

IBGE-FUN.INST.BRAS.GEOGRAFIA E ESTATISTICA

Edital 3/2026

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
3/2026	114601-IBGE-FUN.INST.BRAS.GEOGRAFIA E ESTATISTICA	WEBBER TAVARES DE CARVALHO	20/03/2026 12:03 (v 0.9)
Status	DISPONIBILIZADO		

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Serviços de TIC	74/2026	03603.000077/2025-45

IBGE

PREGÃO ELETRÔNICO

90006/2026

CONTRATANTE (UASG)

IBGE-FUN.INST.BRAS.GEOGRAFIA E ESTATISTICA (UASG 114601)

OBJETO

Contratação de empresa especializada para execução de serviços técnicos contínuos referente ao Serviço Gerenciado de Segurança da Informação de forma REMOTA, pelo período de 24 (vinte e quatro) meses, conforme condições estabelecidas no Termo de Referência, podendo ser renovado até o limite da lei

VALOR TOTAL DA CONTRATAÇÃO

R\$ 6.927.887,52

DATA DA SESSÃO PÚBLICA

Dia 08/04/2026 às 10h (horário de Brasília)

CRITÉRIO DE JULGAMENTO:

menor preço por grupo

MODO DE DISPUTA:

aberto e fechado

TRATAMENTO FAVORECIDO ME/EPP/EQUIPARADAS

SIM

MARGEM DE PREFERÊNCIA PARA ALGUM ITEM

NÃO

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA - IBGE

PREGÃO ELETRÔNICO Nº 90006/2026

(Processo Administrativo: 03603.000077/2025-45)

Torna-se público que o(a) FUNDAÇÃO INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA - IBGE, por meio de sua Gerência de Materiais e Serviços, subordinada à Coordenação de Recursos Materiais, Diretoria Executiva, sediada à Avenida Franklin Roosevelt, 166, Centro, Rio de Janeiro/RJ, realizará licitação, na modalidade **PREGÃO ELETRÔNICO**, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 1º de abril de 2021, e demais legislações aplicáveis e, ainda, de acordo com as condições estabelecidas neste Edital.

1. DO OBJETO

1.1. O objeto da presente licitação é Contratação de empresa especializada para execução de serviços técnicos contínuos referente ao Serviço Gerenciado de Segurança da Informação de forma REMOTA, pelo período de 24 (vinte e quatro) meses, conforme condições estabelecidas no Termo de Referência, podendo ser renovado até o limite da lei, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em grupo único, formados por 3 (três) itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

1.3. Em caso de eventual divergência entre as especificações descritas no CATSER do Catálogo do Compras.gov e as especificações constantes neste Edital, prevalecerão as últimas.

2. DO REGISTRO DE PREÇOS

2.1. Não se aplica à presente contratação.

3. DA PARTICIPAÇÃO NA LICITAÇÃO

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

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

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

3.4. 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.

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

3.6. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto nº 8.538, de 2015, bem como para bens e serviços produzidos com tecnologia produzida no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Lei nº 8.248, de 1991 e art. 8º do Decreto nº 7.174, de 2010.

3.7. Não poderão disputar esta licitação:

3.7.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

3.7.2. sociedade que desempenhe atividade incompatível com o objeto da licitação;

3.7.3. sociedades cooperativas;

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

3.7.5. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

3.7.6. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

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

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

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

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

3.7.11. pessoas jurídicas reunidas em consórcio;

3.7.12. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

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

3.9. O impedimento de que trata o item **3.7.6** será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

3.10. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens **3.7.4 e 3.7.5** poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

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

3.12. O disposto nos itens **3.7.4 e 3.7.5** não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

3.13. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei nº 14.133, de 2021.

3.14. A vedação de que trata o item **3.8** estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

4. DO ORÇAMENTO ESTIMADO

4.1. O orçamento estimado da presente contratação não será de caráter sigiloso.

5. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

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

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

5.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 9.1.1 e 9.12.2 deste Edital.

