidade de realizar Varreduras Autenticadas (Credentialed Scans). O sistema deve possuir um cofre de credenciais seguro integrado, permitindo que o scanner realize o login nos ativos alvo utilizando protocolos administrativos padrão, tais como SSH (para sistemas baseados em Unix/Linux), SMB e WMI (para ambientes Windows) e SNMP (para dispositivos de rede). Através deste acesso autenticado, o motor de análise não deve se limitar a inferir vulnerabilidades baseadas apenas nas respostas de rede (banners de serviço), mas deve ser capaz de interrogar diretamente o sistema operacional para realizar inventário de software instalado, verificar versões de pacotes, identificar atualizações de segurança (patches) ausentes e auditar configurações inseguras locais (hardening), proporcionando uma visão interna precisa do nível de risco do ativo e eliminando drasticamente a ocorrência de falsos positivos comuns em varreduras externas.

3.22.4. Além da detecção técnica, o módulo deve possuir inteligência para classificação e priorização de riscos. Todas as vulnerabilidades identificadas devem ser automaticamente categorizadas de acordo com o padrão internacional CVSS (Common Vulnerability Scoring System), mas o sistema deve permitir a contextualização deste risco, oferecendo relatórios que detalhem não apenas a falha, mas também a solução recomendada (mitigação ou correção), referências cruzadas com bancos de dados públicos (como NVD e CVE), a probabilidade de exploração, bem como se existe algum exploit público da vulnerabilidade e caso exista algum arquivo, script ou documento associado a este exploit também deverá ser exibido e disponibilizado para download na plataforma. A solução deve suportar o agendamento granular de tarefas de varredura, permitindo a execução recorrente e automatizada (diária, semanal, mensal) e a geração de relatórios de análise diferencial (Delta Reports), que evidenciem explicitamente quais novas vulnerabilidades surgiram e quais foram mitigadas entre duas execuções distintas, facilitando o acompanhamento da evolução da postura de segurança ao longo do tempo.

3.22.5. Por fim, o mecanismo de varredura deve ser capaz de auditar a conformidade dos sistemas em relação a políticas de segurança e normas técnicas. O sistema deve permitir a execução de testes de conformidade (Compliance Checks) baseados em guias de boas práticas reconhecidos pelo mercado (como benchmarks do CIS ou políticas de TI específicas), verificando parâmetros como complexidade de senha, serviços desnecessários ativos, permissões de arquivos críticos e configurações de auditoria, gerando evidências técnicas documentais que suportem processos de certificação e auditoria interna.

3.23. ESPECIFICAÇÃO TÉCNICA: MONITORAMENTO AVANÇADO DE ENDPOINTS (EDR) E INTELIGÊNCIA DE AMEAÇAS

3.23.1. A solução contratada deve incorporar um sistema de Detecção e Resposta em Endpoints (EDR - Endpoint Detection & Response) baseado na implantação de agentes de software leves e multiplataforma, compatíveis com os sistemas operacionais Windows, Linux e macOS. Estes agentes devem operar com baixo consumo de recursos computacionais, atuando como sensores avançados capazes de coletar, em tempo real, uma vasta gama de telemetria do sistema, incluindo a criação de processos, modificações no registro do sistema, conexões de rede ativas e alterações no sistema de arquivos. Toda a coleta de dados deve ser enviada de forma criptografada para o servidor central, onde um motor de correlação e decodificação normalizará os eventos para análise imediata.

3.23.2. Diferenciando-se das soluções de antivírus tradicionais baseadas puramente em assinaturas, o módulo EDR deve possuir capacidades avançadas de Análise Comportamental Heurística. O sistema deve ser capaz de monitorar padrões de atividade anômalos que indiquem a presença de malware sofisticado ou ataques em andamento, com ênfase específica na detecção de Ransomware. O motor de análise deve identificar comportamentos característicos, como a modificação ou criptografia massiva de arquivos em curto espaço de tempo, tentativas de exclusão de cópias de sombra (shadow copies) ou injeção de código em processos legítimos do sistema. Complementarmente, a solução deve incluir um módulo de Monitoramento de Integridade de Arquivos (FIM - File Integrity Monitoring) capaz de criar linhas de base (baselines) de arquivos críticos e diretórios de configuração, gerando alertas instantâneos com detalhes de "quem, quando e o quê" sempre que houver uma modificação, criação ou exclusão não autorizada, garantindo a detecção de persistência de ameaças e alterações indevidas.

3.23.3. Para elevar a capacidade de detecção a um nível de estado da arte, a plataforma deve possuir integração nativa e automatizada com redes globais de Inteligência de Ameaças (Threat Intelligence), especificamente consumindo feeds de reputação de IP, hashes de arquivos e domínios maliciosos. Esta integração deve permitir a detecção de ameaças de dia zero (0-day) e a identificação de Indicadores de Comprometimento (IoCs) assim que estes forem observados na rede mundial, correlacionando-os instantaneamente com a atividade interna dos endpoints monitorados. O sistema deve traduzir automaticamente os alertas técnicos gerados para a linguagem tática universal, mapeando cada incidente detectado às táticas e técnicas correspondentes da matriz MITRE ATT&CK, facilitando a compreensão do estágio do ataque e a execução de estratégias de caça a ameaças (Threat Hunting) sobre os dados históricos armazenados.

3.23.4. Um requisito funcional mandatório e distintivo desta solução refere-se à validação de risco de vulnerabilidades detectadas nos endpoints. O sistema não deve apenas informar a existência de uma vulnerabilidade (CVE), mas deve verificar automaticamente em repositórios públicos e privados a existência de códigos de exploração (exploits) conhecidos para aquela falha específica. Caso um exploit seja identificado, a plataforma deve exibir essa correlação crítica e, obrigatoriamente, caso existente, disponibilizar o arquivo, script ou documento técnico associado a este exploit para visualização e download seguro diretamente através da interface do sistema. Esta funcionalidade é essencial para que a equipe de segurança possa validar a efetividade do risco e priorizar correções de falhas que possuem vetores de ataque publicamente armados.

3.23.5. Por fim, a camada de gestão e visualização do EDR deve ser potencializada por Inteligência Artificial Generativa. O sistema deve ser capaz de processar o grande volume de logs e eventos brutos coletados pelos agentes e gerar, automaticamente, Relatórios Consolidados de EDR com narrativas textuais inteligíveis, resumindo incidentes complexos, sugerindo ações de remediação e eliminando a necessidade de análise manual de milhares de linhas de log. Os dados coletados pelos agentes devem alimentar dinamicamente o algoritmo de cálculo de risco unificado da plataforma (Risk Score), influenciando a pontuação global de segurança da organização. A solução deve ainda oferecer ferramentas de gestão de parque, permitindo a exportação completa do inventário de agentes e seus status em formatos estruturados, além de módulos de conformidade que verifiquem automaticamente a aderência dos endpoints a normas regulatórias como PCI-DSS, NIST e LGPD/GDPR.

3.24. ESPECIFICAÇÃO TÉCNICA: MONITORAMENTO DE AMEAÇAS EXTERNAS E VIGILÂNCIA DA DARK WEB

3.24.1. A solução deve incluir um módulo especializado em Inteligência de Ameaças Cibernéticas focado no monitoramento persistente e proativo da "Dark Web", "Deep Web" e outras fontes de dados não indexadas publicamente. Este serviço deve operar de forma contínua, 24 horas por dia, 7 dias por semana, atuando como um radar externo que varre comunidades clandestinas, fóruns de cibercrime, mercados negros digitais, redes peer-to-peer (P2P), canais de chat privados (como Telegram e Discord), "paste sites" e repositórios de vazamento de dados, em busca de qualquer indício de comprometimento relacionado aos ativos digitais da organização contratante.

3.24.2. O escopo de monitoramento deve permitir a configuração e rastreamento de múltiplos identificadores corporativos, incluindo, mas não se limitando a: domínios de e-mail corporativo (ex: @empresa.gov.br), endereços IP públicos, nomes de marcas ou projetos sensíveis e endereços de e-mail pessoais de executivos de alto nível (VIPs). Ao detectar uma correspondência (match) nesses ambientes hostis, a plataforma deve gerar alertas em tempo real, fornecendo contexto detalhado sobre o incidente. O alerta não deve ser apenas informativo; ele deve categorizar a severidade do vazamento e identificar a origem dos dados, distinguindo se o comprometimento ocorreu devido a uma violação direta na organização, um ataque a terceiros (supply chain attack) ou através de malware do tipo infostealer em dispositivos de usuários.

3.24.3. A plataforma deve fornecer visibilidade granular sobre as credenciais comprometidas. Os relatórios de alerta devem exibir, de forma segura (parcialmente ofuscada para proteção), quais senhas foram expostas, permitindo que a equipe de segurança verifique se as credenciais vazadas correspondem às políticas de senha atuais ou se são senhas antigas reaproveitadas. Além de credenciais de login, o sistema deve ser capaz de identificar a exposição de outros tipos de Dados Pessoais Identificáveis (PII), como números de documentos, dados bancários e informações médicas, correlacionando esses achados com os requisitos de notificação de incidentes da Lei Geral de Proteção de Dados (LGPD).

3.24.4. Para garantir uma gestão eficaz desses incidentes externos, o módulo deve possuir funcionalidades de integração com o fluxo de trabalho da equipe de TI. A solução deve permitir a exportação dos dados de monitoramento para relatórios executivos e técnicos, que evidenciem a tendência de exposição da organização ao longo do tempo (gráficos de volume de credenciais vazadas vs. tempo). Além disso, deve oferecer integração via API ou plugins com sistemas de diretório (como Active Directory, Azure AD ou Google Workspace), permitindo, se configurado, o gatilho de ações automáticas de resposta, como a imposição de redefinição de senha para usuários cujas credenciais foram detectadas em dumps de vazamento de alta confiabilidade. O painel de visualização deve oferecer recursos de filtragem avançada, permitindo a segregação de dados por departamento, domínio ou tipo de violação, facilitando a análise de impacto e a priorização de ações corretivas.

3.25. ESPECIFICAÇÃO TÉCNICA: PLATAFORMA DE SIMULAÇÃO DE PHISHING E TREINAMENTO DE CONSCIENTIZAÇÃO

3.25.1. A solução deve fornecer um módulo integrado dedicado à avaliação e treinamento do fator humano na segurança da informação, permitindo a criação, execução e gestão de campanhas simuladas de engenharia social (Phishing) de nível corporativo. A ferramenta deve oferecer flexibilidade total para o desenho de cenários de ataque, permitindo que os administradores avaliem a resiliência dos colaboradores frente a vetores de ataque baseados em e-mail, que constituem a principal porta de entrada para ransomwares e violações de dados.

3.25.2. No que tange à gestão de alvos e audiência, o sistema deve permitir a importação em massa de usuários e grupos através de arquivos estruturados (como CSV), bem como a segmentação destes alvos em grupos distintos (por exemplo: "Diretoria", "Financeiro", "TI"). O gerenciamento de campanhas deve suportar o agendamento preciso de disparos, permitindo definir janelas de tempo específicas para o envio dos e-mails, evitando picos de tráfego de rede e garantindo que os testes ocorram em horários comerciais apropriados.

3.25.3. A capacidade de criação de conteúdo (Templates) deve ser robusta e versátil. O sistema deve possuir um editor HTML completo (WYSIWYG) para a criação de e-mails, mas, crucialmente, deve oferecer uma funcionalidade nativa de Importação e Clonagem de E-mails. Isso deve permitir que o administrador insira o código-fonte de um e-mail real recebido (como uma notificação de redefinição de senha do Microsoft 365 ou um aviso de banco) e o sistema recrie o template fielmente para uso na simulação. Da mesma forma, a plataforma deve permitir a criação de Páginas de Destino (Landing Pages) enganosas, com suporte à Clonagem de Sites Reais: o administrador deve poder inserir a URL de uma página de login legítima e a ferramenta deve copiar automaticamente o HTML, CSS e scripts para criar uma réplica perfeita hospedada no servidor de simulação, destinada a testar se o usuário insere suas credenciais.
3.25.4. Para o envio das campanhas, a solução deve suportar a configuração de Perfis de Envio, permitindo a conexão com qualquer servidor SMTP externo ou relay de e-mail. Deve ser possível customizar os cabeçalhos de e-mail (Headers) para simular remetentes externos ou internos, testando a atenção do usuário aos detalhes de "From:" e "Reply-To".
3.25.5. O sistema de rastreamento e métricas deve ser granular e operar em tempo real. A plataforma deve ser capaz de monitorar e registrar individualmente cada etapa da interação do usuário com a isca, classificando os eventos nos seguintes status: E-mail Enviado, E-mail Aberto (via rastreamento de pixel), Link Clicado e Dados Submetidos (caso o usuário digite credenciais na página falsa). É fundamental que, ao capturar dados submetidos (como senhas), a plataforma possua configurações de privacidade para descartar ou ofuscar essas informações sensíveis, registrando apenas o fato de que a submissão ocorreu, para fins estatísticos, sem armazenar as credenciais reais dos colaboradores.
3.25.6. A solução deve incorporar recursos de Inteligência Artificial (IA) para Geração de Relatórios, ao final de uma campanha, além dos gráficos estatísticos padrão, o sistema deve utilizar algoritmos de IA para processar os dados coletados e gerar automaticamente um relatório analítico textual. Este relatório deve interpretar os resultados, identificando tendências de comportamento (ex: "O departamento Financeiro teve a maior taxa de cliques em horários de almoço"), resumir o desempenho geral da organização frente ao cenário testado e fornecer recomendações executivas de treinamento baseadas na performance observada, economizando horas de análise manual por parte da equipe de gestão.
3.25.7. Por fim, o módulo deve fechar o ciclo de aprendizado oferecendo mecanismos de "Momento de Ensino" (Teachable Moment). Caso o usuário falhe no teste (clique no link ou insira dados), o sistema deve ser capaz de redirecioná-lo automaticamente para uma página educativa configurável, que explique que ele foi alvo de uma simulação, aponte os indicadores de fraude que ele perdeu no e-mail e forneça orientações imediatas de segurança.

3.26. ESPECIFICAÇÃO TÉCNICA: PLATAFORMA DE TESTES DE ESTRESSE E SIMULAÇÃO DE NEGAÇÃO DE SERVIÇO (DDoS)

3.26.1. A solução deve prover um módulo avançado de "teste de estresse" dedicado à validação da resiliência da infraestrutura de rede e aplicações da contratante, a ferramenta deve permitir a execução controlada e autorizada de simulações de ataques de Negação de Serviço Distribuído (DDoS), operando em ambiente isolado ou de produção, com o objetivo de testar a capacidade de throughput dos links, a eficácia das regras de firewall, a performance de balanceadores de carga e a prontidão dos sistemas de mitigação anti-DDoS. O painel de controle deve ser intuitivo, permitindo a configuração granular dos vetores de ataque, duração do teste e intensidade da carga (Requisições por Segundo ou Largura de Banda).
3.26.2. É requisito mandatório que a ferramenta suporte simulações abrangentes na Camada de Transporte (Layer 4) do modelo OSI, cobrindo tanto o protocolo UDP quanto o TCP.
3.26.3. Para simulações baseadas em UDP, o sistema deve oferecer métodos específicos para testar serviços críticos e de tempo real, incluindo:
3.26.4. Amplificação DNS: Simulação de ataques volumétricos refletidos via servidores de nomes.
3.26.5. Protocolos de Voz e Comunicação: Suporte a métodos como Mixamp, Ts3 (TeamSpeak) e Discord, essenciais para validar a estabilidade de sistemas de VoIP e colaboração sob estresse.

3.26.6. Protocolos de Aplicações de Baixa Latência: Capacidade de gerar tráfego específico para serviços que utilizam engines de rede proprietárias, como Raknet, Fivem e vetores genéricos UDP, permitindo testar a infraestrutura em cenários de tráfego de pacotes pequenos e alta frequência (PPS - Packets Per Second).
3.26.7. Para simulações baseadas em TCP (Transmission Control Protocol), a ferramenta deve disponibilizar vetores que explorem o mecanismo de handshake e a manutenção de estado das conexões, incluindo:
3.26.7.1. **TCP SYN Flood:** O teste padrão da indústria para exaurir recursos de conexão de firewalls e servidores.
3.26.7.2. **TCP ACK Flood:** Simulação de tráfego de resposta para testar a capacidade de processamento de pacotes estúrios.
3.26.7.3. **Vetores Avançados:** Métodos como Tcpito e TCP Warp, projetados para simular conexões complexas e testar a capacidade de inspeção profunda de pacotes (DPI) dos dispositivos de segurança.
3.26.8. Complementarmente, a solução deve oferecer capacidades robustas de teste na Camada de Aplicação (Layer 7), focadas em exaurir os recursos de processamento (CPU/Memória) dos servidores web e de aplicação, simulando o comportamento de milhares de usuários simultâneos ou bots maliciosos. Os métodos suportados devem incluir:
3.26.8.1. **HTTP Flood Padrão:** Geração de alto volume de requisições GET/POST legítimas.
3.26.8.2. **HTTP Flood Otimizados:** Variações de alta performance utilizando rotinas de concorrência modernas para maximizar a taxa de requisições por segundo (RPS) com baixo consumo de recursos do gerador.
3.26.8.3. **Simulação de Protocolo Específico:** Suporte a métodos como HTTP Tempesta, focado em explorar a conformidade do servidor com o protocolo HTTP e sua capacidade de lidar com cabeçalhos e formatos de requisição complexos.
3.26.9. O painel de simulação deve incluir mecanismos de segurança operacional ("Safety Switches"). Deve existir uma funcionalidade de Parada de Emergência (Kill Switch) acessível a qualquer momento, permitindo a interrupção imediata de todo o tráfego de teste caso seja detectado impacto negativo não planejado em serviços críticos de produção. Além disso, a ferramenta deve fornecer relatórios pós-teste detalhados, indicando o volume de tráfego gerado, a taxa de sucesso das requisições e a latência observada, servindo como evidência técnica para o planejamento de capacidade da infraestrutura.
3.26.10. Com base nos resultados obtidos, a solução deve apresentar recomendações técnicas de correção e fortalecimento da infraestrutura, orientadas a boas práticas de segurança e desempenho, tais como:
3.26.10.1. Ajustes em políticas de firewall, rate limiting e regras de filtragem;
3.26.10.2. Recomendações para tuning de parâmetros TCP/UDP e mitigação de exaustão de estado;
3.26.10.3. Orientações para otimização de balanceamento de carga, escalabilidade horizontal e capacidade de throughput;
3.26.10.4. Sugestões de aprimoramento na configuração ou integração com soluções de mitigação anti-DDoS;
3.26.10.5. Identificação de melhorias no stack de aplicação para aumento de resiliência em Layer.

