



AGÊNCIA BRASILEIRA DE PROMOÇÃO INTERNACIONAL DO TURISMO
SCN Quadra 2 - Bloco G, - Bairro Asa Norte, Brasília/DF, CEP 70712-907
Telefone: 61 2023-8500 - <http://www.embratur.com.br>

EDITAL Nº 90006/2025

Processo nº 272100.002628/2024-05

Brasília, 04 de junho de 2025.

A AGÊNCIA BRASILEIRA DE PROMOÇÃO INTERNACIONAL DO TURISMO - EMBRATUR, instituída pela Lei nº 14.002, de 22 de maio de 2020, sediada no SCN, Quadra 02, Bloco G, Brasília-DF – CEP 70.712-90, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, do tipo menor preço global, sob a forma de execução indireta, nos termos do art. 11º inciso IV, da Resolução CDE 15, de 8 de maio de 2025, Manual de Licitações e Contratos, e das exigências estabelecidas neste Edital.

Data da sessão: 23 de junho de 2025.

Horário: 10:00h

Local: Portal de Compras do Governo Federal – <https://www.gov.br/compras/pt-br>

UASG: 927988

1. DO OBJETO

- 1.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para a Contratação de empresa para fornecimento de solução integrada de segurança da informação com fornecimento de licenças e serviços, conforme as quantidades e exigências estabelecidas neste instrumento e detalhamento dos serviços descritos no Termo de Referência, Anexo I deste Edital.
- 1.2. A licitação será realizada em grupo único, formados por 04 (quatro) itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.
- 1.3. O critério de julgamento adotado será o **menor preço global** do grupo, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.
- 1.4. O valor estimado do contrato é de **R\$ 1.685.201,50 (um milhão, seiscentos e oitenta e cinco mil duzentos e um reais e cinquenta centavos)**, conforme as especificações abaixo:

ITENS	DESCRIÇÃO/ESPECIFICAÇÃO	QT	Valor Unitário R\$	Valor Total R\$
1	Solução de gerenciamento de vulnerabilidades de segurança e correções automatizadas	340	649,20	220.728,00
2	Solução de correlação de eventos de segurança e resposta a incidentes	750	757,53	568.147,50
3	Solução de proteção avançada para endpoints	340	253,90	86.326,00
4	Serviço de operação, monitoramento e tratamento de eventos de segurança	12	67.500,00	810.000,00
VALOR GLOBAL				R\$ 1.685.201,50

2. DO CREDENCIAMENTO E DA PARTICIPAÇÃO NO PREGÃO.

- 2.1. O Credenciamento é o nível básico do registro cadastral no Sistema de Cadastramento Unificado de Fornecedores - SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.
- 2.1.1. O cadastro no SICAF deverá ser feito no no Sistema de Compras do Governo Federal (www.gov.br/compras), por meio de Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.
- 2.1.2. O credenciamento junto ao provedor do sistema implica na responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para a realização das transações inerentes a este Pregão

2.1.3. Os interessados deverão atender às condições exigidas no cadastramento no Sicafe até o terceiro dia útil anterior à data prevista para recebimento das propostas.

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

2.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados, 03 (três) dias antes da abertura do pregão.

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

2.5. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação.

2.5.1.1. A licitação será de ampla participação.

2.6. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas, para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor individual - MEI, nos limites previstos da [Lei Complementar nº 123, de 2006](#) e do Decreto n.º 8.538, de 2015.

2.7. Não poderão participar desta licitação os interessados:

2.7.1. proibidos de participar de licitações e celebrar contratos com a EMBRATUR, União, Estados, Distrito Federal e Municípios;

2.7.2. que não atendam às condições deste Edital e seu(s) anexo(s);

2.7.3. estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

2.7.4. que estejam sob falência ou de insolvência civil ou dissolução da sociedade;

2.7.5. entidades empresariais que estejam reunidas em consórcio;

2.7.6. organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário);

2.7.7. cujo administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social seja diretor ou empregado da EMBRATUR;

2.7.8. declarados inidôneos pela União, por Estado, pelo Distrito Federal ou pela unidade federativa a que está vinculada, enquanto perdurarem os efeitos da sanção;

2.7.9. constituídos por sócio de empresa que estiver suspensa, impedida ou declarada inidônea;

2.7.10. cujo administrador seja sócio de empresa suspensa, impedida ou declarada inidônea;

2.7.11. constituídos por sócio que tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;

2.7.12. cujo administrador tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;

2.7.13. que tiver, nos seus quadros de diretoria, pessoa que participou, em razão de vínculo de mesma natureza, de empresa declarada inidônea;

2.7.14. que sejam sociedades cooperativas;

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

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

2.7.17. A personalidade jurídica poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste instrumento convocatório ou para provocar confusão patrimonial, sendo estendidos todos os efeitos das sanções aplicadas à pessoa jurídica aos seus administradores e sócios com poderes de administração, observados o contraditório e a ampla defesa (redação conforme artigo 14, da Lei nº 12.846/2013).

2.8. Aplica-se a vedação prevista no item 2.7. acima:

2.8.1. à contratação do próprio empregado ou dirigente, como pessoa física, bem como à participação dele em procedimentos licitatórios, na condição de licitante;

2.8.2. a quem tenha relação de parentesco, até o terceiro grau civil, com:

2.8.2.1. dirigente(s) da EMBRATUR;

2.8.2.2. empregado da EMBRATUR cujas atribuições envolvam a atuação na área responsável pela licitação ou contratação;

2.8.2.3. autoridade do ente público a que a EMBRATUR esteja vinculada.

2.8.3. à empresa cujo proprietário, mesmo na condição de sócio, tenha terminado seu prazo de gestão ou rompido seu vínculo com a EMBRATUR há menos de 6 (seis) meses.

3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

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

3.2. Os licitantes cadastrarão, exclusivamente por meio do sistema eletrônico a proposta com o preços, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecido para abertura da sessão pública.

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

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

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

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

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

3.4. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no [artigo 3º da Lei Complementar nº 123, de 2006](#), estando apto a usufruir do tratamento favorecido estabelecido em seus [arts. 42 a 49](#).

3.4.1. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na [Lei Complementar nº 123, de 2006](#), mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

3.5. A falsidade da declaração de que trata os itens 3.3 ou 3.4 sujeitará o licitante às sanções previstas neste Edital.

3.6. Os licitantes poderão retirar ou substituir a proposta até a abertura da sessão pública.

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

3.8. Os documentos que compõem a proposta dos licitantes e os documentos de habilitação serão disponibilizados para acesso público no sistema ComprasNet somente após a convocação e o envio de anexo pelo licitante via sistema.

3.9. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo quando do cadastramento da proposta e obedecerá às seguintes regras:

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

3.9.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

3.10. O valor final mínimo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

3.10.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço;

3.11. O valor final mínimo parametrizado na forma do item 3.9 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

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

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

4. DO PREENCHIMENTO DA PROPOSTA

4.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, conforme modelo de Proposta Comercial, constante do Anexo III deste Edital.

4.1.1. a licitante deverá complementar o Anexo III com os seguintes dados básicos da empresa:

- a) Razão Social
- b) Nome Fantasia
- c) Inscrição do CNPJ
- d) Inscrição Estadual/Municipal
- e) Endereço completo
- f) Telefone e endereço eletrônico.

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

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

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

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

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

4.7.1. Também poderão ser desclassificadas as propostas que apresentarem o prazo de validade inferior ao previsto no subitem 4.6, quando não houver acordo para o ajustamento de tal validade.

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

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

5.1.3. Os licitantes poderão retirar ou substituir a proposta, quando for o caso, anteriormente inserido no sistema, até a abertura da sessão pública.

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

5.2.1. Será desclassificada a proposta que identifique o licitante.

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

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

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

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

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

5.6. O lance deverá ser ofertado pelo valor total dos itens pertencentes ao grupo.

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

5.7.1. Na competição, não serão aceitos contatos telefônicos, ou via e-mail, com o Pregoeiro e com a equipe de apoio, inclusive para pedidos de exclusão de lances dados equivocadamente, sob pena de aplicação das penalidades cabíveis, já que tal ato configura a identificação da licitante durante a fase de lances, o que é proibido pelas normas.

5.7.2. Após a fase de lances, não serão aceitos contatos telefônicos, ou via e-mail, com o pregoeiro e com a equipe de apoio, sob pena de aplicação das penalidades cabíveis, já que tal ato configura a inobservância aos Princípios da Transparência e Publicidade, tendo em vista que nos ritos do pregão existe o chat e a etapa recursal para que as empresas se manifestem.

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

5.9. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R\$ 0,01 (um centavo de real).

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

5.11. O procedimento adotado é o modo de disputa "aberto e fechado", os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

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

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

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

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

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

- 5.12. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.
- 5.13. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.
- 5.14. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.
- 5.15. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.
- 5.16. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.
- 5.17. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.
- 5.18. Encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos [arts. 44 e 45 da Lei Complementar nº 123, de 2006](#), regulamentada pelo [Decreto nº 8.538, de 2015](#).
- 5.18.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.
- 5.18.2. A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.
- 5.18.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.
- 5.18.4. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.
- 5.19. Havendo eventual empate entre propostas ou lances, o critério de desempate será realizado pelo Portal do Comprasnet.
- 5.19.1. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas ou os lances empatados.
- 5.20. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro poderá 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. O prazo para resposta do licitante será de 05 (cinco) minutos, caso não haja manifestação será considerado o lance final registrado por último no *Comprasnet*.
- 5.20.1. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço de referência definido pela Agência ou por não atender os requisitos do Termo de Referência.
- 5.20.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.
- 5.20.3. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.
- 5.21. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no item 2.7 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:
- a) SICAF;
 - b) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (<https://www.portalttransparencia.gov.br/sancoes/ceis>); e
 - c) Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (<https://www.portalttransparencia.gov.br/sancoes/cnep>).
 - d) Lista de Inidôneos e o Cadastro Integrado de Condenações por Ilícitos Administrativos - CADICON, mantidos pelo Tribunal de Contas da União (TCU); e

e) Para a consulta de licitantes pessoa jurídica, poderá haver a substituição das consultas das alíneas “b”, “c” e “d”, acima, pela Consulta Consolidada de Pessoa Jurídica do TCU (<https://certidoes-apf.apps.tcu.gov.br/>).

5.21.1. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o [artigo 12 da Lei nº 8.429, de 1992](#).

5.21.2. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. ([IN nº 3/2018, art. 29, caput](#))

5.21.2.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. ([IN nº 3/2018, art. 29, §1º](#)).

5.21.2.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. ([IN nº 3/2018, art. 29, §2º](#)).

5.21.2.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

5.21.3. Caso atendidas as condições de participação, será iniciado o procedimento de julgamento.

5.21.4. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com os itens 2.6 e 3.4 deste edital.

5.22. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 02 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital.

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

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

6. DA FASE DE JULGAMENTO

6.1. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no [artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022](#).

6.2. Será desclassificada a proposta vencedora que:

6.2.1. contiver vícios insanáveis;

6.2.2. não obedecer às especificações técnicas contidas no Termo de Referência;

6.2.3. apresentar preços inexequíveis;

6.2.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Embratur;

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

6.3. 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 Embratur.

6.3.1 A inexequibilidade, na hipótese de que trata o **caput**, só será considerada após diligência do pregoeiro, que comprove:

6.3.1.1. que o custo do licitante ultrapassa o valor da proposta; e

6.3.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.4. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

6.4.1. As diligências poderão ser realizadas em qualquer fase da licitação, tanto pelo Pregoeiro como pela Autoridade Competente, vedada a inclusão posterior de documento ou informação que deveria constar originariamente da proposta.

6.4.1.1. A vedação acima citada não alcança documento ausente que não foi juntado com os demais comprovantes de habilitação e/ou da proposta, por equívoco ou falha.

6.5. Erros no preenchimento da Proposta de Preço não constituem motivo para a desclassificação da proposta. A Proposta poderá ser ajustada pelo licitante, no prazo de até 02 (duas) horas, desde que não haja majoração dos preços dos itens e dos grupos e que se comprove que este é o bastante para arcar com todos os custos da contratação;

6.5.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

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

6.5.3. Caso a empresa venha a majorar o preço da proposta, não sanar os vícios ou tenha as justificativas não aceitas pelo Pregoeiro, terá a sua proposta recusada.

6.5.4. É facultado ao Pregoeiro prorrogar o prazo por igual período do subitem 6.10. estabelecido, a partir de solicitação fundamentada feita no *chat* pelo licitante, antes de findo o prazo.

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

7. DA FASE DE HABILITAÇÃO

7.1. A habilitação das licitantes será verificada por meio do SICAF, nos documentos por ele abrangidos.

7.1.1. Caso os documentos exigidos para habilitação não estejam contemplados no SICAF ou não haja disponibilidade de realizar a consulta nos sítios emitentes das certidões vencidas, será exigido o envio da documentação através do comprasnet, no prazo máximo de 02 (duas) horas, após solicitação do pregoeiro no sistema eletrônico.

7.1.2. O envio da documentação de habilitação, respeitado o prazo de 02 (duas) horas, também poderá ser encaminhado juntamente com a proposta, desde que convocado pelo pregoeiro através da funcionalidade chat do comprasnet.

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

7.2. Os documentos necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação serão exigidos para fins de habilitação são os seguintes:

7.2.1. Habilitação jurídica

7.2.1.1. cédula de identidade do representante legal da empresa;

7.2.1.2. prova de registro no órgão competente, no caso de empresário individual;

7.2.1.3. ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado no órgão competente, no caso de sociedade empresária ou Empresa Individual de Responsabilidade Limitada - EIRELI;

7.2.1.4. ato de nomeação ou de eleição dos administradores, devidamente registrado no órgão competente, no caso de Sociedade Anônima ou Limitadas, quando for o caso.

7.2.2. Regularidade Fiscal e Trabalhista

7.2.2.1. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);

7.2.2.2. 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 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional;

7.2.2.3. prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

7.2.2.4. 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;

7.2.2.5. prova de inscrição no cadastro de contribuintes estadual e/ou municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

7.2.2.6. prova de regularidade com a Fazenda Estadual e/ou Municipal do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

7.2.2.7. caso o licitante seja considerado isento dos tributos estaduais ou municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Estadual ou Municipal do seu domicílio ou sede, ou outra equivalente, na forma da lei;

7.2.2.8. A documentação a que se refere o item 7.2.2. poderá ser exigida em qualquer fase da execução contratual ou Ordem de Serviço ou Fornecimento, sendo que sua falta será imediatamente comunicada à CONTRATADA para sanar a irregularidade, sob pena de aplicação de penalidade e/ou rescisão contratual.

7.2.3. Qualificação Econômico-Financeira:

7.2.3.1. Balanço patrimonial e demonstrações contábeis do último exercício social, 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.

7.2.3.1.1. No caso de sociedade anônima e de outras empresas obrigadas à publicação, deverá ser apresentada a cópia da publicação, na imprensa oficial, do Balanço e das Demonstrações Contábeis, além da ata de aprovação devidamente registrada na Junta Comercial.

7.2.3.1.2. Quando não houver a obrigatoriedade de publicação do Balanço e das Demonstrações Contábeis, deverão ser apresentadas cópias legíveis dessas peças, bem como dos termos de abertura e de encerramento do Livro Diário, registrado na Junta Comercial ou no órgão competente.

7.2.3.1.3. No caso de Livro Diário expedido através do Sistema Público de Escrituração Digital – SPED, deverá ser apresentado além do Balanço e das Demonstrações Contábeis, registrado no órgão competente, o termo de abertura e de encerramento do Livro Diário e o Recibo de Entrega de Escrituração Contábil Digital emitido pelo referido sistema.

7.2.3.1.4. Consideram-se “já exigíveis e apresentados na forma da lei” as Demonstrações Contábeis e o Balanço Patrimonial referentes ao exercício social imediatamente antecedente ao ano da licitação, quando a data de apresentação dos documentos de habilitação ocorrer a partir de 01 de maio (art. 1.078, I, do Código Civil), mesmo no caso de licitantes obrigados ao SPED, devendo ser desconsiderado prazo superior para transmissão das peças contábeis digitais estabelecido por atos normativos que disciplinam o citado SPED (conforme entendimento do TCU, Acórdãos 1999/2014 e 119/2016, ambos do Plenário).

7.2.3.1.5. Empresa que, de acordo com a legislação, não tenha apurado as demonstrações contábeis referentes ao seu primeiro exercício social, deverá apresentar balanço de abertura, levantado na data de sua constituição, conforme os requisitos de legislação societária e comercial.

7.2.3.1.6. no caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

7.2.3.1.7. é admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social.

7.2.3.2. Certidão negativa de falência expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio da pessoa física;

7.2.3.2.1. Caso a licitante se encontre em processo de recuperação judicial ou extrajudicial, deverá ser apresentada, por meio da documentação apropriada, a sentença homologatória do plano de recuperação judicial.

7.2.3.3. comprovação da boa situação financeira da empresa, mediante a obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

LG =	Ativo Circulante + Realizável a Longo Prazo
	Passivo Circulante + Passivo Não Circulante

SG =	Ativo Total
	Passivo Circulante + Passivo Não Circulante

LC =	Ativo Circulante
	Passivo Circulante

7.2.3.3.1. 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 patrimônio líquido de, **no mínimo, 10% (dez por cento)** do valor total estimado da contratação.

7.2.4. Qualificação Técnica:

7.2.4.1. O critério de qualificação técnica a ser atendido pelo fornecedor será a apresentação de:

7.2.4.1.1. Declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação;

7.2.4.1.2. Atestado de Capacidade Técnica (ACT), em nome da licitante, emitido por pessoas jurídicas de direito público ou privado, que comprove a execução em serviços de complexidade tecnológica e operacional similares ou superior ao objeto do termo de referência, ou com o item pertinente;

7.2.4.1.3. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

7.2.4.1.3.1. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

7.2.4.1.3.2 Os atestados devem se referir a contratos já concluídos ou já decorrido no mínimo um ano do início de sua execução, exceto se houver sido firmado para ser executado em prazo inferior devendo ser comprovado por meio do contrato e a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente; e

7.2.4.1.3.3. Se referir a fornecimentos de soluções e serviços de cibersegurança compatíveis e similares com o objeto contido neste Termo de Referência. Considera-se como compatível:

7.2.4.1.3.4. Comprovação de execução contrato com quantidades de no mínimo 50% do item 1, 2 e 3;

7.2.4.1.3.5. Comprovação de execução de contrato com objeto compatível ao item 4, devendo a empresa comprar minimamente operação e sustentação de Proteção de endpoint, SIEM e SOAR. Será admitido para fins de comprovação de aptidão técnica atestados com unidade fixa mensal ou métricas equivalentes ao objeto, tais como HST (Hora de Serviço Técnico), HH (Hora-Homem), UST (Unidade de Serviço Técnico), sendo que ao usar métricas baseadas em Horas, deverá comprovar minimamente a execução de 1.050 horas, equivalente à 50% do item.

7.2.4.1.3.6. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

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

7.3. No caso de a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

7.3.1. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no [Decreto nº 8.660, de 29 de janeiro de 2016](#), ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

7.4. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública.

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

7.5. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas.

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

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

7.8. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

7.8.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. ([IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º](#)).

7.9. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. ([IN nº 3/2018, art. 7º, caput](#)).

7.9.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. ([IN nº 3/2018, art. 7º, parágrafo único](#)).

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

7.10.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de 02 (duas) horas, prorrogável por igual período, contado da solicitação do pregoeiro.

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

7.11.1. Os documentos relativos à regularidade fiscal somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

7.12. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para:

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

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

7.12.3. A diligência citada pode alcançar documento ausente que não foi juntado com os demais comprovantes de habilitação e/ou da proposta, por equívoco ou falha.

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

7.14. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 7.10.1.

7.15. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

7.16. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação ([art. 4º do Decreto nº 8.538/2015](#)).

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

7.17.1 Constatada a ocorrência de impeditivos indiretos de licitar e contratar no cadastro da empresa no Sistema de Cadastro Unificado de Fornecedores – SICAF, será aberto processo administrativo para aplicação da desconsideração da personalidade jurídica, com direito contraditório e a ampla defesa, do conforme Acórdão TCU nº 1831/2014 – Plenário, dispondo que a constituição de nova sociedade com sócios em comum ou a existência de elementos que indique o uso de pessoas jurídicas distintas com o mesmo objeto social e com os mesmos sócios, ambos os casos em substituição a outra empresa declarada inidônea para licitar com a Administração Pública, com o objetivo de burlar a aplicação da sanção administrava, constitui abuso de forma e fraude à Lei de Licitações Lei nº 8.666/93, de modo a possibilitar a aplicação da teoria da desconsideração da personalidade jurídica para estenderem-se os efeitos da sanção administrava à nova sociedade constituída.

8. DOS RECURSOS

8.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação.

8.1.1. Qualquer licitante poderá, durante o prazo concedido na sessão pública, não inferior a 10 minutos, de forma imediata após o término do julgamento das propostas e do ato de habilitação ou inabilitação, em campo próprio do sistema, manifestar sua intenção de recorrer, sob pena de preclusão, ficando a autoridade superior autorizada a adjudicar o objeto ao licitante declarado vencedor.

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

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

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

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

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

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

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

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

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

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

8.10. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico www.sei.embratur.com.br.

8.10.1. O acesso de usuário externo ao Sistema Eletrônico de Informações (SEI) da EMBRATUR, para vistas ao processo, exigirá um pré-cadastro;

8.10.2. O representante da empresa deverá encaminhar um e-mail para o endereço eletrônico pregoeiro2@embratur.com.br, solicitando o link para realizar o pré-cadastro, a fim de se obter acesso ao Sistema Eletrônico de Informações (SEI) da EMBRATUR para vistas ao processo, anexando a cópia do Registro Geral (Identidade), do CPF e do comprovante de residência;

8.10.3. O cadastramento somente será efetivado após o encaminhamento e a análise da documentação solicitada pela Administração do SEI na EMBRATUR;

8.10.4. Assim que o cadastro for aprovado, o usuário externo receberá um e-mail com a devida informação e instruções para acesso;

8.10.5. Ao endereço do e-mail pregoeiro2@embratur.com.br deverão ser encaminhadas todas as disponibilizações de acesso aos documentos no SEI/EMBRATUR pertinentes à fase recursal;

8.11. Para fins de análise da admissibilidade do recurso, poderá ser colhida manifestação escrita do setor requisitante e/ou de área competente de acordo com teor da peça recursal.

9. DA REABERTURA DA SESSÃO PÚBLICA

9.1. A sessão pública poderá ser reaberta através das funcionalidades "Reabrir Pregão" ou "Voltar Fase/Ata Complementar" nas seguintes hipóteses:

9.1.1. Reabrir Pregão:

a) Na suspensão temporária administrativa dos trabalhos em função dos seguintes motivos:

- I - horário de almoço;
- II - término do expediente;
- III - exame de conformidade;
- IV - análise de propostas e documentação de habilitação;
- V - realização de diligências;
- VI - Ordem Administrativa de controle interno e/ou externo; e
- VII - outros que vierem a ocorrer na sessão, passíveis de interrupção.

b) Na suspensão temporária em função de ordem emanada pelo poder judiciário.

b1) Quando da condução da fase pública do pregão eletrônico, a partir da sessão inicial de lances até o resultado final do certame, deverá sempre ser avisado, previamente, via sistema (chat), a suspensão temporária dos trabalhos, bem como a data e o horário previstos de reabertura da sessão para o seu prosseguimento, em atendimento aos princípios, em especial os da publicidade e da razoabilidade.

9.1.2. Voltar Fase/Ata Complementar:

a) Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

b) Quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006. Neste caso, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

b1) Todos os licitantes serão convocados através de e-mail disparados pelo Comprasnet para acompanhamento da reabertura da nova sessão.

b2) A convocação por e-mail dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

10. DAS SANÇÕES ADMINISTRATIVAS

10.1. Quem, convocado dentro do prazo de validade da sua proposta, injustificadamente, não assinar o termo de contrato, apresentar documentação falsa, deixar de entregar os documentos exigidos no certame, não mantiver a proposta, cometer fraude fiscal ou comportar-se de modo inidôneo, ficará sujeito às seguintes sanções:

10.1.1. O Licitante quando convocado dentro do prazo de validade da sua proposta injustificadamente, não assinar o termo de contrato, observando-se o direito ao contraditório e ampla defesa, ficará sujeita às penalidades previstas abaixo:

I - multa de 1 % (um por cento) sobre o valor estimado do contrato;

II - suspensão de licitar com a EMBRATUR por 2 (dois) anos.

10.2. A aplicação de sanção fica condicionada ao trânsito de processo administrativo sancionador, que garantirá o contraditório e a ampla defesa.

10.3. A licitante que, durante o transcorrer do certame, apresentar documentação falsa, deixar de entregar os documentos exigidos no certame, não mantiver a proposta, cometer fraude fiscal ou comportar-se de modo inidôneo, observando-se o direito ao contraditório e ampla defesa, ficará sujeita às penalidades previstas abaixo:

I - Suspensão temporária de participação de licitações e de assinar contrato com a EMBRATUR pelo prazo de até 02 (dois) anos:

II - multa de 1 % (um por cento) sobre o valor estimado do contrato;

III - multa de 2 % (dois por cento) sobre o valor estimado do contrato;

a) Suspensão de até 06 (seis), podendo se estender até 24 (vinte e quatro) meses, dependendo da dosimetria da sanção – inciso I:

a1 - Perturbação de qualquer ato na sessão da licitação, seja por mensagens via *chat*, por e-mail e/ou ligações telefônicas;

a2 - Não cumprir os requisitos de habilitação, após a análise de aceitação da proposta, quando o licitante houver declarado que os atendia.

b) Suspensão de 06 (seis), podendo se estender até 24 (vinte e quatro) meses e multa de 1%, dependendo da dosimetria da sanção - incisos I e II:

b1 - Desistir de proposta, salvo por justo motivo decorrente de fato superveniente;

b1.1 – Não encaminhar a proposta no prazo estipulado, após convocação do pregoeiro;

b2 - Solicitar sua própria inabilitação, após a fase de lances, no pregão, salvo por justo motivo decorrente de fato superveniente;

b2.1 – Não encaminhar os documentos de habilitação no prazo estipulado, após convocação do pregoeiro.

b3 - Arguir a inexequibilidade dos próprios preços;

b4 - Não apresentar nova proposta no prazo estabelecido pelo pregoeiro, adaptada ao valor ofertado na fase de lances ou ao obtido mediante negociação;

b5 - Interpor recurso manifestamente protelatório.

c) Suspensão de 24 (vinte e quatro) meses e multa de 2%, dependendo da dosimetria da sanção - Inciso I e III:

c1 - Recusa do licitante vencedor, convocado dentro do prazo de validade de sua proposta, em assinar ou aceitar o contrato, ou retirar o instrumento equivalente.

c2 - Prática de ato inidôneo visando frustrar os objetivos da licitação, a exemplo de conluio entre empresas;

c3 - Apresentação de documentos fraudulentos, adulterados, falsos ou falsificados;

c4 - Fizer declaração falsa, ainda que parcialmente, quanto a qualquer dos requisitos de habilitação exigidos e/ou quanto ao cumprimento de quaisquer das demais exigências previstas no respectivo Edital e seus anexos;

c5 - Cometer fraude fiscal;

c6 - não assinar a Ata de Registro de Preços.

10.4. A dosimetria da sanção deve levar em consideração as razões de fato e de direito apresentadas pela CONTRATADA, a gravidade e abrangência de prejuízos potenciais ou materializados para a EMBRATUR, a reprovabilidade da conduta, devendo respeitar ordem taxativa prevista no artigo 46 do Manual de Licitações e Contratos da EMBRATUR, sendo advertência a mais branda e a suspensão de licitar a mais grave.

10.5. A sanção de multa pode ser aplicada concomitantemente com as demais, sempre que se identificar ganho patrimonial à empresa ou prejuízos significativos à EMBRATUR.

11. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

11.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

11.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

11.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, por meio do endereço eletrônico pregoeiro2@embratur.com.br,

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

11.4.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo agente de contratação, nos autos do processo de licitação.

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

11.6. O pedido de esclarecimento e o de impugnação são procedimentos distintos, atos separados que não podem ser cumulados, não sendo permitida a conversão do pedido de esclarecimento em impugnação ao Edital.

11.7. Caberá ao Pregoeiro, auxiliado pelos responsáveis pela elaboração do Edital e dos anexos, decidir sobre a impugnação no prazo de 3 (três) dias úteis, contados a partir da data de recebimento do pedido de impugnação;

12. DA VISTORIA

12.1. Para o correto dimensionamento e elaboração de sua proposta, a proponente poderá realizar vistoria nas instalações do local de execução dos serviços, acompanhado por colaborador da Gerência de Transformação Digital.

12.1.1. A vistoria poderá ser agendada por meio do telefone: (61) 2023-8730.

12.1.2. A vistoria poderá ser realizada de segunda à sexta-feira, das 09:00h às 12:00h e de 14:00h às 18:00h.

12.2. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital (licitação) ou comunicação entre os potenciais fornecedores (dispensa), estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública, no caso de licitação, ou até o prazo indicado pela Coordenação de Aquisição, no caso de dispensa.

12.3. Para a realização da vistoria, o proponente, ou o seu representante legal, deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para representá-la.

12.4. A não realização da vistoria não poderá servir de justificativa para posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes relativos ao objeto, devendo empresa vencedora assumir os ônus dos serviços decorrentes.

12.5. O proponente deverá declarar que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da contratação, conforme modelo constante no Anexo IV do Termo de Referência.

13. DA APRESENTAÇÃO DA AMOSTRA

13.1. Para efeito de verificação da compatibilidade entre a proposta encaminhada pela proponente e a necessidade de padronização do objeto, a CONTRATANTE, caso não seja possível aferir o atendimento das especificações por meio de folders, fotos do produto ou outro meio idôneo, exigirá a apresentação de amostras.

13.2. Todas as soluções referentes aos itens 1, 2 e 3 do objeto que carecerem de comprovação de atendimento dos requisitos do item 21 do Termo de Referência, farão parte da mesma amostra, e não será concedido tempo adicional devido a quantidade de soluções.

13.3. A licitante deverá enviar por e-mail a relação de representantes que participarão da apresentação da amostra em até 2 (dois) dias após a convocação, sendo no mínimo 2 (dois) e no máximo 6 (seis) representantes simultâneos.

13.4. A demonstração será presencial na sede da Embratur - Agência Brasileira de Promoção Internacional do Turismo, localizada na cidade de Brasília - DF, no Setor Comercial Norte, Quadra 2, Bloco G, Asa Norte. A critério da CONTRATANTE, poderá ser permitido a entrada virtual de algum representante para clarificar questões pontuais que não foram respondidas presencialmente, em que será anotado em ata o motivo da entrada virtual de um representante e a razão pela qual o ponto não foi respondido presencialmente.

13.5. A amostra deverá ser implantada em ambiente controlado da CONTRATANTE em pelo menos 10 ativos e poderá ser manipulada para testes, devendo a licitante ser capaz de demonstrar que a solução consegue atender os requisitos especificados no item 21 do Termo de Referência.

13.6. Todos os custos para a demonstração de amostra será às expensas da licitante.

13.7. A licitante terá 2 (dois) dias úteis após o envio da relação dos representantes para informar os ativos e configurações necessárias para realizar a implantação.