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

5.4.1. 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;

5.4.2. 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;

5.4.3. 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;

5.4.4. 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.

5.5. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

5.6. 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, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei nº 14.133, de 2021.

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

5.6.2. 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.

5.7. Não poderá se beneficiar do tratamento jurídico diferenciado estabelecido nos arts. 42 a 49 da Lei Complementar nº 123, de 2006, a pessoa jurídica:

5.7.1. de cujo capital participe outra pessoa jurídica;

5.7.2. que seja filial, sucursal, agência ou representação, no País, de pessoa jurídica com sede no exterior;

5.7.3. de cujo capital participe pessoa física que seja inscrita como empresário ou seja sócia de outra empresa que receba tratamento jurídico diferenciado nos termos da Lei Complementar nº 123, de 2006, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do art. 3º da referida lei;

5.7.4. cujo titular ou sócio participe com mais de 10% (dez por cento) do capital de outra empresa não beneficiada pela Lei Complementar nº 123, de 2006, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do art. 3º da referida lei;

5.7.5. cujo sócio ou titular seja administrador ou equiparado de outra pessoa jurídica com fins lucrativos, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do art. 3º da referida lei;

5.7.6. constituída sob a forma de cooperativas, salvo as de consumo;

5.7.7. que participe do capital de outra pessoa jurídica;

5.7.8. que exerça atividade de banco comercial, de investimentos e de desenvolvimento, de caixa econômica, de sociedade de crédito, financiamento e investimento ou de crédito imobiliário, de corretora ou de distribuidora de títulos, valores mobiliários e câmbio, de empresa de arrendamento mercantil, de seguros privados e de capitalização ou de previdência complementar;

5.7.9. resultante ou remanescente de cisão ou qualquer outra forma de desmembramento de pessoa jurídica que tenha ocorrido em um dos 5 (cinco) anos-calendário anteriores;

5.7.10. constituída sob a forma de sociedade por ações.

5.7.11. cujos titulares ou sócios guardem, cumulativamente, com o contratante do serviço, relação de pessoalidade, subordinação e habitualidade.

5.8. A falsidade da declaração de que trata os itens 5.4 ou 5.6 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

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

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

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

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

5.12.1. 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

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

5.13. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

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

5.13.2. percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.

5.14. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 5.10 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.

5.15. 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.

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

6. DO PREENCHIMENTO DA PROPOSTA

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

6.1.1. valor unitário e total do item;

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

6.2.1. O licitante NÃO poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação.

6.3. 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.

6.4. 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.

6.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

6.5.1. No regime de incidência não-cumulativa de PIS e COFINS, a cotação adequada será a que corresponde à média das alíquotas efetivamente recolhidas pela empresa, comprovada, a qualquer tempo, por documentos de Escrituração Fiscal Digital da Contribuição (EFD-Contribuições) para o PIS/PASEP e COFINS dos últimos 12 (doze) meses anteriores à apresentação da proposta, ou por outro meio hábil.

6.6. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

6.7. Na presente licitação, a Microempresa e a Empresa de Pequeno Porte poderão se beneficiar do regime de tributação pelo Simples Nacional, caso a futura contratação não se enquadre no pressuposto do §9º, art. 3º, da Lei nº 123/06.

6.8. 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.

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

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

6.11. Caso o critério de julgamento seja o de menor preço, os licitantes devem respeitar os preços máximos previstos no Termo de Referência;

6.12. O descumprimento das regras supramencionadas pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

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

7.1. 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.

7.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

7.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro/Agente de Contratação /Comissão e os licitantes.

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

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

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

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

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

7.9. 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 inexecutível.

7.10. O procedimento seguirá de acordo com o modo de disputa adotado.

7.11. Tendo em vista que o envio de lances na licitação se dará pelo modo de disputa “aberto e fechado”, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

7.11.1. 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.

7.11.2. 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.

7.11.3. 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.

7.11.4. 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.