3.27. ESPECIFICAÇÃO TÉCNICA: MÓDULO DE INTELIGÊNCIA DE FONTES ABERTAS (OSINT) E MAPEAMENTO DE EXPOSIÇÃO EXTERNA

3.27.1 A solução contratada deve integrar um subsistema avançado de Inteligência de Fontes Abertas (OSINT), projetado para automatizar a coleta, processamento e análise de dados publicamente disponíveis relacionados à infraestrutura digital e aos ativos de identidade da organização. Este módulo deve atuar como uma ferramenta de reconhecimento proativo, permitindo que a equipe de segurança visualize a organização sob a ótica de um agente de ameaça externo, identificando vetores de ataque potenciais e exposições inadvertidas antes que sejam exploradas. O sistema deve permitir a execução de análises baseadas em dois eixos principais de entrada: domínios institucionais e identificadores de identidade (endereços de e-mail).

3.27.2. No eixo de análise de infraestrutura e domínios, a ferramenta deve possuir um motor de descoberta automatizada de subdomínios, capaz de identificar ativos esquecidos ou não documentados que pertençam à zona DNS da organização. Complementarmente, o sistema deve realizar uma auditoria profunda dos registros DNS, incluindo a verificação de conformidade e segurança dos registros MX, TXT, e especificamente dos protocolos de autenticação de e-mail, como SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) e DMARC (Domain-based Message Authentication, Reporting, and Conformance). O módulo também deve interrogar bases de dados WHOIS históricas e atuais para identificar informações de registro de domínio, datas de expiração e contatos técnicos associados, alertando sobre possíveis riscos de sequestro de domínio ou exposição de dados de administradores.

3.27.3. Além da infraestrutura de rede, o módulo de OSINT deve ser capaz de realizar a identificação de tecnologias (Fingerprinting) utilizadas nas interfaces web da organização. Isso inclui o mapeamento de servidores web, sistemas operacionais, frameworks de desenvolvimento, linguagens de programação e sistemas de gestão de conteúdo (CMS) ativos. O objetivo é permitir que a equipe de segurança identifique rapidamente quais ativos estão utilizando tecnologias com vulnerabilidades recém-descobertas ou versões descontinuadas (End-of-Life). O sistema também deve possuir capacidades de coleta de metadados em arquivos públicos indexados em motores de busca, visando localizar informações sensíveis ocultas em documentos, como nomes de usuários, caminhos de rede interna e versões de software.

3.27.4. No eixo de inteligência de identidades, o sistema deve permitir a análise profunda de endereços de e-mail corporativos para mapear sua presença digital externa. Isso envolve a verificação de contas associadas em plataformas de redes sociais, fóruns profissionais e serviços de terceiros, bem como o cruzamento desses identificadores com bases de dados de violações históricas. Esta funcionalidade é essencial para identificar perfis de colaboradores que possuam uma pegada digital extensa e que possam ser alvos prioritários de ataques de engenharia social direcionada.

3.27.5. Como requisito fundamental de análise e visualização, a plataforma deve disponibilizar uma interface de Mapeamento Analítico baseado em Grafos de Relacionamento. Esta funcionalidade deve converter os dados textuais coletados em uma representação visual dinâmica de nós e arestas, onde o usuário possa visualizar graficamente as interconexões entre domínios, subdomínios, endereços IP, registros DNS e contas de e-mail. A visualização por grafos deve permitir diferentes layouts de exibição (como visualizações de força, radiais ou hierárquicas), permitindo que o analista identifique padrões de infraestrutura e correlações complexas que seriam invisíveis em tabelas convencionais.

3.27.6. Por fim, o módulo deve ser potencializado por Inteligência Artificial para a Interpretação de Cenários Externos, o sistema deve ser capaz de processar a massa de dados coletada via OSINT e gerar relatórios executivos interpretativos, que não apenas listem os dados encontrados, mas expliquem o nível de severidade da exposição externa e sugiram ações imediatas de endurecimento da superfície de ataque. Os resultados dessas análises externas devem ser integrados ao algoritmo de cálculo de risco unificado da plataforma, garantindo que a visibilidade externa influencie diretamente a pontuação global de postura de segurança da organização.

3.28. ESPECIFICAÇÃO TÉCNICA: SUBSISTEMA DE GESTÃO DE EVIDÊNCIAS, RELATÓRIOS E INTEGRIDADE DE DADOS

3.28.1. A solução deverá disponibilizar um módulo avançado para a geração, custódia e exportação de relatórios técnicos e executivos, consolidando todas as informações coletadas pelos demais módulos (Detecção, Vulnerabilidades, Phishing, DDoS e OSINT). Este subsistema deve ser projetado sob princípios de Segurança da Informação que garantam a tríade da Confidencialidade, Integridade e Disponibilidade, transformando dados operacionais em ativos de inteligência estratégica e evidências auditáveis com validade técnica e jurídica.

3.28.2. No que tange à Confidencialidade e Proteção de Dados, todos os relatórios gerados pela plataforma devem, obrigatoriamente, ser armazenados de forma criptografada "at rest" (em repouso). O sistema deve utilizar algoritmos de criptografia forte de padrão industrial (como AES-256 ou superior) para garantir que as informações sensíveis sobre a infraestrutura da organização, tais como falhas críticas, senhas expostas detectadas ou topologias de rede, fiquem inacessíveis a usuários não autorizados ou em casos de acesso indevido à camada de armazenamento. A visualização e o download desses documentos devem ser restritos por perfis de acesso (RBAC) e protegidos pela camada de autenticação forte (MFA com FIDO2) descrita anteriormente.
3.28.3. Como requisito de Integridade e Não-Repúdio, a plataforma deve incorporar nativamente uma camada de tecnologia de registro distribuído baseada nos princípios de Blockchain, este mecanismo deve atuar da seguinte forma:
3.28.3.1. No exato instante em que qualquer relatório for finalizado pelo sistema, a plataforma deverá gerar automaticamente um Hash Criptográfico único (SHA-256 ou superior) que represente a "impressão digital" digital exata do conteúdo do documento.
3.28.3.2. Este Hash, juntamente com um carimbo de tempo preciso e sincronizado via protocolo NTP de alta confiabilidade, deverá ser registrado em uma estrutura de dados imutável.
3.28.4. O sistema deve permitir a qualquer momento a Verificação de Integridade, onde o usuário possa processar um relatório exportado e o sistema compare o Hash atual com o registro persistido na Blockchain interna. Caso ocorra qualquer alteração, ainda que de um único bit ou caractere no documento após a sua emissão, o sistema deve invalidar a evidência, alertando sobre a quebra de integridade.
3.28.5. Este requisito de imutabilidade rastreada é mandatório para assegurar a conformidade com o Artigo 369 do Código de Processo Civil Brasileiro (CPC/2015) e normas internacionais de auditoria, permitindo que os relatórios sejam utilizados como prova técnica pericial em incidentes de segurança, litígios ou processos de fiscalização da Autoridade Nacional de Proteção de Dados (ANPD).
3.28.6. Funcionalmente, o módulo de relatórios deve oferecer:
3.28.6.1. **Diversidade de Formatos e Níveis:** Capacidade de gerar relatórios em formatos estruturados (JSON, CSV, XML) para integração com outros sistemas, e formatos de leitura humana (PDF, HTML) com diagramação profissional.
3.28.6.2. **Relatórios Executivos (C-Level):** Visões macro com indicadores de desempenho (KPIs), tendências de risco (TruRisk), economia de custos operacionais e status geral de conformidade (LGPD/ISO 27001), utilizando linguagem menos técnica e foco em impacto de negócio.
3.28.6.3. **Relatórios Técnicos Detalhados:** Documentos contendo evidências brutas, logs de tráfego, código-fonte de exploits associados, detalhes de remediação passo a passo e mapeamento completo para a matriz MITRE ATT&CK.
3.28.6.4. **Automação e Agendamento:** Possibilidade de programar a geração e o envio automático de relatórios periódicos para stakeholders específicos via canais seguros, eliminando a necessidade de intervenção manual da equipe de SOC para tarefas rotineiras de report.
3.28.7. Por fim, o sistema deve manter uma Trilha de Auditoria (Audit Log) imutável de todos os relatórios acessados, gerados ou exportados, registrando o usuário, o endereço IP de origem, a data, a hora e o Hash do documento envolvido, garantindo a rastreabilidade total do ciclo de vida da informação dentro da plataforma.

3.29. ESPECIFICAÇÃO TÉCNICA: SUBSISTEMA DE ORQUESTRAÇÃO

3.29.1. A solução deverá integrar nativamente um motor de Orquestração, Automação e Resposta de Segurança (SOAR - Security Orchestration, Automation, and Response), capaz de converter alertas estáticos em fluxos de trabalho dinâmicos e automatizados. Este módulo deve atuar como a camada de inteligência operacional da plataforma, permitindo a conexão lógica entre os diversos componentes internos (como o EDR, o Scanner de Vulnerabilidades e o monitor de Dark Web) e sistemas externos de infraestrutura, visando a redução drástica do Tempo Médio de Resposta (MTTR) e a padronização dos procedimentos operacionais de segurança.

3.29.2. A engine de automação deve possuir uma interface visual de fácil utilização para a construção de fluxos de trabalho, conhecidos como Playbooks, permitindo que analistas definam sequências de ações baseadas em lógica condicional. O sistema deve suportar a criação de gatilhos automáticos (Triggers) ativados por eventos específicos detectados pela plataforma, como a identificação de um malware de alta criticidade, a detecção de um ataque de força bruta ou a descoberta de uma credencial administrativa exposta na rede clandestina. Além dos gatilhos automáticos, a ferramenta deve permitir o disparo manual de Playbooks diretamente a partir do painel de incidentes, conferindo ao operador o controle final sobre ações de remediação complexas.

3.29.3. No que tange à orquestração e conectividade, o módulo deve possuir uma arquitetura aberta e baseada em conectores universais para integração com terceiros via APIs RESTful. A plataforma deve ser capaz de realizar chamadas de entrada e saída, processando dados em formato JSON ou XML e realizando a normalização e transformação dessas informações entre diferentes ferramentas. Isso possibilita que um único fluxo de automação interaja com múltiplos ativos de rede de forma sequencial; por exemplo, ao identificar uma ameaça, o sistema pode simultaneamente consultar a reputação do arquivo em bases de inteligência globais, isolar logicamente o host comprometido através do agente de endpoint, realizar o bloqueio do endereço IP de origem no firewall de borda e notificar a equipe técnica via canais de mensageria corporativa.

3.29.4. A capacidade de automação deve abranger o enriquecimento de dados e a triagem inicial de incidentes. O sistema deve ser capaz de realizar consultas automatizadas para validar a veracidade de um alerta antes de notificar um analista humano, reduzindo a fadiga de alertas e eliminando falsos positivos. Durante a execução de um Playbook, a plataforma deve registrar detalhadamente cada passo executado, incluindo o sucesso ou falha de cada ação individual, gerando logs de execução que sirvam como trilha de auditoria para investigações forenses e melhoria contínua dos processos.

3.29.5. Por fim, o módulo SOAR deve estar intrinsecamente ligado ao sistema de gestão de casos (Case Management) da plataforma. Cada automação executada deve estar vinculada a um ticket ou incidente específico, permitindo que a linha do tempo do evento exiba tanto as ações manuais dos analistas quanto as intervenções automáticas realizadas pelo sistema. A ferramenta deve permitir a criação de bibliotecas de Playbooks reutilizáveis e a customização de variáveis globais, garantindo que a organização possa escalar sua capacidade de resposta à medida que novas ameaças e ativos sejam integrados ao ambiente monitorado.

3.30. ESPECIFICAÇÃO TÉCNICA: SUBSISTEMA DE RESPOSTA A INCIDENTES, PERÍCIA DIGITAL (DFIR) E GOVERNANÇA (GRC)

3.30.1. A solução deverá contemplar um subsistema robusto de Resposta a Incidentes e Perícia Digital, operando de forma nativa e integrada ao ecossistema de segurança para garantir a gestão completa do ciclo de vida de qualquer evento adverso. Este módulo deve atuar como o repositório central de inteligência forense da contratante, permitindo que analistas e investigadores conduzam análises profundas, documentem evidências e reconstruam a cronologia exata de ataques sem a necessidade de alternar entre múltiplas interfaces. A ferramenta deve possibilitar a transição imediata do status de monitoramento para o status de investigação, assegurando que nenhum dado volátil seja perdido entre a detecção do alerta e o início da resposta.

3.30.2. No âmbito da Perícia Digital, a plataforma deve ser capaz de gerar automaticamente linhas do tempo granulares, consolidando em um registro único todos os artefatos técnicos coletados pelos diversos sensores, tais como logs de execução de processos, modificações de chaves de registro, conexões de rede suspeitas, hashes de arquivos maliciosos e logs de auditoria de usuários. O sistema deve permitir a coleta e custódia segura desses artefatos, garantindo que as evidências sejam preservadas com integridade absoluta para fins periciais ou judiciais. A interface de investigação deve suportar a colaboração simultânea entre múltiplos analistas, permitindo o compartilhamento de notas, evidências gráficas e pcap (packet capture) de fluxos de rede associados ao incidente, facilitando a correlação manual de dados com a inteligência fornecida pelo motor de análise da plataforma.

3.30.3. A gestão operacional de incidentes deve ser realizada através de um módulo nativo de Gerenciamento de Casos e Tickets, desenhado especificamente para o fluxo de trabalho de um Centro de Operações de Segurança (SOC). Este componente deve permitir a abertura manual ou automatizada de chamados a partir de qualquer alerta gerado pelo sistema, seguindo os padrões internacionais de resposta a incidentes (preparação, identificação, contenção, erradicação, recuperação e lições aprendidas). O módulo deve possibilitar a definição de fluxos de aprovação, atribuição de responsáveis por nível de perícia, controle de SLAs (Service Level Agreements) de atendimento e resolução, além de categorização customizável baseada no impacto e na urgência dos eventos.

3.30.4. Como requisito funcional crítico e mandatório, a plataforma deve possuir capacidade de integração bidirecional plena e automatizada com a ferramenta de Gerenciamento de Serviços de TI (ITSM) utilizada pela organização. Esta interoperabilidade deve ocorrer via API RESTful ou conectores dedicados, garantindo a sincronização em tempo real de todos os dados relevantes entre o painel de segurança e o sistema de ITSM institucional. A bidirecionalidade implica que qualquer alteração de status realizada no sistema de ITSM (como o encerramento de um chamado, alteração de prioridade ou inclusão de comentários técnicos) deve refletir em tempo real (com um atraso máximo aceito de 15 minutos) no ticket correspondente dentro da plataforma de segurança, e vice-versa. Esta característica é essencial para eliminar a redundância de preenchimento manual, garantir a acurácia dos dados em ambas as pontas e permitir que as equipes de infraestrutura e segurança trabalhem em harmonia, utilizando suas ferramentas de preferência sem perda de contexto ou integridade das informações.

3.30.5. Por fim, o módulo de gestão de tickets e DFIR deve alimentar nativamente o motor de relatórios da plataforma, permitindo a extração de métricas de desempenho operacional, como o Tempo Médio de Detecção (MTTD) e o Tempo Médio de Resposta (MTTR). Todos os registros gerados durante o processo de investigação e as interações realizadas via integração ITSM devem ser protegidos pelo mecanismo de imutabilidade e rastreabilidade rastreada com tecnologia de livro-razão distribuído, assegurando que o histórico de resposta a incidentes da contratante seja inalterável e plenamente auditável a qualquer tempo.

4. MODELO DE EXECUÇÃO DO OBJETO

4.1. Requisitos de Negócio:

4.1.1. A presente contratação orienta-se pelos seguintes requisitos de negócio, visando mitigar riscos e garantir a continuidade dos serviços públicos:

4.1.2. Garantir a implementação das medidas técnicas de segurança exigidas pelo Art. 46 da LGPD, protegendo os dados contra acessos não autorizados e ataques cibernéticos.

4.1.3. Prover visibilidade completa e monitoramento em tempo real dos ativos de TIC e suas vulnerabilidades.

4.1.4. Assegurar capacidade de resposta rápida e automatizada a incidentes cibernéticos (Ransomware, Vazamentos, etc.).

4.2. Requisitos de Capacitação

4.2.1. A solução deve incluir programa de treinamento inicial para administradores, usuários finais e para as equipes técnicas da organização, garantindo que elas estejam capacitadas para operar e manter a solução de forma eficaz.

4.2.2. O fornecedor deve oferecer atualizações técnicas e workshops periódicos para garantir que as equipes estejam atualizadas sobre as melhores práticas e novas funcionalidades.

4.2.3. Capacitar a equipe técnica na operação das plataformas de Defesa Ativa (IPS/NAC) e Proteção de Dados (DLP).

4.2.4. Treinar os administradores na criação de Playbooks de automação de resposta a incidentes (SOAR).

4.2.5. Realizar workshops periódicos sobre tendências de ameaças cibernéticas e novas técnicas de invasão.

4.2.6. Fornecer trilhas de conscientização para usuários finais focadas em prevenção a Phishing e Engenharia Social.

4.2.7. Será necessário treinamento à equipe que atuará com a solução. O treinamento deverá abranger a operação das plataformas, gestão de incidentes e governança de privacidade, destinado a administradores, operadores técnicos e usuários finais (conscientização).
4.2.8. O treinamento deverá ser ministrado em idioma português do Brasil, podendo ser na modalidade presencial ou EaD (ao vivo ou gravado), com emissão de certificados.
4.2.9. A solução deve estar alinhada com as diretrizes da Política Nacional de Cibersegurança, que visa promover a segurança cibernética no Brasil. Isso inclui a adoção de medidas para prevenir, detectar, tratar e responder a ameaças cibernéticas.
4.2.10. A solução deve ser implementada sob um modelo de governança que promova a coordenação e a análise conjunta dos desafios cibernéticos, conforme estabelecido pela Estratégia Nacional de Segurança Cibernética.