13.8. A CONTRATANTE irá disponibilizar o ambiente solicitado em até 3 (três) dias após a solicitação.

13.9. Após a entrega do ambiente configurado, a Licitante terá até 15 (quinze) dias úteis para demonstrar que as soluções atendem os requisitos do item 21, incluindo o tempo para avaliação de erros e corretos.

13.10. O prazo somente será prorrogado em casos de erros, má configuração ou força maior do lado da CONTRATANTE.

13.11. Os prazos poderão ser antecipados nos casos em que o marco estiver concluído e a LICITANTE assim desejar, devendo formalizar por e-mail que está ciente que a antecipação do prazo não concede prazo adicional no cronograma.

13.12. Em até 2 (dois) dias úteis a CONTRATANTE emitirá o relatório conclusivo da análise da demonstração da amostra.

13.13. O cronograma de forma visual está demonstrado na tabela abaixo.

		Dias (úteis)																									
Marco	Responsável	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
Convocação para demonstração de amostra	Contratante	x																									
Envio relação de representantes	Licitante		x	x																							
Envio de solicitação de ambiente	Licitante				x	x																					
Configuração do ambiente para amostra	Contratante						x	x	x																		
Apresentação de amostra	Licitante									x	x	x	x	x	x	x	x	x	x	x	x	x	x	x			
Relatório de análise de amostra	Contratante																								x	x	

14. DAS DISPOSIÇÕES GERAIS

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

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

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

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

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

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

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

14.8. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

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

14.10. O Edital está disponibilizado, na íntegra, nos endereços eletrônicos <https://www.gov.br/compras/pt-br> e <https://embratur.com.br/editais/>

14.11. As diligências poderão ser realizadas em qualquer fase da licitação, tanto pelo Pregoeiro como pela Autoridade Competente, vedada a inclusão posterior de documento ou informação que deveria constar originariamente da proposta e habilitação.

14.11.1. A vedação acima citada não alcança documento ausente que não foi juntado com os demais comprovantes de habilitação e/ou da proposta, por equívoco ou falha.

14.12. Toda análise do pregoeiro em relação ao julgamento, respeitará os princípios da obtenção da proposta mais vantajosa, da competitividade e do formalismo moderado, mesmo que desconsidere itens deste edital, devidamente justificado.

14.13. Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

14.13.1. O adjudicatário terá o prazo de 05 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar instrumento equivalente, conforme o caso, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

14.14. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

- ANEXO I - TERMO DE REFERÊNCIA
- ANEXO II - CATÁLOGO DE SERVIÇO
- ANEXO III - MODELO DE PROPOSTA COMERCIAL
- ANEXO IV - MODELO DE DECLARAÇÃO DE REALIZAÇÃO OU NÃO DE VISTORIA
- ANEXO V - MINUTA DE TERMO DO CONTRATO

ANEXO I - TERMO DE REFERÊNCIA

1. DO OBJETO

1.1. Contratação de empresa para fornecimento de solução integrada de segurança da informação com fornecimento de licenças e serviços, conforme condições, quantidades e exigências estabelecidas neste instrumento:

ITEM	DESCRIÇÃO/ESPECIFICAÇÃO	Unidade de Medida	Quantidade
1	Solução de gerenciamento de vulnerabilidades de segurança e correções automatizadas	Dispositivo	340
2	Solução de correlação de eventos de segurança e resposta a incidentes	Eventos por segundo - EPS	750
3	Solução de proteção avançada para endpoints	Endpoints	340
4	Serviço de operação, monitoramento e tratamento de eventos de segurança	Unidade	12

- 1.1. A presente contratação adotará como regime de execução por preço unitário.
- 1.2. O prazo de vigência do contrato é de 12 (doze) meses, podendo ser prorrogado por interesse das partes até o limite de 10 (dez) anos.
- 1.3. Este serviço é considerado comum.
- 1.4. O valor estimado da contratação será publico, conforme art. 9º do Manual de Licitações e Contratos da Embratur.

2. DO FUNDAMENTO LEGAL

- 2.1. Lei nº 14.002/20 - Instituição da Agência Brasileira de promoção Internacional do Turismo - EMBRATUR.
- 2.2. Manual de Licitações e Contratos da EMBRATUR - Resolução CDE nº 15, de 08 de maio de 2025.
- 2.3. Lei nº 8.078/90 - Código de Defesa do Consumidor.
- 2.4. Lei nº 13.709/18 - Lei Geral de Proteção de dados (LGPD).

3. DA DESCRIÇÃO DA SOLUÇÃO

- 3.1. A solução como um todo abrange a prestação do serviço de integrado de segurança da informação, incluindo licenças e serviços para a proteção do ambiente e contas da Embratur. Os itens são detalhados conforme a seguir.
- 3.2. Item 1 - Solução de gerenciamento de vulnerabilidades de segurança e correções automatizadas
 - 3.2.1. Esta camada de proteção deve implementar visibilidade contínua de vulnerabilidades de segurança, permitindo o gerenciamento de todo o ciclo de vida delas, desde a descoberta até a remediação.
- 3.3. Item 2 - Solução de correlação de eventos de segurança e resposta a incidentes
 - 3.3.1. Esta camada de proteção deverá atuar diretamente na ingestão de eventos de todas as tecnologias de proteção utilizadas no ambiente, além de priorizar e gerar alertas para consolidar a resposta a incidentes de segurança em uma única visão.
- 3.4. Item 3 - Solução de proteção avançada para endpoints
 - 3.4.1. Esta camada de proteção deve atuar diretamente na detecção, investigação e resposta a ameaças em endpoints, utilizando tecnologias avançadas como monitoramento em tempo real, análise de comportamento e inteligência contra ameaças para mitigar riscos e fornecer visibilidade detalhada sobre as atividades nos dispositivos.
- 3.5. Item 4 - Serviço de operação, monitoramento e tratamento de eventos de segurança
 - 3.5.1. Esta camada de proteção deve assegurar a gestão contínua das operações de segurança do ambiente, incluindo o monitoramento, análise e resposta a incidentes. Deve integrar ferramentas e processos para garantir a eficiência no tratamento de ameaças, suporte à conformidade com normas e regulamentos, e a manutenção de uma postura de segurança proativa e alinhada aos objetivos do negócio.
- 3.6. A descrição completa dos requisitos de cada item estão detalhados no item 21.

3.7. REQUISITOS DA CONTRATAÇÃO

3.7.1. Requisitos de Negócio

3.7.1.1. Manter a confidencialidade, integridade e disponibilidade do ambiente tecnológico.

3.7.1.2. Garantir que a infraestrutura da rede de dados da CONTRATANTE seja escalável e possibilitar um aumento significativo no número de conexões de rede, sem comprometimento da qualidade ou do desempenho devido a ataques cibernético.

3.7.1.3. Garantir a disponibilidade, continuidade e qualidade dos serviços para o cumprimento das atividades finalísticas da CONTRATANTE e, consequentemente, o alcance dos resultados desejados para a sociedade.

3.7.1.4. Garantir os meios adequados para que os processos de segurança da informação possam ser aprimorados através da implementação de recurso de proteção adequados.

3.7.2. Requisitos de Capacitação

3.7.2.1. Será necessário treinamento à equipe local da CONTRATANTE. O treinamento poderá ser realizado na modalidade hands-on e de forma remota, no período das 08:00 às 12:00 e das 14:00 às 18:00h. Deverá ter uma duração mínima de 6 horas para cada item licitado.

3.7.2.2. O treinamento deverá abranger o repasse de informações e conhecimentos necessários referente aos conceitos básicos de administração da solução e o esclarecimento de dúvidas das principais rotinas de configuração, gerenciamento, administração e operação.

3.7.2.3. Não deve haver limites quanto aos participantes da equipe técnica da Contratante para o treinamento.

3.7.3. Requisitos Temporais

3.7.3.1. Os serviços referentes aos Itens 01 a 03 devem ser iniciados no prazo máximo de 60 dias corridos, a contar do recebimento da Ordem de Serviço (OS), emitida pela Contratante. Em circunstâncias excepcionais e devidamente justificadas pelo CONTRATADO, esse prazo poderá ser prorrogado até o limite de igual período, mediante autorização prévia da CONTRATANTE.

3.7.3.2. A entrega e instalação das ferramentas que compõe a solução deverão ocorrer em dias úteis e no horário compreendido entre às 9:00 e 17:00h, e poderá ser agendada em data e hora previamente com a CONTRATANTE por meio do e-mail gtd@embratur.com.br.

3.7.3.3. Os serviços serão prestados em Brasília/DF, na Sede Administrativa da Embratur, situada no Setor Comercial Norte Q 2 Bloco G - Asa Norte, Brasília - DF, 70712-907.

3.7.3.4. Os serviços previstos no Item 04 devem ser iniciados no prazo máximo de 5 (cinco) dias corridos, a contar do recebimento da Ordem de Serviço (OS), emitida pela Contratante. Em circunstâncias excepcionais e devidamente justificadas pelo CONTRATADO, esse prazo poderá ser prorrogado por um período equivalente, mediante autorização prévia da CONTRATANTE.

3.7.3.5. Na contagem dos prazos estabelecidos neste Termo de Referência, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

3.7.3.6. Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos. Ressaltando que serão contados os dias a partir da hora em que ocorrer o incidente até a mesma hora do último dia, conforme os prazos.

3.7.4. Requisitos de Experiência Profissional

3.7.5. Cabe exclusivamente à Contratada estruturar sua equipe de trabalho na dimensão que atenda as condições estabelecidas para a prestação dos serviços.

3.7.6. A CONTRATADA deverá prestar os serviços por meio de profissionais cuja qualificação esteja em conformidade com os requisitos definidos neste documento e legalizados para a prestação dos serviços técnicos.

3.7.7. A CONTRATADA deverá ter na equipe para execução do item 4 pelo menos um profissional com 5 anos de experiência atuando em segurança cibernética ou pelo menos duas das certificações: CompTIA Security+, CISM, NCSP, CCSP, CCNA, CHFI, CySA+, CEH ou certificação equivalente na área de segurança.

3.7.8. Requisitos de Formação de Equipe

3.7.9. A Contratada deverá possuir na equipe profissional do fabricante ou profissional certificado pelo fabricante na solução ofertada.

3.7.10. Requisitos de Projeto e de Implementação

3.7.10.1. Todas as subscrições e licenciamentos previstos e necessários para a execução dos serviços devem ser entregues, instalados e configurados na infraestrutura da CONTRATANTE. Excetua-se as licenças utilizadas para execução de itens de prestação de serviço, em que essas podem ser instaladas na infraestrutura da CONTRATADA.

3.7.10.2. As licenças e subscrições devem possibilitar o uso de 100% das características especificadas neste Termo de Referência, assim como proporcionar suporte e atualização de versão dentro do período de vigência contratual.

3.7.10.3. A CONTRATADA deverá apresentar um Plano de Projeto com, no mínimo, os seguintes conteúdos: Definição do escopo; Definição de quais tarefas deverão ser realizadas para implementação e configuração dos itens; Cronograma de Implantação; e Plano de arquitetura e desenho da solução. O Plano de Projeto deverá ser aprovada pela CONTRATANTE.

3.7.10.4. A execução dos serviços contratados deve ser planejada de modo que não cause interrupções e paralisações não programadas, ou qualquer outro tipo de transtorno ao correto funcionamento do ambiente operacional da CONTRANTE.

3.7.10.5. Caso as atividades demandem interrupções no ambiente de TIC da CONTRATADA, as atividades deverão ser realizadas durante janela de manutenção agendada previamente, em horários que não comprometam o funcionamento das atividades do órgão, inclusive aos sábados, domingos e feriados.

3.7.10.6. Será de responsabilidade da CONTRATADA a correção dos problemas técnicos decorrentes de erros identificados na execução dos serviços, sejam operacionais ou por problemas de mau funcionamento das ferramentas, responsabilizando-se por todos os procedimentos e custos envolvidos para resolução, sob pena de incorrer em sanções legais cabíveis, sendo garantida a ampla defesa, exceto quando seja comprovado que o problema se deu devido a mau funcionamento de componentes já existentes no ambiente da CONTRATANTE que sejam pré-requisitos para o funcionamento dos objetos contratados.

3.7.11. Requisitos de Implantação

3.7.11.1. Os serviços deverão observar integralmente os requisitos de Projeto e Implementação previstos neste Termo de Referência.

3.7.11.2. A CONTRATADA será responsável pela implementação de todos os objetos de forma a permitir que todos os itens estejam 100% operacionais, cumprindo todos os passos presentes no plano de projeto definido.

3.7.11.3. Deverão ser fornecidos todos os componentes necessários para garantia de funcionamento de todos os componentes presentes no Termo de Referência.

- 3.7.11.4. A contratada deverá ter profissionais certificados com certificações técnicas em toda a solução ofertada.
- 3.7.11.5. A empresa que realizar a implantação deverá ter técnicos certificados pelo fabricante.
- 3.7.12. **Requisitos de Garantia, Manutenção e Assistência Técnica**
- 3.7.12.1. A garantia dos serviços devem ser compatíveis e respeitar o período de vigência contratual.
- 3.7.12.2. A garantia deverá abranger todas as atualizações de versões de software utilizados para o fornecimento dos serviços.
- 3.7.13. **Requisitos de Metodologia de Trabalho**
- 3.7.13.1. A execução dos serviços está condicionada ao recebimento pela CONTRATADA de Ordem de Serviço (OS) emitida pela CONTRATANTE.
- 3.7.13.2. A OS indicará o serviço, a quantidade e a localidade na qual deverão ser prestados.
- 3.7.13.3. A CONTRATADA deve fornecer meios para contato e registro de ocorrências com funcionamento 24 horas por dia e 7 dias por semana de maneira eletrônica.
- 3.7.13.4. A execução do serviço deve ser acompanhada pela CONTRATADA, que dará ciência de eventuais acontecimentos à CONTRATANTE.
- 3.7.14. **Requisitos de Segurança da Informação e Privacidade**
- 3.7.15. A contratada deverá se submeter à Resolução Direx nº 51/2024, que institui a Política de Segurança da Informação (POSIC), ou a suas atualizações.

4. DA JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

- 4.1. A Embratur, ciente da importância da segurança dos dados institucionais, reconhece as limitações e deficiências em relação a sua gestão de segurança das suas informações. Atualmente, as soluções implantadas estão desatualizadas e sem licenciamento, também não há equipe o suficiente para executar todas as ações de segurança necessárias. Dessa forma, a presente contratação é motivada pela necessidade de implantação de uma solução integrada para o gerenciamento de vulnerabilidades e visibilidade de riscos de segurança da informação no âmbito da Embratur.
- 4.2. O cenário atual relativo à segurança da informação é complexo e sensível, isso se deve a digitalização acelerada dos processos, o que acelerou também o surgimento de novas ameaças. Enquanto a tecnologia evolui para facilitar as atividades cotidianas, agentes mal-intencionados exploram brechas, muitas vezes relacionadas a falhas não identificadas em serviços de TI. Esse cenário ressalta a necessidade de soluções robustas e integradas para proteger organizações contra os crescentes riscos cibernéticos.
- 4.3. Atualmente, se o cibercrime fosse uma economia, seria a 3ª maior economia do mundo (dados de 2021), o que demonstra como esse é um setor altamente lucrativo e financiado. Especialistas afirmam que a questão não é mais "se" ocorrerá um ataque, mas "quando" e "como". Isso se deve, principalmente, ao aumento da dependência de tecnologias digitais, tanto no setor privado quanto no público, tornando os ataques altamente lucrativos para criminosos virtuais.
- 4.4. Observando o Painel de Incidentes Cibernéticos de 2024 do Security Report disponível em <https://www.securityreport.com.br/email/InfoSR2024.html>, podemos visualizar a quantidade de ataques bem-sucedidos nas mais diversas empresas, o que representa prejuízos significativos causados por invasões cibernéticas.
- 4.5. A falta de uma solução de segurança compatível com os riscos da Embratur, pode implicar em paralisação das atividades, perda de dados, falta de monitoramento adequado, passividade nas ações de segurança em de perda de dados e descontinuidade de negócio, podendo comprometer a imagem institucional da Embratur.
- 4.6. A Resolução Direx nº 51/2024 estabelece a Política de Segurança da Informação da Embratur, em que são definidas as responsabilidades quanto a segurança da informação no âmbito da instituição, compete à GTD a implantar uma arquitetura de segurança para proteger as informações, bem como monitorar as ações que possam ir contra a política, o que é realizado de forma precária no momento atual devido falta de ferramentas adequadas.
- 4.7. Cabe destacar que a fragmentação de ferramentas de segurança dificultam a gestão integrada e rápida resposta a incidentes, por isso, esse projeto propõe uma integração de soluções.
- 4.8. Caso o projeto não seja aprovado, a empresa estará vulnerável a interrupções operacionais devido a ataques cibernéticos; risco de perda de dados sensíveis, risco de perda de confiança do mercado e clientes, ou ainda, sofrer penalidades severas por descumprimento de regulamentos de proteção de dados.
- 4.9. Em suma, considerando os riscos e necessidades supramencionados, a contratação de uma solução integrada de segurança com o fornecimento de licenças e serviços é fundamental para a Embratur realizar gestão adequada de segurança da informação, atendendo suas políticas internas e imposições legais, observando a vantajosidade financeira para a Embratur.

5. DO MODELO DE EXECUÇÃO DO OBJETO

- 5.1. O prazo da CONTRATADA se preparar para receber as demandas será de 30 dias corridos, com início imediato à data de assinatura do contrato. Decorrido este período a CONTRATANTE emitirá a Ordem de Serviços que servirá de autorização para o início do projeto. O prazo de preparação faz parte do prazo de vigência do contrato e não faz parte do prazo de realização do projeto.
- 5.2. **Reunião inicial**
- 5.2.1. Após a assinatura do contrato, será realizada a reunião inicial, a ser registrada em ata, convocada pelo gestor do contrato, com a participação do fiscal requisitante, da CONTRATADA e dos demais interessados por ele identificados, cuja pauta observará, pelo menos:
- 5.2.2. presença do representante legal da CONTRATADA, que apresentará o preposto dessa;
- 5.2.3. entrega, por parte da CONTRATADA, do Termo de Compromisso, conforme modelo constante do anexo III, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da CONTRATADA; e TERMO DE CIÊNCIA, conforme modelo constante do anexo V, a ser assinado por todos os empregados da CONTRATADA diretamente envolvidos na contratação;
- 5.2.4. esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato.
- 5.3. **Encaminhamento formal de demandas**
- 5.3.1. O encaminhamento formal de demandas, a cargo do gestor do contrato, ocorrerá por meio de Ordem de Serviço - OS.
- 5.4. **Local de execução dos serviços**
- 5.4.1. Os serviços deverão ser executados de forma remota ou, caso seja necessário, nas dependências da Embratur, localizada na Asa Norte, Brasília - DF, ou em local a ser indicado por essa Agência, na mesma cidade de sua sede, em horário a ser definido pela CONTRATANTE.
- 5.5. **Mecanismos formais de comunicação**

5.5.1. Toda a comunicação entre a CONTRATANTE e a CONTRATADA deverá ser sempre formal como regra, exceto em casos excepcionais que justifiquem outro canal de comunicação.

5.5.2. Os seguintes instrumentos formais poderão ser utilizados para a troca de informações entre a CONTRATANTE e a CONTRATADA: ata de reunião, ofício, e-mail, ordem de serviço ou fornecimento de bens e chamado técnico.

5.6. Manutenção de sigilo e normas de segurança

5.6.1. A CONTRATADA 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.

5.6.2. O Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e Termo de Ciência, a ser assinado por todos os empregados da CONTRATADA diretamente envolvidos na contratação, encontram-se no anexo IV - TERMO DE COMPROMISSO e anexo V - TERMO DE CIÊNCIA.

5.6.3. No caso de substituição ou inclusão de empregados da CONTRATADA, o preposto deverá entregar ao fiscal administrativo do contrato os TERMOS DE CIÊNCIA assinados pelos novos empregados envolvidos na execução dos serviços contratados.

5.6.4. A atuação da CONTRATADA deverá observar a Resolução nº 51/2024 - Política de Segurança da Informação e Comunicação e suas atualizações.

5.7. Modelo de Execução do Serviço de Licenciamento

5.7.1. Os serviços de licenciamento correspondente aos itens 1, 2 e 3 serão solicitados por meio de Ordem de Serviço anual, que especificará as quantidades solicitadas, que servirá como autorização para prestação de serviço.

5.7.2. As licenças deverão ser implantadas no ambiente seguindo o cronograma pactuado entre as partes, não podendo ser maior do que 90 (noventa) dias após o recebimento da Ordem de Serviço.

5.7.3. O pagamento referente ao uso das licenças somente se iniciará após a efetiva implantação das licenças e liberação para o uso da CONTRATANTE, nas quantidades especificadas na Ordem de Serviço.

5.7.4. Mensalmente deverá ser fornecido o Relatório de Situacional, minimamente com informações de tempo de disponibilidade das licenças, licenças em uso, licenças disponíveis e chamados para fabricante abertos e resolvidos.

5.7.5. Nos anos subsequentes de contrato, em que as licenças já estarão implantadas, a liberação das licenças deverá ser iniciada em até 5 (cinco) dias úteis, contados a partir do recebimento da Ordem de Serviço pela CONTRATADA.

5.7.6. Modelo de Execução de Serviço de Segurança

5.7.7. O Item 4 corresponde aos serviços de segurança, que será solicitado por meio de Ordem de Serviço mensal, que servirá como autorização para prestação de serviço.

5.7.8. Para o faturamento mensal dos itens, a contratada deverá emitir e apresentar o "Relatório Mensal de Acompanhamento do Contrato". Esse instrumento de controle deve possuir, no mínimo, a apuração dos indicadores de níveis de serviços, ocorrências e demais informações necessárias à correta identificação do valor mensal a ser pago referente à execução das Ordens de Serviços. Também devem constar as informações detalhadas a seguir:

5.7.8.1. Registro de todas as atividades realizadas para cada solução de proteção envolvida neste certame;

5.7.8.2. Registro de indicadores referentes a cada camada de proteção envolvida;

5.7.8.3. Sumários de quantidade de logs ingeridos para cada fonte integrada ao SIEM;

5.7.8.4. Sumário de todos os incidentes de segurança registrados seguido de quais ações foram tomadas pelo time de resposta;

5.7.8.5. Sumário de injeções de inteligência cibernéticas aplicadas nos eventos de segurança registrados;

5.7.8.6. Sumário de todas as vulnerabilidades de segurança encontradas no período do relatório;

5.7.8.7. Estatísticas de todas as vulnerabilidades que foram corrigidas no período;

5.7.8.8. Resultados completos de testes de segurança direcionados a técnicas de movimentação lateral na rede;

5.7.8.9. Resultados completos de testes de segurança direcionados a política de navegação Web e firewall;

5.7.8.10. Resultados completos de testes de segurança direcionados a solução de proteção de e-mail corporativo;

5.7.8.11. Resultados dos testes de campanhas de phishing realizadas com os usuários da CONTRATANTE;

5.7.8.12. Resultados completos de testes de segurança direcionados a solução de WAF em uso pela CONTRATANTE; e

5.7.8.13. Resultados completos referentes ao nível de maturidade de segurança da CONTRATANTE baseado nos testes de segurança realizados.

5.7.9. O relatório Mensal de Acompanhamento do Contrato poderá ser adaptado, desde que pactuado entre as partes sobre as novas informações.

5.7.10. O prazo para conclusão deverá observar o estabelecido na Ordem de Serviço.

5.7.11. Pelo menos 1 (um) profissional deverá ser alocado nas dependências da CONTRATANTE em horário comercial.

5.7.12. Por se tratar de execução de preço fixo mensal, a equipe de fiscalização poderá fiscalizar o cumprimento das obrigações trabalhistas, sociais e previdenciárias dos profissionais alocados, conforme:

5.7.12.1. No início da execução dos serviços contratados;

5.7.12.2. Durante a execução das Ordens de Serviços;

5.7.12.3. Quando da rescisão do contrato.

6. DA VISTORIA

6.1. Para o correto dimensionamento e elaboração de sua proposta, a proponente poderá realizar vistoria nas instalações do local de execução dos serviços, acompanhado por colaborador da Gerência de Transformação Digital.

6.1.1. A vistoria poderá ser agendada por meio do telefone: (61) 2023-8730.

6.1.2. A vistoria poderá ser realizada de segunda à sexta-feira, das 09:00h às 12:00h e de 14:00h às 18:00h.

6.2. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital (licitação) ou comunicação entre os potenciais fornecedores (dispensa), estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública, no caso de licitação, ou até o prazo indicado pela Coordenação de Aquisição, no caso de dispensa.

6.3. Para a realização da vistoria, o proponente, ou o seu representante legal, deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para representá-la.

6.4. A não realização da vistoria não poderá servir de justificativa para posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes relativos ao objeto, devendo empresa vencedora assumir os ônus dos serviços decorrentes.

6.5. O proponente deverá declarar que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da contratação, conforme modelo constante no Anexo III do Termo de Referência.

7. DAS OBRIGAÇÕES DA CONTRATANTE

7.1. São obrigações da CONTRATANTE:

7.1.1. exigir o recebimento do objeto no prazo e condições estabelecidas no Termo de Referência;

7.1.2. exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;

7.1.3. exercer o acompanhamento e a fiscalização dos serviços, por meio de colaborador especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

7.1.4. notificar a CONTRATADA, por escrito, sobre a ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se de que as soluções por ela propostas sejam as mais adequadas;

7.1.5. efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da CONTRATADA, no que couber;

7.1.6. pagar à CONTRATADA o valor resultante da prestação do serviço, no prazo e condições estabelecidas no Termo de Referência;

7.2. A EMBRATUR não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do objeto do Termo de Referência, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

8. DAS OBRIGAÇÕES DA CONTRATADA

8.1. São obrigações da CONTRATADA:

8.1.1. executar os serviços conforme especificações do Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais (ou da Ordem de Serviços), além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade exigidas;

8.1.2. reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal da contratação, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

8.1.3. responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à EMBRATUR, devendo ressarcir imediatamente a CONTRATANTE em sua integralidade;

8.1.3.1. em caso de ocorrência do previsto no item 8.1.3, a CONTRATANTE ficará autorizada a descontar da garantia exigida no item 14.1 do Termo de Referência, ou dos pagamentos devidos à CONTRATADA, o valor correspondente aos danos sofridos;

8.1.4. utilizar empregados habilitados e com conhecimentos adequados dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

8.1.5. prestar todo esclarecimento ou informação solicitada pela CONTRATANTE ou por seus prepostos, garantindo-lhes o acesso aos documentos relativos à execução do serviço;

8.1.6. garantir o acesso da CONTRATANTE, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do serviço;

8.1.7. submeter previamente, por escrito, à CONTRATANTE, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações deste Termo de Referência (ou do memorial descritivo);

8.1.8. prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação;

8.1.9. manter, durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação;

8.1.10. assumir como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

8.1.11. indicar preposto para representá-la durante a vigência do contrato;

8.1.12. responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990).

9. DA SUBCONTRATAÇÃO

9.1. Não será admitida a subcontratação do objeto do Termo de Referência.

10. DO CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

10.1. O acompanhamento e a fiscalização da execução do contrato/serviço consistem na verificação da conformidade da prestação dos serviços, dos materiais, técnicas e equipamentos empregados, de forma a assegurar o perfeito cumprimento do ajuste, que será exercido por um colaborador da CONTRATANTE.

10.2. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos no Termo de Referência.

10.3. A fiscalização do contrato/serviço, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação à produtividade efetivamente realizada.

10.4. O representante da EMBRATUR anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato/serviço, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das faltas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

10.5. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da CONTRATANTE ou de seus agentes, gestores e fiscais.

10.6. Será observado os indicadores a seguir, afim de se verificar o atendimento de nível mínimo de serviço. As métricas previstas para os Acordo de Nível de Serviço são definidas de forma a servir de insumo para o processo de manutenção da qualidade e aperfeiçoamento do serviço prestado pela CONTRATADA. Estas métricas deverão ser apuradas pela CONTRATADA e reportadas mensalmente à CONTRATANTE.

10.6.1. Indicador Quantidade de chamados (requisição e incidentes) atendidos dentro do prazo

10.6.1.1. De maneira a uniformizar o entendimento quanto a classificação para incidentes e requisições de serviço de segurança da Informação, define-se os níveis de criticidade como:

Nível de Criticidade	Impacto/ Descrição	Início de Atendimento	Prazo para solução
EMERGENCIAL	- Algum tipo de ataque que gerou indisponibilidade em servidores e sistemas críticos, afetando um ou mais usuários; - Infecção ou paralisação generalizada devido a ransomware ou algum outro tipo de malware; - Roubo ou vazamento de dados devido a falha humana ou técnica; - Algum tipo de impacto ou risco grave a empresa ou a equipe de Segurança da Informação; - Quando o problema\incidente é definido com o nível de criticidade "EMERGENCIAL"; *Para impacto de nível emergencial é necessário um profissional no mínimo Sênior	Em até 1 hora corrida	Em até 4 horas corridas
ALTA	- Servidor de produção ou sistema crítico está apresentando instabilidade, degradação ou sofrendo ataques recorrentes q podem acarretar uma exploração ou vazamento de dados; - Alarmes de nível ALTA identificados por ferramentas de SIEM ou ferramenta de segurança que podem ser um falso positivo e necessitam de uma análise para validação; - Quando o problema\incidente é definido com o nível de criticidade "ALTA";	Em até 2 horas corridas	Em até 8 horas corridas
MÉDIA	- Nenhum serviço crítico está envolvido e não existe risco de perda de dados; - Alarmes de nível MÉDIO identificados por ferramentas de SIEM ou ferramenta de segurança que podem ser um falso positivo e necessitam de uma análise para validação; - Quando o problema\incidente é definido com o nível de criticidade "MÉDIA".	Em até 4 horas úteis	Em até 24 horas úteis
BAIXA	- Dúvidas ou apoio à implementação; - Mudanças planejadas; - Novas implementações; - Sugestões de novos recursos ou aprimoramento do Software; - Alarmes de nível BAIXA identificados por ferramentas de SIEM ou ferramenta de segurança que podem ser um falso positivo e necessitam de uma análise para validação; - Evidências de um bloqueio ou tratativa automatizada; - Quando o problema\incidente é definido com o nível de criticidade "BAIXA"	Em até 9 horas úteis	Em até 72 horas úteis.

10.6.1.2. Para efeito desta contratação, estabelecem-se os seguintes níveis mínimos de serviços para a resposta e solução das requisições de serviço e incidentes. Os serviços serão medidos com base em indicadores e níveis mínimos de serviços, vinculados a fórmulas de cálculo específicas, deverão ser executados pela CONTRATADA, e apurados mensalmente, de modo a alcançar as respectivas metas exigidas, conforme tabela a seguir. Os níveis de serviço serão mensurados de forma automatizada, por meio de ferramenta de uso e gestão da CONTRATANTE, e não poderão ser manipulados pela CONTRATADA;

10.6.1.3. Após observadas as características do chamado, será aplicado o Indicador IQC para aferir se os chamados foram atendidos dentro do prazo.