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

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

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

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

7.15. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva da licitação, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

7.16. 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/Agente de Contratação/Comissão aos participantes, no sítio eletrônico utilizado para divulgação.

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

7.18. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial, caso a contratação não se enquadre nas vedações dos §§1º e 2º do art. 4º da Lei nº 14.133, de 2021. 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.

7.18.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento), caso se trate de um pregão, serão consideradas empatadas com a primeira colocada.

7.18.2. 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.

7.18.3. 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 até 5% (cinco por cento), caso se trate de um pregão, na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

7.18.4. 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.

7.18.5. A obtenção do benefício a que se refere o item anterior fica limitada às microempresas e às empresas de pequeno porte que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

7.19. Será assegurado o direito de preferência previsto no artigo 3º da Lei nº 8.248, de 1991, conforme procedimento estabelecido nos artigos 5º e 8º do Decreto nº 7.174, de 2010, nos seguintes termos:

7.19.1. Após a aplicação das regras de preferência para microempresas e empresas de pequeno porte, caberá a aplicação das regras de preferência, sucessivamente, para:

7.19.1.1. bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;

7.19.1.2. bens e serviços com tecnologia desenvolvida no País; e

7.19.1.3. bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal, nos termos do art. 5º e 8º do Decreto 7.174, de 2010 e art. 3º da Lei nº 8.248, de 1991.

7.19.2. Os licitantes classificados que estejam enquadrados no item 7.22.1.1, na ordem de classificação, serão convocados para que possam oferecer nova proposta ou novo lance para igualar ou superar a melhor proposta válida, caso em que será declarado vencedor do certame.

7.19.3. Caso a preferência não seja exercida na forma do item 7.22.1.1, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no item 7.22.1.2, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o item 7.22.1.3 caso esse direito não seja exercido.

7.19.4. As licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

7.20. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

7.21. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

7.21.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

7.21.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

7.21.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

7.21.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

7.22. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

7.22.1. empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

7.22.2. empresas brasileiras;

7.22.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

7.22.4. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

7.23. Esgotados todos os demais critérios de desempate previstos em lei, a escolha do licitante vencedor ocorrerá por sorteio, em ato público, para o qual todos os licitantes serão convocados, vedado qualquer outro processo.

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

7.24.1. Por se tratar de licitação em grupo, a contratação posterior de item específico do grupo exigirá prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou a entidade e serão observados como critério de aceitabilidade os preços unitários máximos definidos no Termo de Referência.

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

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

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

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

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

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

8. DA FASE DE JULGAMENTO

8.1. Encerrada a etapa de negociação, o Pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133, de 2021, legislação correlata e no item 3.9 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

8.1.1. SICAF;

8.1.2. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (<https://portal.datransparencia.gov.br/pagina-interna/603244-cnep>); e.

8.2. A consulta aos cadastros será realizada no nome e no CNPJ da empresa licitante.

8.2.1. A consulta ao CNEP quanto às sanções previstas na Lei nº 8.429, de 1992, também ocorrerá no nome e no CPF do sócio majoritário da empresa licitante, se houver, por força do art. 12 da citada lei.

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

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

8.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação.

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

8.4. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o Pregoeiro verificará se o licitante faz jus ao benefício aplicado.

8.5. 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 nos arts. 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022.

8.6. Será desclassificada a proposta vencedora que:

8.6.1. conter vícios insanáveis;

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

- 8.6.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;
- 8.6.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;
- 8.6.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.
- 8.7. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.
- 8.8. A inexequibilidade, na hipótese de que trata o item anterior, só será considerada após diligência do Pregoeiro, que comprove:
- 8.8.1. que o custo do licitante ultrapassa o valor da proposta; e
- 8.8.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.
- 8.9. 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.
- 8.10. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.
- 8.11. Erros no preenchimento da proposta não constituem motivo para a desclassificação da proposta. A proposta poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação;
- 8.12. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;
- 8.13. 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.
- 8.14. 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.