4.3. Requisitos de Manutenção

4.3.1. Devido às características da solução, há necessidade de prestação de serviços de Suporte Técnico Especializado pela Contratada.
4.3.2. O suporte técnico para incidentes críticos de segurança cibernética deverá estar disponível 24 horas por dia, 7 dias por semana (24x7).
4.3.3. O suporte técnico para ajustes de configuração, parametrização e operação das plataformas deverá estar disponível em horário comercial (08:00h às 18:00h), em dias úteis.
4.3.4. A Contratada deverá realizar manutenções corretivas, evolutivas e atualizações de segurança (patches) na plataforma SaaS, sem custos adicionais, garantindo proteção contra novas ameaças.

4.4. Requisitos Temporais

4.4.1. A solução deverá estar completamente disponibilizada, instalada, configurada e operacional em até 45 (quarenta e cinco) dias corridos, contados a partir da data do recebimento da Ordem de Início dos Serviços, de acordo com a quantidade.
4.4.2. Em caso de necessidade, a Contratada poderá solicitar prorrogação do prazo constante no parágrafo anterior à Contratante.
4.4.3. O suporte em caso de renovação contratual, por meio de termo aditivo, deverá ser prestado de forma automática, ou seja, não deverá sofrer interrupção. Caso ocorra interrupção dos serviços sem justificativa deferida pela fiscalização, o atraso será contado em dias a partir do momento da interrupção.
4.4.4. Não será computado o tempo de atraso quando este estiver sido ocasionado pelo Contratante ou por fatos supervenientes que independam de ações da Contratada, desde que devidamente justificado e aceito pela Contratante.

4.5. Requisitos de Segurança e Privacidade

4.5.1. A solução deve ser capaz de realizar baterias de testes de simulação de ataques baseados em bibliotecas atualizadas de ameaças e exploits, com execução imediata ou agendamentos, abrangendo infiltração de rede e aplicações web, ambos com o fluxo de ator malicioso externo para ativo-alvo interno; e endpoint, com comprometimento e exfiltração em ativo-alvo interno.
4.5.2. A solução de tecnologia deverá contemplar os seguintes aspectos de segurança da informação e privacidade, alinhados com as melhores práticas e normas técnicas:
4.5.2.1. Implementação de controles de segurança baseados nas normas ISO/IEC 27001 e 27002, que abrangem desde a gestão de riscos e políticas de segurança até os controles técnicos e físicos.
4.5.2.2. Apoio na implementação de criptografia de dados em repouso e em trânsito.
4.5.2.3. Apoio na implementação de autenticação multifator (MFA) para acesso aos sistemas, como forma de aumentar a segurança e proteger contra acessos não autorizados.
4.5.2.4. Apoio na implementação de registro e monitoramento de logs de acesso e atividades, permitindo a identificação de possíveis incidentes de segurança e o rastreamento de ações realizadas no sistema.
4.5.2.5. Realização de testes de penetração e análises de vulnerabilidade periódicos.
4.5.2.6. Apoio na implementação de um plano de resposta a incidentes de segurança da informação, que defina os procedimentos a serem seguidos em caso de ocorrência de incidentes.
4.5.2.7. Apoio na implementação de uma política de backup e recuperação de dados, que garanta a disponibilidade das informações em caso de falhas, perdas ou desastres.

4.5.3. Deverá ser disponibilizado documentação e tutoriais passo a passo atualizados para utilização e operação das plataformas, bem como sobre as boas práticas da Segurança de Informação e da LGPD.

4.6. Requisitos Sociais, Ambientais e Culturais

4.6.1. Os sistemas e manuais das soluções ser disponibilizados em idioma português do Brasil, admitindo-se no idioma inglês quando não houver em idioma português do Brasil.

4.6.2. A pretensa contratação deverá seguir, quando aplicável, ao disposto no programa A3P (Agenda Ambiental na Administração Pública) do Ministério do Meio Ambiente, que insere critérios socioambientais nas atividades dos órgãos públicos dos poderes executivo, legislativo e judiciário, das esferas federal, estadual e municipal.

4.6.3. Quanto aos requisitos sociais, os profissionais da Contratada, quando nas dependências do Contratante, deverão apresentar-se vestidos de forma adequada ao ambiente de trabalho.

4.7. Requisitos da Arquitetura Tecnológica

4.7.1. Os serviços deverão ser executados observando-se as diretrizes de arquitetura tecnológica estabelecidas pela área técnica da Contratante.

4.7.2. A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pela Contratante. Caso não seja autorizada, é vedado à Contratada adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pela Contratante.

4.7.3. A solução deverá ser fornecida preferencialmente na modalidade SaaS (Software as a Service), hospedada em nuvem segura com certificações de mercado em Datacenters do Brasil, ou na modalidade On-Premise/Private Cloud quando tecnicamente justificado para proteção de dados sensíveis governamentais.

4.7.4. Para os itens fornecidos como On-Premise serão aceitos também appliances virtuais a serem instalados nas dependências da organização.

4.7.5. A solução deve possuir integração nativa via APIs (REST/SOAP) para interoperabilidade com o ecossistema de TIC do Contratante.

4.8. Requisitos de Projeto e de Implementação

4.8.1. Os serviços deverão observar integralmente os requisitos de projeto descritos a seguir, visando garantir a organização, o controle e o sucesso da entrega:

4.8.1.1. A execução contratual deverá ser gerenciada como um projeto formal, para tanto, a Contratada deverá designar um Gerente de Projetos, que atuará como líder e ponto focal responsável pela gestão das entregas, interlocução com a equipe da Contratante e garantia da qualidade dos resultados.

4.8.1.2. A Contratada deverá apresentar, em reunião de kick-off (início dos trabalhos), um Plano de Implantação e Projeto detalhado (preferencialmente em formato Microsoft Project ou compatível), contendo todas as fases, atividades, cronograma físico-financeiro, matriz de responsabilidades, alocação de recursos humanos e materiais, mapeamento de riscos e interdependências.

4.8.1.3. O Plano de Implantação deverá ser submetido à aprovação da Contratante. A versão final do plano, contendo eventuais ajustes solicitados pela Administração, deverá ser entregue em até 05 (cinco) dias úteis após a reunião inicial.

4.8.1.4. Todas as atividades de projeto correrão por conta e risco da Contratada, sem ônus adicionais de deslocamento ou logística para a Contratante.

4.9. Requisitos de Implantação

4.9.1. Os serviços deverão observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

4.9.1.1. Antes da configuração efetiva, a Contratada deverá realizar um levantamento detalhado (assessment) do ambiente de TIC da Contratante, mapeando a superfície de ataque, inventário preliminar de ativos, volumetria de dados e integrações necessárias (ex: AD/LDAP, sistemas legados).

4.9.1.2. Compreende a ativação das subscrições SaaS, provisionamento dos tenants, instalação de agentes/sensores nos endpoints e servidores, configuração de políticas de segurança (firewall, IPS, DLP), parametrização dos módulos de detecção de ameaças e integração com os serviços de diretório para autenticação de usuários.

4.9.1.3. A implantação só será considerada concluída após a demonstração de funcionalidade completa com dados reais da Contratante, incluindo a realização de testes assistidos de vulnerabilidade.

4.9.1.4. A Contratada deverá apoiar a criação de ambiente de homologação para testes de validação antes da aplicação de políticas críticas em produção.

4.10. Requisitos de Garantia e Manutenção

4.10.1. O prazo de garantia contratual dos serviços e do funcionamento da solução será de 12 (doze) meses, concomitante à vigência do contrato, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto (ou da ativação das subscrições).

4.10.2. A garantia da solução SaaS compreende a manutenção da disponibilidade da plataforma (Uptime mínimo de 99,5% mensal), a correção de falhas de programação (bugs), inconsistências ou erros de processamento, bem como a garantia de integridade e confidencialidade dos dados armazenados.

4.10.3. Para os dispositivos de autenticação (Chaves de Hardware FIDO2) fornecidos, a garantia cobre defeitos de fabricação e falhas de funcionamento, devendo a Contratada realizar a substituição imediata de dispositivos defeituosos, sem ônus para a Contratante, mediante solicitação formal via chamado técnico.

4.10.4. A Contratada deve garantir que a solução receba atualizações periódicas (releases) para incorporação de novas funcionalidades, melhorias de desempenho e, obrigatoriamente, adequações a novas exigências legais ou regulatórias (ex: alterações na LGPD ou normas da ANPD) que surjam durante a vigência contratual.

4.10.5. A Contratada deverá aplicar patches de segurança, correções de vulnerabilidades e atualizações de assinaturas de ameaças na plataforma de forma contínua e transparente, garantindo proteção contra novos vetores de ataque (Zero-Day), preferencialmente em horários que não impactem a operação do órgão.

4.10.6. A garantia inclui o acesso ilimitado ao serviço de suporte técnico (Service Desk) para abertura de chamados, esclarecimento de dúvidas e report de incidentes, devendo a Contratada disponibilizar canais via telefone (0800 ou local), e-mail e portal web.

4.10.7. Durante o período de garantia e vigência, caso a solução apresente reiteradas falhas que comprometam a segurança ou a operação, a Contratante poderá exigir a apresentação de plano de ação corretiva ou, em último caso, a substituição da solução, sem prejuízo das sanções cabíveis.

4.11. Requisitos de Experiência Profissional:

Os serviços técnicos especializados deverão ser prestados por profissionais devidamente qualificados e certificados, garantindo a excelência na execução das atividades de privacidade, segurança ofensiva e gestão de projetos.

4.11.1. **Qualificação da Equipe de Operação e Suporte (SOC):** Para garantir a disponibilidade e a excelência técnica na operação contínua da solução (monitoramento e resposta a incidentes), a Contratada deverá disponibilizar uma equipe de operação (SOC - Security Operations Center) composta por, no mínimo, 02 (dois) profissionais técnicos.

4.11.1.1. A comprovação da capacidade técnica desta equipe se dará mediante a apresentação de certificações válidas. Os profissionais indicados (o conjunto da equipe) deverão deter, no mínimo, 3 (três) certificações distintas dentre as listadas abaixo:

4.11.1.2. CISSP (Certified Information System Security Professional); GSEC (GIAC Security Essentials); CompTIA Security+; Auditor Líder ISO 27001; Auditor Líder ISO 22301; CompTIA CySA+; CISA (Certified Information Systems Auditor).

4.12. Requisitos de Metodologia de Trabalho

4.12.1. A execução dos serviços está condicionada ao recebimento pelo Contratado de Ordem de Serviço (OS) emitida pela Contratante, na qual indicará o serviço, a quantidade e a localidade na qual os deverão ser prestados.

4.12.2. A execução do serviço dever ser acompanhada pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

4.13. Sustentabilidade

4.13.1. A solução deve privilegiar o uso de documentos digitais (paperless) e eficiência energética no processamento de dados. As chaves físicas fornecidas devem atender a normas de restrição de substâncias perigosas (RoHS).

4.14. Garantia da contratação

4.14.1. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, em valor correspondente a 5% (cinco por cento) do valor total do contrato (ou do valor anual, no caso de serviços continuados), com validade durante a execução do contrato e 90 (noventa) dias após o término da vigência contratual.
4.14.2. O prazo para apresentação da garantia será de 10 (dez) dias úteis, contados da data de assinatura do Contrato, prorrogáveis por igual período a critério da Contratante.
4.14.3. A não observância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,2% (dois décimos por cento) do valor da contratação por dia de atraso, até o máximo de 5% (cinco por cento).
4.14.4. O atraso superior a 30 (trinta) dias úteis para apresentação da garantia poderá acarretar a rescisão unilateral da contratação, sem prejuízo das multas previstas.
4.14.5. Caberá à Contratada optar por uma das seguintes modalidades de garantia:
4.14.5.1. Caução em dinheiro ou em títulos da dívida pública:
4.14.5.2. Seguro-Garantia:
4.14.5.3. Fiança Bancária.

5. ESTIMATIVA DE QUANTITATIVOS

Item	Descrição	Unidade	Quantidade Estimada
1	SUBSCRIÇÃO DE PLATAFORMA UNIFICADA DE GESTÃO DE EXPOSIÇÃO, VISIBILIDADE E SEGURANÇA OFENSIVA	Subscrição Anual (Domínios + Endpoints + Containers)	
2	SUBSCRIÇÃO DE PLATAFORMA INTEGRADA DE DEFESA ATIVA	Subscrição Anual (Por IPs)	
3	SUBSCRIÇÃO DE PLATAFORMA INTEGRADA DE PROTEÇÃO DE DADOS E IDENTIDADE	Subscrição Anual (Por Endpoints)	
4	IMPLANTAÇÃO E INTEGRAÇÃO (SETUP) – PLATAFORMA UNIFICADA	Serviço Global	
5	IMPLANTAÇÃO E INTEGRAÇÃO (SETUP) – PLATAFORMA DE DEFESA ATIVA	Serviço Global	
6	IMPLANTAÇÃO E INTEGRAÇÃO (SETUP) – PLATAFORMA DE PROTEÇÃO DE DADOS	Serviço Global	
7	SERVIÇO CONTINUADO DE GESTÃO DE VULNERABILIDADES E OFENSIVA	Mensal	

8	SERVIÇO CONTINUADO DE OPERAÇÃO DE DEFESA ATIVA E RESPOSTA A INCIDENTES (SOC)	Mensal	
9	SERVIÇO TÉCNICO ESPECIALIZADO PARA CUSTOMIZAÇÃO (SOB DEMANDA)	Hora de Serviço Técnico (HST)	

5.1. O custo estimado total da contratação, é de R$ _____ (por extenso), conforme custos unitários apostos.
5.2. A estimativa de custo levou em consideração o risco envolvido na contratação e sua alocação entre Contratante e Contratado, conforme especificado na matriz de risco constante do Contrato.
5.2.1 Serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação.
5.3. As despesas decorrentes da presente contratação correrão à conta de recursos específicos.
5.4. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.
5.5. As 50 (cinquenta) chaves físicas de autenticação FIDO2 constituem fornecimento acessório e indissociável, incluído no preço do Item 1 (subscrição da plataforma unificada), durante toda a vigência contratual, não configurando aquisição autônoma de equipamentos de informática pela Administração.
5.6. Caso a área técnica identifique, ao longo da execução ou por ocasião de eventual prorrogação da Ata de Registro de Preços, a necessidade de recomposição ou renovação dos quantitativos inicialmente estimados, tal possibilidade deverá observar a prévia previsão nos instrumentos de planejamento e convocatórios, com a correspondente adequação da estimativa do valor da contratação, em observância aos princípios da segurança jurídica, da economicidade e da eficiência administrativa.

Cronograma Físico Financeiro

Evento	**Descrição da Etapa / Entrega**	**Prazo Estimado de Execução**	**Parcela de Pagamento (Referência)**
Evento 1	**Fornecimento de Licenças e Hardware** *(Itens 1 a 3 e Chaves Físicas)* - Ativação das subscrições SaaS. - Entrega das Chaves Físicas FIDO2.	01 a 30 dias após a emissão da OS.	100% do valor anual das licenças (conforme item 9.18 deste TR) e 100% do valor das chaves físicas entregues.
Evento 2	**Implantação e Integração (Setup)** *(Itens 4 a 6 do Grupo)*- Levantamento, Instalação, Configuração e Testes.	01 a 45 dias após a emissão da OS.	100% do valor dos itens de Setup (após recebimento definitivo).
Evento 3	**Operação Mensal - SOC e Pentest (Itens 7 e 8)**	Mensal (12 meses).	Pagamento mensal (1/12), condicionado ao IMR/SLA.

Evento 4	**Serviços Sob Demanda** *(Item 9 do Grupo)* - Customizações específicas.	Conforme demanda (durante a vigência).	Pagamento por Hora Técnica (HST) efetivamente executada e homologada.

6. DA VIGÊNCIA DA CONTRATAÇÃO

6.1. O prazo de vigência da contratação é de 12 (doze) meses, contado da data de assinatura do contrato, podendo ser prorrogado por sucessivos períodos, até o limite de 10 (dez) anos (art. 107 da Lei nº 14.133/2021), desde que seja atestada a maior vantagem econômica; haja créditos orçamentários vinculados à contratação e vantagem em sua manutenção; e a Administração entenda que o contrato lhe oferece vantagem.

6.1.1. O serviço é enquadrado como continuado, uma vez que envolve a prestação permanente de serviços essenciais de segurança da informação e cibersegurança para o funcionamento da Administração Pública, sendo a manutenção plurianual, mediante prorrogações, mais vantajosa, considerando a diluição dos custos de implantação (setup) e a curva de aprendizado da solução, conforme justificativa apresentada nos autos.

6.1.2. A extinção por não disposição de créditos orçamentários para sua continuidade ou entendimento de que o contrato não mais lhe oferece vantagem ocorrerá apenas na próxima data de aniversário do contrato e não poderá ocorrer em prazo inferior a 2 (dois) meses, contado da referida data.

6.2. A solução deverá estar completamente disponibilizada, instalada, configurada e operacional em até 45 (quarenta e cinco) dias corridos, contados a partir da data do recebimento da Ordem de Início dos Serviços, de acordo com a quantidade.

6.3. Em caso de necessidade, a Contratada poderá solicitar prorrogação do prazo constante no parágrafo anterior à Contratante.

6.4. O suporte em caso de renovação contratual, por meio de termo aditivo, deverá ser prestado de forma automática, ou seja, não deverá sofrer interrupção. Caso ocorra interrupção dos serviços sem justificativa deferida pela fiscalização, o atraso será contado em dias a partir do momento da interrupção.

7. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

7.1. Do Cenário de Ameaças e Riscos: O atual cenário de segurança cibernética impõe à Administração Pública desafios crescentes. A simples identificação de vulnerabilidades não é mais suficiente; é necessária uma capacidade de **Operação de Segurança (SecOps)** integrada. O Governo Estadual carece de ferramentas que automatizam a resposta a incidentes, visto que a triagem manual de alertas é humanamente inviável diante do volume de ataques automatizados. A ausência de uma plataforma unificada (XDR/SOAR) eleva o **Tempo Médio de Detecção (MTTD)** e o **Tempo Médio de Resposta (MTTR)**, expondo a infraestrutura a riscos de interrupção de serviços essenciais e vazamento de dados sensíveis.

7.2. Da Necessidade de Integração e Eficiência Operacional (Justificativa ITSM): Identificou-se um gargalo operacional crítico: a desconexão entre as ferramentas de segurança e o sistema de gestão de TI (Service Desk/ITSM). Atualmente, a comunicação de incidentes depende de processos manuais, gerando erros, duplicidade e perda de histórico. A contratação de uma solução com **integração bidirecional nativa via API** é imprescindível para garantir que qualquer incidente de segurança gere automaticamente um ticket para a equipe técnica e, crucialmente, que a resolução desse ticket reflita imediatamente no painel de segurança. Isso visa cumprir o princípio da **Eficiência (Art. 37 da CF/88)**, eliminando o retrabalho administrativo.

7.3. Da Necessidade de Validade Jurídica e Forense (Justificativa Blockchain): Considerando a Lei Geral de Proteção de Dados (LGPD) e a responsabilidade civil do Estado, o órgão necessita de garantias robustas sobre a integridade de seus registros. Soluções tradicionais permitem a alteração de logs por administradores, o que pode comprometer investigações internas. A exigência de **imutabilidade de logs e histórico de resposta via Blockchain/Merkle Tree** visa assegurar a cadeia de custódia da prova digital, garantindo que as evidências de conformidade e de resposta a incidentes possuam validade jurídica irrefutável em eventuais auditorias ou litígios.

8. MODELO DE GESTÃO DO CONTRATO

A gestão contratual seguirá o disposto no Decreto nº 11.246/2022 e na Lei nº 14.133/2021, com a seguinte estrutura:

8.1. Instrumentos de Fiscalização:

- **Painel de Monitoramento (Dashboard):** A fiscalização utilizará o próprio painel da solução contratada para verificar a disponibilidade (Uptime) e as métricas de operação (MTTD/MTTR).
- **Relatório Mensal de Execução (RME):** Documento a ser entregue pela CONTRATADA até o 5º dia útil do mês subsequente, contendo:
    - Comprovante de disponibilidade do serviço (SLA).
    - Relatório sintético de vulnerabilidades detectadas e mitigadas.
    - Evidência de integridade dos logs (Hash da última transação no Blockchain).
    - Listagem de chamados de suporte técnico abertos e fechados no período.

8.2. Atores da Fiscalização:

- **Fiscal Técnico:** Servidor da área de TI/Segurança responsável por validar a eficácia técnica da solução, a integração com o ITSM e a qualidade dos relatórios.
- **Fiscal Administrativo:** Responsável pela conferência das notas fiscais, regularidade fiscal da empresa e sanções administrativas.
- **Gestor do Contrato:** Responsável pela coordenação geral e autorização de pagamentos.

8.3. Formas de transferência de conhecimento:

- Ao longo da execução, a Contratada deverá realizar a transferência de conhecimento ("Knowledge Transfer") para a equipe de TIC da Contratante, através de treinamentos on-the-job e documentação técnica atualizada (manuais, topologias, playbooks).
- Ao final do contrato (encerramento ou rescisão), a Contratada obriga-se a realizar a Transição Contratual (Desmobilização) no prazo de até 30 dias, entregando relatório consolidado de postura de segurança cibernética e histórico de incidentes tratados e credenciais de administração exclusivas;
- Após a confirmação do recebimento dos dados pela Contratante, a Contratada deverá excluir de forma segura e irreversível todas as cópias de dados governamentais em sua posse.

8.4. Mecanismos formais de comunicação:

- São definidos como mecanismos formais de comunicação, entre a Contratante e o Contratado, os seguintes:
    - Ordem de Serviço;
    - Ata de Reunião;
    - Ofício;
    - Sistema de abertura de chamados;
    - E-mails e Comunicação via mensageiros como Whatsapp ou Microsoft Teams;

8.5. Manutenção de Sigilo e Normas de Segurança

8.5.1. O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

8.5.2. Todos os profissionais da Contratada deverão assinar Termo de Compromisso e Manutenção de Sigilo antes do início das atividades, e a empresa responderá civil e criminalmente por qualquer vazamento de dados decorrente de sua atuação.

8.6. Subcontratação

8.6.1. É permitida a subcontratação parcial do objeto, até o limite de 30% (trinta por cento) do valor total do contrato, especificamente para as parcelas de serviços técnicos especializados (consultoria, treinamento, operação assistida), vedada a subcontratação do fornecimento principal da plataforma de software e da gestão contratual.

8.6.2. Poderão ser subcontratadas as seguintes parcelas do objeto:

8.6.2.1. Serviços técnicos especializados como:

8.6.2.1.1. Consultoria;

8.6.2.1.2. Treinamento;

8.6.2.1.3. Operação assistida.

8.6.3. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral do Contratado pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades do subcontratado, bem como responder perante o Contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

8.6.4. A subcontratação depende de autorização prévia do Contratante, a quem incumbe avaliar se o subcontratado cumpre os requisitos de qualificação técnica necessários para a execução do objeto.

8.6.5. O Contratado apresentará à Administração documentação que comprove a capacidade técnica do subcontratado, que será avaliada e juntada aos autos do processo correspondente.

8.6.6. É vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na contratação ou atue na fiscalização ou na gestão do contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau.

9. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

9.1. Avaliação da execução do objeto utilizará o Instrumento de Medição de Resultado (IMR), conforme indicadores abaixo, para aferição da qualidade da prestação dos serviços e aplicação de glosas a serem definidas no momento da contratação.

9.2. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que o Contratado não produziu os resultados acordados ou deixou de executar atividades contratadas.

9.3. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços, nem a aplicação de sanções por descumprimento de cláusulas não mensuráveis por indicadores (ex: quebra de sigilo).

Recebimento

9.4. O recebimento do objeto ocorrerá conforme a natureza de cada item do Grupo Único:

9.4.1. Para Licenças de Software e Subscrições (Itens 1, 2 e 3):

9.4.1.1 Recebimento Provisório: Ocorrerá em até 05 (cinco) dias úteis após a entrega das credenciais de acesso, chaves de ativação ou disponibilização do ambiente SaaS, mediante teste de acesso funcional.

9.4.1.2 Recebimento Definitivo: Ocorrerá em até 10 (dez) dias úteis após o provisório, mediante validação de que todas as funcionalidades contratadas estão ativas e operantes conforme especificação técnica.

9.4.2 Para Dispositivos Físicos - Chaves Físicas (Item Hardware):

9.4.2.1 Recebimento Provisório: No ato da entrega física no almoxarifado ou endereço indicado na OS, mediante conferência de volumes e integridade das embalagens.

9.4.2.2 Recebimento Definitivo: Em até 15 (quinze) dias úteis, após conferência unitária, testes por amostragem e ateste de funcionamento.

9.4.3 Para Serviços de Implantação e Configuração (Itens 4, 5 e 6):

9.4.3.1 Serão recebidos definitivamente após a conclusão de cada etapa do cronograma físico-financeiro (ex: "Conclusão do Setup", "Realização do Treinamento"), mediante Relatório Técnico e Lista de Presença aprovados pela Fiscalização.
9.4.4 Para Serviços Continuados Mensais (Itens 7 e 8):
9.4.4.1 Serão recebidos mensalmente, mediante apresentação do Relatório de Serviços Executados e apuração dos indicadores de nível de serviço (IMR/SLA).
Procedimentos de Teste e Inspeção
9.5. Serão adotados os seguintes procedimentos de teste e inspeção para fins de recebimento:
9.5.1 Verificação se todas as funcionalidades descritas no Termo de Referência (ex: varredura de vulnerabilidades, monitoramento de exfiltração de dados via DLP e detecção de ameaças na DarkWeb) estão ativas na plataforma entregue.
9.5.2 Teste de autenticação utilizando as chaves físicas FIDO2 em estações de trabalho aleatórias para confirmar compatibilidade.
9.5.3 Análise dos manuais, topologias e relatórios de setup entregues.
Liquidação
9.6 Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §3º da Instrução Normativa SEGES/ME nº 77/2022.
9.7 O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, nos casos de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.
9.8 Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

I) o prazo de validade;
II) a data da emissão;
III) os dados do contrato e do órgão contratante;
IV) o período respectivo de execução do contrato;
V) o valor a pagar; e
VI) eventual destaque do valor de retenções tributárias cabíveis.

9.9 Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante.
9.10 A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133/2021.
9.11 Prazo de pagamento
9.12 O pagamento será efetuado no prazo máximo de até dez dias úteis, contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.
9.13 No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA-E (ou índice oficial vigente), pro rata die.
Forma de pagamento
9.14 O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.
9.15 Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
9.16 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.
9.16.1 Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

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

Pagamento de Licenças Anuais

9.18 Excepcionalmente, para os itens referentes ao licenciamento de uso de software e subscrições anuais (Itens 1, 2 e 3), admite-se o pagamento integral da anuidade após a entrega e ativação definitiva das licenças, conforme prática usual de mercado para subscrição de software (SaaS) e economia de escala, condicionado às seguintes garantias (Art. 145, § 1º da Lei 14.133/2021):

9.19 O pagamento da anuidade das licenças ocorrerá somente após a emissão do Termo de Recebimento Definitivo da ativação das chaves/acessos, comprovando que a solução está disponível para uso pelo período de 12 meses.

9.20 Garantia de Restituição:

9.20.1 Caso ocorra a rescisão contratual ou descontinuidade da solução por culpa da Contratada antes do término do período de 12 meses já pago, a Contratada obriga-se a restituir o valor proporcional (pro rata) ao período não utilizado, corrigido monetariamente, no prazo de 05 (cinco) dias úteis.

9.21 Para os serviços continuados (ex: suporte, operação de segurança - SOC) e serviços de implantação, NÃO haverá antecipação, devendo o pagamento ocorrer mensalmente ou por etapa executada (postecipado).

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

Garantia da Proposta

10.1 Será exigida a Garantia da Proposta, como requisito de pré-habilitação, correspondente a 1% (um por cento) do valor total estimado da contratação, que deverá ser apresentada anexo da proposta de preços.

10.1.1 A garantia da proposta poderá ser prestada nas mesmas modalidades previstas para a garantia contratual (caução em dinheiro, títulos da dívida pública, seguro-garantia ou fiança bancária).

10.1.2 A garantia deverá ter validade por prazo não inferior a 90 (noventa) dias úteis, contados da data de apresentação da proposta.

10.1.3 A garantia da proposta tem por objetivo assegurar que o licitante vencedor honrará sua oferta e assinará o contrato (ou Ata de Registro de Preços).

10.2 Devolução da Garantia da Proposta:

10.2.1 A garantia da proposta será devolvida aos licitantes não vencedores no prazo de 10 (dez) dias úteis após a homologação do certame.

10.2.2 Ao licitante vencedor, a garantia da proposta será devolvida após a assinatura do contrato e a prestação da garantia contratual, podendo, a critério do interessado, ser utilizada como parte do pagamento desta última.

10.3 Execução da Garantia da Proposta:

10.3.1 A garantia da proposta será executada integralmente se o licitante vencedor se recusar a assinar o contrato (ou a Ata de Registro de Preços) no prazo estabelecido, ou se não apresentar a documentação exigida para a contratação, caracterizando-se a inexecução total da obrigação de contratar.

Do Pregão Eletrônico

10.4 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 (Global do Grupo Único), considerando a obrigatoriedade da adjudicação por grupo conforme justificativa técnica de unicidade e interdependência da solução.

Da Apresentação da Proposta

10.5 Após o encerramento da etapa de lances, o licitante classificado provisoriamente em primeiro lugar deverá encaminhar, no prazo estabelecido no edital (via sistema), a Proposta de Preços Ajustada ao lance vencedor, acompanhada da Proposta Técnica Detalhada e da documentação complementar descrita a seguir.

10.6 A licitante deverá apresentar a Planilha de Quantidades e Preços (Modelo do Edital), contendo:

a) Preços unitários e totais para todos os itens que compõem o Grupo da Solução Integrada, ajustados linearmente ao desconto ofertado no lance global;

b) Indicação da marca/fabricante de cada componente de software e hardware cotado;

c) Assinatura do representante legal da empresa.

10.6.1 O preço cotado deverá incluir todas as despesas com mão-de-obra, encargos sociais, trabalhistas e previdenciários, tributos, taxas, licenças, frete, seguro, deslocamento e quaisquer outros custos diretos e indiretos necessários à perfeita execução do objeto.

10.7 Como condição de aceitabilidade técnica, a licitante vencedora deverá apresentar, juntamente com a proposta comercial ajustada, os seguintes documentos técnicos para análise da equipe de TIC:

10.7.1. Plano de Implantação e Metodologia de Trabalho:

10.7.1.1. Documento descritivo detalhando como a licitante pretende executar o objeto, contendo no mínimo: A descrição das etapas de setup (levantamento, instalação, configuração, testes), ferramentas utilizadas e estratégias para mitigar riscos de interrupção do ambiente. Sugestão de Cronograma de Execução: Cronograma preliminar (gráfico de Gantt ou similar) detalhando os tempos estimados para cada etapa da implantação, considerando o prazo máximo de 45 dias corridos previsto neste TR, contado a partir da emissão da Ordem de Serviço, E a descrição de como será realizada a operação do SOC, o atendimento aos chamados e a atuação da equipe residente.

10.7.2. Documentação Técnica da Solução (Catálogos e Manuais):

10.7.2.1 Apresentação de catálogos técnicos (datasheets), manuais, prospectos ou documentos oficiais do fabricante (em português ou inglês) que comprovem, de forma inequívoca, que a solução de software e os dispositivos de hardware (chaves FIDO2) ofertados atendem a todas as especificações técnicas e requisitos funcionais descritos no Item 3 deste Termo de Referência.

10.8 A não apresentação da Proposta Detalhada, dos Catálogos/Manuais ou a apresentação de solução que não atenda às especificações do TR (conforme análise dos documentos técnicos) ensejará a desclassificação da proposta, sendo convocado o próximo licitante da lista.

Regime de Execução

10.9 O regime de execução do contrato será por Empreitada por Preço Unitário, tendo em vista a natureza da contratação por Sistema de Registro de Preços, onde o pagamento ocorrerá com base nas unidades de serviço ou produtos efetivamente demandados e entregues (Licenças, Horas, Unidades Físicas).

Da exigência Prova de Conceito - PoC

10.10 Havendo o aceite da proposta quanto ao valor, o licitante classificado provisoriamente em primeiro lugar será convocado para realizar uma Prova de Conceito (PoC). A PoC tem como objetivo validar a eficácia da solução de segurança cibernética e adequação à LGPD proposta, demonstrando o atendimento integral aos requisitos técnicos descritos no item 3 e 4 deste Termo de Referência.

10.11 A PoC visa demonstrar, em ambiente controlado, a capacidade da solução em:

10.11.1 Descobrir e mapear ativos de rede (servidores, estações, IoT), detalhando SO, serviços e versões.

10.11.2 Identificar e classificar vulnerabilidades utilizando inteligência artificial para priorização de riscos.

10.11.3 Simular ataques controlados (Pentest e BAS) para validar a eficácia dos controles de segurança.

10.11.4 Detectar vazamentos de credenciais na Dark Web e executar campanhas simuladas de Phishing.

10.11.5 Demonstrar a criação e aplicação de uma regra de bloqueio de exfiltração de dados sensíveis via DLP.

10.11.6 Garantir a autenticidade e integridade dos relatórios gerados, utilizando tecnologias como blockchain para validar a data de registro e o conteúdo (imutabilidade).

Escopo Detalhado da PoC:

A PoC será dividida em etapas funcionais que deverão ser demonstradas sequencialmente:
10.12 Autenticação Segura e Controle de Acesso
10.12.1 Demonstração do login na plataforma utilizando a chave física de segurança (hardware FIDO2) exigida, comprovando que o acesso administrativo é bloqueado sem a presença do dispositivo físico.
10.12.1.1 Verificação da gestão de perfis de acesso e segregação de funções.
10.12.2 **Etapa 2:** Descoberta e Análise de Vulnerabilidades
10.12.2.1 A Contratante informará um website ou IP alvo (ativo de teste).
10.12.2.2 O sistema deverá realizar a coleta de informações (IPs, portas, DNS, subdomínios) e realizar a varredura de vulnerabilidades.
10.12.2.3 A solução deverá detectar falhas (ex: versões desatualizadas, portas indevidas) em uma infraestrutura de teste com vulnerabilidades intencionais disponibilizada ou indicada pela Contratante.
10.12.2.4 Demonstração da priorização automática de riscos com base em IA e contexto da ameaça.
10.12.3 **Etapa 3:** Segurança Ofensiva e Simulações
10.12.3.1 Campanha de Phishing: Criação e disparo de uma campanha simulada para um grupo reduzido de e-mails de teste, demonstrando o painel de monitoramento de cliques e captura de credenciais (simulada).
10.12.3.2 Simulação de DDoS: Demonstração do módulo de simulação de tráfego volumétrico (DDoS) contra um alvo controlado, apresentando métricas de latência e resposta.
10.12.3.3 Pentest Automatizado e BAS: Execução de um teste de intrusão automatizado (Black-box) e uma simulação de brecha (BAS) para validar a resiliência de um endpoint ou aplicação web.
10.12.3.4 Demonstrar mapeamento na matriz MITRE ATT&CK.
10.12.4 **Etapa 4:** Monitoramento de Vazamentos
10.12.4.1 Configuração de um domínio ou termo de busca para monitoramento na Dark Web e demonstração de alertas sobre credenciais ou dados expostos.
10.12.5 **Etapa 5:** Conformidade e Relatórios
10.12.5.1 Geração de Relatórios de Vulnerabilidades.
10.12.5.2 Validação via Blockchain: O licitante deverá gerar os relatórios na plataforma e demonstrar a validação de sua autenticidade e imutabilidade através do registro em blockchain (hash de verificação), comprovando o atendimento ao requisito de validade jurídica.