IQC - Indicador Quantidade de chamados (requisição e incidentes) atendidos dentro do prazo

Finalidade: Apurar a quantidade de chamados atendidos dentro do prazo estabelecido	
Meta a cumprir: 90%	
Instrumento de medição: Ferramenta de registro de chamados	
Periodicidade: Mensal	
Mecanismo de cálculo (%): (Total de chamados atendidos dentro do prazo / Total de chamados abertos no período) x 100	
Faixa no ajuste no pagamento:	
De 80% - 89%	1%
De 70% - 79%	3%
Abaixo de 69%	5%

10.6.2. **Indicador eficácia no tratamento de chamados (requisições, incidentes e incidentes de segurança)**

10.6.2.1. Deve ser considerado a eficácia do tratamento dos chamados, ou seja, se os chamados não estão sendo reabertos após a resolução.

IET - Indicador eficácia no tratamento de chamados (requisições, incidentes e incidentes de segurança)	
Finalidade: Apurar a eficácia do contratado na resolução de chamados	
Meta a cumprir: 80%	
Instrumento de medição: Ferramenta de registro de chamados	
Periodicidade: Mensal	
Mecanismo de cálculo (%): (Total de chamados atendidos - Total de chamados reaberto) / (Total de chamados atendidos) x 100	
Consideram-se atendidos os chamados fechados com solução, não devendo ser considerados os chamados fechados sem solução.	
Faixa no ajuste no pagamento:	
De 70% - 79%	1%
De 60% - 69%	3%
Abaixo de 59%	5%

10.6.3. **Indicador de vinculação da resolução de requisições de serviço à base de conhecimento**

10.6.3.1. A base de conhecimento deve ser vinculada a resolução do chamado, permitindo que a CONTRATANTE esteja no domínio do conhecimento adquirido durante a execução do contrato, dessa forma, deve-se observar o Indicador abaixo.

IBC - Indicador de vinculação da resolução de requisições de serviço à base de conhecimento	
Finalidade: Aferir a cobertura dos padrões de atendimento registrados na base de conhecimento	
Meta a cumprir: 95%	
Instrumento de medição: Ferramenta de registro de chamados	
Periodicidade: Mensal	
Mecanismo de cálculo (%): (Total de requisições com resolução vinculada à base de conhecimento / Total de requisições resolvidas) x 100	
Faixa no ajuste no pagamento:	
De 85% - 94%	1%
De 70% - 84%	3%
Abaixo de 69%	5%

10.6.4. **Indicador de Disponibilidade das Soluções Contratadas**

10.6.4.1. Será aferida o índice de disponibilidade dos serviços ofertados pela CONTRATADA. Será desconsiderado do indicador as situações em que a disponibilidade do serviço não dependa da CONTRATADA, como soluções implantadas on premise na CONTRATANTE.

IDS - Indicador de Disponibilidade das Soluções oferecidas	
Finalidade: Apurar disponibilidade das soluções ofertadas no contrato	
Meta a cumprir: 97%	
Instrumento de medição: Ferramenta monitoramento de disponibilidade	
Periodicidade: Mensal	
Mecanismo de cálculo (%): Total de tempo com disponibilidade no mês / total de tempo no mês X 100	
Faixa no ajuste no pagamento:	
De 90% - 96%	1%
De 80% - 89%	3%
Abaixo de 79%	5%

10.6.4.2. **Indicador de Aderência ao Serviço Contratado**

10.6.5. A aferição da execução contratual para fins de pagamento considerará os critérios do quadro a seguir, em que serão aplicadas as referidas pontuações para efeito de glosa, no caso de a CONTRATADA.

10.6.6. Observa-se que será aplicada glosa de 0,5% a cada 15 pontos, limitando-se a glosa decorrente da análise do quadro a seguir à aplicação do valor máximo de 15% do valor mensal previsto (soma dos itens).

IAS - Indicador de Aderência ao Serviço Contratado

Item	Descrição	Referência	Glosa por inadimplemento
1	Finalizar a requisição de serviço ou incidente sem a devida resolução ou sem realizar os testes necessários para aferir a efetiva resolução	Por ocorrência	10 pontos
2	Finalizar uma requisição de serviço sem documentar os procedimentos executados para atendimento da solicitação	Por ocorrência	5 pontos
3	Finalizar um incidente sem documentar a causa, a solução de contorno (se houver) ou os procedimentos adotados para solução	Por ocorrência	5 pontos
4	Finalizar um problema sem documentar a investigação realizada, a causa-raiz ou a solução aplicada	Por ocorrência	5 pontos
5	Fraudar, manipular ou descaracterizar indicadores/metadados de níveis de serviço por quaisquer subterfúgios, por indicador/meta de nível de serviço manipulado	Por ocorrência	30 pontos
6	Manter profissionais sem formalização ou sem a qualificação exigida para executar serviços contratados, ainda que em casos de substituição temporária	Por ocorrência	30 pontos
7	Causar qualquer indisponibilidade dos serviços do CONTRATANTE por motivo de imperícia ou imprudência na execução das atividades contratuais	Por ocorrência	30 pontos
8	Utilizar indevidamente os recursos de TI (acessos indevidos, utilização para fins particulares)	Por ocorrência	30 pontos
9	Realizar mudanças de configuração nas soluções de segurança sem autorização CONTRATANTE	Por ocorrência	15 pontos
10	Deixar de cumprir ou implementar as rotinas em conformidade com a Política de Segurança ou determinações da equipe de fiscalização do contrato	Por ocorrência	10 pontos
11	Deixar de cumprir ou implementar as rotinas em conformidade com os Planos de Gerenciamento de Incidente de Disponibilidade, de Continuidade e de Recuperação de Desastres das soluções de segurança	Por ocorrência	10 pontos
12	Deixar de executar testes de continuidade de cada solução de segurança da informação em alta disponibilidade, no mínimo, a cada 6 (seis) meses	Por ocorrência	10 pontos
13	Deixar de atuar proativamente em caso de identificação de situação de desconformidade com boas práticas de segurança	Por ocorrência	10 pontos
14	Apresentar mensalmente plano de tratamento de vulnerabilidades, indicando as ações mais efetivas para redução dos riscos	Por ocorrência	20 pontos
15	Deixar de notificar sobre ocorrências recorrentes	Por ocorrência	5 pontos
16	Deixar de emitir o relatório de incidente em até 3 (três) dias úteis após o encerramento do incidente	Por ocorrência	30 pontos
17	Deixar de analisar a viabilidade e o impacto da instalação de novas soluções ou correções	Por ocorrência	20 pontos
18	Deixar de apresentar mensalmente proposta de melhorias no ambiente	Por ocorrência	5 pontos
19	Deixar de cumprir quaisquer obrigações estabelecidas no Termo de	Por ocorrência	15 pontos

	Referência, contrato e apêndices, ainda que não previstas nesta tabela, após reincidência formalmente notificada pela CONTRATANTE		
--	---	--	--

10.6.7. As retenções ou glosas no pagamento serão aplicadas quando a CONTRATADA:

10.6.8. Não atingir os valores mínimos aceitáveis fixados nos Critérios de Aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

10.6.9. Deixar de utilizar materiais e recursos humanos necessários e suficientes para fornecimento da Solução de Tecnologia da Informação, ou utilizá-los com qualidade ou quantidade inferior à demandada.

11. DO RECEBIMENTO E ACEITAÇÃO DO OBJETO

11.1. Após a fiscalização dos serviços prestados, o gestor ou, na ausência deste, o gestor substituto indicará à CONTRATADA que os serviços estão em conformidade com as especificações do Termo de Referência e que está autorizada a emissão da Nota Fiscal/Fatura, sendo que o recebimento se materializará com o atesto da unidade requisitante.

11.2. A indicação de conformidade da execução do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do serviço, ou, em qualquer época, das garantias concedidas e das responsabilidades assumidas (em contrato ou Ordem de Serviço) e por força das disposições legais em vigor.

11.3. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do serviço, às custas da CONTRATADA, sem prejuízo da aplicação de penalidades.

12. DO PAGAMENTO

12.1. O pagamento referente aos itens 1, 2 e 3 do objeto será realizado em sua totalidade após a implantação e entrega das licenças de forma funcional para o período de 12 (doze) meses.

12.2. Entende-se que a licença estará funcional quando:

12.2.1. item 1 - quando todos os ativos do escopo do item estiverem com as licenças aplicadas e for possível visualizar o painel com os ativos e dados de vulnerabilidade;

12.2.2. item 2 - quando o correlacionador estiver recebendo dados de pelo menos 3 ativos enviando logs para o correlacionador e 5 regras criadas e aplicadas;

12.2.3. item 3 - quando todos os ativos do escopo do item estiverem com as licenças aplicadas e for possível visualizar no painel a gestão de todos os ativos com licença e seus respectivos status;

12.3. O pagamento referente ao item 4 será por preço fixo mensal de acordo com a sua data de abertura e conclusão.

12.4. O pagamento somente será autorizado depois de efetuado o "ATESTO" pelo gestor ou, na sua ausência, pelo gestor Substituto do contrato/da Ordem de Serviço na nota fiscal apresentada.

12.5. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à demanda, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

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

12.7. Antes do pagamento à CONTRATADA, será realizada consulta aos documentos comprobatórios da regularidade fiscal e trabalhista, quando for o caso.

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

12.9. Após o atendimento de todas as exigências supramencionadas e aguardado o trâmite processual da EMBRATUR, a Coordenação Financeira deverá efetuar o pagamento **em até 10 (dez) dias úteis**, após o recebimento do referido processo.

12.9.1. Nos casos de eventuais atrasos de pagamento conforme prazo indicado no item 12.6, desde que a CONTRATADA não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela CONTRATANTE, será calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX)	$I = \left(\frac{6}{365} \right)$	I = 0,00016438 TX = Percentual da taxa anual = 6%
----------	------------------------------------	--

13. DO REAJUSTE

13.1. Os preços inicialmente contratados são fixos e irredutíveis no prazo de 1 (um) ano contado da data do início da vigência do contrato.

13.2. Dentro do prazo de vigência do contrato e mediante solicitação da CONTRATADA, os preços contratados poderão sofrer reajuste após o interregno de 1 (um) ano, aplicando-se o **Índice de Custos de Tecnologia da Informação - ICTI** exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

13.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de 1 (um) ano será contado a partir dos efeitos financeiros do último reajuste.

13.4. No caso de atraso ou não divulgação do índice de reajustamento, a CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

- 13.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.
- 13.6. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.
- 13.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de Termo Aditivo.
- 13.8. Fica garantida a possibilidade de reequilíbrio econômico-financeiro dos valores contratuais, que deverá prever os meios de prova das novas definições de mercado que ensejarem o desequilíbrio econômico do contrato, corroborados por planilhas de custos.

14. DA GARANTIA CONTRATUAL

- 14.1. A CONTRATADA, no prazo de **10 (dez) dias** após a assinatura do Termo de Contrato, prestará garantia no valor correspondente a 5% (cinco por cento) do valor do contrato, que será liberada de acordo com as condições previstas no Termo de Referência.
- 14.1.1. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,5% (meio por cento) do valor do contrato por dia de atraso, até o máximo de 2% (dois por cento);
- 14.1.2. O atraso superior a 30 (trinta) dias autoriza a Agência a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme Manual de Licitações e Contratos da EMBRATUR.
- 14.1.3. A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 (noventa) dias posterior ao término da vigência contratual.
- 14.1.4. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:
- 14.1.5. prejuízos advindos do não cumprimento do objeto do contrato;
- 14.1.6. prejuízos diretos causados à Agência decorrentes de culpa ou dolo durante a execução do contrato;
- 14.1.7. multas moratórias e punitivas aplicadas pela Agência à CONTRATADA; e
- 14.1.8. obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA, quando couber.
- 14.2. Caberá à CONTRATADA optar por uma das seguintes modalidades de garantia:
- 14.2.1. caução em dinheiro; ou
- 14.2.2. seguro-garantia; ou
- 14.2.3. fiança bancária.
- 14.3. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação, inclusive quanto aos prazos previstos no item 14.1.
- 14.4. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de **10 (dez) dias úteis**, contados a partir da data em que for notificada.
- 14.5. A CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.
- 14.6. Será considerada extinta a garantia:
- 14.6.1. com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato;
- 14.6.2. ao fim do prazo de 90 (noventa) dias após o término da vigência, caso a CONTRATANTE não comunique a ocorrência de sinistros.

15. DAS SANÇÕES ADMINISTRATIVAS

- 15.1. Pela inexecução total ou parcial do objeto desta contratação, a EMBRATUR pode aplicar à CONTRATADA as seguintes sanções:
- 15.1.1. advertência;
- 15.1.2. multas:
- 15.1.3. de 0,5% (meio por cento) do valor total da Ordem de Serviços, na qual tenha sido entregue ou realizado com atraso, qualquer produto ou serviço a ele destinado, aplicável por dia de atraso, entendendo-se como atraso, o não cumprimento do prazo de realização do serviço;
- 15.1.4. de 0,5% (meio por cento) do valor total da Ordem de Serviços por infração a qualquer de suas cláusulas ou condições, que não as especificadas no subitem anterior, aplicada em dobro na reincidência.
- 15.1.5. suspensão de licitar com a EMBRATUR por até 2 (dois) anos.
- 15.2. A aplicação de sanção fica condicionada ao trânsito de processo administrativo sancionador, que garantirá o contraditório e a ampla defesa.
- 15.3. A dosimetria da sanção deve levar em consideração as razões de fato e de direito apresentadas pela CONTRATADA, a gravidade e a abrangência de prejuízos potenciais ou materializados para a EMBRATUR e a reprovabilidade da conduta, devendo respeitar ordem taxativa prevista no item 15.1, sendo advertência a mais branda e a suspensão de licitar a mais grave.
- 15.4. A sanção de multa pode ser aplicada concomitantemente com as demais, sempre que se identificar ganho patrimonial à CONTRATADA ou prejuízos significativos à EMBRATUR.
- 15.5. No processo de aplicação de penalidades, prevalecerão as normas e procedimentos do Manual de Licitações e Contratos EMBRATUR.

16. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

- 16.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO.
- 16.2. O critério de julgamento da proposta é o menor preço global.
- 16.3. O critério de qualificação técnica a ser atendido pelo fornecedor será a apresentação de:
- 16.3.1. Declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação;
- 16.3.2. Atestado de Capacidade Técnica (ACT), em nome da licitante, emitido por pessoas jurídicas de direito público ou privado, que comprove a execução em serviços de complexidade tecnológica e operacional similares ou superior ao objeto do termo de referência, ou com o item pertinente;

16.3.3. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

16.3.3.1. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

16.3.3.2. Os atestados devem se referir a contratos já concluídos ou já decorrido no mínimo um ano do início de sua execução, exceto se houver sido firmado para ser executado em prazo inferior devendo ser comprovado por meio do contrato e a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente; e

16.3.3.3. Se referir a fornecimentos de soluções e serviços de cibersegurança compatíveis e similares com o objeto contido neste Termo de Referência. Considera-se como compatível:

16.3.3.4. Comprovação de execução contrato com quantidades de no mínimo 50% do item 1, 2 e 3;

16.3.3.5. Comprovação de execução de contrato com objeto compatível ao item 4, devendo a empresa comprar minimamente operação e sustentação de Proteção de endpoint, SIEM e SOAR. Será admitido para fins de comprovação de aptidão técnica atestados com unidade fixa mensal ou métricas equivalentes ao objeto, tais como HST (Hora de Serviço Técnico), HH (Hora-Homem), UST (Unidade de Serviço Técnico), sendo que ao usar métricas baseadas em Horas, deverá comprovar minimamente a execução de 1.050 horas, equivalente à 50% do item.

16.3.3.6. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

16.3.3.7. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

16.3.3.8. A CONTRATANTE, a qualquer tempo e a seu critério, poderá efetuar diligências acerca de quaisquer documentos ou dados apresentados, solicitando das proponentes e das pessoas jurídicas referidas na documentação apresentada, esclarecimentos e/ou informações complementares, sejam estes em forma de apresentação de portfólios, prospectos, visitas técnicas, amostras do objeto cotado para melhor avaliação ou teste, antes da definição do julgamento deste certame.

16.4. Nesta contratação não há parcelamento dos itens, pois o agrupamento é tecnicamente viável. Ademais, justifica-se pela vantagem econômica para a administração, uma vez que o objeto se compõe de itens inter-relacionados e o seu agrupamento viabiliza a qualidade da prestação dos serviços por uma única empresa, proporcionando ganhos de economia, eficácia e eficiência.

Ressalta-se também, que por se tratar de um serviço de segurança da informação, o agrupamento proporciona uniformidade das atividades a serem executadas, de acordo com a expectativa e orientações desta Agência e sem considerável variação na qualidade dos serviços prestados.

17. DOS RECURSOS ORÇAMENTÁRIOS

17.1. As despesas para atender a esta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da EMBRATUR para o exercício de 2025 na classificação abaixo:

17.1.1. Classificação da Despesa: 33904006 - LOCAÇÃO DE SOFTWARES

17.1.2. Órgão: 54000 – Ministério do Turismo - MTUR

17.1.3. Gestão/Unidade: EMBRATUR – Agência Brasileira de Promoção Internacional do Turismo

17.1.4. Função: 04 – Administração

17.1.5. Subfunção: 122 – Administração Geral

17.1.6. Programa de Trabalho: Gestão e Manutenção da EMBRATUR

18. DA APRESENTAÇÃO DA AMOSTRA

18.1. Para efeito de verificação da compatibilidade entre a proposta encaminhada pela proponente e a necessidade de padronização do objeto, a CONTRATANTE, caso não seja possível aferir o atendimento das especificações por meio de folders, fotos do produto ou outro meio idôneo, exigirá a apresentação de amostras.

18.2. Todas as soluções referentes aos itens 1, 2 e 3 do objeto que carecerem de comprovação de atendimento dos requisitos do item 21 farão parte da mesma amostra, e não será concedido tempo adicional devido a quantidade de soluções.

18.3. A licitante deverá enviar por e-mail a relação de representantes que participarão da apresentação da amostra em até 2 (dois) dias após a convocação, sendo no mínimo 2 (dois) e no máximo 6 (seis) representantes simultâneos.

18.4. A demonstração será presencial na sede da Embratur - Agência Brasileira de Promoção Internacional do Turismo, localizada na cidade de Brasília – DF, no Setor Comercial Norte, Quadra 2, Bloco G, Asa Norte. A critério da CONTRATANTE, poderá ser permitido a entrada virtual de algum representante para clarificar questões pontuais que não foram respondidas presencialmente, em que será anotado em ata o motivo da entrada virtual de um representante e a razão pela qual o ponto não foi respondido presencialmente.

18.5. A amostra deverá ser implantada em ambiente controlado da CONTRATANTE em pelo menos 10 ativos e poderá ser manipulada para testes, devendo a licitante ser capaz de demonstrar que a solução consegue atender os requisitos especificados no item 21.

18.6. Todos os custos para a demonstração de amostra será às expensas da licitante.

18.7. A licitante terá 2 (dois) dias úteis após o envio da relação dos representantes para informar os ativos e configurações necessárias para realizar a implantação.

18.8. A CONTRATANTE irá disponibilizar o ambiente solicitado em até 3 (três) dias após a solicitação.

18.9. Após a entrega do ambiente configurado, a Licitante terá até 15 (quinze) dias úteis para demonstrar que as soluções atendem os requisitos do item 21, incluindo o tempo para avaliação de erros e corretos.

18.10. O prazo somente será prorrogado em casos de erros, má configuração ou força maior do lado da CONTRATANTE.

18.11. Os prazos poderão ser antecipados nos casos em que o marco estiver concluído e a LICITANTE assim desejar, devendo formalizar por e-mail que está ciente que a antecipação do prazo não concede prazo adicional no cronograma.

18.12. Em até 2 (dois) dias úteis a CONTRATANTE emitirá o relatório conclusivo da análise da demonstração da amostra.

18.13. O cronograma de forma visual está demonstrado na tabela abaixo.

		Dias (úteis)																								
Marco	Responsável	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

19. DO OBJETIVO ESTRATÉGICO E ESTRATÉGIA ESG

20. **DA MATRIZ DE RISCO**

Eventos supervenientes	Ações Mitigadoras	Responsabilidade da Contratada	Responsabilidade do Contratante
Execução ineficiente do contrato	O fiscal deve participar da elaboração do Edital e anexos, além de receber treinamento específico		X
Situações na prestação dos serviços que configurem caso fortuito ou força maior	Suspender ou rescindir o contrato, com possibilidade de contratar remanescente		X
Manutenção e modernização - Custos de manutenção adicionais por previsão incorreta	Exigência de experiência prévia para o correto acompanhamento na prestação do serviço, gerenciando adequadamente os riscos de defeitos inesperados	X	
Não cumprimento dos limites de qualidade previstos no item 3. DESCRIÇÃO DA SOLUÇÃO DE TIC	Fiscalização constante do contrato a fim de observar se os níveis estabelecidos no contrato estão sendo cumpridos e proceder a glosas quando pertinentes.	X	X

Não cumprimento de prazos	Sanções contratuais impostas pela CONTRATANTE por atraso no cumprimento dos prazos.	X	X
---------------------------	---	---	---

21. REQUISITOS DA SOLUÇÃO

21.1. A solução de TIC consiste no fornecimento das seguintes plataformas, componentes e serviços conforme especificações técnicas detalhadas a seguir:

21.2. Item 1 - Solução de gerenciamento de vulnerabilidades de segurança e correções automatizadas

21.2.1. Características gerais

21.2.1.1. Toda a solução deverá ser de mesma marca, sem qualquer tipo de customização não autorizada pelo fabricante;

21.2.1.2. Caso a solução ofertada não possua o framework de correção das vulnerabilidades, este poderá ser ofertado por agentes e visões separadas;

21.2.1.3. A solução deve realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance);

21.2.1.4. Deve estar licenciada para no mínimo 340 ativos.

21.2.1.5. A solução deverá estar operacional em 97% do tempo do mês, considerando os aspectos de disponibilidade que competem à CONTRATADA.

21.2.1.6. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;

21.2.1.7. Deve possibilitar, por meio da console, no mínimo 2 (dois) métodos de escaneamento:

21.2.1.8. Scan ativo; e

21.2.1.9. Scan passivo.

21.2.1.10. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;

21.2.1.11. A solução deve ser licenciada pelo número de endereços IP ou dispositivos (assets);

21.2.1.12. A solução deve fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externos ou de terceiros;

21.2.1.13. Caso a solução dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela CONTRATADA.

21.2.1.14. A solução deverá suportar API (Application Programming Interface) baseada em REST (Representational State Transfer) para automação de processos e integração com aplicações terceiras.

21.2.1.15. A solução deve possuir integração via SDK no mínimo as seguintes linguagens: Python, Powershell, Javascript, Java, Bash e PHP;

21.2.1.16. A solução deve incluir a opção de varredura diretamente no sistema operacional em estações de trabalho e servidores;

21.2.1.17. O resultado da varredura em Sistemas Operacionais devem ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades;

21.2.1.18. A solução deve permitir o agrupamento de scanners para facilitar o gerenciamento e aplicação de políticas;

21.2.1.19. A solução deve realizar a varredura tanto de dispositivos na rede interna, dispositivos expostos a demais redes externas, tanto quanto dispositivos em nuvens públicas como Azure, AWS ou GCP;

21.2.1.20. O escaneamento para os dispositivos expostos deve ser realizado através de SCANS (ENGINE) do próprio fabricante, alocados no Brasil;

21.2.1.21. Os scanners e sensores agentes deverão ser gerenciados por uma única plataforma, de maneira centralizada;

21.2.1.22. O acesso a console de gerenciamento deve ser fornecida para pelo menos 5 usuários simultâneos;

21.2.1.23. A solução deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM);

21.2.1.24. A solução deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção;

21.2.1.25. A solução deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (outputs);

21.2.1.26. A solução deve fornecer controle de acesso baseado em função (RBAC- Role Based Access Control) para controlar o acesso do usuário a conjuntos de dados e funcionalidades;

21.2.1.27. A solução deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e dashboards;

21.2.1.28. A solução deve ter a capacidade de excluir determinados endereços IP do escopo de qualquer varredura ou scan;

21.2.1.29. A solução deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito;

21.2.1.30. A solução deve suportar métodos de autenticação usando bases de autenticação local, como Active Directory, OpenID Connect (OIDC), Security Assertion Markup Language (SAML) ou OAuth 2.0 para uso de SSO (Single Sign-On);

21.2.1.31. A solução deve ser capaz de orquestrar scanners ilimitados dentro da infraestrutura;

21.2.1.32. A solução não deve impor nenhum limite de quantidade de scanners implementados dentro da infraestrutura;

21.2.1.33. A solução deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de email;

21.2.1.34. A solução deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características Sistema Operacional, Endereço IP, DNS, NetBIOS Host, MAC, Tipo da instância, Nome da instância, ID da instância, Região da instância, Software instalado e Ativos avaliados;

21.2.2. Dos requisitos e relatórios e painéis gerenciais

21.2.2.1. A solução deverá possuir painéis gerenciais (dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a aplicação de filtros para resultados personalizados;

21.2.2.2. Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento;

21.2.2.3. Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução;

21.2.2.4. Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um exploit disponível e informações do ativo;

- 21.2.2.5. A solução deve permitir a customização de dashboards/relatórios;
- 21.2.2.6. A solução deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas;
- 21.2.2.7. A solução deve ser capaz de produzir relatórios, pelo menos, nos seguintes formatos: HTML, PDF e CSV;
- 21.2.2.8. A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos;
- 21.2.2.9. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);
- 21.2.2.10. A solução deve suportar o envio automático de relatórios para destinatários específicos;
- 21.2.2.11. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
- 21.2.2.12. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
- 21.2.3. Das varreduras
- 21.2.3.1. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como appliances virtuais;
- 21.2.3.2. A solução deve suportar varredura com e/ou sem agente, de maneira ativa e passiva, distribuídas em diferentes localidades e regiões e gerenciar todos por uma console central;
- 21.2.3.3. A solução deve realizar monitoramento contínuo de vulnerabilidades em sistemas operacionais;
- 21.2.3.4. A conexão entre o monitoramento dos sistemas operacionais e o sistema gerenciamento deve ser através de protocolo seguro;
- 21.2.3.5. A solução deve ser configurável para permitir a otimização das configurações de varredura;
- 21.2.3.6. A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory), root para sistemas Linux e Mac OS;
- 21.2.3.7. A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
- 21.2.3.8. A solução deve suportar o agendamento de scans personalizados, incluindo a capacidade de executar varreduras em tempos designados, com frequência pré-determinada;
- 21.2.3.9. A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de inserção manual;
- 21.2.3.10. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
- 21.2.3.11. A solução deve ser capaz de realizar em tempo real a descoberta de vulnerabilidades nas seguintes tecnologias:
- 21.2.3.12. Cloud Services;
- 21.2.3.13. Data Leakage;
- 21.2.3.14. Database;
- 21.2.3.15. IoT;
- 21.2.3.16. Mobile Devices;
- 21.2.3.17. Operating System;
- 21.2.3.18. Peer-To-Peer;
- 21.2.3.19. Web Servers;
- 21.2.3.20. Web Clients;
- 21.2.3.21. A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;
- 21.2.3.22. A solução deve em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede;
- 21.2.4. Da análise e priorização de vulnerabilidades
- 21.2.4.1. A solução deve ser capaz de exibir ambos severidade e pontuação, com base em CVSS (Common Vulnerability Scoring System) e inteligência de ameaças;
- 21.2.4.2. A solução deve utilizar sistema de pontuação e priorização das vulnerabilidades que utilize no mínimo:
- 21.2.4.3. CVSS Impact Score;
- 21.2.4.4. Idade da Vulnerabilidade;
- 21.2.4.5. Maturidade de códigos de exploração da vulnerabilidade encontrada;
- 21.2.4.6. Frequência de uso da vulnerabilidade em ataques e campanhas atuais;
- 21.2.4.7. Disponibilidade do código de exploração da vulnerabilidade;
- 21.2.4.8. Presença de módulos de exploração de vulnerabilidade em frameworks automatizados de exploração de vulnerabilidades como CANVAS, Metasploit e Core Impact; e
- 21.2.4.9. Popularidade da vulnerabilidade em fóruns e comunicações na Darkweb.
- 21.2.4.10. O mecanismo de priorização deve ser sujeito a modificações e atualizações diárias com base em inteligência de ameaças;
- 21.2.5. Da Análise de Risco do Ambiente
- 21.2.5.1. A solução deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;
- 21.2.5.2. O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;
- 21.2.5.3. Deve ser capaz de calcular a criticidade dos ativos da organização;
- 21.2.5.4. A solução deve ser capaz de realizar um benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor;
- 21.2.5.5. A solução deve prover visão sobre quais ações de remediação reduzem o maior nível de risco do ambiente;

- 21.2.5.6. A solução deve também permitir a visualização de ações de remediação agregadas para visão consolidada de redução de risco;
- 21.2.5.7. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;
- 21.2.5.8. A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo);
- 21.2.5.9. A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos;
- 21.2.5.10. A solução deve oferecer uma capacidade de comparação (benchmarking) da pontuação referente a exposição cibernética com outros players da mesma indústria assim como outras empresas do mercado;
- 21.2.5.11. A solução deve permitir um acompanhamento histórico do nível de exposição da organização;
- 21.2.5.12. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução;
- 21.2.5.13. A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade;
- 21.2.5.14. A solução deve permitir a segregação lógica entre áreas distintas da empresa afim de obter a pontuação referente exposição cibernética por área;
- 21.2.6. Da descoberta de ativos
- 21.2.6.1. A solução deve ser capaz de realizar escaneamento de descoberta de rede utilizando os seguintes critérios como alvo: IP, CIRD e Range;
- 21.2.6.2. A solução deve disponibilizar modelos de escaneamento de descoberta, ajustável, com os seguintes tipos de scan:
- 21.2.6.3. Enumeração de Hosts;
- 21.2.6.4. Identificação de Sistema Operacional (SO);
- 21.2.6.5. Port Scan (Portas comuns);
- 21.2.6.6. Port Scan (Todas as portas);
- 21.2.6.7. Customizado;
- 21.2.6.8. A solução deve permitir realizar escaneamento de descoberta customizado podendo ser parametrizado de acordo com a necessidade;
- 21.2.6.9. A parametrização do escaneamento de descoberta deve, no mínimo, conter os seguintes requisitos:
- 21.2.6.10. Descoberta de Host;
- 21.2.6.11. Ping o host remoto;
- 21.2.6.12. Usar descoberta rápida;
- 21.2.6.13. Métodos de ping;
- 21.2.6.14. ARP;
- 21.2.6.15. TCP;
- 21.2.6.16. ICMP; e
- 21.2.6.17. UDP.
- 21.2.6.18. Escaneamento de descoberta em redes de impressora;
- 21.2.6.19. Port Scanning:
- 21.2.6.20. portas;
- 21.2.6.21. considerar portas não escaneadas como fechadas; e
- 21.2.6.22. range de portas a serem escaneadas.
- 21.2.6.23. Enumerar Portas locais:
- 21.2.6.24. SSH;
- 21.2.6.25. WMI; e
- 21.2.6.26. SNMP;
- 21.2.6.27. Descoberta de Serviços:
- 21.2.6.28. Sondar todas as portas para encontrar serviços;
- 21.2.6.29. Procurar por serviços baseado em SSL/TLS; e
- 21.2.6.30. Enumerar todas as cifras SSL/TLS.
- 21.2.6.31. A solução deve realizar descoberta de ativo de forma passiva e adicionado automaticamente na console de gerenciamento;
- 21.2.6.32. A solução deve descobrir passivamente quando um host é adicionado na rede;
- 21.2.7. Da avaliação de vulnerabilidade
- 21.2.7.1. A solução deve ser capaz de realizar testes sem a necessidade de agentes instalados no dispositivo destino para detecção de vulnerabilidades;
- 21.2.7.2. A solução deve detectar e classificar através de severidades, riscos e vulnerabilidades;
- 21.2.7.3. A solução deve também fornecer informações detalhadas sobre a natureza da vulnerabilidade, evidências da existência da vulnerabilidade e recomendações para mitigá-los;
- 21.2.7.4. A solução deve incluir uma saída detalhada das vulnerabilidades descobertas como versões de DLL esperadas e encontradas;
- 21.2.7.5. A solução deve ser compatível com CVE e fornecer pelo menos 10 anos de cobertura CVE;
- 21.2.7.6. A solução deve identificar vulnerabilidades específicas para o Active Directory com os seguintes padrões de verificação:

- 21.2.7.7. Contas administrativas vulneráveis a Kerberoasting attack;
- 21.2.7.8. Utilização de criptografia vulnerável com autenticação Kerberos;
- 21.2.7.9. Contas com pré-autenticação do Kerberos desabilitada;
- 21.2.7.10. Verificação de usuários com a opção de nunca expirar a senha com a opção habilitada;
- 21.2.7.11. Verificar validação de fragilidades do tipo "Unconstrained Delegation";
- 21.2.7.12. Verificação de "Pre-Windows 2000 Compatible Access";
- 21.2.7.13. Verificação de validade de chaves mestras "Kerberos KRBtgt";
- 21.2.7.14. Verificação de "SID History Injection";
- 21.2.7.15. Verificação de "Printer Bug Exploit";
- 21.2.7.16. Verificação de "Primary Group ID"; e
- 21.2.7.17. Verificação de usuários com Passwords em branco.
- 21.2.7.18. A solução deve suportar o uso de SMB e WMI para verificação de sistemas Microsoft Windows;
- 21.2.7.19. A solução deve ser capaz de iniciar automaticamente serviços de registro remoto em sistemas Windows ao executar uma varredura credenciada;
- 21.2.7.20. A solução deve ser capaz de parar automaticamente o serviço de registro remoto em sistemas Windows novamente assim que a varredura estiver completa;
- 21.2.7.21. O scanner deve oferecer suporte a shell seguro (SSH) com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix;
- 21.2.7.22. A solução deve fornecer auditoria de patch (MS Bulletins) para as principais versões de Windows;
- 21.2.7.23. A solução deve fornecer varredura para aplicativos comerciais diversos e proprietários, incluindo, mas não limitando-se a: Java, Adobe, Oracle, Apple, Microsoft, Aruba, Fortinet, etc;
- 21.2.7.24. A solução deve incluir classificação de severidades de acordo com o padrão Sistema Comum de Pontuação de Vulnerabilidade Versão (CVSS2 e CVSS 3);
- 21.2.7.25. A solução deve fornecer informações acerca da disponibilidade de códigos de exploração das vulnerabilidades encontradas em frameworks de exploração para as plataformas mais populares: Core, Metasploit e Canvas;
- 21.2.7.26. A solução deve informar se a vulnerabilidade pode e está sendo ativamente explorada por código malicioso (malware);
- 21.2.7.27. Deve ser capaz de identificar e classificar vulnerabilidades de máquinas virtuais em nuvem pública em infraestruturas como serviço nas plataformas, minimamente em AWS, Microsoft Azure e Google Cloud;
- 21.2.8. Da auditoria de Configuração
- 21.2.8.1. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;
- 21.2.8.2. A solução deve fornecer benchmarks de auditoria de segurança e configuração para conformidade regulatória e outros padrões de práticas recomendadas pela área ou fabricantes;
- 21.2.8.3. A solução deve realizar verificações de auditoria contendo as de segurança, com indicação de sucesso ou falha, baseado nos principais frameworks reconhecidos pela indústria, pelo menos os seguintes:
- 21.2.8.4. Center for Internet Security Benchmarks (CIS);
- 21.2.8.5. Defense Information Systems Agency (DISA) STIGs;
- 21.2.8.6. Health Insurance Portability and Accountability Act (HIPAA);
- 21.2.8.7. Payment Card Industry Data Security Standards (PCI DSS);
- 21.2.8.8. A solução deve fornecer auditoria de programas antivírus para determinação de presença e status de inicialização;
- 21.2.8.9. A solução deve fornecer auditorias de configuração com base benchmarks em CIS (Center for Internet Security) L1 e L2, para ambos os sistemas operacionais Microsoft Windows e Linux;
- 21.2.8.10. A solução deve permitir auditoria de conformidade em servidores Windows, Linux, Bancos de Dados SQL Server, PostgreSQL e MySQL, a fim de determinar se estão configurados de acordo com os principais Framework de segurança como, por exemplo, CIS e DISA;
- 21.2.8.11. A solução deve oferecer validação e suporte a SCAP (Security Content Automation Protocol);
- 21.2.9. Análise dinâmica de vulnerabilidades para aplicações Web
- 21.2.9.1. A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;
- 21.2.9.2. A solução deve ser capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);
- 21.2.9.3. Deve estar licenciado para no mínimo 5 FQDNs simultâneos;
- 21.2.9.4. A solução deve avaliar no mínimo os padrões de segurança OWASP Top 10;
- 21.2.9.5. Deve ser capaz de identificar no mínimo 50.000 CVE'S;
- 21.2.9.6. A solução deve possuir templates prontos de varreduras entre simples e extensos;
- 21.2.9.7. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:
- 21.2.9.8. cookies, headers, local storage, formulários e links;
- 21.2.9.9. nomes e valores de parâmetros da aplicação;
- 21.2.9.10. elementos JSON e XML; e
- 21.2.9.11. elementos DOM.
- 21.2.9.12. A solução deve permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;

- 21.2.9.13. A solução deve ser capaz de utilizar scripts customizados de crawler com parâmetros definidos pelo usuário;
- 21.2.9.14. A solução deve excluir determinadas URLs da varredura através de expressões regulares;
- 21.2.9.15. A solução deve excluir determinados tipos de arquivos através de suas extensões;
- 21.2.9.16. A solução deve instituir no mínimo os seguintes limites:
- 21.2.9.17. Número máximo de URLs para crawler e navegação;
- 21.2.9.18. Número máximo de diretórios para varreduras;
- 21.2.9.19. Número máximo de elementos DOM;
- 21.2.9.20. Tamanho máximo de respostas;
- 21.2.9.21. Limite de requisições de redirecionamentos;
- 21.2.9.22. Tempo máximo para a varredura;
- 21.2.9.23. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web; e
- 21.2.9.24. Número máximo de requisições HTTP por segundo.
- 21.2.9.25. A solução deve detectar congestionamento de rede e limitar os seguintes aspectos da varredura:
- 21.2.9.26. Limite em segundos para timeout de requisições de rede; e
- 21.2.9.27. Número máximo de timeouts antes que a varredura seja abortada.
- 21.2.9.28. A solução deve agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
- 21.2.9.29. A solução deve enviar notificações através de no mínimo E-mail;
- 21.2.9.30. A solução deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques;
- 21.2.9.31. A solução deve avaliar sistemas web utilizando protocolos HTTP e HTTPS;
- 21.2.9.32. A solução deve possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizado a ser enviada durante os testes;
- 21.2.9.33. A solução deve ser compatível com avaliação de web services REST e SOAP;
- 21.2.9.34. Deverá suportar no mínimo os seguintes esquemas de autenticação:
- 21.2.9.35. Autenticação básica (digest);
- 21.2.9.36. NTLM;
- 21.2.9.37. Form de login;
- 21.2.9.38. Autenticação de Cookies; e
- 21.2.9.39. Autenticação através de Bearer.
- 21.2.9.40. A solução deve exibir os resultados das varreduras em tendência temporal para acompanhamento de correções e introdução de novas vulnerabilidades;
- 21.2.9.41. A solução deve exibir os resultados agregados de acordo com as categorias do OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project);
- 21.2.9.42. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
- 21.2.9.43. Para cada vulnerabilidade encontrada, devem ser exibidas as evidências dela em seus detalhes;
- 21.2.9.44. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc), deve evidenciar nos detalhes do evento encontrado:
- 21.2.9.45. Payload injetado;
- 21.2.9.46. Evidência em forma de resposta da aplicação;
- 21.2.9.47. Detalhes da requisição HTTP; e
- 21.2.9.48. Detalhes da resposta HTTP.
- 21.2.9.49. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;
- 21.2.9.50. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação dessas;
- 21.2.9.51. A solução deve possuir suporte a varreduras de componentes como as linguagens de programação, os frameworks (AngularJS, ReactJS e similares), servidores Web (Apache2, Nginx, Apache Tomcat, IIS Windows e similares) e os CMS (Wordpress, Joomla e similares).
- 21.2.10. Análise em ambiente Microsoft Active Directory
- 21.2.10.1. A solução deve ser capaz de identificar vulnerabilidades ocultas em configurações dedicadas ao Active Directory;
- 21.2.10.2. A solução deve oferecer medidas preventivas de hardening para o Active Directory;
- 21.2.10.3. A solução deve ter a capacidade de identificar ataques específicos direcionados à estrutura do Active Directory (AD);
- 21.2.10.4. A solução deve fornecer análises detalhadas de cada configuração incorreta que represente riscos de segurança, apresentando informações de forma acessível e contextualizada para as equipes envolvidas;
- 21.2.10.5. A solução deve incluir recomendações de correção para cada configuração incorreta identificada no Active Directory;
- 21.2.10.6. A solução deve ter a capacidade de avaliar relações de confiança perigosas entre florestas e domínios;
- 21.2.10.7. A solução deve capturar as mudanças que ocorrem no AD e demonstrar na console de administração;
- 21.2.10.8. A solução deve possuir dashboard com os principais ataques e vulnerabilidades por domínio;
- 21.2.10.9. A solução deve possuir capacidade nativa de criação de dashboards customizados;
- 21.2.10.10. A solução deve permitir a correlação de mudanças no Active Directory e desvios de segurança;
- 21.2.10.11. A solução deve analisar em detalhes um ataque explorando as descrições através do framework MITRE ATT&CK;

- 21.2.10.12. A solução deve prover interface web para gerenciamento de todas as funcionalidades;
- 21.2.10.13. A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;
- 21.2.10.14. A solução deve ter a capacidade de realizar alterações no Active Directory, seus objetos e atributos;
- 21.2.10.15. A solução não deve armazenar ou sincronizar nenhuma credencial de objetos do Active Directory;
- 21.2.10.16. A solução deve suportar ambientes com múltiplas florestas e domínios;
- 21.2.10.17. A solução deve suportar monitoramento contínuo de ambientes com Active Directory com o nível funcional de floresta e domínio a partir do 2003;
- 21.2.10.18. A solução deve suportar reter os eventos coletados por no mínimo um ano;
- 21.2.10.19. A solução deve descobrir e mapear a superfície de ataque do Active Directory e seus domínios monitorados com os seguintes padrões:
- 21.2.10.20. Não depender de agentes ou sensores para coleta de informações do AD;
- 21.2.10.21. A solução deve seguir as boas práticas de menor privilégio, a conta de serviço utilizada para conexão com o Active Directory, sendo o menor nível de acesso esperado para a conta de serviço como parte do grupo Domain User; e
- 21.2.10.22. Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles.
- 21.2.10.23. A solução deve analisar continuamente a postura de segurança do AD, minimamente avaliando:
- 21.2.10.24. Validação de GPOs desvinculadas, desabilitadas ou órfãs;
- 21.2.10.25. Validação de contas desativadas em grupos privilegiados;
- 21.2.10.26. Domínio usando uma configuração perigosa de compatibilidade com versões anteriores por meio de alterações no atributo dSHuristics;
- 21.2.10.27. Validação de atributos relacionados a roaming de credenciais vulneráveis (msPKI-DPAPIMasterKeys) gerenciados por um usuário sem privilégios;
- 21.2.10.28. Validação de domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como NTLMv1;
- 21.2.10.29. Validação de contas com senhas que nunca expiram;
- 21.2.10.30. Validação de senhas reversíveis em GPOs;
- 21.2.10.31. Validação de uso de senhas reversíveis em contas de usuário;
- 21.2.10.32. Validação de utilização de protocolo criptográfico fraco (Ex. DES) em contas de usuário;
- 21.2.10.33. Validação de uso do LAPS (Solução de senha de administrador local) para gerenciar senhas de contas locais com privilégios;
- 21.2.10.34. Validação se o domínio possui um nível funcional desatualizado;
- 21.2.10.35. Validação de contas de usuário utilizando senha antiga;
- 21.2.10.36. Validação se o atributo AdminCount está definido em usuários padrão;
- 21.2.10.37. Validação do uso recente da conta de administrador padrão;
- 21.2.10.38. Validação de usuários com permissão para ingressar computadores no domínio;
- 21.2.10.39. Validação de contas dormentes;
- 21.2.10.40. Validação de computadores executando um sistema operacional obsoleto;
- 21.2.10.41. Validação de restrições de logon para usuários privilegiados em ambiente com múltiplos tiers (1, 2 e 3) de segregação de ativos;
- 21.2.10.42. Validação de direitos perigosos configurados no Schema do AD;
- 21.2.10.43. Validação de relação de confiança perigosa com outras Florestas e Domínios;
- 21.2.10.44. Validação de contas que possuem um atributo perigoso de histórico SID (SID History);
- 21.2.10.45. Validação de contas utilizando controle de acesso compatível com versões anteriores ao Windows 2000;
- 21.2.10.46. Validação da última alteração de senha do KDC;
- 21.2.10.47. Validação de contas que podem ter senha em branco/vazia;
- 21.2.10.48. Validação de utilização do grupo nativo Protected Users;
- 21.2.10.49. Validação de privilégios sensíveis (Ex. Debug a program, Replace a process level token, etc.) atribuídos aos usuários;
- 21.2.10.50. Validação de possível senha em clear-text;
- 21.2.10.51. Validação de sanidade das GPOs e componentes CSEs (Client-Side Extension);
- 21.2.10.52. Validação de uso de algoritmos de criptografia fracos na PKI do Active Directory;
- 21.2.10.53. Validação de contas de serviço com SPN (Service Principal Name) que fazem parte de grupos privilegiados;
- 21.2.10.54. Validação de contas anormais nos grupos administrativos padrão do AD;
- 21.2.10.55. Validação de consistência no container adminSDHolder;
- 21.2.10.56. Validação de delegação Kerberos perigosa;
- 21.2.10.57. Validação em permissões de objetos raiz que permitem ataques do tipo DCSync;
- 21.2.10.58. Validação de políticas de senha fracas aplicadas aos usuários;
- 21.2.10.59. Validação do ID do grupo primário do usuário (Primary Group ID);
- 21.2.10.60. Validação de permissões em GPOs sensíveis associadas aos Containers Configuration, Sites, Root Partition e OUs sensíveis como Domain Controllers;
- 21.2.10.61. Controladores de domínio gerenciados por usuários ilegítimos;
- 21.2.10.62. Validação de certificado mapeado através de atributo altSecurityIdentities em contas privilegiadas; e
- 21.2.10.63. Validação de uso de protocolo Netlogon inseguro (ZeroLogon/CVE2020-1472).

- 21.2.10.64. A solução deve identificar vulnerabilidades e configurações incorretas do AD à medida que são introduzidas sendo;
- 21.2.10.65. Identificar todas as vulnerabilidades e configurações incorretas no AD;
- 21.2.10.66. Monitorar relações de confiança perigosas em toda a estrutura AD;
- 21.2.10.67. Apresentar ameaças e alterações sem a necessidade de scans estáticos e programados no Active Directory e sua infraestrutura;
- 21.2.10.68. Apresentar as ameaças e alterações em tempo real ou em menos de cinco minutos;
- 21.2.11. Detecção e resposta a ataques:
 - 21.2.11.1. Monitorar continuamente os indicadores de possíveis ataque como DCSync, DCShadow, Password Spraying, Password Guessing/Brute Force, Lsaas Injection nos controladores de domínio, Golden Ticket, NTLM Relay, entre outros;
 - 21.2.11.2. Detecção de ataques ao AD em tempo real ou em menos de um minuto;
 - 21.2.11.3. Análise detalhada do ataque, apresentando ativo de origem, vetor de ataque, controlador de domínio afetado, técnica aplicada;
 - 21.2.11.4. Apresentação de ataques em uma linha do tempo;
 - 21.2.11.5. Investigar ameaças, reproduzir ataques e procurar por backdoors;
 - 21.2.11.6. Permitir busca ágil de eventos específicos na base da solução através de queries customizadas;
 - 21.2.11.7. A solução deve ser capaz de enviar alertas por e-mail;
 - 21.2.11.8. A solução nativamente deve ser capaz de se integrar com SIEM através de protocolo SYSLOG;
 - 21.2.11.9. A solução deve ser capaz de filtrar e enriquecer os eventos que serão enviados para o SIEM;
 - 21.2.11.10. A solução deve produzir regras YARA na detecção de ataques (Ex. DCSync, Golden Ticket) identificados pela ferramenta;
 - 21.2.11.11. A solução deve possuir conjunto de APIs REST, todas as chamadas disponíveis devem estar contidas na documentação;
 - 21.2.11.12. A solução deve permitir a criação de listas de exclusões, suportando minimamente exclusão por domínios do AD monitorados e por itens analisados;
- 21.2.12. Correção automatizada de vulnerabilidades de segurança
 - 21.2.12.1. A plataforma deverá ser ofertada em modelo SaaS (Software as a Service), ou seja, não deve requerer recursos computacionais on-premises para ser implementada.
 - 21.2.12.2. A plataforma deve prover visibilidade e cobertura em tempo real para os sistemas operacionais e aplicações utilizadas nos ativos da organização, ou seja, qualquer alteração no inventário (instalação / desinstalação / alteração de aplicativos deve ser refletida instantaneamente na solução).
 - 21.2.12.3. A plataforma deve fornecer uma solução integrada para gerenciamento de vulnerabilidade, priorização de risco e remediação em uma única plataforma.
 - 21.2.12.4. A plataforma deve prover pelo menos dois métodos de autenticação (Ex: usuário e senha, e-mail de verificação, SAML2).
 - 21.2.12.5. A plataforma deve ter a possibilidade de instalar um componente na rede interna para fazer o caching de patches, atendendo requisitos de ativos que não podem realizar download das atualizações diretamente da internet, bem como este componente não deve ocasionar custo adicional. Tal componente deve ser executado em pelo menos um dos seguintes sistemas operacionais: Ubuntu ou Red Hat Linux.
 - 21.2.12.6. Deve prover atualização de patches para servidores sem interrupção do serviço principal, sem forçar a reinicialização desse.
 - 21.2.12.7. A plataforma deve atualizar não apenas o Sistema operacional, mas também as aplicações instaladas nos ativos.
 - 21.2.12.8. Deve trabalhar com reconhecimento automático de aplicações instaladas nos hosts, mantendo também o fluxo de atualizações disponível.
 - 21.2.12.9. Deve fornecer gerenciamento de patches fim a fim para o sistema operacional Windows;
 - 21.2.12.10. Deve fornecer gerenciamento de patches para aplicações de terceiros no Windows;
 - 21.2.12.11. Deve fornecer gerenciamento de patch para o sistema operacional Linux;
 - 21.2.12.12. Deve fornecer gerenciamento de patches para aplicativos de terceiros no Linux e não apenas na camada de SO.
 - 21.2.12.13. Deve fornecer gerenciamento de patches para o sistema operacional Mac.
 - 21.2.12.14. Para o sistema operacional Windows, minimamente, as seguintes aplicações devem poder ser atualizadas:
 - 21.2.12.15. 7-zip;
 - 21.2.12.16. Adobe Reader;
 - 21.2.12.17. Adobe Acrobat Reader;
 - 21.2.12.18. Adobe Photoshop;
 - 21.2.12.19. Adobe Creative Cloud;
 - 21.2.12.20. Autocad;
 - 21.2.12.21. Bizagi Modeler Free
 - 21.2.12.22. Openssl;
 - 21.2.12.23. Opera;
 - 21.2.12.24. Python;
 - 21.2.12.25. Google Chrome;
 - 21.2.12.26. Mozilla Firefox;
 - 21.2.12.27. Mozilla Thunderbird;
 - 21.2.12.28. Oracle Java;
 - 21.2.12.29. Microsoft Visual Studio;
 - 21.2.12.30. Microsoft System Center;
 - 21.2.12.31. Microsoft SQL Server;

- 21.2.12.32. Microsoft Exchange;
- 21.2.12.33. Microsoft Edge;
- 21.2.12.34. Microsoft Internet Explorer;
- 21.2.12.35. Microsoft Outlook;
- 21.2.12.36. Microsoft Visio;
- 21.2.12.37. Microsoft Windows Defender;
- 21.2.12.38. Notepad++;
- 21.2.12.39. PowerBI;
- 21.2.12.40. Microsoft IIS;
- 21.2.12.41. PDF Reader;
- 21.2.12.42. Zoom;
- 21.2.12.43. Vmware Workstation;
- 21.2.12.44. Webex;
- 21.2.12.45. Whatsapp; e
- 21.2.12.46. VLC.
- 21.2.12.47. Para os sistemas operacionais Linux, minimamente, as seguintes aplicações devem poder ser atualizadas:
- 21.2.12.48. Abrt;
- 21.2.12.49. Adduser;
- 21.2.12.50. Alsa-Lib
- 21.2.12.51. Alsa-Tools-Firmware;
- 21.2.12.52. Apparmor;
- 21.2.12.53. Appport;
- 21.2.12.54. Apt;
- 21.2.12.55. Apt-Utills;
- 21.2.12.56. Base-Files;
- 21.2.12.57. Bash;
- 21.2.12.58. Binutils;
- 21.2.12.59. BZIP2;
- 21.2.12.60. Chrony;
- 21.2.12.61. Coreutils;
- 21.2.12.62. Crontabs;
- 21.2.12.63. Curl;
- 21.2.12.64. Dash;
- 21.2.12.65. Debianutils;
- 21.2.12.66. Device-Mapper;
- 21.2.12.67. Diffstat;
- 21.2.12.68. Diffutils;
- 21.2.12.69. Dirmngr;
- 21.2.12.70. Distro-Info;
- 21.2.12.71. Dnsutils;
- 21.2.12.72. Dpkg;
- 21.2.12.73. Elfutils;
- 21.2.12.74. Fdisk;
- 21.2.12.75. Findutils;
- 21.2.12.76. Firewallld;
- 21.2.12.77. FTP;
- 21.2.12.78. Gdisk;
- 21.2.12.79. Git;
- 21.2.12.80. GLIB2;
- 21.2.12.81. Glibc;
- 21.2.12.82. Glibc-Common;
- 21.2.12.83. GNUPG2;
- 21.2.12.84. Gnupg-Utills;
- 21.2.12.85. Grep;
- 21.2.12.86. Grub2-Tools;

- 21.2.12.87. Grub-Common;
- 21.2.12.88. Gzip;
- 21.2.12.89. Iproute;
- 21.2.12.90. Iprutils;
- 21.2.12.91. Iptables;
- 21.2.12.92. Iputils;
- 21.2.12.93. Kernel-Tools;
- 21.2.12.94. Kmod;
- 21.2.12.95. Libcap;
- 21.2.12.96. Mount;
- 21.2.12.97. Net-Tools;
- 21.2.12.98. Openssh;
- 21.2.12.99. Openssl;
- 21.2.12.100. Open-Vm-Tools;
- 21.2.12.101. PAM;
- 21.2.12.102. Passwd;
- 21.2.12.103. Patchutils;
- 21.2.12.104. Perl;
- 21.2.12.105. Postfix;
- 21.2.12.106. Python;
- 21.2.12.107. RPM;
- 21.2.12.108. Rsyslog;
- 21.2.12.109. Shadow-Utils;
- 21.2.12.110. Sqlite;
- 21.2.12.111. Sudo;
- 21.2.12.112. Tar;
- 21.2.12.113. Tcpdump;
- 21.2.12.114. Telnet;
- 21.2.12.115. Time;
- 21.2.12.116. Unzip;
- 21.2.12.117. Vim;
- 21.2.12.118. Wget;
- 21.2.12.119. Yum;
- 21.2.12.120. Zerofree; e
- 21.2.12.121. Zip.
- 21.2.12.122. Para os sistemas operacionais MAC, minimamente, as seguintes aplicações devem poder ser atualizadas:
- 21.2.12.123. Zoom;
- 21.2.12.124. Adobe Creative Cloud;
- 21.2.12.125. Google Chrome;
- 21.2.12.126. Whatsapp;
- 21.2.12.127. Safari;
- 21.2.12.128. Davince Resolve;
- 21.2.12.129. Mozilla Firefox.
- 21.2.12.130. Deve prover avaliação contínua de vulnerabilidades para identificação de quais atualizações devem ser instaladas em cada host.
- 21.2.12.131. Deve fornecer painel com priorização de ameaças com base nos ativos, aplicações ou sistemas operacionais.
- 21.2.12.132. A priorização de vulnerabilidade e correções a serem realizadas deve ser combinada com um motor inteligência interna a própria solução.
- 21.2.12.133. O processo de priorização e remediação de vulnerabilidades deve acompanhar todo o seu ciclo de vida, ou seja, descoberta/identificação, correção manual ou automatizada e contabilização nas visões para acompanhamento das ações que foram tomadas.
- 21.2.12.134. A própria ferramenta deve conter um processo de classificação de risco para priorizar a correção de vulnerabilidades descobertas, trazendo contexto de risco daquilo que precisa de atenção imediata.
- 21.2.12.135. Deve prover uma visão de classificação de risco baseada em ativos.
- 21.2.12.136. Deve prover classificação de risco por aplicação.
- 21.2.12.137. Deve apresentar a classificação de risco e priorizar as vulnerabilidades a serem corrigidas em ordem de criticidade não só do CVE, mas também em relação à um contexto de performance, situação do ambiente e tipos de ativo.
- 21.2.12.138. Deve fornecer detecção de vulnerabilidades a serem corrigidas em tempo real.
- 21.2.12.139. Deve prover meios para conter a exploração de softwares em tempo real;

- 21.2.12.140. Deve ter a funcionalidade de proteção contra exploração de vulnerabilidades, sem necessariamente instalar um patch de correção ("patch virtual"), utilizando o mesmo agente de patch management.
- 21.2.12.141. Deve possuir informações de CVE tanto recentes quanto legados, tal capacidade deve ser comprovada por documentações oficiais.
- 21.2.12.142. Deve manter a base de dados atualizada constantemente, no tocante a novas vulnerabilidades e patches de correção a serem instalados nos ativos.
- 21.2.12.143. Deve permitir a execução de comandos de forma remota em todos os dispositivos que possuem os agentes instalados.
- 21.2.12.144. Deve permitir o agendamento de instalação das atualizações (Patches) ou execução de script de forma remota.
- 21.2.12.145. Deve possibilitar a execução de ações automáticas pré-configuradas e personalizadas (Ações Automáticas).
- 21.2.12.146. As ações automáticas devem possibilitar a instalação automática de patches baseado em critérios personalizáveis, como:
- 21.2.12.147. Atualizações de sistema operacional;
- 21.2.12.148. Atualizações de aplicações específicas;
- 21.2.12.149. Por severidade/criticidade do patch de correção;
- 21.2.12.150. Toda instalação de patch deve permitir a opção de reinicialização automática da estação/servidor, dando também a opção para que o usuário cancele o restart, se necessário.
- 21.2.12.151. Deve ser possível enviar "pop-ups" para os usuários, quando esses estiverem pendentes de reinicialização.
- 21.2.12.152. Deve possibilitar a geração de scripts para Windows, Linux e Mac.
- 21.2.12.153. Deve possuir proteção contra vulnerabilidades de dia 0 (zero day).
- 21.2.12.154. Deve possuir mecanismos de "Ações recomendadas", de forma a guiar as correções a serem realizadas.
- 21.2.12.155. Deve suportar segregação de função por usuário, ou seja, permitir que usuários da mesma empresa tenham permissões diferentes dentro da plataforma.
- 21.2.12.156. Deve ser capaz de segregar diferentes ativos entre diferentes grupos de usuários com diferentes níveis de permissão.
- 21.2.12.157. A segregação de ativos por grupos, deve respeitar características dinâmicas, de forma a movimentar os ativos entre os grupos de forma automática. Tal característica deve suportar a configuração, minimamente, dos seguintes atributos (Para movimentação automática dos ativos):
- 21.2.12.158. Nome do ativo;
- 21.2.12.159. Tipo do ativo;
- 21.2.12.160. Nível de risco do ativo;
- 21.2.12.161. Status do ativo;
- 21.2.12.162. CVE's específicos detectados no ativo;
- 21.2.12.163. Aplicações específicas instaladas nos ativos, assim como a versão detectada;
- 21.2.12.164. Sistema operacional e versão desse;
- 21.2.12.165. Deve permitir a instalação do agente por linha de comando (Powershell, cmd, bash, etc); e
- 21.2.12.166. Permitir a instalação de agente por meio de GPO ou qualquer outra plataforma de software deployment utilizada.
- 21.2.12.167. Os agentes devem ser capazes de scanear as plataformas Windows, Linux e Mac.
- 21.2.12.168. Para o sistema operacional Windows, as seguintes versões, minimamente, devem ser suportadas:
- 21.2.12.169. Windows 7, 8, 8.1, 10 e 11; e
- 21.2.12.170. Windows server 2008, 2012, 2016, 2019, 2022 e 2025.
- 21.2.12.171. Para o sistema operacional Linux, as seguintes distribuições, minimamente, devem ser suportadas:
- 21.2.12.172. Centos;
- 21.2.12.173. Redhat;
- 21.2.12.174. Fedora;
- 21.2.12.175. Ubuntu;
- 21.2.12.176. Debian;
- 21.2.12.177. Kali Linux;
- 21.2.12.178. Amazon Linux; e
- 21.2.12.179. Oracle Linux.
- 21.2.12.180. Para o sistema operacional Mac, devem ser suportado o Mac OS Catalina ou superior.
- 21.2.12.181. O agente não deve depender de nenhum componente externo, não fornecido, para seu pleno funcionamento.
- 21.2.12.182. O agente deve funcionar de forma oculta no sistema operacional, não apresentando interface para o usuário final.

21.3. **Item 2 - Solução de correlação de eventos de segurança e resposta a incidentes**

21.3.1. Arquitetura

- 21.3.1.1. Deve ser on-premise ou baseada em nuvem (Cloud), de forma a manter todos os eventos armazenados na nuvem do fabricante da solução.
- 21.3.1.2. A solução deverá estar operacional em 97% do tempo do mês, considerando os aspectos de disponibilidade que competem à CONTRATADA.
- 21.3.1.3. Não serão aceitos serviços entregues por meio de software livre ou open-source.
- 21.3.1.4. A solução deve fornecer componentes já licenciados para coleta e envio de logs/tráfego até a plataforma central.
- 21.3.1.5. O componente para coleta de logs/tráfego deve fornecer a possibilidade de instalação em servidores Windows, Linux ou imagens prontas previamente fornecidas.