9. DA FASE DE HABILITAÇÃO

- 9.1. Os documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.
- 9.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.
- 9.2. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.
- 9.3. 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.

9.4.. Quando permitida a participação de consórcio de empresas, a habilitação técnica, quando exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.

9.4.1. Se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte e o termo de referência exigir requisitos de habilitação econômico-financeira, haverá um acréscimo de 10% (dez por cento) para o consórcio em relação ao valor exigido para os licitantes individuais.

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

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

9.7. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei.

9.8. 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.

9.9. 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.

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

9.10.1. 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.

9.11. 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.

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

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

9.12.1. 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/Agente de Contratação/Comissão.

9.12.2. Na hipótese de a fase de habilitação anteceder a fase de apresentação de propostas e lances, os licitantes encaminharão, por meio do sistema, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto no § 1º do art. 36 e no § 1º do art. 39 da Instrução Normativa SEGES nº 73, de 30 de setembro de 2022.

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

9.13.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

9.14. Encerrado o prazo para envio da documentação de que trata o item 9.13.1, poderá ser admitida, mediante decisão fundamentada do Pregoeiro, a apresentação de novos documentos de habilitação ou a complementação de informações acerca dos documentos já apresentados pelos licitantes, em até 02 (duas) horas, para:

9.14.1. a aferição das condições de habilitação do licitante, desde que decorrentes de fatos existentes à época da abertura do certame;

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

9.14.3. suprimimento da ausência de documento de cunho declaratório emitido unilateralmente pelo licitante;

9.14.4. suprimimento da ausência de certidão e/ou documento de cunho declaratório expedido por órgão ou entidade cujos atos gozem de presunção de veracidade e fé pública.

9.15. Findo o prazo assinalado sem o envio da nova documentação, restará preclusa essa oportunidade conferida ao licitante, implicando sua inabilitação.

9.16. 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.

9.17. 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 9.12.1.

9.18. 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.

9.19. 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.

10. DO TERMO DE CONTRATO

10.1. Após a homologação e adjudicação, caso se conclua pela contratação, será firmado termo de contrato, ou outro instrumento equivalente.

10.2. O adjudicatário terá o prazo de 5 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o termo de contrato ou instrumento equivalente, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste Edital.

10.3. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou instrumento equivalente, a Administração poderá: a) encaminhá-lo para assinatura, mediante correspondência postal com aviso de recebimento (AR), para que seja assinado e devolvido no prazo de 5 (cinco) dias úteis, a contar da data de seu recebimento; b) disponibilizar acesso a sistema de processo eletrônico para que seja assinado digitalmente em até 5 (cinco) dias úteis; ou c) outro meio eletrônico, assegurado o prazo de 5 (cinco) dias úteis para resposta após recebimento da notificação pela Administração.

10.4. Os prazos dos itens 10.2 e 10.3 poderão ser prorrogados, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

10.5. O prazo de vigência da contratação é o estabelecido no Termo de Referência.

10.6. Na assinatura do contrato ~~e~~ será exigido o Cadastro Informativo de Créditos não Quitados do Setor Público Federal – Cadin e a comprovação das condições de habilitação e contratação consignadas neste Edital, que deverão ser mantidas pelo fornecedor durante a vigência do contrato.

11. DA ATA DE REGISTRO DE PREÇOS

11.1. Não se aplica à presente contratação.

12. DA FORMAÇÃO DO CADASTRO DE RESERVA

12.1. Não se aplica à presente contratação.

13. DOS RECURSOS

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

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

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

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

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

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

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

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

13.5. 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.

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

13.7. 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.

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

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

13.10. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico licitacoes@ibge.gov.br.

14. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

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

14.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a Pregoeiro/Agente de Contratação/Comissão/a durante o certame;

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

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

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

14.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

14.1.2.4. deixar de apresentar amostra;

14.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

14.1.3. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

14.1.4. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

14.1.5. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

14.1.6. fraudar a licitação;

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

14.1.7.1. agir em conluio ou em desconformidade com a lei;

14.1.7.2. induzir deliberadamente a erro no julgamento;

14.1.7.3. apresentar amostra falsificada ou deteriorada;

14.1.8. praticar atos ilícitos com vistas a frustrar os objetivos da licitação

14.1.9. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

14.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, após regular processo administrativo, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

14.2.1. advertência;

14.2.2. multa;

14.2.3. impedimento de licitar e contratar e

14.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

14.3. Na aplicação das sanções serão considerados:

14.3.1. a natureza e a gravidade da infração cometida.

14.3.2. as peculiaridades do caso concreto

14.3.3. as circunstâncias agravantes ou atenuantes

14.3.4. os danos que dela provierem para a Administração Pública

14.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

14.4. A multa será recolhida no prazo máximo de 10 (dez) dias úteis, a contar da comunicação oficial.

14.4.1. Para as infrações previstas nos itens 14.1.1, 14.1.2 e 14.1.3, a multa será de 0,5% a 15% do valor do contrato licitado.

14.4.2. Para as infrações previstas nos itens 14.1.5, 14.1.6, 14.1.7, 14.1.8, 14.1.9 e 14.1.9, a multa será de 15% a 30% do valor do contrato licitado.

14.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

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

14.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 14.1.1, 14.1.2, 14.1.3 e 14.1.4, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

14.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 14.1.5, 14.1.6, 14.1.7, 14.1.8 e 14.1.9, bem como pelas infrações administrativas previstas nos itens 14.1.1, 14.1.2 e 14.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei nº 14.133, de 2021

14.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 14.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

14.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

14.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

14.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

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

14.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

14.15. Para a garantia da ampla defesa e contraditório dos licitantes, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como os cadastrados pela empresa no SICAF.

14.15.1. Os endereços de e-mail informados na proposta comercial e/ou cadastrados no Sicafe serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

15. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

15.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

15.2. 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.

15.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, pelos seguintes meios: licitacoes@ibge.gov.br

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

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

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

16. DAS DISPOSIÇÕES GERAIS

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

16.2. 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.

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

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

16.5. 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.

16.6. 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.

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

16.8. 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.

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

16.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP): <https://www.ibge.gov.br/acesso-informacao/licitacoes-e-contratos.html> e endereço eletrônico licitacoes@ibge.gov.br.

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

16.11.1. ANEXO I - Termo de Referência;

16.11.1.1. ANEXO I-A - ESPECIFICAÇÃO TÉCNICA;

16.11.1.2. ANEXO I-B - DESCRIÇÃO DO AMBIENTE COMPUTACIONAL DO IBGE;

16.11.1.3. ANEXO I-C - TERMO DE COMPROMISSO DE MANUTENÇÃO DO SIGILO;

16.11.1.4. ANEXO I-D - TERMO DE CIÊNCIA;

16.11.1.5. ANEXO I-E - SISTEMAS DO IBGE AGRUPADOS POR TEMA;

16.11.1.6. ANEXO I-F - Termo de Responsabilidade de Terceiros sobre Ativo de Tecnologia do IBGE;

16.11.1.7. ANEXO I-G - Modelo de Ordem de Serviço (OS) ou Ticket para abertura de chamados.

16.11.1.8. Apêndice do ANEXO I - ESTUDO TÉCNICO PRELIMINAR.

16.11.2. Anexo II – Minuta de Termo de Contrato;

16.11.3. Anexo III - Modelo da Proposta Comercial.

Rio de Janeiro, na data da assinatura eletrônica.

ASSINATURA DA AUTORIDADE COMPETENTE

17. Responsáveis

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

CLAUDIA GOULART DE SIQUEIRA

Pregoeiro



Assinou eletronicamente em 20/03/2026 às 12:03:18.