10.13 Condições de Execução da PoC:

10.13.1 A licitante convocada terá o prazo de até 05 (cinco) dias úteis, contados da data de convocação pelo Agente de Contratação/Pregoeiro, para iniciar a PoC.
10.13.2 A PoC será realizada preferencialmente de forma remota, através de videoconferência (com compartilhamento de tela), ou presencialmente na sede da Contratante, a critério da Administração, em data e horário agendados com antecedência mínima de 05 (cinco) dias úteis.
10.13.3 A sessão da PoC será gravada para fins de registro no processo administrativo.
10.13.4 A Contratante poderá disponibilizar um link para que os demais licitantes interessados acompanhem a demonstração como ouvintes (sem direito a manifestação durante a prova).
10.13.5 O licitante deverá disponibilizar os recursos (licenças de teste, chaves físicas, ambiente de nuvem) necessários para a demonstração, sem ônus para a Contratante.
10.13.6 O tempo máximo para a realização da PoC será de 01 (um) dia, podendo ser prorrogado a critério da equipe técnica da Contratante caso haja necessidade de aprofundamento em algum teste.
10.13.7 O cronograma detalhado (horário de início, sequência dos testes, plataforma de vídeo) deverá ser acordado com a equipe técnica da Contratante antes do início dos testes.

10.14 Critérios de Aceite

10.14.1 A solução será considerada APROVADA se demonstrar o funcionamento de 80% das funcionalidades críticas testadas (itens 10.11.1 a 10.11.5), e integralmente os requisitos denominados obrigatórios, a fim de atender aos mandatórios do apenso de roteiro para sua respectiva realização.
10.14.2 O não atendimento de qualquer requisito obrigatório ou a falha na execução das simulações implicará na REPROVAÇÃO da PoC e consequente desclassificação da proposta, sendo convocado o próximo classificado.

Exigência de Qualificação Técnica

10.15 Declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.
10.15.1 A declaração acima poderá ser substituída por declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação.

Comprovação da Capacidade Técnica Operacional (Operacional)

10.16 Comprovação da aptidão para desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto desta licitação, realizada por meio de atestado(s) ou certidão(ões) fornecido(s) por pessoa jurídica de direito público ou privado, demonstrando que a licitante já executou ou executa serviços com as seguintes características mínimas:

10.16.1 Fornecimento de Solução de Cibersegurança

10.16.1.1. Atestado(s) comprovando que a licitante forneceu, implantou e prestou suporte técnico a solução de segurança cibernética corporativa (SaaS ou On-Premise) contendo funcionalidades de gestão de vulnerabilidades, testes de intrusão automatizados, monitoramento na DarkWeb, e realização de Testes DDoS para um quantitativo de ativos (endpoints/IPs) equivalente ou superior a 30% (trinta por cento) da quantidade estimada para o Item 1 deste Termo de Referência.
10.16.2 Operação de Segurança Cibernética (SOC/MSSP):
10.16.2.1. Atestado(s) comprovando a prestação de serviços continuados de monitoramento, detecção e resposta a incidentes (Centro de Operações de Segurança - SOC), incluindo a triagem de alertas e execução de playbooks de resposta, por um período mínimo de 12 (doze) meses.
10.17 Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.
10.18 O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato ou outro documento comprobatório que deu suporte à contratação, endereço atual do Contratante e local em que foram prestados os serviços, entre outros documentos.
10.19 Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.
10.20 Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras quando acompanhados de tradução para o português, salvo se comprovada a inidoneidade da entidade emissora.
10.21 A apresentação, pelo fornecedor, de certidões ou atestados de desempenho anterior emitido em favor de consórcio do qual tenha feito parte será admitida, desde que atendidos os requisitos do art. 67, §§ 10 e 11, da Lei nº 14.133/2021 e regulamentos sobre o tema.

Comprovação da Capacidade Técnica Profissional

10.22 A licitante deverá comprovar que possui em seu quadro permanente, ou mediante declaração de compromisso de contratação futura, a equipe técnica necessária para a execução dos serviços, conforme perfis definidos neste Termo de Referência. A comprovação dar-se-á mediante a apresentação da relação nominal dos profissionais, acompanhada de currículos, comprovação de vínculo e das seguintes certificações obrigatórias:

10.22.1 Equipe de Operação e Suporte (SOC/NOC):

10.22.1.1. Comprovação de excelência técnica da equipe operacional (mínimo de 02 profissionais) por meio da apresentação de, no mínimo, 3 (três) certificações distintas (no somatório da equipe) dentre as listadas abaixo, válidas:

10.22.1.1.1. CISSP (Certified Information System Security Professional); GSEC (GIAC Security Essentials); CompTIA Security+; Auditor Líder ISO 27001; Auditor Líder ISO 22301; CompTIA CySA+; CISA (Certified Information Systems Auditor); Offensive Security Certified Professional (OSCP).

10.22.2 Especialista em Testes de Intrusão (Pentester):

10.22.2.1. Comprovação de 01 (um) profissional designado para o serviço de Pentest detentor de pelo menos uma das seguintes certificações válidas:

10.22.2.2. EC-Council Certified Ethical Hacker (CEH); OU CompTIA PenTest+; OU Offensive Security Certified Professional (OSCP); OU GIAC Penetration Tester (GPEN).

10.22.3 Analista de Segurança Cibernética (Residente):

10.22.3.1. Comprovação de 01 (um) profissional detentor de certificação técnica em Segurança da Informação (ex: CompTIA Security+, CySA+, ou equivalente baseado na ISO 27001).

10.23 A comprovação de vínculo profissional se fará com a apresentação de cópia da carteira de trabalho (CTPS), contrato social (sócio), contrato de prestação de serviços ou declaração de contratação futura acompanhada de anuência do profissional.

10.24 Em caso de substituição dos responsáveis técnicos durante a execução contratual, a Contratada deverá promover a substituição por profissionais de qualificação equivalente ou superior, sem ônus para a Contratante.

Instalação de escritório

10.25 Nos termos do art. 67, inciso III, da Lei nº 14.133/2021, o licitante deverá apresentar declaração formal de que dispõe ou de que instalará, até a assinatura do contrato ou início da execução, escritório ou base operacional no Estado de Sergipe, preferencialmente no município de Aracaju, bem como de que possui instalações, aparelhamento e equipe técnica adequados à plena execução do objeto, responsabilizando-se pela manutenção da estrutura necessária durante toda a vigência contratual.

10.25.1 A exigência justifica-se pela necessidade de garantir a interlocução imediata e a gestão administrativa presencial da equipe residente (Analista de Privacidade) alocada nas dependências da Contratante, bem como para assegurar o cumprimento dos Acordos de Nível de Serviço (SLA) que demandem presença física para manutenção ou reuniões estratégicas de crise.

10.25.2 A comprovação da instalação do escritório deverá ocorrer no prazo máximo de 60 (sessenta) dias, contados a partir da assinatura do Contrato.

10.25.3 O escritório deverá dispor de infraestrutura mínima de comunicação (telefone, internet) e pessoal administrativo capaz de receber notificações, citações e resolver pendências contratuais in loco.

Carta de Solidariedade do Fabricante

10.26 Caso a licitante não seja a fabricante da solução de software ofertada, deverá apresentar Carta de Solidariedade ou Declaração de Parceria emitida pelo fabricante (ou distribuidor oficial no Brasil), garantindo o fornecimento das licenças, o suporte técnico de terceiro nível e a continuidade do serviço durante toda a vigência contratual.

Consórcio

Fica PERMITIDA a participação de empresas reunidas em consórcio, nos termos do art. 15 da Lei nº 14.133/2021, visando ampliar a competitividade e permitir que empresas de diferentes especialidades (ex: Empresa de Serviços Gerenciados de Segurança - MSSP + Revendedor de Licenças de Software) somem esforços para atender à complexidade do Grupo Único.

10.27 O consórcio deverá obedecer às seguintes regras:

10.27.1 Comprovação de compromisso público ou particular de constituição de consórcio;

10.27.2 Indicação da empresa líder, que será responsável pela representação perante a Administração;

10.27.3 Apresentação dos documentos de habilitação de cada consorciada;

10.27.4 O atestado de capacidade técnica poderá ser apresentado por qualquer das consorciadas, admitindo-se o somatório para atingir os requisitos.
10.27.5 Responsabilidade solidária dos integrantes pelos atos praticados em consórcio

11. SANÇÕES ADMINISTRATIVAS E SLA

PAPÉIS E RESPONSABILIDADES

11.1 São obrigações da CONTRATANTE:

11.1.1 Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução, nos termos da Lei nº 14.133/2021 e IN SGD/ME nº 94/2022.
11.1.2 Encaminhar formalmente a demanda por meio de Ordem de Serviço (OS) ou Ordem de Fornecimento, especificando os quantitativos, locais de entrega (para chaves físicas) e prazos.
11.1.3 Disponibilizar a infraestrutura de hardware e software básico necessária para a implantação dos componentes locais da solução (Appliances Virtuais), incluindo:
a) Ambiente de virtualização compatível (VMware ESXi 6.7+ ou similar);
b) Licenciamento de Sistemas Operacionais (Windows Server 2016+ ou RHEL 8+) e Banco de Dados (se não embutidos no appliance).
c) Conectividade de rede, endereços IP e regras de firewall necessárias para a comunicação dos agentes com a nuvem da solução.
11.1.4 Fornecer as credenciais de acesso (físico e lógico) necessárias para que a equipe da Contratada realize a instalação, configuração e testes no ambiente, observadas as normas de segurança interna.
11.1.5 Analisar e aprovar o Plano de Implantação e os relatórios técnicos apresentados pela Contratada.
11.1.6 Disponibilizar local de trabalho adequado (mesa, cadeira, ponto de rede/energia) para o profissional residente (Analista de Segurança Cibernética), quando nas dependências da Contratante.
11.1.7 Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável.
11.1.8 Efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato, mediante ateste de conformidade dos serviços e produtos entregues.

11.2 São obrigações do CONTRATADO:

11.2.1 Indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato.
11.2.2 Executar os serviços conforme as especificações técnicas, níveis de serviço (SLA) e prazos estabelecidos neste Termo de Referência e na proposta aceita.
11.2.3 Quanto à Implantação e Operação:
a) Realizar o levantamento preliminar do ambiente (assessment) e apresentar o Plano de Projeto em até 05 (cinco) dias úteis após a reunião inicial;
b) Entregar as Licenças de Uso em até 30 (trinta) dias corridos após a reunião inicial.
c) Entregar a solução instalada, configurada e operante em até 45 (quarenta e cinco) dias corridos;
d) Garantir que os componentes de software instalados no ambiente da Contratante sejam entregues livres de vírus, malware ou backdoors.
11.2.4 Quanto aos Dispositivos Físicos (Hardware):
a) Fornecer as chaves de segurança físicas (FIDO2) originais, novas e lacradas, conforme quantitativo da OS;
b) Realizar a substituição imediata, em até 48 (quarenta e oito) horas, de qualquer dispositivo que apresente defeito ou falha de funcionamento.
11.2.5 Quanto à Equipe e Escritório:
a) Manter, durante toda a execução do contrato, equipe técnica compatível com os requisitos de qualificação e certificação exigidos (Perfil Residente e Especialistas Remotos);

b) Substituir, no prazo máximo de 24 (vinte e quatro) horas, qualquer profissional residente que se ausente (por férias, licença ou demissão), garantindo a continuidade do serviço;
c) Comprovar a instalação e funcionamento do escritório de apoio em Aracaju/SE no prazo de até 60 (sessenta) dias da assinatura do contrato.
d) Garantir canais de comunicação diretos e suporte presencial, quando solicitado, para reuniões de gestão de crise ou incidentes críticos que não possam ser resolvidos remotamente
11.2.6 Responder integralmente por eventuais danos causados à Contratante ou a terceiros, decorrentes de imperícia, negligência ou imprudência na execução dos serviços, incluindo incidentes de vazamento de dados causados por falha comprovada da solução ou da equipe contratada.

11.3. O contrato estará sujeito a Acordo de Nível de Serviço (SLA).

- Meta: Disponibilidade da Plataforma ≥ 99,5%.
- Penalidade: Desconto de 2% sobre a fatura mensal para cada 0,1% abaixo da meta.

Na execução dos serviços de suporte, deverão ser observados os seguintes prazos máximos de atendimento (SLA), conforme severidade do incidente:

Severidade	**Prazo máximo de início de atendimento (Resposta)**	**Prazo máximo de solução de problema (Contorno/Resolução)**
Crítica	30 minutos	24 horas
Alta	2 horas	2 dias úteis
Normal	4 horas	4 dias úteis
Baixa	8 horas	6 dias úteis

ANEXO II

ATA DE REGISTRO DE PREÇOS N.º XXX/2026

PROCESSO N.º 174/2026-COMPRAS.GOV-SEPLAN

PREGÃO N.º 377/2026

SECRETARIA ESPECIAL DE GESTÃO DAS CONTRATAÇÕES, LICITAÇÕES E LOGÍSTICA - SECLOG	
Endereço: **Rua Duque de Caxias, n.º 346, Bairro São José**	**Cidade:** **Aracaju UF.:** **Sergipe**
CNPJ/MF Nº 13.128.798/0010-94	
Representante Legal: **XXXXXXXXXXXXX**	**Nome:** **XXXXXXXXXXXXX**

A #orgaonome#, consoante Ato de homologação constante às fls. #numero_folha processo#, do Procedimento Administrativo constante no Processo Virtual.º #num_processo_virtual#, considerando o disposto na Portaria n.º #portaria# SECLOG, levando em consideração o julgamento da licitação na modalidade de Pregão n.º #num_pregao# com Registro de Preços, publicado no Diário Oficial do Estado e no Portal Nacional de Contratações Públicas - PNCP em #data_publicação_do#, com certame aberto em #data-_licitacao#, às #hora_licitacao# horas resolve registrar os preços das empresas, nas quantidades estimadas anuais, de acordo com a classificação por elas alcançadas por lote, atendendo as condições previstas no Instrumento Convocatório e as constantes desta Ata de Registro de Preços. Este procedimento licitatório obedecerá, integralmente, ao Decreto nº 342/2023 e à Lei nº 14.133/2021.

CLÁUSULA PRIMEIRA: OBJETO

A presente Ata tem por objeto o **#objeto#**, visando atender às necessidades dos órgãos e entidades do Estado de Sergipe, o qual deverá observar o disposto nos Anexos que são partes integrantes e complementares do Instrumento Convocatório, de acordo com as especificações do Edital de Pregão n.º **#num_pregao#** e seus anexos, que passam a fazer parte desta Ata, juntamente com a documentação e propostas de preços apresentadas pelas licitantes classificadas em primeiro lugar por lote, conforme consta nos autos do Processo n.º**#número do Processo# - #orgaonome#**.

Parágrafo Único - Este instrumento não obriga a Administração Pública a firmar contratações nas quantidades estimadas, podendo ocorrer licitações específicas para a aquisição do(s) objeto(s), obedecida à legislação pertinente, sendo assegurado ao detentor do registro a preferência de fornecimento, em igualdade de condições.

CLÁUSULA SEGUNDA: DA VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS

A assinatura da Ata de Registro de Preços realizar-se-á através de certificação digital no padrão ICP-Brasil e protocolado virtualmente, no sítio https://www.edocsergipe.se.gov.br/protocolo-externo/.

O prazo de vigência da Ata de Registro de Preços oriunda desta licitação é de 12 (doze) meses, contados da data de publicação do extrato desta Ata no Diário Oficial do Estado, nos termos do art. 193 do Decreto Estadual nº 342/2023, e poderá ser prorrogado, por igual período, desde que comprovado o preço vantajoso.

CLÁUSULA TERCEIRA: DA GERÊNCIA DA PRESENTE ATA DE REGISTRO DE PREÇOS

O gerenciamento deste instrumento caberá à **#orgaonome#**, através da **#setor_responsavel#**, no seu aspecto operacional e legal.

CLÁUSULA QUARTA: DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

Os preços registrados, a especificação do material, os quantitativos, as marcas, as empresas fornecedoras e as representantes legais encontram-se elencados na presente Ata (§ 1.º da Cláusula Primeira), em ordem de classificação das propostas por lote.

CLÁUSULA QUINTA: DO(S) LOCAL(IS) E PRAZOS(S) DE ATENDIMENTO

A prestação de serviços deverá ser iniciada, em conformidade com a solicitação dos órgãos participantes do Estado de Sergipe, no prazo de #qtd_dias_para_entrega#, contados a partir da emissão do empenho.

Parágrafo único – A entrega deverá ocorrer nos ambiente de produção do órgão beneficiado dos órgãos solicitantes, da grande Aracaju/SE.

CLÁUSULA SEXTA: DAS CONDIÇÕES DE FORNECIMENTO

As empresas detentoras do preço registrado poderão ser convidadas a firmar contratações de fornecimento, observadas as condições fixadas nesta Ata e seus Anexos e na legislação pertinente.

Parágrafo Primeiro - As contratações dos serviços registrados neste instrumento serão efetuadas através de Contrato de Prestação de Serviços, emitidas pelo órgão participante, contendo: n.º da ata, nome da empresa, objeto, especificação, obrigações da Contratada, endereço e data da entrega

Parágrafo Segundo – O Contrato de Prestação de Serviços será encaminhado ao fornecedor, que deverá assiná-la e devolvê-la ao órgão solicitante no prazo de 3 (três) dias consecutivos, a contar da data do seu recebimento;

Parágrafo Terceiro - Se o fornecedor com preço registrado em primeiro lugar recusar-se a assinar o Contrato de Prestação de Serviços poderão ser convocados os demais fornecedores classificados na licitação.