- 21.3.1.6. Deverá estar licenciada, em nome da CONTRATADA, de forma a manter o processamento em tempo real ou realizar o buffer dos eventos, mesmo que o tráfego de eventos ultrapasse o volume licenciado nas horas de pico.
- 21.3.1.7. Suportar um tráfego de logs de, no mínimo, 750 eventos por segundo (EPS).
- 21.3.1.8. Deve possuir capacidade de recebimento e armazenamento, mínimo, de todos os logs de ativos de segurança, alertas de segurança, tráfego de pacotes, dentre outras informações relacionadas, em formato bruto (raw) e/ou metadados, necessárias para fins de correlacionamento e forense, com armazenamento mínimo de 365 dias;
- 21.3.1.9. Deve ter a capacidade de manter os itens coletados indexados para buscas rápidas por pelo menos 60 dias. Itens a serem buscados em datas superiores ao período de indexação devem respeitar o período de retenção do tópico anterior.
- 21.3.2. Requisitos Gerais
- 21.3.2.1. Deverá ser capaz de gerenciar de forma eficiente incidentes de segurança. O software de gerenciamento de incidentes de segurança deve permitir a definição de um processo abrangente desde o registro e triagem inicial de um incidente até sua resolução e prevenção.
- 21.3.2.2. Deve permitir a automação de fluxos de forma gráfica, incluindo estágios, tarefas paralelas ou sequenciais, regras de decisão e aprovação, sem a necessidade de programação ou alteração de código fonte para as integrações já existentes.
- 21.3.2.3. Deve permitir automatização e orquestração de fluxos relacionados a resposta de incidentes de segurança, integrando e simplificando as operações.
- 21.3.2.4. Deve fornecer visibilidade, rastreabilidade e indexação dos eventos detectados, integrando as várias ferramentas de segurança que a entidade possui, aumentando a capacidade de detecção e maturidade da segurança cibernética.
- 21.3.2.5. Deve permitir acelerar a resposta às lacunas de segurança cibernética por meio de análise contextual, automação de processos e capacidade de articulação para investigação, utilizando fluxos de análise e inteligência associada às metodologias de ataque de grupos de cibercrime.
- 21.3.2.6. Deve identificar, registrar e indexar incidentes de segurança rapidamente, registrando os eventos relatados pelas soluções que a CONTRATADA atualmente possui.
- 21.3.2.7. Deve permitir integração e interoperabilidade com o ecossistema de segurança da entidade, independentemente da marca dos produtos de segurança utilizados.
- 21.3.2.8. Deve permitir a integração baseada em fluxos de trabalho através do cruzamento de dados das soluções de segurança como Firewalls, IPSs e sistemas de chamados.
- 21.3.2.9. Deve possuir controle granular de níveis de acesso a plataforma.
- 21.3.2.10. Deve funcionar, obrigatoriamente, com autenticação de dois fatores nativa, sendo eles: OTP, SMS ou voz.
- 21.3.2.11. Deve permitir que você configure políticas restritas de senha como período de redefinição, bloqueio por tentativas sem sucesso, histórico de senha e desativação de usuários por tempo de inatividade.
- 21.3.2.12. Deve registrar e listar todos os alertas ativos, permitindo filtros e pesquisas sob demanda em uma linguagem de queries.
- 21.3.2.13. Deve permitir a criação de listas a serem utilizadas durante as pesquisas, com objetivo de poder facilmente utilizá-las para inclusão ou remoção de recursos na busca, evitando a repetição de comandos, tornando as ações de caça a ameaças (hunting) mais ágeis.
- 21.3.2.14. Deve possuir alertas indicando a gravidade do incidente, permitindo a detecção, validação e investigação, a fim de reconstruir toda a cadeia do ataque.
- 21.3.2.15. Deve suportar uma linha do tempo visual em relação aos eventos registrados.
- 21.3.2.16. Deve oferecer suporte à integração com soluções de segurança de terceiros. A integração deve ser baseada em syslog, ingestão/absorção de alertas e/ou análise de tráfego de rede.
- 21.3.2.17. Deve permitir a criação de painéis e dashboards com gráficos de gestão, de forma ágil e intuitiva, sem a necessidade de programação e alteração do código-fonte.
- 21.3.2.18. Deve permitir aos atendentes e solucionadores de incidentes a possibilidade de criação de seus próprios painéis e gráficos dentro da solução, compartilhando sempre que necessário com grupos ou usuários específicos, permitindo gerenciamento das permissões de compartilhamento de acordo com os perfis de cada usuário.
- 21.3.2.19. Deve permitir a criação de gráficos, utilizando como origem de dados, as informações de diferentes soluções de segurança da organização.
- 21.3.2.20. Deve permitir configurar o envio automático e agendado de relatórios e gráficos gerenciais para grupos de usuários ou usuários específicos.
- 21.3.2.21. Deve incluir painéis unificados, buscas e relatórios, para facilitar a transição da detecção para a investigação e a resposta subsequente ao incidente relatado.
- 21.3.2.22. O coletor da solução deverá ser capaz de coletar, aplicar parsing, normalizar e categorizar os eventos dos dispositivos monitorados em tempo próximo ao real.
- 21.3.2.23. Deve possuir parsing, para interpretação automática de logs, para pelo menos as seguintes marcas/soluções:
- 21.3.2.24. AWS;
- 21.3.2.25. Google workspace;
- 21.3.2.26. Apache;
- 21.3.2.27. Aruba;
- 21.3.2.28. Cisco;
- 21.3.2.29. Citrix;
- 21.3.2.30. Nutanix;
- 21.3.2.31. Docker;
- 21.3.2.32. Fortinet;
- 21.3.2.33. Graylog;
- 21.3.2.34. HP;
- 21.3.2.35. McAfee;

21.3.2.36. Microsoft;

21.3.2.37. Nagios;

21.3.2.38. Nginx;

21.3.2.39. Vmware;

21.3.2.40. Deve fornecer um módulo de UEBA ao qual possa ser utilizado para análise avançada do comportamento de entidades (computadores e usuários) aos quais podem estar envolvidos em atividades maliciosas. O módulo de UEBA deve utilizar técnicas avançadas para análise de comportamento sendo possível correlacionar eventos e extrair informações relevantes as quais devem ser utilizadas para definir o perfil de risco das entidades.

21.3.2.41. Deve analisar os tipos de log enviados e realizar sugestões de envio de importantes fontes de detecção de malware na qual ele não está recebendo logs. Exemplo: a organização não está enviando logs de firewall e DHCP, tais logs ampliam o poder de detecção da plataforma. Este recurso deve estar em execução automaticamente.

21.3.2.42. Deve possuir dashboards e relatórios que classifiquem os logs que foram devidamente classificados, permitindo também a rápida visualização dos que não foram, para que as ações de "parsing" possam ser planejadas.

21.3.2.43. Deve possuir dashboards prontos que são alimentados a partir da ingestão de logs para pelo menos, os seguintes fabricantes:

21.3.2.44. AWS;

21.3.2.45. Cisco;

21.3.2.46. Google Cloud Platform;

21.3.2.47. McAfee;

21.3.2.48. Microsoft;

21.3.2.49. Microsoft Azure;

21.3.2.50. Nutanix; e

21.3.2.51. Fortinet.

21.3.2.52. Deve possuir meios de monitoramento de saúde de todos os sensores que enviam logs para a console central.

21.3.2.53. Caso alguma fonte pare de enviar logs, a plataforma deve informar automaticamente os administradores para verificação.

21.3.2.54. Deve possuir nativamente integrações para serviços de nuvem como AWS, Azure e GPC.

21.3.3. Inteligência de Ameaças

21.3.3.1. Deve incluir regras de correlação e inteligência de ameaças.

21.3.3.2. Deve incluir um pacote de regras para detecção. Elas devem ser alimentadas automaticamente, sem gerar impacto ou solicitar intervenção de um analista. Por sua vez, ela deve permitir a criação de regras personalizadas pela CONTRATADA, incluído a entrada manual de novos indicadores de comprometimento.

21.3.3.3. Deve fornecer uma boa variedade de regras de inteligência já criadas e disponíveis para detecção de ameaças e também permitir customização de novas para atender necessidades específicas.

21.3.3.4. Deve incluir inteligência de ameaças que revise, valide e compare as fontes que estão sendo utilizadas para detecção de ameaças.

21.3.3.5. Deve incluir a descrição das famílias de malware.

21.3.3.6. Deve fornecer atribuição automática de alertas a grupos de APTs.

21.3.3.7. O fabricante deve possuir especialistas em segurança que estejam monitorando as ameaças atuais ao redor do mundo, gerando a partir disso, novos pacotes de regras para aprimorar a solução em seu nível de detecção. Tal serviço não deve ocasionar custo adicional para a CONTRATANTE.

21.3.3.8. O fabricante deve rastrear grupos de crimes cibernéticos, a fim de aprimorar regras de detecção a partir de incidentes globais.

21.3.3.9. Deve utilizar uma rede de inteligência que processa diversas amostras de malware exclusivas por dia.

21.3.3.10. Deve injetar inteligência nos dados de log registrados.

21.3.3.11. Deve oferecer análises sobre "beaconing", permitindo no mínimo, a detecção de malwares que tentam estabelecer contato com "Command and Control".

21.3.3.12. Deve incluir como fonte de inteligência as ameaças, plataformas de segurança contratadas e permitir identificar a telemetria e o perfil de proliferação de um ataque, além de ter informações sobre vítimas e táticas, técnicas e procedimentos geralmente utilizados pelo invasor.

21.3.3.13. Deve possibilitar consultas de segurança específicas (Buscando referências a malwares ou ataques conhecidos), incluindo análise, para no mínimo:

21.3.3.14. URLs;

21.3.3.15. Domínios;

21.3.3.16. Hashes MD5;

21.3.3.17. Endereços IP.

21.3.3.18. Deve permitir a criação de listas a serem utilizadas com escopo de inteligência, facilitando assim o uso dessas em regras ou mesmo para customizar detecções específicas do negócio.

21.3.3.19. Depois que uma ameaça for detectada, ela deve relacionar as informações registradas na plataforma central e as vincular fornecendo detalhes de inteligência.

21.3.3.20. Deve oferecer análises mínimas em:

21.3.3.21. Beaconing;

21.3.3.22. Beaconing Diferencial;

21.3.3.23. Geo-feasibility;

21.3.3.24. Uso indevido de credenciais;

21.3.3.25. Detecção de conexão não reconhecida;

- 21.3.3.26. Detecção de Fast-Flux DNS;
- 21.3.3.27. Entropia DNS;
- 21.3.3.28. Detecção de ataques via PowerShell;
- 21.3.3.29. Detecção de Exfiltração de Dados;
- 21.3.3.30. Detecção de conexões de entrada SSH, Telnet, SMB e RDP que sejam anômalas;
- 21.3.3.31. Detecção de contas comprometidas com VPN; e
- 21.3.3.32. Detecção de movimento lateral.
- 21.3.3.33. Deve permitir que sejam realizadas pesquisas em seu ambiente para atividades de "caça" a malwares e atividades maliciosas.
- 21.3.3.34. Deve possuir capacidade analítica de eventos/tráfego, independente das regras, para detecção de no mínimo os seguintes comportamentos:
- 21.3.3.35. Uso suspeito de chave da API Amazon Web Services (AWS);
- 21.3.3.36. Login de autenticação multifator anormal do Duo com base no histórico de login anterior deste usuário;
- 21.3.3.37. Atividade anormal do Google Cloud Platform (GCP) por um usuário;
- 21.3.3.38. Logon anormal no Google workspace com base no histórico de logon anterior deste usuário;
- 21.3.3.39. Login anormal do protocolo RDP (Remote Desktop Protocol) com base no histórico de login anterior deste usuário;
- 21.3.3.40. Download ou upload anormal de arquivo do Google drive com base no histórico anterior deste usuário;
- 21.3.3.41. Tráfego de rede para domínios semelhantes a (permutações) do domínio da organização descoberto. Isso pode indicar um ataque de phishing ou alguma outra atividade suspeita.
- 21.3.3.42. Detecção de força bruta no Linux, realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.
- 21.3.3.43. Detecção de força bruta do Google workspace, realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.
- 21.3.3.44. Vários logins de RDP pelo mesmo usuário.
- 21.3.3.45. Vários logins de RDP no mesmo host.
- 21.3.3.46. Login de VPN anormal com base no histórico de login de VPN anterior do usuário.
- 21.3.3.47. Uma conta de usuário foi excluída dentro de 24 horas após sua criação.
- 21.3.3.48. Detecção de força bruta do Windows NT LAN Manager (NTLM), realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.
- 21.3.3.49. Vários erros de "usuários únicos não encontrados" de uma fonte. Isso pode indicar uma tentativa de enumeração do usuário.
- 21.3.3.50. Vários processos exclusivos de um usuário ou host dentro de um curto período de tempo. Isso pode indicar atividade de reconhecimento.
- 21.3.3.51. Capacidades de Investigação
- 21.3.3.52. Deve incluir recursos de workflow para resposta a incidentes de segurança.
- 21.3.3.53. Deve ser capaz de coordenar os processos de segurança atuais no nível de alertas de rede e alertas de outras soluções de segurança.
- 21.3.3.54. Deve fornecer recursos de busca e pesquisa nas estações de trabalho, de acordo com os seguintes exemplos:
- 21.3.3.55. Ampla pesquisa por comportamentos maliciosos conhecidos;
- 21.3.3.56. Caça proativa de atividades suspeitas;
- 21.3.3.57. Investigação completa nos endpoints comprometidos;
- 21.3.3.58. Procurar evidências de intrusões avançadas como ameaças sem arquivo (fileless).
- 21.3.3.59. Deve fornecer recursos de resposta em tempo real, para no mínimo:
- 21.3.3.60. Investigar todos as atividades em terminais suspeitos;
- 21.3.3.61. Reproduzir a linha do tempo completa de um ataque avançado;
- 21.3.3.62. Capturar detalhes da atividade que ocorreu durante intrusões;
- 21.3.3.63. Executar uma análise aprofundada no nível de acesso ao disco, análise de memória e detecção de rootkit.
- 21.3.3.64. Depois que a solução detectar um alerta, essa deve fornecer pelo menos as seguintes informações:
- 21.3.3.65. A inteligência em torno do alerta detectado;
- 21.3.3.66. Métodos de detecção da ameaça em questão;
- 21.3.3.67. Mostrar graficamente uma linha do tempo de eventos relacionados ao alerta detectado;
- 21.3.3.68. Dicas de pesquisa para orientar os analistas em todo o processo de resposta a incidentes. Essas dicas devem estar associadas à experiência que o fabricante tem em responder a incidentes críticos de segurança em empresas em todo o mundo;
- 21.3.3.69. Mostrar os eventos brutos (raw data) que geraram o alerta; e
- 21.3.3.70. Histórico de eventos associados.
- 21.3.3.71. A visualização de um caso deve permitir pelo menos, as seguintes ações:
- 21.3.3.72. Controle do Nome, Status, Prioridade, Classificação e Descrição do caso;
- 21.3.3.73. Permitir que o caso seja assinado para algum usuário;
- 21.3.3.74. Permitir que qualquer log/evento relacionado possa ser adicionado e visualizado;
- 21.3.3.75. Permitir a visualização de todos os alertas/incidentes envolvidos no caso;
- 21.3.3.76. Permitir que o caso seja exportado em formatos CSV e JSON; e
- 21.3.3.77. Permitir a adição e visualização de comentários no caso.

- 21.3.3.78. Durante o processo de resposta a incidentes, quando um caso for fechado, todos alertas relacionados também devem ser fechados. No caso de alertas que pertencem a mais de um caso, esses devem permanecer abertos.
- 21.3.3.79. Deve incluir dicas intuitivas de investigação, trazendo automaticamente no mínimo, os seguintes dados para consulta no alerta:
- 21.3.3.80. Existem outras regras alertadas para esse IP de origem?
- 21.3.3.81. Existem regras acionadas que foram baseadas em sensores de inteligência, relacionadas a algum desses índices de comprometimento?
- 21.3.3.82. Quais logs estão disponíveis para este dispositivo?
- 21.3.3.83. Quais logs estão disponíveis para este IP?
- 21.3.3.84. Em quais outros hosts esse malware foi encontrado?
- 21.3.3.85. Existem outros logs com esse hash?
- 21.3.3.86. Existem alertas relacionados usando o IP do agente?
- 21.3.3.87. Existem alertas relacionados usando o este dispositivo?
- 21.3.3.88. Existem alertas relacionados usando o hash envolvido no incidente?
- 21.3.3.89. No nível analista/operador, a solução deve fornecer:
- 21.3.3.90. Um painel de pesquisa, onde são registrados alertas e casos atribuídos aos analistas;
- 21.3.3.91. Detalhe de alertas como: nível de risco, nome do alerta, tipo de alerta, origem, data da primeira ocorrência, data da última ocorrência, número de eventos, resumo, fontes e destino, status do alerta e opções de: exportação do alerta nos formatos CSV e JSON para excluir e/ou fechá-lo;
- 21.3.3.92. Cada alerta deve poder ser atribuído a um analista específico, para iniciar o processo de investigação, contenção, caça, etc.;
- 21.3.3.93. Deve haver um painel de casos, que permita a criação, gerenciamento e alocação de casos, a fim de rastrear as atividades e o tempo de resposta de cada analista;
- 21.3.3.94. Cada caso pode conter vários alertas, várias anotações, para validar o estado evolutivo na resposta a um incidente;
- 21.3.3.95. A ferramenta deve poder atribuir a cada caso níveis de: prioridade, gravidade e, como opção, outro tipo de classificação;
- 21.3.3.96. Cada caso deve ter: Descrição, Eventos, Alertas, Revisões e Notas, bem como o registro do qual o analista foi designado ou modificou o caso.
- 21.3.3.97. Deve ter a capacidade de realizar pesquisas para o processo de busca proativa e reativa nos eventos e metadados coletados de maneira automática.
- 21.3.3.98. Deve ter um módulo de pesquisa avançada ou indexação de pesquisa que contenha:
- 21.3.3.99. Um módulo de ajuda de sintaxe;
- 21.3.3.100. Um módulo de histórico de pesquisas;
- 21.3.3.101. Um módulo de pesquisa salva como favorita; e
- 21.3.3.102. Capacidade de salvar a pesquisa.
- 21.3.3.103. As pesquisas devem ter uma sintaxe completa baseada em Query Language contemplando documentação completa e atualizada.
- 21.3.3.104. Deve incluir opções de pesquisa, com base em cada um dos campos de metadados, como: Domínio, porta de destino, método HTTP, metaclasses, porta de origem, useragent, IP de Origem, IP de destino, etc.
- 21.3.3.105. Deve possuir um módulo de UEBA ao qual poderá ser utilizado para melhor compreensão dos eventos, identificando possíveis entidades (equipamentos ou usuários) envolvidos anteriormente em outros eventos maliciosos ou suspeitos.
- 21.3.3.106. A visualização de um alerta/incidente deve permitir pelo menos, as seguintes ações:
- 21.3.3.107. Assinar o incidente para um analista;
- 21.3.3.108. Marcar como falso positivo;
- 21.3.3.109. Adicionar o alerta em um caso para um trabalho aprofundado envolvendo mais pessoas e artefatos de investigação;
- 21.3.3.110. Fechar ou suprimir o alerta;
- 21.3.3.111. Exportar o alerta para CSV ou JSON;
- 21.3.3.112. Fazer pesquisas de Índices de comprometimento diretamente em bases externas como VirusTotal e DomainTools;
- 21.3.3.113. Adicionar através de um clique, artefatos em listas para facilitar o trabalho de investigação e melhorar a assertividade das regras de detecção;
- 21.3.3.114. Visualizar a correlação de índices de comprometimento em outros incidentes abertos ou fechados;
- 21.3.3.115. Consultar análises realizadas automaticamente em bases de inteligência cibernética;
- 21.3.3.116. Analisar o histórico de modificações no incidente;
- 21.3.3.117. Adicionar comentários no incidente;
- 21.3.3.118. Quando realiza análise em sandbox para artefatos envolvidos em incidentes, permitir a visualização das modificações que o binário realizou.
- 21.3.3.119. Ao visualizar um tipo de evento, a plataforma deve permitir, a partir de cliques com o mouse (Sem necessidade de escrita de query), incrementar as buscas, para pelo menos as seguintes ações:
- 21.3.3.120. Realizar uma busca por qualquer campo daquela classe. Exemplo: Ip de origem/destino, hash md5, destinatário/remetente, ações aplicadas, etc;
- 21.3.3.121. No caso de uma busca já estar sendo realizada, deve ser possível adicionar qualquer campo listado na busca atual para seguimento das atividades de hunting;
- 21.3.3.122. Deve ser possível também realizar exclusões na busca a partir do valor de qualquer campo listado;
- 21.3.3.123. Dever ser possível realizar um agrupamento de qualquer valor listado, formando automaticamente um dashboard, estabelecendo as contagens e classificações de acordo com os valores dos campos;

21.3.3.124. Quando visualizado algum índice de comprometimento, deve ser possível realizar pesquisas em bases externas como VirusTotal e DomainTools;

21.3.3.125. Deve ser possível adicionar índices de comprometimento em listas para facilitar as buscas e criação de regras.

21.3.3.126. Deve permitir que as buscas mais realizadas sejam salvas para execução rápida sempre que necessário.

21.3.3.127. Toda busca realizada deve ter a possibilidade de ser transformada em uma regra para detecção de comportamentos desejados.

21.4. **Item 3 - Solução de proteção avançada para endpoints**

21.4.1. Características Gerais

21.4.1.1. As licenças devem ser disponibilizadas por meio de subscrição e devem permanecer plenamente ativas até 30 dias após o término do contrato;

21.4.1.2. A solução deverá estar operacional em 97% do tempo do mês, considerando os aspectos de disponibilidade que competem à CONTRATADA.

21.4.1.3. Capacidade de remover remotamente e automaticamente, de forma nativa ou com uso de scripts, qualquer solução de segurança (própria ou de terceiros) que estiver presente nas estações e servidores;

21.4.1.4. Capacidade de instalar remotamente a solução de segurança nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO (Group Policy) do Microsoft Active Directory;

21.4.1.5. Deve registrar em arquivo de log todas as atividades efetuadas pela solução e deve enviar também essas informações para a console de gerência centralizada da solução;

21.4.1.6. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto;

21.4.1.7. A comunicação de rede entre o cliente e o servidor de administração deve ser criptografada;

21.4.1.8. Integração com serviços de diretórios da solução Microsoft Active Directory ou OpenLDAP;

21.4.1.9. A solução deverá ser compatível com os seguintes sistemas operacionais:

21.4.1.10. Endpoints Windows 7 ou superior e servidores Windows Server 2019 ou superior; e

21.4.1.11. Servidores e estações de trabalho com, no mínimo, os sistemas operacionais GNU/Linux:

21.4.1.12. Plataforma 32-bits:

21.4.1.13. Red Hat Linux 6.7 e superiores;

21.4.1.14. CentOS 6.7 e superiores; e

21.4.1.15. Debian 9.4 e superiores.

21.4.1.16. Plataforma 64-bits:

21.4.1.17. Ubuntu 18.04 e superiores;

21.4.1.18. Red Hat Enterprise Linux 6.7 e superiores;

21.4.1.19. CentOS 6.7 e superiores;

21.4.1.20. Debian 9.4 e superiores;

21.4.1.21. SUSE Server 12 e superiores;

21.4.1.22. Oracle Linux 7.0 e superiores;

21.4.1.23. Oracle Linux 8.0 e superiores; e

21.4.1.24. Oracle Linux 9.0 e superiores.

21.4.1.25. A CONTRATADA deverá fornecer todos os softwares auxiliares necessários para o funcionamento da solução e sem custo adicional;

21.4.1.26. A solução e seus softwares auxiliares, que estejam implantados localmente, devem continuar funcionando após o término do contrato com as últimas atualizações baixadas antes do encerramento do contrato;

21.4.1.27. Não será permitido o envio de arquivos, links, endereços e quaisquer outras informações proprietárias da CONTRATANTE para a nuvem. Será permitido apenas o tráfego de dados e metadados imprescindíveis para o funcionamento da solução;

21.4.1.28. Qualquer módulo da solução que tenha de ser necessariamente hospedado ou que tenha de usar recursos em nuvem deve satisfazer os requisitos mínimos de segurança da informação nos termos deste Termo de Referência;

21.4.1.29. A solução deve ser capaz de gerenciar o agendamento de atualizações e instalações de políticas e agentes;

21.4.1.30. Todas as funcionalidades dos módulos especificados devem ser otimizadas, adaptativa ou manualmente, para endpoints e servidores com poucos recursos computacionais (CPU, RAM e disco) de modo a não comprometer a utilização do ativo protegido;

21.4.1.31. Todos os módulos auxiliares imprescindíveis ao funcionamento da console de gerenciamento devem ser implementados em alta disponibilidade.

21.4.1.32. A solução deverá possuir seu gerenciamento centralizado;

21.4.1.33. A console de gerenciamento deverá ser única e não deverá possuir limite de endpoints e servidores gerenciados.

21.4.2. Solução de Proteção de computadores

21.4.2.1. A solução de gerência centralizada deve:

21.4.2.2. permitir a geração de relatórios, visualizar eventos, gerenciar políticas e, preferencialmente, a criação de painéis de controle customizados;

21.4.2.3. permitir, de forma nativa ou por meio da utilização de scripts, a visualização da situação, dos recursos instalados (CPU, memória, discos, conexões de rede, dentre outros), softwares instalados, em tempo real, de todos os ativos administrados pela console de gerenciamento centralizada;

21.4.2.4. gerenciar estações de trabalho, servidores de rede e servidores de arquivos protegidos pela solução de segurança;

21.4.2.5. ser capaz de importar a estrutura da solução Microsoft Active Directory para descoberta de máquinas;

- 21.4.2.6. permitir, por meio da console de gerenciamento, a criação de políticas para a retenção em servidor de rede de arquivos que violam as políticas de segurança definidas para os ativos abrangidos pela solução;
- 21.4.2.7. monitorar diferentes sub-redes a fim de encontrar máquinas novas para serem adicionadas à proteção; para soluções em nuvem será aceito o uso do Microsoft Active Directory, scripts ou outras ferramentas para executar tal função;
- 21.4.2.8. A solução deverá ser capaz de identificar no mínimo as seguintes informações no descobrimento da rede:
- 21.4.2.9. Tipo de sistema operacional;
- 21.4.2.10. Fabricante;
- 21.4.2.11. Mac Address;
- 21.4.2.12. Versão do Sistema Operacional;
- 21.4.2.13. Endereço(s) IP(s); e
- 21.4.2.14. Hostname;
- 21.4.2.15. ser capaz de, assim que detectar máquinas novas, nativamente ou através de Script nos diretórios da solução Microsoft Active Directory, sub-redes ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o agente da solução instalado. Caso não possua, deve instalar o agente da solução automaticamente ou por ação do administrador;
- 21.4.2.16. definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
- 21.4.2.17. fornecer, de forma nativa ou por meio da exportação de relatório, as seguintes informações dos ativos protegidos:
- 21.4.2.18. Quais módulos de segurança estão instalados;
- 21.4.2.19. Quais módulos de segurança estão com o serviço iniciado;
- 21.4.2.20. Quais módulos de segurança estão atualizados;
- 21.4.2.21. Minutos/horas desde a última conexão do ativo com o servidor administrativo;
- 21.4.2.22. Minutos/horas desde a última atualização;
- 21.4.2.23. Data e horário da última varredura executada no ativo;
- 21.4.2.24. Versão dos módulos de segurança instalados no ativo;
- 21.4.2.25. Quantidade de ameaças identificadas no ativo;
- 21.4.2.26. Nome do ativo;
- 21.4.2.27. Domínio ou grupo de trabalho do ativo;
- 21.4.2.28. Sistema operacional;
- 21.4.2.29. Endereço IP;
- 21.4.2.30. Eventos de segurança relacionados aos aplicativos instalados no ativo; e
- 21.4.2.31. Informações sobre incidentes no painel central.
- 21.4.2.32. Exportar relatórios, de forma nativa ou por meio de API, para os tipos de arquivos PDF e HTML e, opcionalmente, para os tipos de arquivos XML, CSV e JSON.
- 21.4.2.33. Gerar, de forma preferencial, eventos (traps) SNMP (Protocolo Simples de Gerenciamento de Rede) para monitoramento de eventos.
- 21.4.2.34. Enviar e-mails para contas específicas em caso de algum evento específico.
- 21.4.2.35. A solução deverá ser capaz de apresentar o risco do aplicativo de terceiros baseados no seu CVSS;
- 21.4.2.36. A solução deverá ser capaz de realizar uma varredura afim de identificar aplicativos de terceiros instalados no ambiente.
- 21.4.2.37. O modulo de inventário de aplicativos deverá suportar todos os sistemas operacionais listados no item 21.4.1.10.
- 21.4.2.38. Reportar vulnerabilidades de softwares presentes nos ativos ou possuir mecanismos de proteção contra exploração de vulnerabilidades.
- 21.4.2.39. Disponibilizar a criação de perfis e papéis de acesso. Exemplo: Administradores, operadores, monitores.
- 21.4.2.40. Ser capaz de se integrar com a solução Microsoft Active Directory ou serviço de diretório OpenLDAP para a autenticação no painel central de gerência ou suportar autenticação por OpenID Connect (OIDC), Security Assertion Markup Language (SAML) ou OAuth 2.0 para realizar Single Sign On (SSO).
- 21.4.2.41. Ser capaz de gerar relatório forense detalhando o modus operandi de cada malware identificado e informar qual foi o vetor de contaminação/entrada em cada ocorrência.
- 21.4.2.42. Possuir console única de visibilidade e de consolidação de gerenciamento integrado do ambiente monitorado por múltiplos ativos (endpoints, servidores e dispositivos).
- 21.4.2.43. Possuir integração com syslog ou SIEM.
- 21.4.2.44. Possuir integração com a solução de SOAR prevista no item 2.
- 21.4.2.45. Ser capaz de desativar temporariamente funcionalidades da solução, quando necessário para efeitos de suporte, localmente, mas protegida com senha.
- 21.4.2.46. Ser capaz de gerenciar o envio de alertas e notificações.
- 21.4.2.47. Centralizar a gerência de todos os recursos e funcionalidades especificadas.
- 21.4.2.48. Permitir o agendamento e envio de relatórios por e-mail.
- 21.4.2.49. Permitir a criação de relatórios customizados.
- 21.4.2.50. Possuir modelos predefinidos de relatórios de forma a facilitar a geração de relatórios.
- 21.4.2.51. Ser capaz de criptografar toda comunicação entre o painel de gerenciamento e a solução.
- 21.4.2.52. Ser gerenciada totalmente por console web.