IBGE-FUN.INST.BRAS.GEOGRAFIA E ESTATISTICA

Termo de Referência 27/2026

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
27/2026	114601-IBGE-FUN.INST.BRAS.GEOGRAFIA E ESTATISTICA	PRISCILLA DE FREITAS MONDINI BELLETTI	10/03/2026 17:15 (v 0.6)
Status			
CONCLUIDO			

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Serviços de TIC	74/2026	03603.000077/2025-45

1. Processo Administrativo nº xxxxx.xxxxxx/xxxx-xx

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de empresa especializada para execução de serviços técnicos contínuos referente ao Serviço Gerenciado de Segurança da Informação de forma REMOTA, pelo período de 24 (vinte e quatro) meses, conforme condições estabelecidas no presente Termo de Referência, podendo ser renovado até o limite da lei, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

Grupo	Item	Especificação	CATSER	Métrica ou Unidade de Medida	Quantidade	Valor Unitário Mensal Estimado	Valor Total Estimado
1	1	Gestão de Riscos - Processo integrado envolvendo a Gestão de Vulnerabilidades, Gestão de Riscos, Compliance e Monitoração de Marca	27014	Mês	24	R\$ 173.488,00	R\$ 4.163.712,00
		Gestão de Incidentes -					

	2	Processo integrado envolvendo a Análise de Incidentes Globais e o Monitoramento de Incidentes	27014	Mês	24	R\$ 71.397,98	R\$ 1.713.551,52
	3	Resposta aos Incidentes - Processo integrado envolvendo a prevenção, bloqueio e resposta aos incidentes, bem como a análise de sua causa raiz	27014	Mês	24	R\$ 43.776,00	R\$ 1.050.624,00
		Total					R\$ 6.927.887,52

1.1.1. A presente contratação tem por objeto a prestação de serviço especializado de Centro de Operações de Segurança (SOC) remoto, com funcionamento ininterrupto (24x7), visando garantir a detecção, análise, resposta e mitigação de incidentes de segurança da informação no ambiente tecnológico da instituição.

Classificação do objeto quanto à heterogeneidade ou complexidade

1.2. O(s) serviço(s) objeto desta contratação são caracterizados como **comum(ns)**, conforme justificativa constante do Estudo Técnico Preliminar.

1.3. O serviço é enquadrado como continuado tendo em vista que a contratação de um serviço de Security Operations Center (SOC) remoto 24x7 configura-se como serviço continuado, pois trata-se de atividade essencial à manutenção da segurança da informação e da infraestrutura tecnológica da Administração Pública. A interrupção desse serviço comprometeria a integridade dos ativos informacionais, a continuidade dos serviços públicos e a proteção contra ameaças cibernéticas, conforme previsto no art. 6º, inciso XV da Lei nº 14.133/2021, que define serviços contínuos como aqueles decorrentes de necessidades permanentes ou prolongadas, sendo a vigência plurianual mais vantajosa considerando:

- 1.3.1. Maior previsibilidade orçamentária e contratual, reduzindo os riscos de descontinuidade do serviço;
- 1.3.2. Economia de escala e melhores condições comerciais, com possibilidade de negociação de preços mais vantajosos em contratos de maior duração;
- 1.3.3. Redução de custos administrativos, ao evitar sucessivas licitações para o mesmo objeto;
- 1.3.4. Maior estabilidade operacional, essencial para serviços críticos como o monitoramento contínuo de segurança da informação.

Prazo de vigência

1.4. O prazo de vigência da contratação é de 24 (vinte e quatro) meses contados da assinatura do contrato, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

1.5. O contrato ou outro instrumento hábil que o substitua oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A presente contratação justifica-se conforme o Decreto nº 9.507 de 2018, artigo 4º, parágrafo 2º, não podem ser objeto de execução indireta as atividades inerentes às categorias funcionais abrangidas pelo plano de cargos do órgão ou entidade. No entanto, o IBGE não tem, em seu plano de cargos, uma categoria funcional para a área de informática, sendo os funcionários de nível médio no IBGE, quase em sua totalidade, na categoria de “técnico em informações geográficas e estatísticas” e os de nível superior “tecnologista em informações geográficas e estatísticas” e/ou “analista em planejamento, gestão e infraestrutura em informações geográficas e estatísticas”.