CLÁUSULA SÉTIMA: DAS OBRIGAÇÕES DO FORNECEDOR:

São obrigações do detentor do preço registrado, além das demais prevista nesta Ata e nos Anexos que integram e complementam o Edital relativo ao Pregão Eletrônico n.º **#num_pregao#:**

I – Executar o fornecimento dos produtos nos padrões estabelecidos pela **#orgaonome#**, desde que formalizada a contratação, de acordo com o especificado nesta Ata e no Anexo I do Edital, que fazem parte deste instrumento, responsabilizando-se por eventuais prejuízos decorrentes do descumprimento de qualquer cláusula ou condição aqui estabelecida;

II – Após a contratação, comunicar antecipadamente a data e horário da entrega, não sendo aceito o produto que estiver em desacordo com as especificações constantes deste instrumento nem quaisquer pleitos de faturamento extraordinários sob o pretexto de perfeito funcionamento e conclusão do objeto contratado;

III - Prestar os esclarecimentos que forem solicitados pela Administração, cujas reclamações se obriga a atender prontamente, bem como dar ciência à **#orgaonome#**, imediatamente e por escrito, de qualquer anormalidade que verificar quando da execução da Ata de Registro de Preços;

IV - Dispor-se a toda e qualquer fiscalização da #orgaonome#, no tocante à prestação dos serviços, conforme contrato de fornecimento, assim como ao cumprimento das obrigações previstas nesta Ata;

V - Prover todos os meios necessários à garantia da plena prestação dos serviços, inclusive considerados os casos de greve ou paralisação de qualquer natureza, observado o contrato de fornecimento;

VI – A descontinuidade dos serviços cujo fornecimento incumbe ao detentor do preço registrado não poderá ser alegado como motivo de força maior para o atraso, má execução ou inexecução do contrato de fornecimento e não a eximirá das penalidades a que está sujeita pelo não cumprimento dos prazos e demais condições estabelecidas;

VII – Possibilitar à **#orgaonome#** efetuar vistoria nas instalações do fornecedor, a fim de verificar as condições para o atendimento do objeto registrado;

VIII – Comunicar imediatamente à **#orgaonome#** qualquer alteração ocorrida no endereço, conta bancária e outros julgados necessários para o recebimento de correspondência.

IX– Respeitar e fazer cumprir a legislação de segurança e saúde no trabalho, previstas nas normas reguladoras e pertinentes;

X– Fiscalizar o perfeito cumprimento do fornecimento a que se obrigou, cabendo-lhe, integralmente, os ônus decorrentes. Tal fiscalização dar-se-á independente da que será exercida pela **#orgaonome#**;

XI – Indenizar terceiros e/ou a **#orgaonome#** mesmo em caso de ausência ou omissão de fiscalização de sua parte, por quaisquer danos ou prejuízos causados, devendo o fornecedor adotar todas as medidas preventivas, com fiel observância às exigências das autoridades competentes e às disposições legais vigentes;

XII – Substituir e/ou sanar as falhas dos serviços, num prazo máximo de até 15 (quinze) dias consecutivos, sujeitando-se às penalidades cabíveis, observado o contrato de fornecimento;

XIII – Manter seus empregados, quando nas dependências dos órgãos participantes, devidamente identificado com crachá subscrito pela detentora do preço registrado contratada, no qual constará, no mínimo, sua razão social e o nome completo do empregado;

XIV – Arcar com as despesas para a entrega do objeto no local indicado, após a contratação;

XV – Informar nas documentação técnica dos serviços prestados, mediante etiqueta ou gravação na própria embalagem, em letras de tamanho compatível, os seguintes dados: N.º e data do Contrato de Prestação de Serviços e o nome da fornecedora ou fabricante;

XVI – Após contratação, aceitar nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, de até 25% (vinte e cinco por cento) do valor inicialmente contratado, servindo como base de cálculo para as alterações os preços unitários constantes na proposta vencedora;

XVII – Manter, durante toda vigência da Ata, todas as condições de habilitação e qualificação exigidas no Edital relativo à licitação da qual decorreu o presente ajuste, nos termos do Art. 113, VI, do Decreto Estadual nº 342/2023, que será observado, quando dos pagamentos à detentora do preço registrado;

XVIII– Solicitar à **#orgaonome#**, em tempo hábil, quaisquer informações ou esclarecimentos que julgar necessário, que possam vir a comprometer a execução do objeto contratual;

XIX – É vedada a cessão ou transferência no todo ou em parte do objeto contido na Ata ou no contrato de prestação de serviços, bem como a subcontratação, salvo autorização prévia e por escrito da #orgaonome#.

CLÁUSULA OITAVA: DAS RESPONSABILIDADES DO FORNECEDOR

São responsabilidades do Fornecedor Detentor do Preço Registrado:

I - todo e qualquer dano que causar à **#orgaonome#** ou a terceiros, ainda que culposo, praticado por seus prepostos, empregados ou mandatário, não excluindo ou reduzindo essa responsabilidade à fiscalização ou acompanhamento da **#orgaonome#**;

II- qualquer tipo de autuação ou ação que venha a sofrer em decorrência do fornecimento em questão, bem como pelos contratos de trabalho de seus empregados, mesmos nos casos que envolvam eventuais decisões judiciais, eximindo a **#orgaonome#** de qualquer solidariedade ou responsabilidade;

III - por quaisquer multas, indenizações ou despesas impostas à Contratada pela autoridade competente, em decorrência do descumprimento de lei ou de regulamento a ser observado na execução do contrato, desde que devidas e pagas, as quais serão reembolsadas à **#orgaonome#**, que ficará, de pleno direito, autorizada a descontar, de qualquer pagamento devido à detentora do preço registrado, o valor correspondente;

IV - em caso de consórcio, responsabilizar-se, solidariamente, entre as empresas consorciadas, conforme determina o art. 97 do Decreto Estadual nº 342/2023 e art. 15 da Lei nº 14.133/2021

Parágrafo Primeiro – A DETENTORA DO PREÇO REGISTRADO autoriza a **#orgaonome#** a descontar o valor correspondente aos referidos danos ou prejuízos diretamente das faturas pertinentes aos pagamentos que lhe forem devidos, ou da garantia contratual, independentemente de qualquer procedimento judicial, assegurada a prévia defesa;

Parágrafo Segundo – A ausência ou omissão da fiscalização da **#orgaonome#** não eximirá a DETENTORA DO PREÇO REGISTRADO das responsabilidades previstas nesta Ata.

CLÁUSULA NONA: OBRIGAÇÕES DA #orgaonome#

A **#orgaonome#** ou órgãos participantes obriga-se a:

I - indicar os locais e horários em que deverão ser entregues o objeto;

II - permitir ao pessoal da CONTRATADA acesso ao local da entrega desde que observadas as normas de segurança;

III- efetuar os pagamentos devidos nas condições estabelecidas nesta Ata e no Edital;

IV – notificar a Contratada de qualquer irregularidade encontrada no fornecimento do objeto.

CLÁUSULA DÉCIMA: DO PAGAMENTO

A #orgaonome# ou órgãos participantes efetuarão o pagamento à Contratada, através de crédito em conta corrente mantida pela Contratada, no prazo máximo de 30 (dias) dias depois da prestação dos serviços que forem solicitados, contados a partir da data da apresentação da nota fiscal/fatura discriminativa, acompanhada do correspondente Contrato de Prestação de Serviços, com o respectivo ateste da unidade responsável pelo recebimento, de que o fornecimento foi realizado a contento.

Parágrafo Primeiro – Caso seja constatada alguma irregularidade nas notas fiscais/fatura, estas serão devolvidas ao fornecedor, para as necessárias correções, com as informações que motivaram sua rejeição, contando-se o prazo para o pagamento da data da sua reapresentação;

Parágrafo Segundo - Para fazer jus ao pagamento, a empresa deverá apresentar, juntamente com o documento de cobrança, prova de regularidade perante o FGTS – CRF, Certidões Negativas de Débitos junto às Fazendas Federal (abrangendo os débitos relativos a tributos federais, à dívida ativa da União, e as contribuições previdenciárias e de terceiros), e do Imposto sobre Operações relativas à Circulação de Mercadorias e Prestação de Serviços de Transporte Interestadual e Intermunicipal e de Comunicação (ICMS) da sede da Contratada;

Parágrafo Terceiro - Nenhum pagamento será efetuado à Contratada enquanto houver pendência de liquidação de obrigação financeira, em virtude de penalidade ou inadimplência contratual;

Parágrafo Quarto - Não haverá, sob hipótese alguma, pagamento antecipado.

Parágrafo Quinto - Os preços registrados poderão ser atualizados periodicamente, na forma do art. 199 do Decreto Estadual nº 342/2023, observadas as condições e os procedimentos previstos na legislação aplicável.

Parágrafo Sexto - Os preços registrados poderão ser objeto de revisão extraordinária, nas hipóteses e condições previstas nos arts. 196 a 198 do Decreto Estadual nº 342/2023, quando comprovada a

ocorrência dos pressupostos legais para a recomposição do equilíbrio econômico-financeiro.

Parágrafo Sétimo - Os preços dos contratos decorrentes desta Ata de Registro de Preços poderão ser reajustados após o interregno mínimo de 12 (doze) meses, contado da data-base da proposta vencedora, mediante aplicação do Índice Nacional de Preços ao Consumidor Amplo – IPCA, ou de outro índice que venha a substituí-lo, observado o disposto no instrumento contratual.

Parágrafo Oitavo - No caso de atraso de pagamento, será utilizado, para atualização do valor mencionado no "caput" desta Cláusula, o IPCA, do período compreendido entre a data final do adimplemento e a do efetivo pagamento;

Parágrafo Nono – Nenhum pagamento isentará a Contratada das suas responsabilidades e obrigações, nem implicará aceitação definitiva do fornecimento.

CLÁUSULA DÉCIMA PRIMEIRA: DA REVISÃO DOS PREÇOS REGISTRADOS E DO REAJUSTE DOS CONTRATOS DECORRENTES DA ATA

Os preços registrados manter-se-ão inalterados pelo período de vigência da presente Ata, admitida a revisão no caso de desequilíbrio da equação econômico-financeira inicial deste Instrumento e a atualização periódica nos termos do art. 199 do Decreto Estadual nº 342/2023.

Parágrafo Primeiro – Caso o preço registrado torne-se superior à média dos preços de mercado, a **#orgaonome#** solicitará, ao fornecedor, redução do preço registrado, de forma a adequá-lo ao preço de mercado.

Parágrafo Segundo - Os fornecedores que não aceitarem reduzir seus preços aos valores praticados pelo mercado serão liberados do compromisso assumido, sem aplicação de penalidade.

Parágrafo Terceiro – Fracassada a negociação com o primeiro colocado, a **#orgaonome#** convocará as demais empresas com preços registrados para o lote, se for o caso, ou ainda os fornecedores classificados, respeitadas as condições de fornecimento, os preços e os prazos do primeiro classificado, para a redução do preço, hipótese em que poderão ocorrer as alterações na ordem de classificação das empresas com preço registrado;

Parágrafo Quarto - Quando o preço de mercado tornar-se superior aos preços registrados, a **#orgaosigla#** poderá liberar o fornecedor do compromisso assumido, sem aplicação da penalidade, caso o fornecedor comunique formalmente a impossibilidade de manutenção do preço antes do pedido de fornecimento, e se confirmada a veracidade dos motivos e comprovantes apresentados, e convocar os demais fornecedores para assegurar igual oportunidade de negociação.

Parágrafo Quinto - Os contratos decorrentes desta Ata de Registro de Preços terão seus preços reajustados após o interregno mínimo de 12 (doze) meses, contado da data-base da proposta vencedora, mediante aplicação do Índice Nacional de Preços ao Consumidor Amplo – IPCA, ou de outro índice que venha a substituí-lo, observado o disposto no respectivo instrumento contratual e na legislação aplicável.

CLÁUSULA DÉCIMA SEGUNDA: DO CANCELAMENTO DO PREÇO REGISTRADO NA ATA DE REGISTRO DE PREÇOS

A presente Ata de Registro de Preços poderá ser cancelada de pleno direito, nas seguintes situações:

I - Quando o fornecedor não cumprir as obrigações constantes desta Ata de Registro de Preços;

II - Quando o fornecedor não assinar o Contrato de Prestação de Serviços no prazo estabelecido;

III - Quando o fornecedor der causa à rescisão administrativa do Contrato de Prestação de Serviços decorrente deste Registro de Preços, nas hipóteses previstas na Lei nº 14.133/2021;

IV - Em qualquer hipótese de inexecução total ou parcial do Contrato de Prestação de Serviços decorrente deste Registro;

V- Os preços registrados se apresentarem superiores aos praticados no mercado e restarem infrutíferas as providências adotadas nos termos da cláusula anterior;

VI- Por razão de interesse público devidamente demonstrado e justificado pela **#orgaonome#.**

Parágrafo Primeiro – Ocorrendo cancelamento do preço registrado, o fornecedor será formalmente comunicado

Parágrafo Segundo – A solicitação do fornecedor para cancelamento dos preços registrados poderá não ser aceita pela **#orgaonome#**, facultando-se a este, nesse caso, a aplicação das penalidades previstas na Ata;

Parágrafo Terceiro – Caso a **#orgaonome#** não se utilize da prerrogativa de cancelar esta Ata, a seu exclusivo critério, poderá suspender a sua execução e/ou sustar o pagamento das faturas até que o fornecedor cumpra integralmente a condição contratual exigida.

CLÁUSULA DÉCIMA TERCEIRA: DAS INCIDÊNCIAS FISCAIS

São obrigações do Contratado:

I– Os tributos, emolumentos, contribuições fiscais e parafiscais, custos e despesas que sejam devidos em decorrência direta ou indireta do presente contrato serão de responsabilidade do CONTRATADO;

II – O CONTRATADO declara haver levado em conta, na apresentação de sua proposta, os tributos, emolumentos, contribuições fiscais e parafiscais, encargos trabalhistas e todas as despesas incidentes sobre a compra do material, não cabendo quaisquer reivindicações devidas a erros nessa avaliação, para efeito de solicitar revisão de preço por recolhimento determinados pela autoridade competente.

CLÁUSULA DÉCIMA QUARTA: DAS SANÇÕES ADMINISTRATIVAS

Pelo atraso injustificado, pela inexecução total ou parcial do objeto pactuado, conforme o caso, a Contratante poderá aplicar ao FORNECEDOR as seguintes sanções, garantida a prévia defesa:

I – Advertência;

II – Multa, observados os seguintes limites máximos:

a) 0,3 % (três décimos por cento) por dia, até o trigésimo dia de atraso, sobre o valor do fornecimento ou serviço não realizado, ou sobre a etapa do cronograma físico de obras não cumprido;

b) 10 % (dez por cento) sobre o valor total ou parcial da obrigação não cumprida, com o consequente cancelamento da nota de empenho ou documento equivalente;

III- impedimento de licitar e de contratar com o Estado de Sergipe pelo prazo de até 3 (três) anos;

IV - Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação.

Parágrafo Primeiro - O valor da multa aplicada será descontado do valor da garantia prestada, retido dos pagamentos devidos pela Administração ou cobrado judicialmente, sendo corrigida monetariamente, de conformidade com a variação do IPCA, a partir do termo inicial, até a data do efetivo recolhimento.

Parágrafo Segundo - A contagem do período de atraso na execução dos ajustes será realizada a partir do primeiro dia útil subsequente ao do encerramento do prazo estabelecido para o cumprimento da obrigação.

Parágrafo Terceiro - Quando a Contratada motivar rescisão contratual, será responsável pelas perdas e danos decorrentes para a **#orgaonome#;**

Parágrafo Quarto - Se a licitante vencedora deixar de assinar o contrato dentro de 5 (cinco) dias corridos, contados da data da notificação escrita, sem justificativa por escrito aceita por esta Secretaria, decairá do direito de vencedora, sujeitando-se, ainda, à imposição das sanções elencadas nos incisos I a IV desta cláusula.

Parágrafo Quinto - A inexecução total ou parcial dos serviços objeto desta licitação poderá ensejar sua rescisão, nos termos dos artigos 137 a 139, da Lei nº 14.133/2021.

CLÁUSULA DÉCIMA QUINTA: DOS RECURSOS ORÇAMENTÁRIOS

As despesas decorrentes desta contratação correrão à conta dos recursos consignados no orçamento do Estado de Sergipe para os exercícios alcançados pelo prazo de validade da Ata de Registro de Preços, a cargo do órgão contratante, cujos programas de trabalho e elementos de despesas específicos constarão na respectiva Nota de Empenho.

CLÁUSULA DÉCIMA SEXTA: DAS DISPOSIÇÕES FINAIS

As partes ficam, ainda, adstritas às seguintes disposições:

I - Todas as alterações que se fizerem necessárias serão registradas por intermédio de lavratura de termo aditivo à presente Ata de Registro de Preços;

II - Integram esta Ata o Edital de Pregão nº **#num_pregao#:** e seus anexos e as propostas das empresas classificadas para cada grupo, por lote;

III - É vedado caucionar ou utilizar o presente contrato para qualquer operação financeira, sem prévia e expressa autorização da **#orgaonome#;**

CLÁUSULA DÉCIMA SÉTIMA: DO FORO

O foro designado para julgamento de quaisquer questões judiciais resultantes deste edital será o da Comarca de Aracaju/SE.
E, por estarem assim, justas e contratadas, as partes assinam este instrumento, a fim de que produza seus efeitos legais.

Aracaju (SE), xxx de xxxx de 202x.

WALTER PEREIRA LIMA
SECRETÁRIO ESPECIAL DE GESTÃO DAS CONTRATAÇÕES, LICITAÇÕES E LOGÍSTICA

ANEXO DA ATA DE REGISTRO DE PREÇOS

(Tabela de itens)

ATA DE REGISTRO DE PREÇOS Nº XXXXX/2026

(EXTRATO DO PExxx/2026 PUBLICADO EM xx/xx/2026 – DIÁRIO OFICIAL/SE)

Este documento é parte integrante da Ata de Registro de Preços nº 00X/200X, celebrada entre a Secretaria Especial das Contratações, Licitações e Logística e as empresas cujos preços estão a seguir registrados por item, em face da realização do Pregão Eletrônico nº 0X/2026.

EMPRESA (razão social): XXXXXXXXXXX

CNPJ: xxxxxxx Inscrição Estadual – XXXXXXXXXXXXXXX

ENDEREÇO: XXXXXXXXXX. CEP XXXXXXXXX.