- 21.4.2.53. A solução de Proteção de Computadores deve possuir as seguintes características e funcionalidades:
- 21.4.2.54. ser capaz de atualizar os pacotes de instalação com as últimas vacinas ou trabalhar com uma abordagem baseada em inteligência artificial e machine learning;
- 21.4.2.55. ser capaz de identificar e bloquear, no mínimo, os seguintes tipos de malwares: ameaças de dia zero (zero-day), direcionamento, ransomware, spyware, worm, adware, bot(nets), rootkits, trojan, fileless virus, vírus;
- 21.4.2.56. ser capaz de, no mínimo, identificar artefatos maliciosos por meio das seguintes técnicas: análise baseada em assinaturas ou equivalente, análise baseada em reputação (hashes de Indicadores de Comprometimento) machine learning com pré-execução, análise comportamental, análise heurística, mecanismo de emulação, mecanismo de inteligência artificial, análise de comunicações de rede;
- 21.4.2.57. possuir os seguintes módulos de segurança:
- 21.4.2.58. firewall;
- 21.4.2.59. proteção de navegadores web, ou a solução deverá ser capaz de bloquear ataques do tipo fileless;
- 21.4.2.60. controle de aplicação, ou a solução deverá ser capaz de identificar aplicativos de terceiros vulneráveis e bloquear através de hash;
- 21.4.2.61. filtro de reputação web nativo, ou a partir de integração com ferramentas de terceiros, ou a solução deverá através de seus motores realizar os bloqueios de ataques maliciosos no navegador;
- 21.4.2.62. controle de dispositivos;
- 21.4.2.63. detecção e resposta para computadores (endpoint detection and response);
- 21.4.2.64. proteção de memória; e
- 21.4.2.65. proteção anti-malware para computadores com GNU/Linux.
- 21.4.2.66. possuir módulo de prevenção de perda de dados (Data Loss Protection – DLP) ou controle de dispositivos periféricos, assim prevenindo a perda de dados;
- 21.4.2.67. aplicação de políticas e mecanismos de segurança que alertem e protejam contra ameaças a vulnerabilidades em sistemas operacionais e nas aplicações instaladas;
- 21.4.2.68. ser dotada de um módulo de controle de aplicação com as seguintes características:
- 21.4.2.69. possibilitar a criação de política de bloqueio de execução de aplicações por: nome de arquivo ou diretório ou hash;
- 21.4.2.70. possibilitar a criação de política para a liberação de aplicações assinadas por uma autoridade certificadora raiz confiável. A ferramenta deverá possuir uma relação prévia de autoridades certificadoras confiáveis e a CONTRATANTE poderá importar as suas;
- 21.4.2.71. possibilitar a liberação e bloqueio de aplicações por meio de white list e black list de aplicações;
- 21.4.2.72. aplicar o controle de aplicação em tempo de execução;
- 21.4.2.73. monitorar alterações em arquivos e chaves de registro em tempo real e possuir mecanismos de proteção;
- 21.4.2.74. possuir proteção contra adulteração de programas (executáveis, binários, DLLs, scripts, etc);
- 21.4.2.75. possibilitar a criação de políticas para computadores específicos, onde somente será permitido executar programas autorizados (white list) ou serão bloqueados os programas não autorizados (black list);
- 21.4.2.76. na lista de bloqueio via política de controle de aplicação;
- 21.4.2.77. ser capaz de permitir e bloquear a instalação e a execução de programas específicos, categorias de programas (no caso de endpoints), de acordo com política definida pela CONTRATANTE;
- 21.4.2.78. analisar as ações de cada aplicação em execução no endpoint ou servidor, gravando tais ações executadas e comparando-as com sequências características de atividades suspeitas ou perigosas; e
- 21.4.2.79. analisar qualquer tentativa de edição, exclusão ou gravação do registro do Windows ou de arquivos de configuração em distribuições GNU/Linux antes de sugerir ações e bloquear comportamentos suspeitos e perigosos.
- 21.4.2.80. ser dotada de um módulo de controle de dispositivos com as seguintes características:
- 21.4.2.81. capaz de controlar a utilização de dispositivos removíveis permitindo a identificação e o controle de leitura, escrita e execução. Os seguintes padrões de portas físicas devem ser suportados: USB, Thunderbolt, Firewire, CD/DVD, SD Card, eSATA e micro USB;
- 21.4.2.82. ser capaz de identificar, permitir e bloquear a utilização de dispositivos acoplados nos ativos protegidos pela solução; e
- 21.4.2.83. ser capaz de identificar e impedir movimentos laterais suspeitos e maliciosos por meio do isolamento do equipamento gerenciado.
- 21.4.2.84. Verificar a confiabilidade dos executáveis e caso não seja confiável, deverá possuir capacidade para impedir sua execução.
- 21.4.2.85. Ser capaz de bloquear a execução de executáveis em geral em dispositivos removíveis.
- 21.4.2.86. Ser capaz de verificar a integridade de arquivos do sistema operacional e de programas instalados.
- 21.4.2.87. Ser capaz de registrar na base de reputação os novos malwares identificados.
- 21.4.2.88. Ser dotada de um módulo de proteção de memória capaz de identificar e bloquear ações maliciosas realizadas por softwares permitidos. Exemplo: execução de shellcodes, comandos, ações com privilégios elevados, etc.
- 21.4.2.89. Capaz de remover arquivos maliciosos automaticamente.
- 21.4.2.90. Ser capaz de mover arquivos suspeitos para área protegida no computador ou tomar alguma ação de mitigação de tais arquivos, de acordo com a definição em política.
- 21.4.2.91. Ser capaz de mover arquivos maliciosos para servidor de rede de acordo com a definição em política ou permitir a recuperação do arquivo no computador por meio da console de gerenciamento centralizada.
- 21.4.2.92. Ser capaz de tratar exceções, evitando o bloqueio e até mesmo a verificação de processos, diretórios e executáveis especificados em políticas.
- 21.4.2.93. Ser capaz de se integrar com sistemas SIEM ou SOAR externos.
- 21.4.2.94. Ser capaz de detectar a presença de soluções de proteção de computadores de outro fabricante que possa causar incompatibilidade.

- 21.4.2.95. Ser dotada de um módulo de proteção de navegação web capaz de verificar tráfego nos browsers mais utilizados no mercado executando bloqueio por reputação ou categorização do URL.
- 21.4.2.96. Ser dotada de um módulo de filtro de conteúdo web capaz de adicionar sites da web em uma lista de exclusão (black list) e em uma lista de permissão (white list).
- 21.4.2.97. Ser dotada de proteção contra desinstalação por meio de senha.
- 21.4.2.98. Ser dotada de um módulo de firewall para endpoints e servidores gerenciado a partir da console de gerência centralizada, com filtragem de pacotes e de aplicativos;
- 21.4.2.99. Utilizar um agente único nos endpoints e servidores, de modo a atender todas as funcionalidades, não sendo permitido o uso de agentes simultâneos no mesmo ativo.
- 21.4.2.100. Ser dotada de um módulo de proteção contra ransomware capaz de desfazer quaisquer alterações criptográficas nos arquivos dos endpoints e servidores.
- 21.4.3. Solução de Detecção e Resposta de Ameaças contra computadores
- 21.4.3.1. O módulo de Endpoint Detection and Response deve possuir as seguintes características:
- 21.4.3.2. possibilitar a investigação nos endpoints e servidores Windows e GNU/Linux via console de gerenciamento, por meio de consultas customizadas que serão realizadas em todos os computadores com o módulo ativado;
- 21.4.3.3. possibilitar a detecção e identificação de atividades suspeitas em todos os computadores com o módulo ativado;
- 21.4.3.4. gerar trilha de auditoria dos eventos nos computadores com o módulo ativo. As informações de auditoria devem conter, no mínimo:
- 21.4.3.5. informações sobre processos: criados, finalizados, hash SHA-1 e SHA-256, ID, Time, User, comando que iniciou o processo, RAM utilizada pelo processo e Threads criados pelo processo, registros e bibliotecas alteradas;
- 21.4.3.6. informações sobre conexões de rede: endereço IP de origem e destino, portas de origem e destino;
- 21.4.3.7. informações sobre arquivos: nome do arquivo, data de criação, data de modificação e data de exclusão;
- 21.4.3.8. informações sobre registros de sistema: nomes de chaves e valores correspondentes. Os valores deverão constar nos registros; e
- 21.4.3.9. informações sobre Sistema Operacional: versão, grupo de usuários locais, membros de grupos de usuários locais e usuários locais.
- 21.4.3.10. consultas à trilha de auditoria via console de gerenciamento centralizada;
- 21.4.3.11. permitir a execução de scripts (PowerShell, VisualBasic, BAT ou Python em computadores Windows e ShellScript ou Python em servidores GNU/Linux) ou de ações pré-definidas e customizáveis (no mínimo: isolar o host, verificar IoC's e isolar ou prevenir a execução de arquivos);
- 21.4.3.12. possuir políticas pré-configuradas;
- 21.4.3.13. permitir a criação de coletores de informações e a execução de scripts sob demanda em computadores;
- 21.4.3.14. armazenar os eventos nos computadores e disponibilizar consulta a eles via console de gerenciamento.
- 21.4.3.15. Solução contra exploração do ambiente Active Directory:
- 21.4.3.16. Capacidade de rodar simulações de ataques descobrindo backdoors e hooks persistentes no Microsoft Active Directory;
- 21.4.3.17. Monitoração comportamental determinando o risco e por conseguinte o bloqueio da ameaça, protegendo contra os ataques de ransomware e stealthy, tal como scripts maliciosos em Powershell e WMI;
- 21.4.3.18. A solução deve ter a capacidade de ser implementada a partir do cliente de Proteção do Endpoint do próprio fabricante;
- 21.4.3.19. A solução deve ter a capacidade avançada de segurança de endpoints especificamente para ser implementada na defesa do MS Active Directory para lidar contra os ataques de Stealthy e APTs, protegendo o AD contra ataques iniciados a partir de qualquer endpoint com acesso à rede, seja ele dentro ou fora do domínio;
- 21.4.3.20. A solução deve ter a capacidade de detecção, investigação e contenção de intrusões;
- 21.4.3.21. A solução deve ter a capacidade específica de interromper a atividade de reconhecimento, implementando a contenção de ataques a partir do endpoint, impedindo que os atacantes usem o MS Active Directory para roubar credenciais de domínio e iniciar os ataques de movimentação lateral;
- 21.4.3.22. A solução deve ter a capacidade de realizar simulações contínuas e automatizadas de ataques para encontrar backdoors e hooks de persistência no MS Active Directory;
- 21.4.3.23. A solução deve ter a capacidade de aprender autonomamente a estrutura do MS Active Directory da organização em sua totalidade e utilizar esses dados para criar uma extensão de estrutura autêntica e ilimitada, possibilitando utilizar este ambiente como isca para os atacantes em uma perspectiva dos ativos conectados ao domínio, utilizando a monitoração da interação dos atacantes com esta estrutura para bloquear ações derivadas, tais como o bloqueio de novos comandos, injeção de códigos em outros aplicativos e até mesmo um simples comando de conectividade (ex.: ping);
- 21.4.3.24. A solução deve ter a capacidade de utilizar metodologias exclusivas de resposta a incidentes para um ambiente corporativo de domínio do MS Active Directory, fornecendo relatórios forenses em tempo real que capturam fases reais de reconhecimento do ambiente atacado, o roubo de credenciais e movimentações laterais que foram executadas pelo atacante;
- 21.4.3.25. A solução deve ter a capacidade de documentar a cadeia de ataque até a vítima zero identificando a origem do ataque, possibilitando avaliar se o ataque é um incidente local, assim como externo; A solução deve ter a capacidade de implementar uma mitigação automatizada interrompendo o processo mal-intencionado no endpoint, impedindo, assim, a violação em tempo real, bloqueando sua capacidade de criar outro processo, sobrescrever outra parte da memória, executar comandos de reconhecimento e até mesmo se comunicar com a rede;
- 21.4.3.26. A solução deve ter a capacidade de implementar uma avaliação de ameaças do ambiente do MS Active Directory, examinando erros de configuração de domínio, vulnerabilidades e ameaças persistentes, utilizando-se uma ferramenta para reunir informações sobre a segurança do MS Active Directory;
- 21.4.3.27. A ferramenta deve ter a capacidade de ao verificar uma configuração incorreta ou um backdoor, gerar um relatório em HTML com recomendações sobre correções;
- 21.4.3.28. A solução deve ter a capacidade de implementar avaliações para vulnerabilidades e erros de configurações especificamente para o MS Active Directory, utilizando a técnica de simulação de ataques para no mínimo:
- 21.4.3.29. Avaliação de conta de usuário, implementando a descoberta de contas de administradores potencialmente perigosas;

- 21.4.3.30. Avaliação de vulnerabilidade do Kerberos, implementando a descoberta de controladores de domínio que permitam a modificação de certificado de atributo privilegiado;
- 21.4.3.31. Avaliação de Contas de Serviço, implementando a descoberta de contas de serviço vulneráveis expostos ao cracking do Kerberos;
- 21.4.3.32. Avaliação de Local Admin Traversal, implementando a descoberta de rotas de movimento lateral usando a conta de administrador local;
- 21.4.3.33. Avaliação LDAP, validando controladores de domínio que permitem conexões anônimas ou não criptografadas;
- 21.4.3.34. Avaliação de hosts que permitem a descoberta de rede;
- 21.4.3.35. A solução deve ter a capacidade de mascarar a topologia do domínio MS Active Directory, dificultando a análise do ambiente, onde toda tentativa de consulta (query) deve ser controlada pelo endpoint;
- 21.4.3.36. A solução deve ter a capacidade de gerar novos objetos mascarados com base no esquema de nomenclatura e topologia atual do Órgão, implementando a capacidade de aprender os computadores, os usuários, as regras de nomenclatura utilizada nos usuários administradores, recriando os novos objetos com base neste aprendizado;
- 21.4.3.37. A solução deve ter a capacidade de configurar conforme a necessidade do Órgão o fator multiplicador de mascaramento de acordo com cada objeto, variando para cima ou para baixo implementado a quantidade desejada de objetos falsos distribuídos pela solução;
- 21.4.3.38. A solução deve ter a capacidade de mascarar minimamente os seguintes objetos dentro do MS Active Directory:
- 21.4.3.39. Contas de usuários com acessos;
- 21.4.3.40. Servidores conectados ao domínio; Desktop conectados ao domínio;
- 21.4.3.41. Notebooks conectados ao domínio;
- 21.4.3.42. Contas de Serviço expostas a possíveis ataques de "Kerberoasting";
- 21.4.3.43. A solução deve ter a capacidade de quando um ataque for detectado, gerar um alerta a partir do endpoint, em conjunto com uma verificação sob demanda reunindo informações forenses específicas relacionadas ao ataque;
- 21.4.3.44. A solução deve ter a capacidade de automatizar o processo forense e verificar as informações corretas, somente quando um ataque é detectado, garantindo a priorização correta reduzindo a incidência de falsos positivos;
- 21.4.3.45. A solução deve ter a capacidade de utilizar-se da Manipulação de Memória implantada nos endpoints após sua autenticação, sem a necessidade de nenhuma instalação nos Controladores de Domínio e sem o uso de agentes em execução no disco dos endpoints;
- 21.4.3.46. A solução deve ter a capacidade de ser implantada sem a necessidade de monitoramento de rede, sem nenhum tipo de alteração de rede, sem nenhuma alteração no MS Active Directory;
- 21.4.3.47. Deve possuir proteção a integridade do Active Directory (AD), tanto da perspectiva do Endpoint quando do próprio Active Directory;
- 21.4.3.48. Deve possuir proteção contra técnicas de reconhecimento do domínio, sendo capaz de detectar um invasor que utilize técnicas de movimentação lateral e roubo de credenciais válidas;
- 21.4.3.49. Deve proteger contra intrusões realizadas a partir de processos, usuários e terminal;
- 21.4.3.50. Deve ser capaz de identificar vulnerabilidades, erros de configurações e possíveis Backdoors presentes no Active Directory;
- 21.4.3.51. Deve ser capaz de proteger alterações no Active Directory sem a necessidade de instalação de agentes ou de componentes adicionais;
- 21.4.3.52. Deve ser capaz de detectar e proteger roubos de credenciais no ambiente que utilizem as técnicas Pass-the-Hash e Pass-the-Ticket;
- 21.4.3.53. Deve ter a capacidade de alarmar Tentativas de Força-Bruta de máquinas que estejam fora do domínio;
- 21.4.3.54. Deve detectar ataques que ocorram na fase de pós-violação, detectando as fases de reconhecimento, roubo de credenciais e movimentações laterais;
- 21.4.3.55. Deve fornecer proteção contra no mínimo os seguintes ataques:
- 21.4.3.56. Pass-The Ticket;
- 21.4.3.57. Pass-The-Hash;
- 21.4.3.58. Overpass-The-Hash;
- 21.4.3.59. Forged PAC;
- 21.4.3.60. DCSync;
- 21.4.3.61. Enumeração de Sessão;
- 21.4.3.62. Golden Tickets;
- 21.4.3.63. Deve detectar pontos de persistência maliciosos no Sistema;
- 21.4.3.64. Deve ser capaz de listar processos e credenciais carregados na memória em um determinado momento do tempo.
- 21.4.3.65. A solução deve ser capaz de listar, no mínimo:
- 21.4.3.66. Estatísticas avançadas de rede;
- 21.4.3.67. Lista de processos;
- 21.4.3.68. Tickets do Kerberos na memória;
- 21.4.3.69. Tentativas de Pass-the-Hash;
- 21.4.3.70. Histórico de navegação e downloads no endpoint;
- 21.4.3.71. Deve ser capaz de conter um ataque de forma automática ao Active Directory;
- 21.4.3.72. Deve ter a capacidade de a partir das atividades detectadas classificá-las com severidades: Baixa, Média e Alta;
- 21.5. **Item 4 - Serviço de operação, monitoramento e tratamento de eventos de segurança**
- 21.5.1. Os serviços especializados listados deverão conter as seguintes frentes de atuação:
- 21.5.1.1. Serviços de operação e sustentação de segurança;
- 21.5.1.2. Serviço de Gestão de Incidentes de Segurança; e

21.5.1.3. Serviço de descoberta, gestão de vulnerabilidades de segurança e validação de segurança.

21.5.2. **Requisitos Gerais**

21.5.3. Os serviços de atendimento de requisições deverão ser prestados em horário comercial corrente do CONTRATANTE, de segunda-feira a sexta-feira, de forma híbrida;

21.5.4. Os serviços de atendimento de incidentes deve ser prestados em escala 24/7, podendo a CONTRATADA trabalhar no regime de plantão;

21.5.5. Os serviços de monitoramento deverão estar funcionais 24/7;

21.5.6. O serviço será realizado por meio de pagamento fixo mensal, vinculado ao atendimento de níveis mínimos de serviços, não se configurando como de dedicação exclusiva de mão de obra, contratação por homem/hora e tampouco por postos de trabalho.

21.5.7. Para a adequada execução do serviço, foi estimado como necessário 1 Administrador em segurança da Informação - Sênior e 2 Administrador em segurança da Informação - Pleno, podendo a CONTRATADA readequar a quantidade e realizar ajustes na composição, desde que atenda todos os níveis de serviços e a outros requisitos desse Termo de Referência.

21.5.8. O modelo de execução desse serviço deverá ser híbrida, com pelo menos um profissional alocado presencialmente nas dependências da CONTRATANTE em horário comercial de segunda-feira a sexta-feira.

21.5.8.1. A Operação deve se preparar para prestação de serviço para o seguinte cenário tecnológico (superfície de ataque):

ID	Descrição	Quantidade
1	Estações windows	280
2	Servidores Windows	10
3	Servidores Linux	16
4	Firewalls de aplicação	5
5	Firewall de rede	1
6	Switches de rede	14
7	Wireless Lan (WLAN)	30
8	Balanceadores de carga	1
9	IPS/IDS	1
10	Servidores VPN	1
11	Web proxy	1
12	Hypervisors	1
13	Web servers	5
14	Servidores Banco de dados	4
15	Servidores de Mail	1
16	Solução de backup	1
17	Impressoras	15
18	Sistema de vigilância	1
19	Sistemas	2
20	Aplicativos no code	6
21	Portais	3
22	Usuários	280
23	Volume de dados no ambiente (em Tb)	5

21.5.8.2. O catálogo de serviço contempla a implementação, suporte, administração diária e sustentação de todos os serviços envolvidos neste Termo de Referência, bem como o suporte, administração diária e sustentação de todos os outros ativos de segurança, como os listados abaixo. O catálogo completo está no Anexo I desse Termo.

- NewGeneration Firewall - FortiGate;
 - WebFilter;
 - Application control;
 - IDS/IPS;
 - Proxy;
 - VPN;
- WAF;
- Proteção de endpoint/Anti-vírus/anti-malware (contratado nesse certame);
- SIEM e SOAR (contratados nesse certame);
- Gestão de vulnerabilidade (contratados nesse certame);
- Patching management (contratados nesse certame);
- Anti-Dos - CloudFlare;
- Anti-spam - GSuite;
- DLP - GSuite;
- Backup - Veeam e Exagrid;
- Network Access Control - Clearpass Aruba/Cloudflare;
- PAM (a ser contratado);

21.5.9. O rol de ativos elencado acima não é taxativo e outras ferramentas que a CONTRATANTE venha a contratar e que CONTRATANTE e CONTRATADA concordem que se trata de um ativo de segurança da informação, será incorporado ao catálogo de serviço da equipe de Operação em Segurança. Para cada novo ativo ou troca de solução, será concedido um prazo de 90 (noventa) dias corridos de período de adaptação.

21.5.10. Quando um novo ativo de segurança for incluído no parque tecnológico ou um ativo for substituído por outro fabricante/marca/modelo, a CONTRATANTE irá realizar o repasse de conhecimento e fornecer manuais para a adequada sustentação do ativo.

21.5.10.1. Entende-se por implementação, todos os passos necessários para completa instalação dos serviços, seguindo as melhores práticas para cada tema envolvido, de modo que esses fiquem completamente operacionais para utilização no ambiente;

21.5.11. Entende-se por suporte, o acompanhamento contínuo de saúde dos serviços, assim como aplicação de correções para qualquer comportamento anômalo identificado, assim como a instalação de novas versões e patches de correção;

- 21.5.12. Entende-se por administração diária, que a CONTRATADA será responsável pela administração de todos os passos técnicos e processos que envolvem os serviços de segurança da informação, de forma que essas sejam 100% integradas ao ambiente da CONTRATANTE, porém utilizando a mão de obra da CONTRATADA;
- 21.5.13. Entende-se por sustentação, que a CONTRATADA será responsável pela sustentação de todos os ativos e serviços de segurança, sendo responsáveis pela implementação de cada processo, integração ou interação técnica de qualquer natureza envolvendo os serviços de segurança da informação;
- 21.5.14. Fica fora do escopo da CONTRATADA, apenas atividades que envolvam interação com as ferramentas de rede e infraestrutura da CONTRATANTE, porém a CONTRATADA ainda fica responsável pela indicação de todas as necessidades de segurança para que os times responsáveis possam desenvolver suas tarefas.
- 21.5.15. A CONTRATADA deverá seguir o processo de mudança estabelecido pela CONTRATANTE.
- 21.5.16. A CONTRATADA deverá implementar conceitos de Threat Hunting, monitorando de forma contínua todos eventos correlacionados;
- 21.5.17. As manutenções preventivas e/ou corretivas, que representem risco de interrupção do(s) serviço(s), deverão ser agendadas e realizadas fora do horário regular, salvo quando expressamente autorizado;
- 21.5.18. As manutenções programadas, que impliquem em extensiva parada do ambiente serão realizadas durante um final de semana. Tais atividades realizadas fora do horário regular não ensejarão qualquer pagamento adicional em relação ao estabelecido no contrato, portanto a CONTRATADA deverá prever esta situação em sua composição de custos;
- 21.5.19. Todos os serviços de manutenção corretiva e preventiva são considerados de natureza contínua e deverão minimizar a necessidade de parada do ambiente em produção;
- 21.5.20. A CONTRATADA deverá de forma proativa, analisar políticas e processos de segurança da CONTRATANTE e realizar sugestões de melhoria a serem implementadas em conjunto com todas as equipes envolvidas.
- 21.5.21. Os serviços deverão ser executados por profissionais habilitados, com base em programas de formação e/ ou certificações oficiais dos serviços envolvidos neste Termo de Referência;
- 21.5.22. A CONTRATADA deverá elaborar e manter atualizados os Planos de Capacidade, de Gerenciamento de Incidentes, de Disponibilidade, de Continuidade e de Recuperação de Desastres para os serviços objeto deste Termo;
- 21.5.23. Os serviços devem ser executados de acordo com normas, procedimentos e técnicas adotadas pela CONTRATANTE;
- 21.5.24. Deverá ser fornecido à CONTRATANTE acesso à console dos serviços fornecidos para que seja possível o acompanhamento, auditoria e direcionamento de ações no ambiente;
- 21.5.25. A CONTRATADA deverá comunicar a CONTRATANTE quanto a ocorrência de qualquer incidente de segurança, seguido de todas as ações de remediação realizadas.
- 21.5.26. Os contatos para notificação de incidentes críticos ou fluxos para aprovação de ações serão documentados durante o período de implementação.
- 21.5.27. A CONTRATADA deverá assumir atividades de customização de interpretação de logs/eventos que possam não ser interpretados nativamente pelo SIEM. Tais atividades não deverão ter nenhum custo adicional.
- 21.5.28. A CONTRATADA deverá customizar e disponibilizar dashboards/relatórios solicitados pela CONTRATANTE. Essas visões serão armazenadas na console do SIEM e poderão ser consultadas a qualquer momento. Tais atividades não deverão ter nenhum custo adicional e serão realizadas dentro do horário comercial.
- 21.5.29. Sempre que necessário, a CONTRATADA deverá customizar regras de detecção no SIEM, atendendo boas práticas de segurança da informação e também a demandas específicas da CONTRATANTE.
- 21.5.30. Qualquer atividade realizada fora do horário comercial não deverá atribuir nenhum custo adicional para a CONTRATANTE.
- 21.5.31. Qualquer atualização de plataformas envolvidas na contratação não deverá ter nenhum custo adicional para a CONTRATANTE.
- 21.5.32. A CONTRATADA deverá realizar ações referentes a resposta a incidentes de segurança, envolvendo sempre que necessário responsáveis por soluções administradas por time terceiros, com o objetivo de manter a disponibilidade e qualidade de todos os serviços tecnológicos.
- 21.5.33. Sempre que necessário envolvimento de times terceiros que administram outras soluções da CONTRATANTE, a CONTRATADA deverá enviar os incidentes preenchidos, analisados e contextualizados, apenas para tomada de decisão e/ou execução de ações pontuais.
- 21.5.34. Toda interação com times terceiros deverão ser realizadas por e-mail ou através da ferramenta de chamados da CONTRATANTE, ficando a cargo da CONTRATANTE definir qual meio será adotado.
- 21.5.35. A CONTRATADA deverá ter fluxos de resposta a incidentes bem definidos para os mais variados tipos de incidentes existentes.
- 21.5.36. A CONTRATADA deverá criar relatórios gerenciais a serem apresentados e entregues para a CONTRATANTE mensalmente, em dia a ser definido no período de implementação. Os dados deste relatório poderão ser customizados a pedido da CONTRATANTE, de modo a atender necessidades específicas de negócio. Adicionalmente, os relatórios devem conter índices de resposta a incidentes, indicadores e efetividade de todas os serviços contratados.
- 21.5.37. Todas as ações de resposta a incidentes executadas pela CONTRATADA deverão ser armazenadas em procedimentos operacionais, para consultas sempre que necessário.
- 21.5.38. A contratada deverá detectar e reportar qualquer tipo de incidentes que tenham características de reincidência.
- 21.5.39. Serão considerados incidentes de segurança, minimamente, as seguintes ações:
- 21.5.39.1. Aplicações maliciosas detectadas em estações de trabalho e servidores;
- 21.5.39.2. Exploração de vulnerabilidades;
- 21.5.39.3. Uso indevido de credenciais;
- 21.5.39.4. Phishing ou spam;
- 21.5.39.5. Ataques de Força Bruta;
- 21.5.39.6. Execução de códigos ou scripts maliciosos;
- 21.5.39.7. Ataques de saturação;
- 21.5.39.8. Comunicações com IPs ou domínios maliciosos;

- 21.5.39.9. Atividades que tenham o intuito de comprometer a integridade de ativos e entidades da CONTRATANTE;
- 21.5.39.10. Atividades que tenham o intuito de comprometer a confidencialidade de informações da CONTRATANTE;
- 21.5.39.11. Atividades que tenham o intuito de comprometer a disponibilidade dos serviços tecnológicos oferecidos pela CONTRATANTE.
- 21.5.39.12. A CONTRATADA deverá disponibilizar um canal e um e-mail, possibilitando que a CONTRATANTE comunique qualquer incidente de segurança não detectado por soluções de segurança existentes, para que as devidas investigações sejam realizadas.
- 21.5.39.13. A CONTRATADA deverá operar todas as plataformas contidas nesta contratação, de forma a realizar todas as atividades pertinentes a essas (Exceto ações de infraestrutura específicas administradas pela CONTRATANTE), seguindo melhores práticas recomendadas pelos fabricantes e potencializando ao máximo a capacidade de entrega de cada plataforma.
- 21.5.39.14. A CONTRATADA deverá entregar um relatório de implementação das soluções (as-built) contidas neste certame, contendo todos os passos realizados para implementação e configuração das soluções.
- 21.5.39.15. A CONTRATADA deverá finalizar a requisição de serviço ou incidente com a devida resolução registrada na ferramenta de demanda, documentando todos os procedimentos executados no atendimento. Bem como, deverá realizar testes necessários para aferir a efetiva resolução.
- 21.5.39.16. A CONTRATADA deverá documentar a causa-raiz, a solução de contorno (se houver) e os procedimentos adotados no atendimento do chamado.
- 21.5.39.17. A CONTRATADA deverá vincular o chamado à base de conhecimento.
- 21.5.39.18. A CONTRATADA deverá obter autorização da CONTRATANTE para realizar mudanças nas configurações das soluções, observando sempre a Política de Segurança da Informação - POSIC da CONTRATANTE, normas e planos vigentes;
- 21.5.40. Serviços de operação e sustentação de segurança**
- 21.5.40.1. Tem por objetivo sustentar e operar todas as soluções e serviços de segurança do ambiente da CONTRATANTE, trabalhando em conjunto com times de sustentação da CONTRATANTE para agregar inteligência e eficiência.
- 21.5.40.2. A execução desse serviço de forma contínua pela CONTRATADA compreende as atividades relacionadas aos serviços de segurança para operacionalizar o ambiente da CONTRATANTE. Compreende o rol mencionado no item 21.5.8.2.
- 21.5.40.3. Realizar acompanhamento da execução dos serviços para o cumprimento dos níveis de serviço estabelecidos;
- 21.5.40.4. Priorizar os atendimentos críticos, conforme definição do CONTRATANTE;
- 21.5.40.5. Monitorar de forma permanente e realizar avaliações críticas sobre os produtos e serviços de segurança do CONTRATANTE;
- 21.5.40.6. Traçar curvas de comportamento, definir a volumetria média de acessos e identificar comportamentos não usuais, visando antecipar a identificação de incidentes de segurança, antes mesmo de impacto nos serviços;
- 21.5.40.7. Atuar proativamente na antecipação e identificação de incidentes de segurança, antes mesmo do impacto nos serviços;
- 21.5.40.8. Reagir aos eventos de Segurança da Informação que possam afetar a disponibilidade, integridade ou confidencialidade das informações existentes nos sistemas ou serviços de TI do CONTRATANTE;
- 21.5.40.9. Atuar quando ocorrer a falha dos controles de segurança ou situação previamente desconhecida e que tenha probabilidade de comprometer os sistemas e serviços de TI;
- 21.5.40.10. Prover a CONTRATANTE com os relatórios técnicos e gerenciais suficientes para a comprovação dos serviços realizados;
- 21.5.40.11. Colaborar com a atuação da equipe técnica da CONTRATANTE em situações críticas de trabalho, bem como interagir com os usuários quando a situação requerer;
- 21.5.40.12. Criar e manter atualizada a base de conhecimento, com o apoio e aprovação da CONTRATANTE, com os procedimentos sistematizados contemplando todas as soluções de problemas resolvidos com respostas padronizadas, relacionando a base de conhecimento com cada chamado atendido;
- 21.5.40.13. Implantar as melhorias solicitadas pelos servidores da CONTRATANTE através das aberturas de chamados no sistema de gestão de serviços de TI;
- 21.5.40.14. Sugerir novas tecnologias para modernizar o ambiente tecnológico, buscando subsidiar a equipe da CONTRATANTE na gestão de segurança da informação;
- 21.5.40.15. Administrar todas as soluções de escopo de segurança da informação;
- 21.5.40.16. Abrir chamados técnicos para os serviços de suporte técnico remoto das soluções de hardware e software relacionados à Segurança da Informação no ambiente tecnológico do CONTRATANTE;
- 21.5.40.17. Finalizar a requisição de serviço ou incidente com a devida resolução registrada na ferramenta de demanda, documentando todos os procedimentos executados no atendimento. Bem como, deverá realizar testes necessários para aferir a efetiva resolução.
- 21.5.40.18. Documentar a causa-raiz, a solução de contorno (se houver) e os procedimentos adotados no atendimento do chamado.
- 21.5.40.19. Vincular o chamado à base de conhecimento.
- 21.5.40.20. Obter autorização da CONTRATANTE para realizar mudanças nas configurações das soluções, observando sempre a Política de Segurança da Informação - POSIC da CONTRATANTE, normas e planos vigentes;
- 21.5.40.21. Realizar as atividades em estrita observância à Política de Segurança da Informação e Comunicação (POSIC), demais normas estipuladas pela CONTRATANTE e planos vigentes;
- 21.5.40.22. Implantar as melhorias solicitadas pela CONTRATANTE nos ativos de segurança;
- 21.5.40.23. Participar, quando solicitado, de reunião com os gerentes e participantes dos projetos de desenvolvimento e manutenção de sistemas e administração de dados, a fim de prover soluções para projetos/atividades em andamento;
- 21.5.40.24. Realizar de forma contínua análise de vulnerabilidades, apontando todas as correções que precisam ser realizadas. Tal serviço deve também priorizar aquilo que representa maior criticidade ao ambiente da CONTRATANTE;
- 21.5.40.25. Realizar testes de continuidade de cada solução de segurança da informação em alta disponibilidade, no mínimo, a cada 6 (seis) meses.
- 21.5.40.26. A CONTRATADA deverá realizar a gestão de privilégios de todas as aplicações executadas nas estações de trabalho e servidores Windows, de forma a permitir que apenas aplicações válidas tenham poder de execução;
- 21.5.40.27. A CONTRATADA deverá fazer a gestão do controle de acesso a rede de forma contínua, interagindo com o time de redes da CONTRATANTE, de forma a manter processos eficazes de descoberta, classificação e avaliação de postura de dispositivos que acessam a rede, contribuindo também

para criação de processos que venham permitir o fácil controle/isolamento de dispositivos que venham a fornecer riscos para o ambiente.