2.1.1 A Diretoria de Informática é responsável pelos serviços de manutenção de hardware e software, correio eletrônico, infraestrutura de rede, operação e gerenciamento do backbone e de redes locais, firewall, segurança da informação em nível institucional, servidores web, videoconferência, telefonia IP, comunicação de dados e sistemas de informação corporativos (desenvolvimento e manutenção).

2.1.2 Os recursos em tecnologia da informação utilizados no IBGE compreendem computadores com diferentes capacidades de processamento e armazenamento, desde PDAs, desktops e notebooks de uso geral a computadores e equipamentos servidores com configuração específica pra atender requisitos de missões e operações científicas de alto nível de complexidade.

2.1.3 Todo o ambiente computacional do IBGE, instalado em todas as unidades, opera de forma integrada, ou seja, os recursos e configurações de toda plataforma computacional são gerenciados de forma centralizada pela Diretoria de Informática a partir da Diretoria de Informática, no Rio de Janeiro, de forma a garantir a governança adequada desta plataforma, o controle dos ativos disponíveis aos usuários (desktops, notebooks, estações servidoras, scanners, recursos de impressão, recursos de digitalização), o controle dos ativos de rede (roteadores, switches, redes sem fio), gerenciamento completo da segurança da informação (firewalls integrados, mecanismos antivírus, mecanismos antispam), o controle de serviços oferecidos aos usuários (correio eletrônico, servidores FTP, plataforma Intranet /Internet), a gerência de mudanças e o controle de aplicações de gestão disponíveis para a comunidade (sistemas administrativos). A gestão centralizada de todos os recursos objetiva economia e eficiência nestas atividades, vez que permite a concentração de especialistas atendendo a demandas remotamente, sem a necessidade de disponibilização de diversos recursos nas unidades remotas caso o serviço fosse distribuído.

2.1.4 A arquitetura de Informática do IBGE reflete a evolução das Tecnologias da Informação e Comunicação (TICs) e vem sendo modificada ao longo dos anos, de maneira a manter-se um equilíbrio entre os anseios e diretrizes institucionais e governamentais e a disponibilidade de recursos financeiros, visando, além disso, a manutenção e/ou melhoria da qualidade dos trabalhos do IBGE, com a diminuição dos custos e o atendimento das necessidades da Instituição. Desta forma, os impactos de não realizar a contratação neste momento são a vulnerabilidade dos dados da Instituição.

2.1.5 Necessidade da contratação do serviço:

2.1.5.1 IBGE, como órgão oficial de produção de estatísticas lida, em parte de seu trabalho, com informações sensíveis a todos os brasileiros e empresas do país. Diante disso, preocupados com o sigilo das informações prestadas ao IBGE, a Instituição sempre se preocupa em garantir a confidencialidade, integridade, autenticidade e disponibilidade das informações, pilares esses de uma Política de Segurança das Informações e Comunicações – POSIC.

2.1.5.2 Associado a esses princípios, é indispensável considerar os princípios fundamentais da estatística que são utilizados para nortear as boas práticas do tema, e devem sempre ser difundidos entre os colaboradores do IBGE.

2.1.5.3 O compromisso legal do IBGE em manter a privacidade do informante e o sigilo das informações prestadas, conforme previsto na Lei n. 5534, de 14.11.68, torna indispensável a implementação de controles rígidos de segurança da informação e comunicações, permitindo que as atividades desempenhadas na Instituição tratem as

informações e estudos de natureza estatística, geográfica, cartográfica, demográfica e administrativa com a devida segurança para garantir a legalidade de suas ações.