TEL/FAX (79) xxxxxxxxx,

E-MAIL: xxxxxxxxxx

Item	Especificação	Quantidade Total	Preço unitário	Marca/modelo

_____

NOME DA EMPRESA

REPRESENTANTE: xxxxxx
RG: xxxxx CPF: xxxxxxx

ANEXO III - MINUTA DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS DE TIC

PREGÃO ELETRÔNICO Nº 377/2026

QUALIFICAÇÃO DA CONTRATANTE

ESTADO DE SERGIPE, ATRAVÉS DA SECRETARIA ESPECIAL DE GESTÃO DAS CONTRATAÇÕES, LICITAÇÕES E LOGÍSTICA, ÓRGÃO INTEGRANTE DA ADMINISTRAÇÃO DIRETA DO ESTADO DE SERGIPE.	
ENDEREÇO: XXXXXXXXXXXX	CIDADE: ARACAJU UF.: SERGIPE
CNPJ Nº XXXXXXXXXXXX	
REPRESENTANTE LEGAL: XXXXXXXXXXXX	NOME: XXXXXXXXXXXX
ESTADO CIVIL: XXXXXX	PROFISSÃO: XXXXXXX
CPF N.º XXXXXXX	RG N.º XXXXXXX

QUALIFICAÇÃO DA CONTRATADA

RAZÃO SOCIAL:	
ENDEREÇO:	
TELEFONE:	
Nº DO CNPJ:	
Nº DA INS. ESTADUAL:	
REPRESENTANTE LEGAL:	
Nº DO CPF:	
Nº DA CART. IDENTIDADE:	

O presente contrato está de acordo com a Lei nº 14.133/2021 e sua legislação suplementar, regendo-se pelas cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA - DO OBJETO

O presente Contrato tem por objeto a Contratação de solução de software do tipo Plataforma Unificada de Operações de Cibersegurança operando em arquitetura centralizada, capaz de consolidar em um único console as funções de: Detecção e Resposta a Ameaças (XDR), Gestão de Vulnerabilidades, Inteligência de Ameaças, Simulação de Ataques (Segurança Ofensiva), Automação de Resposta a Incidentes (SOAR) e Governança, Risco e Conformidade (GRC), incluindo mecanismos de integridade de dados via Blockchain, na modalidade Software as a Service (SaaS), visando atender às necessidades dos órgãos e entidades do Estado de Sergipe, conforme especificações detalhadas constantes nos Anexos I (Termo de Referência) do Edital referentes ao Pregão nº 377/2026, os integrantes a este independente de transcrição.

Complementarmente, vinculam esta contratação, independentemente de transcrição:

a)) o Termo de Referência;

b)) o Edital da Licitação;

c)) a proposta da CONTRATADA;

d)) eventuais anexos dos documentos supracitados.

CLÁUSULA SEGUNDA - DA FORMA DE EXECUÇÃO DO OBJETO CONTRATUAL

O objeto deste contrato será executado conforme descrição prevista no termo de referência e o disposto no Edital, no Termo de Referência e neste instrumento.

§ 1º - O seu recebimento dar-se-á de acordo com o artigo 138, do Decreto Estadual nº 342/2023 e art. 140 da Lei nº 14.133/2021.

§2º - Poderá ser designada comissão para recebimento dos bens ou serviços, nos termos do art. 138, II do Decreto Estadual nº 342/2023 e art. 140 da Lei nº 14.133/2021.

§ 3º - O recebimento provisório ou definitivo do objeto do contrato não exclui a responsabilidade civil a ele relativa, nem a ético-profissional, pela perfeita execução do contrato.

§ 4º - 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, complementarmente, no Termo de Referência, anexo a este Contrato.

CLÁUSULA TERCEIRA - DO PREÇO, DAS CONDIÇÕES DE PAGAMENTO

O valor total do contrato é de R$ XXXXXXXXXX (XXXXXXXXXXXXXXXX). A contratante somente pagará à contratada pela efetiva execução dos serviços, após liquidação da obrigação.

§ 1° - 1º O pagamento será realizado conforme os eventos de execução e os critérios de medição e recebimento estabelecidos no Termo de Referência.

§2º Para as licenças e subscrições anuais, o pagamento poderá ser realizado integralmente após a ativação definitiva e o respectivo recebimento definitivo, observadas as condições estabelecidas no Termo de Referência.

§3º Os serviços de implantação e integração serão pagos após a conclusão e o recebimento definitivo da respectiva etapa.

§4º Os serviços continuados de operação do SOC e Pentest serão pagos mensalmente, mediante medição e ateste da execução, observados os níveis de serviço e os critérios de medição estabelecidos no Termo de Referência.

§5º Os serviços sob demanda serão pagos de acordo com as horas técnicas efetivamente executadas e homologadas, observadas as condições estabelecidas no Termo de Referência.

§6º O prazo para pagamento será de até 10 (dez) dias úteis, contado da finalização da liquidação da despesa, observadas as disposições do Termo de Referência e da legislação aplicável.

§ 7° - A contratante reterá percentual, conforme código da Receita Federal, sobre o valor bruto da nota fiscal, do recibo ou da fatura, a título de retenção do Imposto de Renda incidente na fonte de que trata o art. 157, inciso I, da Constituição Federal, consoante o que dispõem as Instruções Normativas RFB n.ºs 1234/2012 e 2145/2023 e o Decreto Estadual n.º 331, de 27 de junho de 2023.

§8º - Para fazer jus ao pagamento, a empresa deverá apresentar, juntamente com o documento de cobrança, prova de regularidade perante o FGTS – CRF, Certidões Negativas de Débitos junto às Fazendas Federal (abrangendo os débitos relativos a tributos federais, à dívida ativa da União, e as contribuições previdenciárias e de terceiros), Estadual e Municipal do domicílio do contratado.

§9º - Nenhum pagamento será efetuado à empresa, enquanto houver pendência de liquidação de obrigação financeira, em virtude de penalidade ou inadimplência contratual.

§10º - Caso se faça necessária a reapresentação de qualquer Nota Fiscal/Fatura por culpa do contratado, o prazo previsto no §1º reiniciar-se-á a contar da data da respectiva reapresentação.

§11º - Não haverá, sob hipótese alguma, pagamento antecipado.

§12º - No caso de atraso de pagamento, será utilizado, para atualização do valor, o Índice Nacional de Preços ao Consumidor Amplo - IPCA/IBGE.

§13º - Garante-se ao Contratado o direito de manutenção do equilíbrio econômico-financeiro do contrato, nos termos do art. 127 e seguintes do Decreto Estadual nº 342/2023 e dispositivos da Lei nº 14.133/2021, a ser efetivado por meio de Termo Aditivo.

§14º - Em caso de consórcio, as regras de faturamento devem obedecer ao disposto no art. 98 do Decreto Estadual

nº 342/2023 e art. 15 da Lei nº 14.133/2021.

§15 - Quando houver controvérsia sobre a execução do objeto quanto à dimensão, qualidade ou quantidade, a CONTRATANTE comunicará a CONTRATADA para emissão de Nota Fiscal relativa à parcela incontroversa, para efeito de liquidação e pagamento, conforme o art. 143 da Lei nº 14.133/2021.

§16 - A CONTRATANTE responderá aos pedidos de reestabelecimento do equilíbrio econômico-financeiro no prazo máximo de 30 (trinta) dias, contado do protocolo do requerimento devidamente instruído, admitida prorrogação motivada por igual período.

§17 – DO REAJUSTE - Os preços contratados poderão ser reajustados após o interregno mínimo de 12 (doze) meses, contado da data-base estabelecida no instrumento convocatório, mediante aplicação do Índice Nacional de Preços ao Consumidor Amplo – IPCA/IBGE, ou outro índice que venha a substituí-lo, observada a legislação aplicável.

§18º O reajuste será formalizado por apostilamento, quando cabível, observadas as disposições da Lei nº 14.133/2021 e do Decreto Estadual nº 342/2023.

§19º O restabelecimento do equilíbrio econômico-financeiro do contrato, quando cabível, observará as hipóteses e procedimentos previstos na legislação aplicável, no Edital e no Termo de Referência.

§20º O pagamento dos serviços sujeitos a Acordo de Nível de Serviço – SLA observará os critérios de medição, níveis de desempenho, indicadores, metas, descontos e demais condições estabelecidos no Termo de Referência, inclusive quanto à aplicação das glosas decorrentes do não atingimento dos níveis de serviço.

CLÁUSULA QUARTA - DA VIGÊNCIA

O presente Contrato terá vigência de 12 (doze) meses, contados a partir da data de sua assinatura e poderá ser prorrogado com vistas à obtenção de preços e condições mais vantajosas para a Administração, na forma dos arts. 120 a 122, do Decreto Estadual nº 342/2023 e art. 107 e seguintes da Lei nº 14.133/2021.

Parágrafo único - A prorrogação de que trata esta cláusula é condicionada à avaliação, pelo Gestor do Contrato, da vantajosidade da medida, a qual deverá ser realizada motivadamente, com base no Histórico de Gestão do Contrato e nos princípios da manutenção da necessidade, economicidade e oportunidade da contratação.

CLÁUSULA QUINTA - DOTAÇÃO ORÇAMENTÁRIA.

As despesas com o pagamento do referido objeto correrão por conta das seguintes dotações orçamentárias:

UNIDADE ORÇAMENTÁRIA	CLASSIFICAÇÃO FUNCIONAL PROGRAMÁTICA	PROJETO/ ATIVIDADE	ELEMENTO DE DESPESA	FONTE DE RECURSO	ESTIMATIVA ANUAL

CLÁUSULA SEXTA - DO DIREITO E RESPONSABILIDADE DAS PARTES

I - A CONTRATADA, durante a vigência deste Contrato, compromete-se a:

a) Executar o serviço em estrita observância às disposições do Edital e da proposta e ainda conforme as responsabilidades dispostas a seguir.

b) Manter durante a execução do Contrato, todas as condições de habilitação e qualificação exigidas na licitação;

c) Prestar garantia contratual, no valor correspondente a 5% (cinco por cento) do valor do contrato, podendo optar por fiança-bancária, seguro-garantia ou caução em dinheiro ou em títulos da dívida pública, conforme art. 96 e seguintes da Lei 14.133/2021;

d) Responsabilizar-se pelos danos causados diretamente à Contratante ou a terceiros decorrentes de sua culpa ou dolo na execução do Contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pela Contratante;

e) Não transferir a outrem, no todo ou em parte, o Contrato firmado com a Contratante, sem prévia e expressa anuência desta;

f) Não realizar associação com outrem, cessão ou transferência total ou parcial, bem como a fusão, cisão ou incorporação, sem prévia e expressa anuência do Contratante;

g) Designar preposto para atender aos chamados e exigências da Contratante;

h) Em caso de consórcio, responsabilizar-se solidariamente entre as empresas consorciadas, conforme determina o art. 97 do Decreto Estadual nº 342/2023.

II - O CONTRATANTE, durante a vigência deste Contrato, compromete-se a:

a) Fornecer à contratada as informações necessárias ao cumprimento do presente contrato;

b) Assegurar o livre acesso dos empregados da Contratada a todos os locais onde se fizerem necessários os serviços;

c) Acompanhar e fiscalizar a execução dos serviços;

d) Anotar em registro próprio todas as ocorrências relacionadas com a execução dos serviços contratados, determinando o que for necessário à regularização das faltas ou irregularidades observadas;

e) Efetuar o pagamento à Contratada de acordo com o estabelecido no Contrato.

CLÁUSULA SÉTIMA - DAS OBRIGAÇÕES COMPLEMENTARES DA CONTRATADA

Sem prejuízo do disposto na Cláusula Sexta, a CONTRATADA obriga-se, ainda, a:

a) atender às determinações regulares do fiscal ou gestor do Contrato, ou da autoridade superior, prestando todo esclarecimento ou informação solicitados;

b) reparar, corrigir ou refazer, às suas expensas, os serviços que apresentarem falhas, defeitos ou incorreções decorrentes da execução, no prazo estabelecido pelo fiscal do contrato, observadas as disposições do Termo de Referência;;

c) responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, ficando a CONTRATANTE autorizada a descontar dos pagamentos devidos ou da garantia, quando exigida, o valor correspondente aos danos sofridos;

d) responsabilizar-se pelo cumprimento das obrigações trabalhistas, sociais, previdenciárias, tributárias, fiscais e comerciais previstas em Acordo, Convenção ou Dissídio Coletivo de Trabalho aplicáveis, cuja inadimplência não transfere responsabilidade à CONTRATANTE nem poderá onerar o objeto do Contrato;

e) comunicar ao fiscal do Contrato, tempestivamente e em prazo não superior a 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente verificado no local da execução;

f) 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 pessoas ou bens de terceiros;

g) cumprir, durante a execução do Contrato, a reserva de cargos prevista em lei para pessoa com deficiência, reabilitado da Previdência Social ou aprendiz, comprovando-a no prazo fixado pelo fiscal do Contrato;

h) guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato;

i) arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los caso o previsto inicialmente não seja satisfatório para o atendimento do objeto, exceto nas hipóteses do art. 124, II, "d", da Lei nº 14.133/2021;

j) cumprir as normas de segurança e saúde do trabalho, não submetendo trabalhadores a condições degradantes, jornadas exaustivas, servidão por dívida ou trabalho forçado, e observando as vedações ao trabalho infantil e ao trabalho noturno, perigoso ou insalubre de menores;

k) receber e dar tratamento adequado a denúncias de discriminação, violência e assédio no ambiente de trabalho;

l) não contratar, durante a vigência do Contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente da CONTRATANTE ou de agente público com função na licitação, fiscalização ou gestão do Contrato, nos termos do art. 48, parágrafo único, da Lei nº 14.133/2021;

m) prestar todo esclarecimento ou informação solicitados pela CONTRATANTE, garantindo-lhe acesso, a qualquer tempo, ao local dos trabalhos e aos documentos relativos à execução contratual;

n) realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo ser exigida a capacitação de técnicos da CONTRATANTE ou da nova empresa que continuará a execução;

o) ceder à CONTRATANTE os direitos patrimoniais relativos ao objeto contratado, quando este configurar obra imaterial de caráter tecnológico insuscetível de privilégio, incluindo o fornecimento de dados, documentos e elementos de informação pertinentes à tecnologia de concepção, desenvolvimento e aplicação da obra, para livre utilização e alteração pela CONTRATANTE sem necessidade de nova autorização.

CLÁUSULA OITAVA - DAS OBRIGAÇÕES COMPLEMENTARES DO CONTRATANTE

Sem prejuízo do disposto na Cláusula Sexta, a CONTRATANTE obriga-se, ainda, a:

a) exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com o Contrato e seus anexos;

b) notificar a CONTRATADA, por escrito, sobre vícios, defeitos, incorreções, imperfeições, falhas ou irregularidades verificadas na execução do objeto, fixando prazo para que sejam substituídos, reparados ou corrigidos, total ou parcialmente, às expensas da CONTRATADA;

c) comunicar a CONTRATADA para emissão de Nota Fiscal relativa à parcela incontroversa da execução, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução, conforme o art. 143 da Lei nº 14.133/2021;

d) aplicar à CONTRATADA as sanções previstas em lei e neste Contrato;

e) não praticar atos de ingerência na administração da CONTRATADA, tais como indicar pessoas para executar o objeto, fixar salário inferior ao legal, estabelecer vínculo de subordinação com empregado da CONTRATADA, condicionar o pagamento a reembolso de salários, ou demandar tarefas fora do escopo contratado;

f) explicitamente decidir sobre todas as solicitações e reclamações relacionadas à execução do Contrato, ressalvados requerimentos manifestamente impertinentes, protelatórios ou de nenhum interesse para a boa execução do ajuste, no prazo de _____, admitida prorrogação motivada por igual período;

g) notificar os emitentes de garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais, quando exigida garantia;

h) comunicar à CONTRATADA eventual alteração posterior do projeto, na hipótese do art. 93, §2º, da Lei nº 14.133/2021.

Parágrafo único - A Administração não responderá por compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do Contrato, nem por danos causados a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

CLÁUSULA NONA - DA SUBCONTRATAÇÃO

As regras sobre subcontratação do objeto são aquelas estabelecidas no Termo de Referência, anexo a este Contrato, sendo vedada a subcontratação em desacordo com as condições ali fixadas.

Parágrafo único - Em caso de consórcio, aplicam-se as regras de responsabilidade solidária já previstas na alínea "h" do item I da Cláusula Sexta, sem prejuízo do art. 97 do Decreto Estadual nº 342/2023 e dos arts. 15 e 97 da Lei nº 14.133/2021.

CLÁUSULA DÉCIMA - DAS OBRIGAÇÕES RELATIVAS À PROTEÇÃO DE DADOS PESSOAIS (LGPD)

As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou deste Contrato, desde a apresentação da proposta, independentemente de declaração ou aceitação expressa.

§1º - Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso, de acordo com a boa-fé e com os princípios do art. 6º da LGPD, sendo vedado o compartilhamento com terceiros fora das hipóteses legais.

§2º - A CONTRATANTE deverá ser informada, no prazo de 5 (cinco) dias úteis, sobre todos os contratos de suboperação de dados firmados ou a serem celebrados pela CONTRATADA.

§3º - Encerrado o tratamento dos dados nos termos do art. 15 da LGPD, é dever da CONTRATADA eliminá-los, ressalvadas as hipóteses do art. 16 da LGPD, inclusive quando necessária a guarda de documentação para comprovação de cumprimento de obrigações legais ou contratuais, enquanto não prescritas.

§4º - É dever da CONTRATADA orientar e treinar seus empregados quanto aos deveres, requisitos e responsabilidades decorrentes da LGPD, exigindo de suboperadores e subcontratados o cumprimento desta cláusula, permanecendo integralmente responsável por sua observância.

§5º - A CONTRATANTE poderá realizar diligência para aferir o cumprimento desta cláusula, devendo a CONTRATADA atender prontamente a pedidos de comprovação, inclusive quanto a eventual descarte de dados

realizado.

§6º - Bancos de dados formados a partir deste Contrato, notadamente os que armazenem dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos (art. 37 da LGPD), em formato interoperável que garanta sua reutilização pela Administração nas hipóteses previstas na LGPD.

§7º - O Contrato está sujeito a alteração nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado por autoridade competente, em especial a ANPD.