- 21.5.40.28. Execução de mudanças de configuração nos ativos sob sua administração;
- 21.5.40.29. Execução das atividades relativas aos normativos e governança da CONTRATANTE naquilo que for relativo à sua área de atuação.
- 21.5.40.30. As atividades abaixo deverão ser realizadas de forma contínua, a fim de manter o processo de melhoria contínua no que tange segurança da informação:
- 21.5.40.31. Implementação, sustentação e administração da solução de SIEM;
- 21.5.40.32. Configuração de repositórios e processamento de logs/eventos;
- 21.5.40.33. Criação/envio de procedimentos para envio de logs para soluções administradas por equipes terceiras;
- 21.5.40.34. Customização da interpretação dos logs sempre que necessário;
- 21.5.40.35. Criação/configuração de alertas para cada tipo de log processado;
- 21.5.40.36. Monitoramento de saúde de recebimento de logs de todas as fontes configuradas para envio;
- 21.5.40.37. Configuração e disponibilização dos agentes de privilégios;
- 21.5.40.38. Criação/Manutenção de regras de detecção;
- 21.5.40.39. Implementação, sustentação e administração da solução de gestão de vulnerabilidades;
- 21.5.40.40. Sustentação e administração da solução de controle de acesso à rede;
- 21.5.40.41. Configurar políticas para análise e correção de posturas indesejadas;
- 21.5.40.42. Apontar vulnerabilidades por ordem de criticidade e acompanhar o processo de remediação dessas;
- 21.5.40.43. Analisar eventos da solução de proteção de endpoint;
- 21.5.40.44. Analisar a viabilidade e o impacto da instalação de novas soluções ou correções;
- 21.5.40.45. Analisar os alertas de ativos desatualizados;
- 21.5.40.46. Atuar proativamente em caso de identificação de situação de desconformidade com boas práticas de segurança;
- 21.5.40.47. Manter atualizado as regras DLP;
- 21.5.40.48. Reportar ocorrências recorrentes; e
- 21.5.40.49. Reporte de melhorias de segurança identificadas no ambiente.
- 21.5.40.50. Criar, em colaboração com a CONTRATANTE, casos de uso (regras) que devem ser implementados no SIEM fornecido;
- 21.5.40.51. Revisar periodicamente as regras do SIEM, realizando as adaptações e evoluções necessárias; e
- 21.5.40.52. A CONTRATADA deverá produzir e entregar informação de inteligência acionável, na forma de procedimentos para triagem de alertas e procedimentos para resposta a incidentes, correspondentes às regras do SIEM.
- 21.5.40.53. A CONTRATADA deverá apresentar mensalmente o plano de tratamento de vulnerabilidades, indicando as ações mais efetivas para a redução de riscos.
- 21.5.40.54. A CONTRATADA deverá acionar o fabricante das ferramentas sempre que necessário, sem nenhum custo adicional para o CONTRATANTE.
- 21.5.40.55. Qualquer atividade técnica, referente à serviços relacionados ao escopo de soluções listadas no item 21.5.8.2 que eventualmente não tenham sido listados, também serão de responsabilidade da CONTRATADA.
- 21.5.40.56. Fica fora do escopo da CONTRATADA apenas atividades referentes a sustentação referente as ferramentas de rede e infraestrutura da CONTRATANTE, onde os times de sustentação local deverão ser acionados para qualquer tratativa necessária.

21.5.41. **Serviço de Gestão de Incidentes de Segurança**

- 21.5.41.1. Tem por objetivo analisar, remediar, conter e documentar os eventos de segurança da informação que foram transformados em um incidente de segurança da informação. Tal serviço deverá ser executado obedecendo os frameworks NIST e SANS de resposta a incidente de segurança da informação e boas práticas de mercado.
- 21.5.41.2. Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação da CONTRATANTE, levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade.
- 21.5.41.3. O início do processo de resposta a incidente de segurança se dará, sempre que um evento adverso for detectado pelas plataformas responsáveis ou através do serviço de monitoramento, porém não se limitando a estes. Poderá o corpo técnico de segurança da CONTRATANTE, a qualquer tempo, abrir um incidente de segurança.
- 21.5.41.4. Após o incidente de segurança aberto, será de responsabilidade do grupo de resposta a incidente de segurança da CONTRATADA, analisar os logs e artefatos enviados, a fim de no primeiro instante identificar as fontes geradoras de tais logs.
- 21.5.41.5. Uma vez realizado as análises iniciais do incidente gerado, o grupo de resposta a incidente de segurança da CONTRATADA, deverá trabalhar para identificar quais foram os principais vetores de ataque ao ambiente do CONTRATANTE.
- 21.5.41.6. Como próximo passo o grupo de resposta a incidente de segurança da CONTRATADA, deverá comunicar ao time de segurança da informação da CONTRATANTE as informações iniciais sobre o incidente de segurança gerado, e quais serão as linhas de atuação para solução do incidente.
- 21.5.41.7. Juntamente com a CONTRATANTE o grupo de resposta a incidente de segurança da CONTRATADA, deverá definir a severidade do incidente de segurança. A severidade do incidente de segurança da informação será definida através da combinação de urgência e impacto, onde impacto é definido como a medida de criticidade do negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente.
- 21.5.41.8. Após análises iniciais do incidente, caberá ao o grupo de resposta a incidente de segurança, realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e/ou artefato (malware).
- 21.5.41.9. Todo o processo de análise e resultados obtidos devem ser documentados a todo tempo na ferramenta de gestão de incidente da segurança da informação, para que o CONTRATANTE acompanhe todos os passos para a solução do incidente.
- 21.5.41.10. Uma vez identificado comportamento e os principais vetores de ataque, o grupo de resposta a incidente de segurança da CONTRATADA deverá definir e executar uma estratégia para a mitigação e contenção do ataque em questão. Caso seja necessário qualquer tipo de alteração no parque

computacional da CONTRATANTE, para contenção e mitigação do incidente, deverá antes ser autorizado tal alteração pelo corpo técnico de segurança da CONTRATANTE.

21.5.41.11. Mitigado o incidente de segurança, o próximo passo exigido é que a CONTRATADA, através do grupo de resposta a incidente de segurança, inicie o processo de recolhimento de toda e quaisquer evidências, bem como a identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo, para execução de análise forense do caso.

21.5.41.12. Deve-se reunir os dados coletados durante o processo de tratamento de incidente, para iniciar o processo de análise forense desse, ainda pelo grupo de resposta a incidente de segurança. Tal análise deve ser realizada com o objetivo de identificar (pessoas, locais e/ou eventos), correlacionando todas as informações reunidas, e gerando como produto final um Relatório técnico sobre o incidente de segurança em questão, que deverá ser entregue em até 3 (três) dias úteis após o encerramento do incidente.

21.5.41.13. O grupo de resposta a incidente de segurança da CONTRATADA, deve documentar na ferramenta de incidente de segurança, as lições aprendidas do incidente de segurança em questão, formando durante todo o período de vigência do contrato uma grande base de conhecimento sobre ataques adversos.

21.5.41.14. O regime de execução deste serviço deverá ser 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano);

21.5.41.15. A contratada deverá prover serviços de resposta aos incidentes de segurança da informação diante os eventos registrados no monitoramento;

21.5.41.16. Analisar os incidentes reportados na ferramenta de DLP;

21.5.41.17. A CONTRATADA deverá prover inteligência de proteção contra ataques cibernéticos e serviços de pesquisa e desenvolvimento de inteligência de proteção contra ataques cibernéticos, sendo responsável por:

21.5.41.18. Pesquisar novos tipos de ataques, vírus, malwares, Botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela CONTRATADA;

21.5.41.19. O serviço deve ser capaz de detectar em tempo real, ameaças alimentadas pelas seguintes bases de inteligência:

21.5.41.20. Relatórios de ameaças e segurança;

21.5.41.21. Relatórios de Botnets e centros de Comando e Controle;

21.5.41.22. Identificação de exploit kits;

21.5.41.23. Indicadores de ataques "ZeroDays";

21.5.41.24. Indicadores de comprometimento, suspeitas e avisos informativos;

21.5.41.25. Inteligência de tendências;

21.5.41.26. Proxies anônimos;

21.5.41.27. Classificação de sites; e

21.5.41.28. Endereços de rede TOR.

21.5.42. **Serviço de descoberta, gestão de vulnerabilidades de Segurança e validação de segurança**

21.5.42.1. A CONTRATADA deverá implementar camadas de gerenciamento completo de vulnerabilidades no ambiente da CONTRATANTE, desde a descoberta até a resolução das vulnerabilidades.

21.5.42.2. Para a correção de cada vulnerabilidade, a CONTRATADA deverá interagir com o time da CONTRATANTE para acompanhar todas as trilhas de resolução da vulnerabilidade.

21.5.42.3. No caso de correções de vulnerabilidades em softwares não cobertos pelo software de gestão de patches já em uso pela CONTRATANTE, a CONTRATADA deverá sugerir opções disponíveis para resolução definitiva do problema.

21.5.42.4. Para vulnerabilidades encontradas em sistemas WEB e servidores sustentados, a CONTRATADA deve colaborar com o time de sustentação desse ambiente da CONTRATANTE para demonstrar a vulnerabilidade identificada, apontar os caminhos de resolução, aplicar a correção em conjunto e acompanhar o processo de validação do serviço hospedado no ativo em questão.

21.5.42.5. A CONTRATANTE será responsável pela sustentação de todos os scanners de vulnerabilidades necessários para cobertura completa e contínua do ambiente da CONTRATADA. No caso de utilização de máquinas virtuais, o time de virtualização da CONTRATANTE deverá ser envolvido em toda as atividades onde se faça necessário intervenções diretamente no console do componente.

21.5.42.6. A CONTRATADA deverá realizar scans de vulnerabilidade contínuos no ambiente da CONTRATANTE, de forma a manter conhecimento a qualquer vulnerabilidade encontrada.

21.5.42.7. A CONTRATADA deverá gerir os relatórios e planejar as ações de correção de forma a zelar para que o ambiente da CONTRATANTE tenha sempre o menor nível de risco possível, quanto a vulnerabilidades existentes que tenham sido encontradas durante os scans.

21.5.42.8. Os scans de vulnerabilidade deverão ser executados em todo o ambiente de forma a manter o ambiente cobertos quanto ao conhecimento de possíveis brechas de segurança existentes. No caso de ambientes onde a segregação de rede não permita comunicação direta com o servidor que realiza o scan, a CONTRATADA deverá implementar agentes que façam os scans com periodicidade a ser definida.

21.5.42.9. Deverá automatizar processos para remediação automática de vulnerabilidades de segurança em sistemas operacionais e aplicações instaladas nas estações/servidores;

21.5.42.10. Deverá impor um fluxo de atualizações passando pela fase de homologação antes de produção;

21.5.42.11. O fluxo deve ser automatizado e sem interrupção de forma a manter o ambiente sempre seguro frente a novas vulnerabilidades descobertas;

21.5.42.12. No caso de sistemas que não possam ser atualizados, a CONTRATADA deverá indicar melhores práticas de segurança para proteção do ativo e diminuição da superfície de ataque que permeia aquele ativo.

21.5.42.13. Os profissionais alocados deverão realizar varreduras de segurança, a partir da solução de validação de segurança para verificar se os ativos de segurança são vulneráveis e podem não responder à ameaças cibernéticas existentes;

21.5.42.14. O serviço deve ser capaz de revisar a eficiência dos ativos de segurança em ambiente de produção sem causar danos ou degradação do ambiente;

21.5.42.15. Os ativos de segurança a serem validados contemplam, no mínimo, IDS/IPS, Firewall, Endpoint Security e WAF;

- 21.5.42.16. Deve avaliar o nível de segurança fornecido por um grupo de endpoints e ativos de segurança de rede independentemente de fabricante e tecnologia;
- 21.5.42.17. Deve avaliar o resultado da varreduras, relatar ameaças relevantes e propor medidas de mitigação às ameaças de forma contínua, além de permitir a visualização para cada cenário de ataque;
- 21.5.42.18. Deverão ser verificadas as configurações no firewall da solução de proteção de endpoint e/ou firewall de modo a identificar e prevenir possibilidades para atacantes navegarem lateralmente pela rede corporativa.
- 21.5.42.19. Deverão ser verificadas as configurações nos ativos para evitar a efetividade de ataque do tipo command and control, onde o atacante consegue fechar conexão com o centro de controle para efetivação da ação maliciosa.
- 21.5.42.20. Deverão ser verificadas as configurações nos ativos de forma a verificar se é possível realizar acessos à URL's por categorização, de forma a validar a política de acesso web já em implementada pela CONTRATANTE.
- 21.5.42.21. Deve ser verificado as configurações relativas ao SMTP, com o intuito de verificar se há brechas que permitem ataques tanto a partir da Internet para o domínio corporativo quanto entre contas de domínios corporativos;
- 21.5.42.22. As verificações das configurações do SMTP poderão ser testadas por meio de simulação de phishing com ferramenta Gophish ou similar, de forma a testar os bloqueios de spam nos ativos de segurança, a capacidade de resposta dos usuários a ameaças deste gênero.
- 21.5.42.23. Para as verificações de segurança e reforço das configurações, deve ser observados técnicas, táticas e procedimentos contidos nos principais frameworks de mercado como Cis Control, MITRE ATT&CK, OWASP e NIST.
- 21.5.42.24. Deve gerar relatórios de todas varreduras e ataques realizados, estabelecendo um benchmark de proteção a ser comparado a cada teste, de forma a fornecer relatórios de progresso ou declínio na efetividade das demais tecnologias de proteção em uso.

ANEXO II - CATÁLOGO DE SERVIÇO

Este catálogo de serviço apresenta as atividades definidas para execução do Item 4 - Serviço de operação, monitoramento e tratamento de eventos de segurança.

A estrutura desse catálogo é separada em quatro partes, de acordo com o tema da atividade:

1. Serviços de operação e sustentação de segurança;
2. Serviço de Gestão de Incidentes de Segurança; e
3. Serviço de descoberta, gestão de vulnerabilidades de segurança e validação de segurança.

Este catálogo poderá ser alterado para melhor representar as atividades executadas no contrato, sempre respeitando o objeto, e desde que não represente impacto financeiro e as duas partes concordem com a alteração.

Serviços de operação e sustentação de segurança	
ID	Serviço
OP1	Instalação de solução de segurança
OP2	Implantar solução de segurança
OP3	Instalação dos clientes via console
OP4	Atualização de console
OP5	Atualização dos Clientes via console
OP6	Configuração de proteção endpoint
OP7	Configuração de políticas de Firewall
OP8	Configuração de Políticas de IPS
OP9	Configuração de Políticas IDS
OP10	Configuração de Políticas de Integridade do host
OP11	Configuração de políticas de Controle de Aplicações e Dispositivos
OP12	Criação de pacotes customizados para instalação do agente
OP13	Configuração de Políticas de Grupo
OP14	Configuração de integração (Servidores de Autenticação Suportados)
OP15	Criação de Relatório de situação do parque (Atualização dos clientes)
OP16	Configuração do método de autenticação de contas de administradores
OP17	Configuração de política de segurança (L4/L7)
OP18	Aplicação de política de Threat Prevention (antivírus, anti-spyware/bot ou IPS)
OP19	Configurar integração com base de usuários (auth / AD)
OP20	Aplicar controle de uso de aplicação por usuário/grupo de usuário
OP21	Atualização firmware (SO)
OP22	Criação de rota ou correção de tráfego assimétrico
OP23	Configuração de PBF (Policy Based Forwarding)
OP24	Aplicação de política de SSL Decryption

OP25	Aplicação de categoria de URL filtering baseada em usuário/grupo de usuário
OP26	Análise/criação de IOC (Indicator of Compromise)
OP27	Criação de assinatura customizada para identificação e controle de aplicação
OP28	Aplicação de políticas de QoS
OP29	Health Check (relatório de adoção de uso de boas práticas de config)
OP30	Criar/Atualizar/Excluir regra no WAF
OP31	Criar/Atualizar/Excluir regra DLP
OP32	Criar/Atualizar/Excluir acessos VPN
OP33	Acompanhar testes de backup
OP34	Criar/Atualizar/Excluir regras no anti-spam
OP35	Atualizar topologia de segurança
OP36	Atualizar Web Filter
OP37	Gerenciar proxy
OP38	Configuração de scans customizados
OP39	Criar/Atualizar/Excluir caso de uso SIEM
OP40	Criar/Atualizar/Excluir monitoramento de credenciais administrativas
OP41	Criar/Atualizar/Excluir gestão de credencias entre aplicações
OP42	Executar mudanças de configuração
OP43	Realizar teste de continuidade
OP44	Gerenciar controle de acesso em ativo
OP45	Relatório técnico de segurança
OP46	Revisão de segurança em projeto de software
OP47	Criar/Atualizar/Excluir Normativo em Segurança
OP48	Criar/Atualizar/Excluir Plano de Continuidade
OP49	Criar/Atualizar/Excluir Procedimento Operacional
Serviço de Gestão de Incidentes de Segurança	
ID	Serviço
IS1	Eventos de Informação
IS2	Eventos de Aviso
IS3	Eventos de Exceção
IS4	Identificação da Causa
IS5	Tratamento da Causa
IS6	Aplicação da correção
IS7	Validação do contorno do incidente
IS8	Encerramento do registro do incidente
IS9	Criar/Atualizar/Excluir Procedimento Operacional de recuperação de incidente
IS10	Relatório técnico de incidente de segurança
Serviço de descoberta, gestão de vulnerabilidades de segurança e validação de segurança	
ID	Serviço
V1	Checagem (scan) e varredura em ativos de rede
V2	Checagem (scan) e varredura em aplicações web
V3	Análise de falso positivo em ativos de rede
V4	Análise de falso positivo em aplicações web
V5	Informativo sobre vulnerabilidades em ativos de rede
V6	Informativo sobre vulnerabilidades em aplicações web
V7	Suportar correções das vulnerabilidades em ativos de rede
V8	Suportar correções das vulnerabilidades em aplicações web
V9	Monitorar uso de credenciais administrativas
V10	Monitorar gestão de credenciais de aplicações
V11	Apresentar abordagem dinâmica para priorizar correções
V12	Automação de processo para remediação automática de vulnerabilidades

V13	Testar efetividade de implementações de segurança
V14	Relatório técnico de segurança

ANEXO III – PROPOSTA COMERCIAL

1. Pela presente proposta, declaramos inteira submissão aos preceitos em vigor no Manual de Licitações e Contratos da EMBRATUR até a presente data, bem como a todas as cláusulas e condições do Termo de Referência do Processo SEI nº 272100.002628/2024-05 EMBRATUR.
2. Propomos prestar à EMBRATUR, pelo valor a seguir, os serviços, objeto do Termo de Referência, obedecendo as quantidades conforme tabela.
3. Em caso de divergência dos preços apresentados em algarismos e por extenso, prevalecerá este último.
4. O prazo de validade desta proposta é de 90 (noventa) dias, contados a partir da sua assinatura e o prazo para a execução dos serviços será de acordo com o Termo de Referência.
5. Declaramos que nos preços propostos estão incluídos todos os custos e despesas diretas e indiretas referentes ao objeto da contratação.

ITEM	DISCRIMINAÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de gerenciamento de vulnerabilidades de segurança e correções automatizadas	Dispositivo	340	R\$	R\$
2	Solução de correlação de eventos de segurança e resposta a incidentes	Eventos por segundo - EPS	750	R\$	R\$
3	Solução de proteção avançada para endpoints	Endpoints	340	R\$	R\$
4	Monitoramento de comportamento e mitigação de riscos de usuários administradores de TI	Unidade	80	R\$	R\$
5	Proteção para aplicações	Unidade	10	R\$	R\$
6	Serviço de operação, monitoramento e tratamento de eventos de segurança	Unidade	12	R\$	R\$
TOTAL					R\$

Brasília, ____ de ____ de 2025

(Nome e cargo do proprietário ou representante legal da Empresa e assinatura)

Nome da Empresa:					
CNPJ:					
Telefone de contato:					
Representante Legal (nome e cargo) ou proprietário (nome):					
Endereço:					
CEP:		Cidade:		UF:	
Cart. Ident. Nº:		Expedido por:		CPF:	
Cargo:					
Representante Legal da Empresa					

ANEXO IV - MODELO DE DECLARAÇÃO DE REALIZAÇÃO OU NÃO DE VISTORIA

DECLARAÇÃO DE VISTORIA

Empresa _____ CNPJ _____.

Declaro, para fins de participação no certame referente ao Processo SEI nº 272100.002628/2024-05 - EMBRATUR, que vistoriei o ambiente tecnológico da Agência Brasileira de Promoção Internacional do Turismo, localizada nesta cidade de Brasília – DF, no Setor Comercial Norte, Quadra 2, Bloco G, Asa Norte, inteirando-me das condições e exigências constantes no Termo de Referência, relativo à contratação de pessoa jurídica para fornecimento de solução integrada de segurança da informação com fornecimento de licenças e serviços, conforme condições, quantidades e exigências estabelecidas no certame.

Brasília-DF, ____ de _____ de 2024.

Representante da Licitante_____
Representante da Embratur

ou

DECLARAÇÃO – NÃO VISTORIA

Declaro que a empresa _____, sediada à _____, CNPJ N°: _____, telefone _____, não teve interesse em realizar a vistoria nos locais onde serão executados os serviços Objeto do certame referente ao Processo SEI nº 272100.002628/2024-05 - Embratur, se responsabilizando por todas as consequências por este ato.

(Local), __ de _____ de _____.

(Assinatura do representante legal ou procurador)_____
Nome do representante legal ou procurador

(Número da Carteira de Identidade e CPF)

Observação: Esta declaração deverá ser feita, preferencialmente, em papel timbrado da empresa.

ANEXO V - MINUTA DE TERMO DE CONTRATO

TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº XX/20XX, que celebram entre si a EMBRATUR e a empresa XXXX, tendo por objeto XXXXXX.

AA **EMBRATUR - AGÊNCIA BRASILEIRA DE PROMOÇÃO INTERNACIONAL DO TURISMO**, com sede no SCN, Quadra 2, bloco G, Ed. Embratur, Térreo - Bairro Asa Norte, Brasília/DF, CEP 70712-907, inscrita no CNPJ sob o nº 35.842.428/0001-66, instituída pela Lei nº 14.002, de 22 de maio de 2020, doravante denominada **CONTRATANTE**, neste ato representada pelo Diretor-Presidente **XXXX**, brasileiro, casado/solteiro/divorciado, residente em Brasília/DF, inscrito no CPF nº XXXX, portador da Carteira de Identidade nº XXXXX, nomeado pelo Decreto da Presidência da República de XX/XXX/XXXX,

publicado no D.O.U., seção 2, página 01, e seu Diretor de XXXXXX, brasileiro, casado/solteiro/divorciado, residente em Brasília/DF, inscrito no CPF nº XXXXX, portador da Carteira de Identidade nº XXXX, nomeado pelo Decreto da Presidência da República de XX/XXX/XXXX, publicado no D.O.U., em XX/XX/XXX, seção 2, página XX, e a empresa XXXXX, inscrita no CNPJ sob o nº XXXXXXXX, sediada na XXXXXXXXXX, doravante designada **CONTRATADA**, neste ato representada pelo Sr(a) XXXXXXXX, portador(a) da Carteira de Identidade nº XXXXXXXX e CPF nº XXXXXX, residente em XXXXX, em observância ao Manual de Licitações e Contratos da EMBRATUR, pelos princípios da teoria geral dos contratos e pelas disposições de direito privado, resolvem celebrar o presente Termo de Contrato, mediante as cláusulas e condições a seguir enunciadas:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. Contratação de empresa para fornecimento de solução integrada de segurança da informação com fornecimento de licenças e serviços, conforme condições, quantidades e exigências estabelecidas neste contrato e no Termo de Referência.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão nº xxxxx e à proposta vencedora, independentemente de transcrição.

1.3. Objeto da contratação:

PREENCHER CONFORME A PROPOSTA VENCEDORA

CLÁUSULA SEGUNDA – DA VIGÊNCIA

2.1. O Contrato terá vigência de 12 (doze) meses, contados a partir da data de assinatura ou contados a partir de xx/xx/20xx, podendo ser prorrogado por iguais e sucessivos períodos, até o limite de 10 (dez) anos, conforme dispõe o art. 41 do Manual de Licitações e Contratos da EMBRATUR, desde que haja autorização formal da autoridade competente e observados os seguintes requisitos:

2.1.1. Os serviços tenham sido prestados regularmente;

2.1.2. Esteja formalmente demonstrado que a forma de prestação dos serviços tem natureza continuada;

2.1.3. Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

2.1.4. Seja juntada justificativa e motivo, por escrito, de que a EMBRATUR mantém interesse na realização do serviço;

2.1.5. Seja comprovado que o valor do contrato permanece economicamente vantajoso para a EMBRATUR;

2.1.6. Haja manifestação expressa da CONTRATADA informando o interesse na prorrogação; e

2.1.7. Seja comprovado que a CONTRATADA mantém as condições iniciais de habilitação.

CLÁUSULA TERCEIRA – DO PREÇO

3.1. O valor total da contratação é de R\$..... (.....).

3.2. No valor acima estão incluídos todos os custos e todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

3.3. O valor acima é meramente estimativo, de forma que os pagamentos devidos à CONTRATADA dependerão dos quantitativos de serviços efetivamente prestados ou fornecidos o produto.

CLÁUSULA QUARTA – DA DOTAÇÃO ORÇAMENTÁRIA

4.1. As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, prevista no orçamento da EMBRATUR para o exercício de 20xx na classificação abaixo:

Classificação da Despesa: XX.XX.XX.XX (xxxxxxx)

Órgão: 54000 – Ministério do Turismo - MTUR

Gestão/Unidade: EMBRATUR – Agência Brasileira de Promoção Internacional do Turismo

Função:

Subfunção:

Programa de Trabalho:

CLÁUSULA QUINTA – DO PAGAMENTO

5.1. O pagamento referente aos itens 1, 2 e 3 do objeto será realizado em sua totalidade após a implantação e entrega das licenças de forma funcional para o período de 12 (doze) meses.

5.2. Entende-se que a licença estará funcional quando:

5.2.1. item 1 - quando todos os ativos do escopo do item estiverem com as licenças aplicadas e for possível visualizar o painel com os ativos e dados de vulnerabilidade;

5.2.2. item 2 - quando o correlacionador estiver recebendo dados de pelo menos 3 ativos enviando logs para o correlacionador e 5 regras criadas e aplicadas;

5.2.3. item 3 - quando todos os ativos do escopo do item estiverem com as licenças aplicadas e for possível visualizar no painel a gestão de todos os ativos com licença e seus respectivos status;

5.3. O pagamento referente ao item 4 será por preço fixo mensal de acordo com a sua data de abertura e conclusão.

5.4. O pagamento somente será autorizado depois de efetuado o “ATESTO” pelo gestor ou, na sua ausência, pelo gestor Substituto do contrato/da Ordem de Serviço na nota fiscal apresentada.

5.5. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à demanda, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

- 5.6. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
- 5.7. Antes do pagamento à CONTRATADA, será realizada consulta aos documentos comprobatórios da regularidade fiscal e trabalhista, quando for o caso.
- 5.8. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.
- 5.9. Após o atendimento de todas as exigências supramencionadas e aguardado o trâmite processual da EMBRATUR, a Coordenação Financeira deverá efetuar o pagamento em até 10 (dez) dias úteis, após o recebimento do referido processo.
- 5.9.1. Nos casos de eventuais atrasos de pagamento conforme prazo indicado no item 5.6, desde que a CONTRATADA não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela CONTRATANTE, será calculada mediante a aplicação da seguinte fórmula:

$EM = I \times N \times VP$, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX)	$I = (6 / 100) / 365$	I = 0,00016438 TX = Percentual da taxa anual = 6%
----------	-----------------------	--

CLÁUSULA SEXTA – DO REAJUSTE

- 6.1. Os preços inicialmente contratados são fixos e irremovíveis no prazo de 1 (um) ano contado da data do início da vigência do contrato.
- 6.2. Dentro do prazo de vigência do contrato e mediante solicitação da CONTRATADA, os preços contratados poderão sofrer reajuste após o interregno de 1 (um) ano, aplicando-se o Índice de Custos de Tecnologia da Informação - ICTI exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.
- 6.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de 1 (um) ano será contado a partir dos efeitos financeiros do último reajuste.
- 6.4. No caso de atraso ou não divulgação do índice de reajustamento, a CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.
- 6.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.
- 6.6. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.
- 6.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de Termo Aditivo.
- 6.8. Fica garantida a possibilidade de reequilíbrio econômico-financeiro dos valores contratuais, que deverá prever os meios de prova das novas definições de mercado que ensejarem o desequilíbrio econômico do contrato, corroborados por planilhas de custos.

CLÁUSULA SÉTIMA – DA GARANTIA CONTRATUAL

- 7.1. A CONTRATADA, no prazo de 10 (dez) dias após a assinatura do Termo de Contrato, prestará garantia no valor correspondente a 5% (cinco por cento) do valor do contrato, que será liberada de acordo com as condições previstas no Termo de Referência.
- 7.1.1. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,5% (meio por cento) do valor do contrato por dia de atraso, até o máximo de 2% (dois por cento);
- 7.1.2. O atraso superior a 30 (trinta) dias autoriza a Agência a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme Manual de Licitações e Contratos da EMBRATUR.
- 7.1.3. A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 (noventa) dias posterior ao término da vigência contratual.
- 7.1.4. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:
- 7.1.5. prejuízos advindos do não cumprimento do objeto do contrato;
- 7.1.6. prejuízos diretos causados à Agência decorrentes de culpa ou dolo durante a execução do contrato;
- 7.1.7. multas moratórias e punitivas aplicadas pela Agência à CONTRATADA; e
- 7.1.8. obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA, quando couber.
- 7.2. Caberá à CONTRATADA optar por uma das seguintes modalidades de garantia:
- 7.2.1. caução em dinheiro; ou
- 7.2.2. seguro-garantia; ou
- 7.2.3. fiança bancária.
- 7.3. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação, inclusive quanto aos prazos previstos no item 7.1.
- 7.4. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados a partir da data em que for notificada.
- 7.5. A CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.
- 7.6. Será considerada extinta a garantia:

- 7.6.1. com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato;
- 7.6.2. ao fim do prazo de 90 (noventa) dias após o término da vigência, caso a CONTRATANTE não comunique a ocorrência de sinistros.

CLÁUSULA OITAVA - DO MODELO DE EXECUÇÃO DO OBJETO

8.1. O prazo da CONTRATADA se preparar para receber as demandas será de 30 dias corridos, com início imediato à data de assinatura do contrato. Decorrido este período a CONTRATANTE emitirá a Ordem de Serviços que servirá de autorização para o início do projeto. O prazo de preparação faz parte do prazo de vigência do contrato e não faz parte do prazo de realização do projeto.

8.2. Reunião inicial

8.2.1. Após a assinatura do contrato, será realizada a reunião inicial, a ser registrada em ata, convocada pelo gestor do contrato, com a participação do fiscal requisitante, da CONTRATADA e dos demais interessados por ele identificados, cuja pauta observará, pelo menos:

8.2.2. presença do representante legal da CONTRATADA, que apresentará o preposto dessa;

8.2.3. entrega, por parte da CONTRATADA, do Termo de Compromisso, conforme modelo constante do anexo III, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da CONTRATADA; e TERMO DE CIÊNCIA, conforme modelo constante do anexo V, a ser assinado por todos os empregados da CONTRATADA diretamente envolvidos na contratação;

8.2.4. esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato.

8.3. Encaminhamento formal de demandas

8.3.1. O encaminhamento formal de demandas, a cargo do gestor do contrato, ocorrerá por meio de Ordem de Serviço - OS.

8.4. Local de execução dos serviços

8.4.1. Os serviços deverão ser executados de forma remota ou, caso seja necessário, nas dependências da Embratur, localizada na Asa Norte, Brasília - DF, ou em local a ser indicado por essa Agência, na mesma cidade de sua sede, em horário a ser definido pela CONTRATANTE.

8.5. Mecanismos formais de comunicação

8.5.1. Toda a comunicação entre a CONTRATANTE e a CONTRATADA deverá ser sempre formal como regra, exceto em casos excepcionais que justifiquem outro canal de comunicação.

8.5.2. Os seguintes instrumentos formais poderão ser utilizados para a troca de informações entre a CONTRATANTE e a CONTRATADA: ata de reunião, ofício, e-mail, ordem de serviço ou fornecimento de bens e chamado técnico.

8.6. Manutenção de sigilo e normas de segurança

8.6.1. A CONTRATADA 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.

8.6.2. O Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e Termo de Ciência, a ser assinado por todos os empregados da CONTRATADA diretamente envolvidos na contratação, encontram-se no anexo IV - TERMO DE COMPROMISSO e anexo V - TERMO DE CIÊNCIA.

8.6.3. No caso de substituição ou inclusão de empregados da CONTRATADA, o preposto deverá entregar ao fiscal administrativo do contrato os TERMOS DE CIÊNCIA assinados pelos novos empregados envolvidos na execução dos serviços contratados.

8.6.4. A atuação da CONTRATADA deverá observar a Resolução nº 51/2024 - Política de Segurança da Informação e Comunicação e suas atualizações.

8.7. Modelo de Execução do Serviço de Licenciamento

8.7.1. Os serviços de licenciamento correspondente aos itens 1, 2 e 3 serão solicitados por meio de Ordem de Serviço anual, que especificará as quantidades solicitadas, que servirá como autorização para prestação de serviço.

8.7.2. As licenças deverão ser implantadas no ambiente seguindo o cronograma pactuado entre as partes, não podendo ser maior do que 90 (noventa) dias após o recebimento da Ordem de Serviço.

8.7.3. O pagamento referente ao uso das licenças somente se iniciará após a efetiva implantação das licenças e liberação para o uso da CONTRATANTE, nas quantidades especificadas na Ordem de Serviço.

8.7.4. Mensalmente deverá ser fornecido o Relatório de Situacional, minimamente com informações de tempo de disponibilidade das licenças, licenças em uso, licenças disponíveis e chamados para fabricante abertos e resolvidos.

8.7.5. Nos anos subsequentes de contrato, em que as licenças já estarão implantadas, a liberação das licenças deverá ser iniciada em até 5 (cinco) dias úteis, contados a partir do recebimento da Ordem de Serviço pela CONTRATADA.

8.7.6. Modelo de Execução de Serviço de Segurança

8.7.7. O Item 4 corresponde aos serviços de segurança, que será solicitado por meio de Ordem de Serviço mensal, que servirá como autorização para prestação de serviço.

8.7.8. Para o faturamento mensal dos itens, a contratada deverá emitir e apresentar o "Relatório Mensal de Acompanhamento do Contrato". Esse instrumento de controle deve possuir, no mínimo, a apuração dos indicadores de níveis de serviços, ocorrências e demais informações necessárias à correta identificação do valor mensal a ser pago referente à execução das Ordens de Serviços. Também devem constar as informações detalhadas a seguir:

8.7.8.1. Registro de todas as atividades realizadas para cada solução de proteção envolvida neste certame;

8.7.8.2. Registro de indicadores referentes a cada camada de proteção envolvida;

8.7.8.3. Sumários de quantidade de logs ingeridos para cada fonte integrada ao SIEM;

8.7.8.4. Sumário de todos os incidentes de segurança registrados seguido de quais ações foram tomadas pelo time de resposta;

8.7.8.5. Sumário de injeções de inteligência cibernéticas aplicadas nos eventos de segurança registrados;

8.7.8.6. Sumário de todas as vulnerabilidades de segurança encontradas no período do relatório;

8.7.8.7. Estatísticas de todas as vulnerabilidades que foram corrigidas no período;

8.7.8.8. Resultados completos de testes de segurança direcionados a técnicas de movimentação lateral na rede;

- 8.7.8.9. Resultados completos de testes de segurança direcionados a política de navegação Web e firewall;
- 8.7.8.10. Resultados completos de testes de segurança direcionados a solução de proteção de e-mail corporativo;
- 8.7.8.11. Resultados dos testes de campanhas de phishing realizadas com os usuários da CONTRATANTE;
- 8.7.8.12. Resultados completos de testes de segurança direcionados a solução de WAF em uso pela CONTRATANTE; e
- 8.7.8.13. Resultados completos referentes ao nível de maturidade de segurança da CONTRATANTE baseado nos testes de segurança realizados.
- 8.7.9. O relatório Mensal de Acompanhamento do Contrato poderá ser adaptado, desde que pactuado entre as partes sobre as novas informações.
- 8.7.10. O prazo para conclusão deverá observar o estabelecido na Ordem de Serviço.
- 8.7.11. Pelo menos 1 (um) profissional deverá ser alocado nas dependências da CONTRATANTE em horário comercial.
- 8.7.12. Por se tratar de execução de preço fixo mensal, a equipe de fiscalização poderá fiscalizar o cumprimento das obrigações trabalhistas, sociais e previdenciárias dos profissionais alocados, conforme:
- 8.7.12.1. No início da execução dos serviços contratados;
- 8.7.12.2. Durante a execução das Ordens de Serviços;
- 8.7.12.3. Quando da rescisão do contrato.

CLÁUSULA NONA – DO REGIME DE EXECUÇÃO DOS SERVIÇOS E FISCALIZAÇÃO

9.1. O acompanhamento e a fiscalização da execução do contrato/serviço consistem na verificação da conformidade da prestação dos serviços, dos materiais, técnicas e equipamentos empregados, de forma a assegurar o perfeito cumprimento do ajuste, que será exercido por um colaborador da CONTRATANTE.

9.2. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos no Termo de Referência.

9.3. A fiscalização do contrato/serviço, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação à produtividade efetivamente realizada.

9.4. O representante da EMBRATUR anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato/serviço, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das faltas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

9.5. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da CONTRATANTE ou de seus agentes, gestores e fiscais.

9.6. Será observado os indicadores a seguir, afim de se verificar o atendimento de nível mínimo de serviço. As métricas previstas para os Acordo de Nível de Serviço são definidas de forma a servir de insumo para o processo de manutenção da qualidade e aperfeiçoamento do serviço prestado pela CONTRATADA. Estas métricas deverão ser apuradas pela CONTRATADA e reportadas mensalmente à CONTRATANTE.

9.6.1. Indicador Quantidade de chamados (requisição e incidentes) atendidos dentro do prazo

9.6.1.1. De maneira a uniformizar o entendimento quanto a classificação para incidentes e requisições de serviço de segurança da Informação, define-se os níveis de criticidade como:

Nível de Criticidade	Impacto/ Descrição	Início de Atendimento	Prazo para solução
EMERGENCIAL	- Algum tipo de ataque que gerou indisponibilidade em servidores e sistemas críticos, afetando um ou mais usuários; - Infecção ou paralisação generalizada devido a ransomware ou algum outro tipo de malware; - Roubo ou vazamento de dados devido a falha humana ou técnica; - Algum tipo de impacto ou risco grave a empresa ou a equipe de Segurança da Informação; - Quando o problema\incidente é definido com o nível de criticidade "EMERGENCIAL"; *Para impacto de nível emergencial é necessário um profissional no mínimo Sênior	Em até 1 hora corrida	Em até 4 horas corridas
ALTA	- Servidor de produção ou sistema crítico está apresentando instabilidade, degradação ou sofrendo ataques recorrentes q podem acarretar uma exploração ou vazamento de dados; - Alarmes de nível ALTA identificados por ferramentas de SIEM ou ferramenta de segurança que podem ser um falso positivo e necessitam de uma análise para validação; - Quando o problema\incidente é definido com o nível de criticidade "ALTA";	Em até 2 horas corridas	Em até 8 horas corridas
MÉDIA	Nenhum serviço crítico está envolvido e não existe risco de perda de dados;	Em até 4 horas úteis	Em até 24 horas úteis

	- Alarmes de nível MÉDIO identificados por ferramentas de SIEM ou ferramenta de segurança que podem ser um falso positivo e necessitam de uma análise para validação; - Quando o problema\incidente é definido com o nível de criticidade "MÉDIA".		
BAIXA	- Dúvidas ou apoio à implementação; - Mudanças planejadas; - Novas implementações; - Sugestões de novos recursos ou aprimoramento do Software; - Alarmes de nível BAIXA identificados por ferramentas de SIEM ou ferramenta de segurança que podem ser um falso positivo e necessitam de uma análise para validação; - Evidências de um bloqueio ou tratativa automatizada; - Quando o problema\incidente é definido com o nível de criticidade "BAIXA"	Em até 9 horas úteis	Em até 72 horas úteis.

9.6.1.2. Para efeito desta contratação, estabelecem-se os seguintes níveis mínimos de serviços para a resposta e solução das requisições de serviço e incidentes. Os serviços serão medidos com base em indicadores e níveis mínimos de serviços, vinculados a fórmulas de cálculo específicas, deverão ser executados pela CONTRATADA, e apurados mensalmente, de modo a alcançar as respectivas metas exigidas, conforme tabela a seguir. Os níveis de serviço serão mensurados de forma automatizada, por meio de ferramenta de uso e gestão da CONTRATANTE, e não poderão ser manipulados pela CONTRATADA;

9.6.1.3. Após observadas as características do chamado, será aplicado o Indicador IQC para aferir se os chamados foram atendidos dentro do prazo.

IQC - Indicador Quantidade de chamados (requisição e incidentes) atendidos dentro do prazo	
Finalidade: Apurar a quantidade de chamados atendidos dentro do prazo estabelecido	
Meta a cumprir: 90%	
Instrumento de medição: Ferramenta de registro de chamados	
Periodicidade: Mensal	
Mecanismo de cálculo (%): $(\text{Total de chamados atendidos dentro do prazo} / \text{Total de chamados abertos no período}) \times 100$	
Faixa no ajuste no pagamento:	
De 80% - 89%	1%
De 70% - 79%	3%
Abaixo de 69%	5%

9.6.2. Indicador eficácia no tratamento de chamados (requisições, incidentes e incidentes de segurança)

9.6.2.1. Deve ser considerado a eficácia do tratamento dos chamados, ou seja, se os chamados não estão sendo reabertos após a resolução.

IET - Indicador eficácia no tratamento de chamados (requisições, incidentes e incidentes de segurança)	
Finalidade: Apurar a eficácia do contratado na resolução de chamados	
Meta a cumprir: 80%	
Instrumento de medição: Ferramenta de registro de chamados	
Periodicidade: Mensal	
Mecanismo de cálculo (%): $(\text{Total de chamados atendidos} - \text{Total de chamados reaberto}) / (\text{Total de chamados atendidos}) \times 100$	
Consideram-se atendidos os chamados fechados com solução, não devendo ser considerados os chamados fechados sem solução.	
Faixa no ajuste no pagamento:	
De 70% - 79%	1%
De 60% - 69%	3%
Abaixo de 59%	5%

9.6.3. Indicador de vinculação da resolução de requisições de serviço à base de conhecimento

9.6.3.1. A base de conhecimento deve ser vinculada a resolução do chamado, permitindo que a CONTRATANTE esteja no domínio do conhecimento adquirido durante a execução do contrato, dessa forma, deve-se observar o Indicador abaixo.

IBC - Indicador de vinculação da resolução de requisições de serviço à base de conhecimento	
Finalidade: Aferir a cobertura dos padrões de atendimento registrados na base de conhecimento	
Meta a cumprir: 95%	
Instrumento de medição: Ferramenta de registro de chamados	
Periodicidade: Mensal	
Mecanismo de cálculo (%): $(\text{Total de requisições com resolução vinculada à base de conhecimento} / \text{Total de requisições resolvidas}) \times 100$	
Faixa no ajuste no pagamento:	
De 85% - 94%	1%
De 70% - 84%	3%
Abaixo de 69%	5%

9.6.4. Indicador de Disponibilidade das Soluções Contratadas

9.6.4.1. Será aferida o índice de disponibilidade dos serviços ofertados pela CONTRATADA. Será desconsiderado do indicador as situações em que a disponibilidade do serviço não dependa da CONTRATADA, como soluções implantadas on premise na CONTRATANTE.

IDS - Indicador de Disponibilidade das Soluções oferecidas	
Finalidade: Apurar disponibilidade das soluções ofertadas no contrato	
Meta a cumprir: 97%	
Instrumento de medição: Ferramenta monitoramento de disponibilidade	
Periodicidade: Mensal	
Mecanismo de cálculo (%): $\text{Total de tempo com disponibilidade no mês} / \text{total de tempo no mês} \times 100$	
Faixa no ajuste no pagamento:	
De 90% - 96%	1%
De 80% - 89%	3%
Abaixo de 79%	5%

9.6.4.2. Indicador de Aderência ao Serviço Contratado

9.6.5. A aferição da execução contratual para fins de pagamento considerará os critérios do quadro a seguir, em que serão aplicadas as referidas pontuações para efeito de glosa, no caso de a CONTRATADA.

9.6.6. Observa-se que será aplicada glosa de 0,5% a cada 15 pontos, limitando-se a glosa decorrente da análise do quadro a seguir à aplicação do valor máximo de 15% do valor mensal previsto (soma dos itens).

IAS - Indicador de Aderência ao Serviço Contratado			
Item	Descrição	Referência	Glosa por inadimplemento
1	Finalizar a requisição de serviço ou incidente sem a devida resolução ou sem realizar os testes necessários para aferir a efetiva resolução	Por ocorrência	10 pontos
2	Finalizar uma requisição de serviço sem documentar os procedimentos executados para atendimento da solicitação	Por ocorrência	5 pontos
3	Finalizar um incidente sem documentar a causa, a solução de contorno (se houver) ou os procedimentos adotados para solução	Por ocorrência	5 pontos
4	Finalizar um problema sem documentar a investigação realizada, a causa-raiz ou a solução aplicada	Por ocorrência	5 pontos
5	Fraudar, manipular ou descaracterizar indicadores/metadados de níveis de serviço por quaisquer subterfúgios, por indicador/meta de nível de serviço manipulado	Por ocorrência	30 pontos
6	Manter profissionais sem formalização ou sem a qualificação exigida para executar serviços contratados, ainda que em casos de substituição temporária	Por ocorrência	30 pontos

7	Causar qualquer indisponibilidade dos serviços do CONTRATANTE por motivo de imperícia ou imprudência na execução das atividades contratuais	Por ocorrência	30 pontos
8	Utilizar indevidamente os recursos de TI (acessos indevidos, utilização para fins particulares)	Por ocorrência	30 pontos
9	Realizar mudanças de configuração nas soluções de segurança sem autorização CONTRATANTE	Por ocorrência	15 pontos
10	Deixar de cumprir ou implementar as rotinas em conformidade com a Política de Segurança ou determinações da equipe de fiscalização do contrato	Por ocorrência	10 pontos
11	Deixar de cumprir ou implementar as rotinas em conformidade com os Planos de Gerenciamento de Incidente de Disponibilidade, de Continuidade e de Recuperação de Desastres das soluções de segurança	Por ocorrência	10 pontos
12	Deixar de executar testes de continuidade de cada solução de segurança da informação em alta disponibilidade, no mínimo, a cada 6 (seis) meses	Por ocorrência	10 pontos
13	Deixar de atuar proativamente em caso de identificação de situação de desconformidade com boas práticas de segurança	Por ocorrência	10 pontos
14	Apresentar mensalmente plano de tratamento de vulnerabilidades, indicando as ações mais efetivas para redução dos riscos	Por ocorrência	20 pontos
15	Deixar de notificar sobre ocorrências recorrentes	Por ocorrência	5 pontos
16	Deixar de emitir o relatório de incidente em até 3 (três) dias úteis após o encerramento do incidente	Por ocorrência	30 pontos
17	Deixar de analisar a viabilidade e o impacto da instalação de novas soluções ou correções	Por ocorrência	20 pontos
18	Deixar de apresentar mensalmente proposta de melhorias no ambiente	Por ocorrência	5 pontos
19	Deixar de cumprir quaisquer obrigações estabelecidas no Termo de Referência, contrato e apêndices, ainda que não previstas nesta tabela, após reincidência formalmente notificada pela CONTRATANTE	Por ocorrência	15 pontos

9.6.7. As retenções ou glosas no pagamento serão aplicadas quando a CONTRATADA:

9.6.8. Não atingir os valores mínimos aceitáveis fixados nos Critérios de Aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

9.6.9. Deixar de utilizar materiais e recursos humanos necessários e suficientes para fornecimento da Solução de Tecnologia da Informação, ou utilizá-los com qualidade ou quantidade inferior à demandada.

9.7. Após a fiscalização dos serviços prestados, o gestor ou, na ausência deste, o gestor substituto indicará à CONTRATADA que os serviços estão em conformidade com as especificações do Termo de Referência e que está autorizada a emissão da Nota Fiscal/Fatura, sendo que o recebimento se materializará com o atesto da unidade requisitante.

9.8. A indicação de conformidade da execução do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do serviço, ou, em qualquer época, das garantias concedidas e das responsabilidades assumidas (em contrato ou Ordem de Serviço) e por força das disposições legais em vigor.

9.9. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do serviço, às custas da CONTRATADA, sem prejuízo da aplicação de penalidades.

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

10.1. São obrigações da CONTRATANTE:

10.1.1. exigir o recebimento do objeto no prazo e condições estabelecidas no Termo de Referência;

10.1.2. exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;

10.1.3. exercer o acompanhamento e a fiscalização dos serviços, por meio de colaborador especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

10.1.4. notificar a CONTRATADA, por escrito, sobre a ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se de que as soluções por ela propostas sejam as mais adequadas;

10.1.5. efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da CONTRATADA, no que couber;

10.1.6. pagar à CONTRATADA o valor resultante da prestação do serviço, no prazo e condições estabelecidas no Termo de Referência;

10.2. A EMBRATUR não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do objeto do Termo de Referência, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

10.3. São obrigações da CONTRATADA:

10.3.1. executar os serviços conforme especificações do Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais (ou da Ordem de Serviços), além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios

necessários, na qualidade e quantidade exigidas;

10.3.2. reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal da contratação, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

10.3.3. responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à EMBRATUR, devendo ressarcir imediatamente a CONTRATANTE em sua integralidade;

10.3.4. em caso de ocorrência do previsto no item 10.3.3, a CONTRATANTE ficará autorizada a descontar da garantia exigida no item 7.1 do contrato, ou dos pagamentos devidos à CONTRATADA, o valor correspondente aos danos sofridos;

10.3.5. utilizar empregados habilitados e com conhecimentos adequados dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

10.3.6. prestar todo esclarecimento ou informação solicitada pela CONTRATANTE ou por seus prepostos, garantindo-lhes o acesso aos documentos relativos à execução do serviço;

10.3.7. garantir o acesso da CONTRATANTE, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do serviço;

10.3.8. submeter previamente, por escrito, à CONTRATANTE, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações deste Termo de Referência (ou do memorial descritivo);

10.3.9. prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação;

10.3.10. manter, durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação;

10.3.11. assumir como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

10.3.12. indicar preposto para representá-la durante a vigência do contrato;

10.3.13. responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990).

CLÁUSULA DÉCIMA PRIMEIRA – DAS SANÇÕES ADMINISTRATIVAS

11.1. Pela inexecução total ou parcial do objeto desta contratação, a EMBRATUR pode aplicar à CONTRATADA as seguintes sanções:

11.1.1. advertência;

11.1.2. multas:

11.1.3. de 0,5% (meio por cento) do valor total da Ordem de Serviços, na qual tenha sido entregue ou realizado com atraso, qualquer produto ou serviço a ele destinado, aplicável por dia de atraso, entendendo-se como atraso, o não cumprimento do prazo de realização do serviço;

11.1.4. de 0,5% (meio por cento) do valor total da Ordem de Serviços por infração a qualquer de suas cláusulas ou condições, que não as especificadas no subitem anterior, aplicada em dobro na reincidência.

11.1.5. suspensão de licitar com a EMBRATUR por até 2 (dois) anos.

11.2. A aplicação de sanção fica condicionada ao trânsito de processo administrativo sancionador, que garantirá o contraditório e a ampla defesa.

11.3. A dosimetria da sanção deve levar em consideração as razões de fato e de direito apresentadas pela CONTRATADA, a gravidade e a abrangência de prejuízos potenciais ou materializados para a EMBRATUR e a reprovabilidade da conduta, devendo respeitar ordem taxativa prevista no item 11.1, sendo advertência a mais branda e a suspensão de licitar a mais grave.

11.4. A sanção de multa pode ser aplicada concomitantemente com as demais, sempre que se identificar ganho patrimonial à CONTRATADA ou prejuízos significativos à EMBRATUR.

11.5. No processo de aplicação de penalidades, prevalecerão as normas e procedimentos do Manual de Licitações e Contratos EMBRATUR.

CLÁUSULA DÉCIMA SEGUNDA – DAS RESCISÃO

12.1. O presente Termo de Contrato poderá ser rescindido sem prejuízo da aplicação das penalidades previstas neste contrato.

12.2. Os casos de rescisão contratual serão formalmente motivados.

12.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa.

12.4. O termo de rescisão, sempre que possível, será precedido da:

12.4.1. Avaliação dos eventos contratuais já cumpridos ou parcialmente cumpridos;

12.4.2. Relação dos pagamentos já efetuados e ainda devidos; e

12.4.3. Verificação quanto à exigibilidade de indenizações e/ou multas.

CLÁUSULA DÉCIMA TERCEIRA - DAS ALTERAÇÕES

13.1. As alterações contratuais por acordo entre as partes, desde que justificadas, e as decorrentes de necessidade de prorrogação, constarão de Termos Aditivos.

13.2. Os contratos poderão ser aditados, nas hipóteses de complementação, acréscimo ou supressão que se fizerem nos serviços, em até 25% (vinte e cinco por cento) do valor inicialmente contratado.

13.3. Nenhum acréscimo ou supressão poderá exceder os limites estabelecidos no item 13.2, salvo as supressões resultantes de acordo celebrado entre os contratantes.

CLÁUSULA DÉCIMA QUARTA - DA MATRIZ DE RISCO

14.1. Na hipótese de ocorrência de um dos eventos listados na Matriz de Riscos deste termo (item 14.8), a CONTRATADA deverá, no prazo de 01 (um) dia útil, notificar a EMBRATUR sobre o ocorrido, em documento com as seguintes informações mínimas:

- 14.1.1. Detalhamento do evento ocorrido, incluindo sua natureza, a data da ocorrência e sua duração estimada;
- 14.1.2. As medidas que estavam em vigor para mitigar o risco de materialização do evento, quando houver;
- 14.1.3. As medidas que irá tomar para fazer cessar os efeitos do evento e o prazo estimado para que esses efeitos cessem;
- 14.1.4. As obrigações contratuais que não foram cumpridas ou que não irão ser cumpridas em razão do evento; e
- 14.1.5. Outras informações relevantes.
- 14.2. Após a notificação, a EMBRATUR decidirá quanto ao ocorrido ou poderá solicitar esclarecimentos adicionais à CONTRATADA. Em sua decisão a EMBRATUR poderá isentar temporariamente à CONTRATADA do cumprimento das obrigações contratuais afetadas pelo evento.
- 14.3. A concessão de isenção não exclui a possibilidade de aplicação das sanções.
- 14.4. O reconhecimento pela EMBRATUR dos eventos descritos no item 14.8 (Matriz de Riscos) deste termo que afetem o cumprimento das obrigações contratuais, com responsabilidade indicada exclusivamente a CONTRATADA, não dará ensejo à recomposição do equilíbrio econômico financeiro do Contrato, devendo o risco ser suportado exclusivamente pela CONTRATADA.
- 14.5. Os fatos imprevisíveis, ou previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do contrato, não previstos no item 14.8 (Matriz de Riscos), serão decididos mediante acordo entre as partes, no que diz respeito à recomposição do equilíbrio econômico financeiro do contrato.
- 14.5.1. O contrato poderá ser rescindido, quando demonstrado que todas as medidas para sanar os efeitos foram tomadas e mesmo assim a manutenção do contrato se tornar impossível ou inviável nas condições existentes ou é excessivamente onerosa.
- 14.6. Fica a CONTRATADA autorizada a prestar serviços indicados neste Termo com maior qualidade devido a inovações metodológicas ou tecnológicas.
- 14.7. A CONTRATADA não pode inovar no modelo de execução e em suas responsabilidades contratuais.
- 14.8. Matriz de Riscos:

Eventos supervenientes	Ações Mitigadoras	Responsabilidade da Contratada	Responsabilidade do Contratante
Execução ineficiente do contrato	O fiscal deve participar da elaboração do Edital e anexos, além de receber treinamento específico		X
Situações na prestação dos serviços que configurem caso fortuito ou força maior	Suspender ou rescindir o contrato, com possibilidade de contratar remanescente		X
Manutenção e modernização - Custos de manutenção adicionais por previsão incorreta	Exigência de experiência prévia para o correto acompanhamento na prestação do serviço, gerenciando adequadamente os riscos de defeitos inesperados	X	
Não cumprimento dos limites de qualidade previstos no item 3. DESCRIÇÃO DA SOLUÇÃO DE TIC	Fiscalização constante do contrato a fim de observar se os níveis estabelecidos no contrato estão sendo cumpridos e proceder a glosas quando pertinentes.	X	X
Não cumprimento de prazos	Sanções contratuais impostas pela CONTRATANTE por atraso no cumprimento dos prazos.	X	X

CLÁUSULA DÉCIMA QUINTA – DAS VEDAÇÕES

- 15.1. É vedado à CONTRATADA:
- 15.1.1. Caucionar ou utilizar este Termo de Contrato para qualquer operação financeira; e
- 15.1.2. Interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

CLÁUSULA DÉCIMA SEXTA – DOS CASOS OMISSOS

16.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas no Manual de Licitações e Contratos da EMBRATUR, por meio da DIREX (Diretoria Executiva) e demais normas federais aplicáveis e, subsidiariamente, as normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA SÉTIMA – DA PUBLICAÇÃO

17.1. O extrato deste contrato será publicado no site oficial da Embratur, conforme previsto no art. 2º da Portaria EMBRATUR nº 26, de 31 de maio de 2023.

CLÁUSULA DÉCIMA OITAVA – DO FORO

18.1. Fica eleito o foro da cidade de Brasília-DF para dirimir as questões decorrentes da execução deste contrato.

E, por assim estarem justas e acertadas, foi lavrado o presente contrato e disponibilizado por meio do Sistema Eletrônico de Informações – SEI, o qual, depois de lido e achado conforme, vai assinado pelas partes, perante duas testemunhas.

ANEXOS:

ANEXO I – TERMO DE COMPROMISSO

ANEXO II – TERMO DE CIÊNCIA

ANEXO I – TERMO DE COMPROMISSO

O _____, sediado em _____, CNPJ nº _____, doravante denominado CONTRATANTE, e, de outro lado, a _____, sediada em _____, CNPJ nº _____, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º ____/20____ doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção; CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes;

Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA; II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO. I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretroatável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que: I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes; V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo a CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

A CONTRATANTE elege o foro da Justiça Federal da Seção Judiciária do Distrito Federal, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

DE ACORDO

CONTRATANTE	CONTRATADA
_____ Nome	_____ Nome

_____, _____ de _____ de 20____.

IDENTIFICAÇÃO			
Contrato N°:			
Objeto:			
Contratante:			
Gestor do Contrato:		Matrícula:	
Contratada:		CNPJ:	
Preposto da Contratada:		CPF:	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes na Contratante.

CIÊNCIA	
CONTRATADA – FUNCIONÁRIOS	
Nome Matrícula	Nome Matrícula



Documento assinado eletronicamente por **Marcelo Ribeiro Freixo, Presidente**, em 04/06/2025, às 17:23, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site http://sei.embratur.com.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1127799** e o código CRC **CF687FDD**.