CLÁUSULA DÉCIMA PRIMEIRA – DA GARANTIA CONTRATUAL

A contratada deverá prestar garantia contratual, no valor correspondente a 5% (cinco por cento) do valor do contrato, podendo optar por fiança-bancária, seguro-garantia ou caução em dinheiro ou em títulos da dívida pública, conforme art. 96 e seguintes da Lei 14.133/2021.

Parágrafo único - O valor de eventual multa aplicada será descontado da garantia prestada, retido dos pagamentos devidos ou cobrado judicialmente, corrigido monetariamente pelo IPCA desde o termo inicial até a data do efetivo recolhimento.

CLÁUSULA DÉCIMA SEGUNDA - DAS PENALIDADES E MULTAS.

Pela inexecução total ou parcial do Contrato, a Administração poderá, garantida a prévia defesa, aplicar à (ao) CONTRATADA (O) as seguintes sanções:

I - Advertência;

II - Multa, observados os seguintes limites máximos:

a)) 0,3 % (três décimos por cento) por dia, até o trigésimo dia de atraso, sobre o valor do fornecimento ou serviço não realizado, ou sobre a etapa do cronograma físico de obras não cumprido;

b)) 10 % (dez por cento) sobre o valor total ou parcial da obrigação não cumprida, com o consequente cancelamento da nota de empenho ou documento equivalente;

III - Impedimento de licitar e de contratar com o Estado de Sergipe, pelo prazo de até 3 (três) anos;

IV - Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação.

§ 1º O valor da multa aplicada será descontado do valor da garantia prestada, retido dos pagamentos devidos pela Administração ou cobrado judicialmente, sendo corrigida monetariamente, de conformidade com a variação do IPCA, a partir do termo inicial, até a data do efetivo recolhimento.

§ 2º A contagem do período de atraso na execução dos ajustes será realizada a partir do primeiro dia útil

subsequente ao do encerramento do prazo estabelecido para o cumprimento da obrigação.

§ 3º São asseguradas à CONTRATADA, em qualquer hipótese, a prévia defesa e a ampla defesa, nos termos dos arts. 155 e seguintes da Lei nº 14.133/2021, sem prejuízo das demais regras acerca de infrações e sanções definidas no Termo de Referência.

CLÁUSULA DÉCIMA TERCEIRA - DA RESCISÃO

Independentemente de notificações ou interpelações judiciais ou extrajudiciais, constituem motivos para rescisão do Contrato as situações previstas nos artigos nos 137 a 139, da Lei nº 14.133/2021.

§ 1º - O presente Contrato poderá ser rescindido, também, por conveniência administrativa, a juízo do Contratante, sem que caiba à Contratada qualquer ação ou interpelação judicial.

§ 2º - Na ocorrência da rescisão prevista no "caput" desta cláusula, nenhum ônus recairá sobre o Contratante em virtude desta decisão, ressalvado o disposto no § 2º do artigo 138 da Lei nº 14.133/2021 e alterações.

§ 3º - O Contrato será extinto, ainda, quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado; se as obrigações não forem cumpridas no prazo, a vigência ficará prorrogada até a conclusão do objeto, cabendo à Administração providenciar a readequação do cronograma fixado.

§ 4º - A alteração social ou a modificação da finalidade ou estrutura da CONTRATADA não ensejará a extinção do Contrato se não restringir sua capacidade de concluí-lo; havendo mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

§ 5º - O Contrato poderá ainda ser extinto caso se constate que a CONTRATADA mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão contratante ou com agente público que tenha atuado na licitação, na fiscalização ou na gestão do Contrato, ou com cônjuge, companheiro ou parente destes em linha reta, colateral ou por afinidade até o terceiro grau (art. 14, IV, da Lei nº 14.133/2021).

CLÁUSULA DÉCIMA QUARTA - DOS DIREITOS DO CONTRATANTE NO CASO DE RESCISÃO

Na hipótese de rescisão administrativa do presente Contrato, a Contratada reconhece, de logo, o direito do Contratante de adotar, no que couber, as medidas previstas no artigo 139, da Lei nº 14.133/2021.

A CONTRATANTE poderá, ainda:

a) nos casos de obrigação de pagamento de multa pela CONTRATADA, reter a garantia prestada, para fins de execução, conforme a legislação de regência;

b) nos casos de necessidade de ressarcimento de prejuízos causados à Administração, nos termos do art. 139, IV, da Lei nº 14.133/2021, reter os eventuais créditos existentes em favor da CONTRATADA decorrentes do Contrato; e

c) exigir que o termo de extinção seja precedido, sempre que possível, de balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos, relação dos pagamentos já efetuados e ainda devidos, e apuração de indenizações e multas, sem prejuízo do reconhecimento de eventual desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório.

CLÁUSULA DÉCIMA QUINTA - DA LEGISLAÇÃO APLICÁVEL À EXECUÇÃO DO CONTRATO E OS CASOS OMISSOS

O presente Contrato fundamenta-se:

I - nos termos do Pregão Eletrônico nº. 377/2026 que, simultaneamente:

a) constam do Processo Administrativo 174/2026-COMPRAS.GOV-SEPLAN

b) não contrarie o interesse público;

II - nas demais determinações da Lei 14.133/2021 e nos Decretos Estaduais, principalmente, o Decreto Estadual n° 342/2023;

III - nos preceitos do Direito Público;

IV - supletivamente, nos princípios da Teoria Geral dos Contratos e nas disposições do Direito Privado.

V - subsidiariamente, na Lei nº 8.078, de 1990 (Código de Defesa do Consumidor) e nos princípios gerais dos contratos.

Parágrafo único - Os casos omissos e quaisquer ajustes que se fizerem necessários, em decorrência deste Contrato, serão acordados entre as partes, lavrando-se, na ocasião, Termo Aditivo.

CLÁUSULA DÉCIMA SEXTA - DA PUBLICAÇÃO.

Os contratos e seus aditamentos serão divulgados no Portal Nacional de Contratações Públicas (PNCP), no sítio eletrônico oficial do órgão ou entidade licitante e no portal de compras do Estado de Sergipe – COMPRASNET.SE e seu extrato no Diário Oficial do Estado, e a divulgação deverá ocorrer em até 20 (vinte) dias úteis da data de sua assinatura, nos termos do art.143 do Decreto Estadual nº 342/2023 e art. 94, I da Lei nº 14.133/2021.

CLÁUSULA DÉCIMA SÉTIMA - DAS ALTERAÇÕES.

Este instrumento poderá ser alterado na ocorrência de quaisquer fatos estipulados no artigo 125, da Lei 14.133/2021, devidamente comprovados.

§ 1º - A Contratada fica obrigada a aceitar, nas mesmas condições contratuais, os acréscimos e supressões que se fizerem necessários, até o limite legal previsto, calculado sobre o valor inicial atualizado do contrato.

§2º - As alterações contratuais deverão ser promovidas mediante termo aditivo, submetido à prévia aprovação da consultoria jurídica da CONTRATANTE, salvo justificada necessidade de antecipação de efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês; registros que não caracterizem alteração contratual poderão ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133/2021.

CLÁUSULA DÉCIMA OITAVA - DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

A fiscalização e o acompanhamento serão, em conformidade com o Decreto Estadual nº 342/2023 e art. 117 e seguintes da Lei nº 14.133/2021, com a designação de XXXXXXX para fiscalizar e acompanhar a execução deste contrato.

§ 1º - À fiscalização compete, entre outras atribuições, verificar a conformidade da execução do Contrato com as normas especificadas, se os procedimentos são adequados para garantir a qualidade desejada.

§ 2º - A ação da fiscalização não exonera A CONTRATADA de suas responsabilidades contratuais.

§ 3º - 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 do Termo de Referência, anexo a este Contrato, cabendo à fiscalização observá-los no exercício de suas atribuições.

CLÁUSULA DÉCIMA NONA - DO FORO

As partes contratantes elegem o Foro da Capital do Estado de Sergipe como único competente para dirimir as questões que porventura surgirem na execução do presente Contrato, com renúncia expressa por qualquer outro.

E, por estarem justas e contratadas, as partes assinam este instrumento a fim de que produza seus efeitos legais.

Aracaju/SE, ____de _____ de 202X.

_____

(nome do titular do Órgão) CONTRATADA

}

ANEXO IV - RELAÇÃO DE UNIDADES PARTICIPANTES

ORGÃO/ENTIDADE	ENDEREÇO
Secretaria de Estado da Educação - SEED	Rua Gutemberg Chagas, 169 - Dia Bairro: Inácio Barbosa CEP: 49040-780 TEL.: 3211-0816
Secretaria de Estado da Saúde - SES	Avenida Augusto Franco, nº 3.150 - Centro Administrativo da Saúde Senador Gilvan Rocha Bairro: Ponto Novo CEP: 49097-670 TEL.: 3226-8311
Secretaria de Estado da Segurança Pública - SSP	Praça Tobias Barreto, 20 Bairro: São José CEP: 49015-130 TEL.: 32165400

ANEXO V

TERMO DE ADESÃO

Termo de adesão referente à Registro de Preço n° xxxxx para XXXXXXXXXXXXXXXXXX, que entre si fazem a ***SECRETARIA ESPECIAL DAS CONTRATAÇÕES, LICITAÇÕES E LOGÍSTICA****, unidade gerenciadora do Sistema de Registro de Preços, e o(a)****(inserir o nome do órgão aderente).***

Eu, ...(inserir nome da autoridade competente do órgão contratante), portador(a) do RG n.º ..... (inserir número do RG) e do CPF n.º .....(inserir número do CPF), na qualidade de .....(inserir o cargo da autoridade), dou anuência ao processo de contratação centralizada para ..... (inserir objeto do contrato), número ..... (inserir número do processo), responsabilizando-me pelo acompanhamento da execução do contrato e demais incumbências pertinentes ao processo, nos termos do Decreto n.º 342/2023 e da Lei nº 14.133/2021.

Informo que as despesas decorrentes para a execução contratual correrão por conta da seguinte dotação orçamentária:

UNIDADE ORÇAMENTÁRIA	CLASSIFICAÇÃO FUNCIONAL PROGRAMÁTICA	PROJETO OU ATIVIDADE	ELEMENTO DE DESPESA	FONTE DE RECURSO	VALOR ESTIMATIVA ANUAL
XXXXX	XXXXX	XXXXX	XXXXX	XXXXX	XXXXX

Aracaju (SE), de de 2026.

_____

(inserir nome do dirigente e do órgão aderente)

ANEXO VI - MODELOS DE DECLARAÇÃO

MODELO DE DECLARAÇÃO I

ENQUADRAMENTO COMO MICROEMPRESA OU EMPRESA DE PEQUENO PORTE

(Obrigatória para Microempresas ou Empresas de Pequeno Porte)

À Secretaria Especial das Contratações, Licitações e Logística - SECLOG
A/C: Senhor Pregoeiro
PREGÃO ELETRÔNICO Nº 377/2026
PROCESSO Nº 174/2026-COMPRAS.GOV-SEPLAN

[nome da empresa], [qualificação: tipo de sociedade (Ltda, S.A, etc.)], [endereço completo], inscrita no CNPJ sob o n.º [xxxx], neste ato representada pelo [cargo] [nome do representante legal], portador da Carteira de Identidade n.º [xxxx], inscrito no CPF sob o n.º [xxxx], DECLARA, sob as penalidades da lei, que se enquadra como Microempresa ou Empresa de Pequeno Porte, nos termos do art. 3º da Lei Complementar n.º 123 de 14 de dezembro de 2006 c/c art. 4º da Lei nº 14.133/2021, estando apta a fruir os benefícios e vantagens legalmente instituídas por não se enquadrar em nenhuma das vedações legais impostas pelo § 4º do art. 3º da Lei Complementar n.º 123 de 14 de dezembro de 2006.

Declaro, para os fins do disposto no art. 4º da Lei nº 14.133/2021, não ter celebrado contratos com a Administração Pública, no ano-calendário desta licitação, cuja soma ultrapasse o valor de R$ 4.800.000,00. De tal modo, declaro ser:

( ) MICROEMPRESA – Receita bruta anual igual ou inferior a R$ 360.000,00 e estando apta a fruir os benefícios e vantagens legalmente instituídas por não se enquadrar em nenhuma das vedações legais impostas pelo § 4º do art. 3º da Lei Complementar nº 123/06 c/c art. 4º da Lei nº 14.133/2021

( ) EMPRESA DE PEQUENO PORTE– Receita bruta anual superior a R$ 360.000,00 e igual ou inferior a R$ 4.800.000,00, estando apta a fruir os benefícios e vantagens legalmente instituídas por não se enquadrar em nenhuma das vedações legais impostas pelo § 4º do art. 3º da Lei Complementar nº 123/06.

Observações:

• Esta declaração poderá ser preenchida somente pela licitante enquadrada como ME ou EPP, nos termos da LC 123, de 14 de dezembro de 2006;

• A não apresentação desta declaração será interpretada como não enquadramento da licitante como ME ou EPP, nos termos da LC nº 123/2006, ou a opção pela não utilização do direito de tratamento diferenciado.

MODELO DE DECLARAÇÃO II

DECLARAÇÃO DE FALÊNCIA E RECUPERAÇÃO EMPRESARIAL

À Secretaria Especial das Contratações, Licitações e Logística - SECLOG
A/C: Senhor Pregoeiro
PREGÃO ELETRÔNICO Nº 377/2026
PROCESSO Nº 174/2026-COMPRAS.GOV-SEPLAN

A Empresa XXXXXXXXXXXXXXX, inscrita no CNPJ sob o n.º XXXXXXXXXXXXXX, sediada na [ENDEREÇO COMPLETO], por intermédio de seu representante legal, [NOME COMPLETO], portador da Cédula de Identidade n.º XXXXXXX e do CPF n.º XXXXXXXXXX, DECLARA, sob as penas da lei, que, até a presente data, a mesma não se encontra em recuperação extrajudicial ou estado falimentar. Declara ainda, não estar sofrendo penalidades de Inidoneidade no âmbito da Administração Federal, Estadual, Municipal ou do Distrito Federal, arcando civil e criminalmente pela presente afirmação, bem como da total aceitação das condições estipuladas no referido Edital e seus anexos.

( ) Declaro estar em processo de recuperação judicial cujo plano de recuperação fora aprovado pelo juízo competente

.....
Local/Data

.....
Assinatura do Representante Legal da Licitante

MODELO DE DECLARAÇÃO IV

DECLARAÇÃO DE EMPREGADO MENOR

À Secretaria Especial das Contratações, Licitações e Logística - SECLOG
A/C: Senhor Pregoeiro
PREGÃO ELETRÔNICO Nº 377/2026
PROCESSO Nº 174/2026-COMPRAS.GOV-SEPLAN

Declaro, para fins do disposto no inciso VI do art. 68 da Lei nº 14.133, de 1º de abril de 2021, que a empresa _____, inscrita no CNPJ (MF) no _____, inscrição estadual no _____, estabelecida em _____, não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos.

Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz ( ).

.....
Local/Data

.....
Assinatura do Representante Legal da Licitante

MODELO DE DECLARAÇÃO V

ELABORAÇÃO DE PROPOSTA INDEPENDENTE

À Secretaria Especial das Contratações, Licitações e Logística - SECLOG
A/C: Senhor Pregoeiro
PREGÃO ELETRÔNICO Nº 377/2026
PROCESSO Nº 174/2026-COMPRAS.GOV-SEPLAN

(Identificação completa do representante da licitante), como representante devidamente constituído de (Identificação completa da licitante), declara, sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que:

A proposta anexa foi elaborada de maneira independente pela Licitante, e o conteúdo da proposta não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato desta licitação, por qualquer outro meio ou por qualquer pessoa;

A intenção de apresentar a proposta anexa não foi informada, discutido com ou recebido de qualquer outro participante potencial ou de fato desta licitação, por qualquer meio ou por qualquer pessoa;

Que não tentou, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato da licitação atinente ao Pregão Eletrônico em referência quanto a participar ou não da referida licitação;

Que o conteúdo da proposta anexa não será, no todo ou em parte, direta ou indiretamente, comunicado ou discutido com qualquer outro participante potencial ou de fato da licitação atinente ao Pregão Eletrônico referenciado antes da adjudicação do objeto da referida licitação;

Que o conteúdo da proposta anexa não foi, no todo ou em parte, direta ou indiretamente, informado a, discutido com ou recebido de qualquer integrante da SECLOG antes da abertura oficial das PROPOSTAS; e

Que está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la, responsabilizando-se pela execução do objeto no prazo do Edital e que os preços se referem a preços usuais de mercado.

.....

Local/Data

.....

Assinatura do Representante Legal da Licitante

MODELO DE DECLARAÇÃO VI

DECLARAÇÃO DE NÃO UTILIZAÇÃO DE TRABALHO DEGRADANTE OU FORÇADO

À Secretaria Especial das Contratações, Licitações e Logística - SECLOG
A/C: Senhor Pregoeiro
PREGÃO ELETRÔNICO Nº 377/2026
PROCESSO Nº 174/2026-COMPRAS.GOV-SEPLAN

Declaro, para fins do disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal de 05 de outubro de 1988, que a empresa _____, inscrita no CNPJ (MF) no _____, inscrição estadual no _____, estabelecida em _____, não possui em sua cadeia produtiva, empregados executando trabalho degradante ou forçado.

.....
Local/Data

.....
Assinatura do Representante Legal da Licitante

MODELO DE DECLARAÇÃO VII

DECLARAÇÃO DE ATENDIMENTO AO DISPOSTO NO ART. 93 DA LEI Nº 8.213, DE 24 DE JULHO DE 1999

À Secretaria Especial das Contratações, Licitações e Logística - SECLOG
A/C: Senhor Pregoeiro
PREGÃO ELETRÔNICO Nº 377/2026
PROCESSO Nº 174/2026-COMPRAS.GOV-SEPLAN

Declaro, para os devidos fins, que a empresa _____, inscrita no CNPJ (MF) no _____, inscrição estadual no _____, estabelecida em _____, não possui, em sua cadeia produtiva, 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, e que atende à reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

.....

Local/Data

.....

Assinatura do Representante Legal da Licitante