2.1.6 Justificativa das especificações técnicas do serviço:

2.1.6.1 A infraestrutura de Tecnologia da Informação e Comunicação (TIC) é um componente estratégico para o desempenho das atividades técnicas e administrativas do IBGE que gera, armazena e processa uma grande quantidade de dados e informações através da utilização de sistemas corporativos, da digitalização e da produção de documentos eletrônicos. A infraestrutura de rede disponibiliza serviços tais como: correio eletrônico, acesso à internet, sistemas corporativos no padrão web, telefonia IP, Gestão Eletrônica de Documentos, videoconferência, compartilhamento de arquivos, entre outros.

2.1.6.2 A arquitetura de Informática do IBGE reflete a evolução das Tecnologias da Informação e Comunicação (TICs) e vem sendo modificada ao longo dos anos, de maneira a manter-se um equilíbrio entre os anseios e diretrizes institucionais e governamentais e a disponibilidade de recursos financeiros, visando, além disso, a manutenção e/ou melhoria da qualidade dos trabalhos do IBGE, com a diminuição dos custos e o atendimento das necessidades da Instituição.

2.1.6.3 A aquisição da solução de segurança e teste de invasão visa manter a estratégia atual de defesa contra diversos tipos de ameaças aos nossos sistemas, tornando-os mais seguros e eficientes no que tange a proteção dos dados e acessos por pessoas não autorizadas.

2.1.6.4 Com o intuito de minimizar ataques, faz se necessário a utilização de Solução a qual busca eliminar as falhas ou brechas que possam ser utilizadas por hackers ou demais pessoas mal-intencionadas para ter acesso a dados e informações confidenciais.

2.2. O objeto da contratação está previsto no Plano de Contratações Anual 2026, conforme detalhamento a seguir:

- I) ID PCA no PNCP: 33787094000140-0-000019/2026.;
- II) Data de publicação no PNCP: 12/02/2025;
- III) Id do item no PCA: 141;
- IV) Classe/Grupo: Serviço de Gerenciamento em Tecnologia da Informação e da Computação;
- V) Identificador da Futura Contratação: 114601-74/2026;
- VI) Número do DFD: 213/2025.

2.9. O objeto da contratação também está alinhado com a Estratégia de Governo Digital 2025 e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2026 do IBGE, conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	Objetivos Estratégicos
17	Adotar soluções genéricas de TI
18	Garantir o nivelamento tecnológico dos projetos institucionais

ID	Ação do PDTI	ID	Meta do PDTI associada
17	Adotar soluções genéricas de TI	Diretriz 2	Trazer maior agilidade ao desenvolvimento e à padronização dos recursos de TI, por meio de soluções genéricas e abrangentes que possam ser aproveitadas para mais de um projeto, pesquisa ou processo.
18	Garantir o nivelamento tecnológico dos projetos institucionais	Diretriz 3	Assegurar que os projetos institucionais tenham simetria e nivelamento tecnológico quanto aos equipamentos e aos sistemas, padronizando a infraestrutura e os sistemas de TICs em uso.
		Diretriz 4	Expandir a infraestrutura de comunicações para integrar todas as unidades organizacionais, inclusive a rede de agências.

2.10. O objeto da contratação será integrado à Plataforma Gov.br, nos termos do Decreto nº 8.936, de 19 de dezembro de 2016, e suas atualizações, de acordo com as especificações deste Termo de Referência.

2.11. A demanda do IBGE tem como base as seguintes informações e histórico de necessidades:

2.11.1. Devido à complexidade e criticidade das informações administradas pelo IBGE, enquanto instituição, bem como para melhor gerenciar a Segurança da Informação nos seus aspectos de confidencialidade, integridade e disponibilidade, em conformidade com sua Política de Segurança da Informação (POSIC), este serviço se faz extremamente necessário para garantir a integridade e segurança dos dados trabalhados.

2.11.2. Para que haja maior visibilidade e controle acerca do risco relacionado à segurança das informações e de eventuais incidentes, optou-se pela contratação de empresa especializada para realizar os serviços contemplados neste edital, checando assim o nível de segurança do IBGE e contribuindo na gestão de segurança.

2.11.3. A contratação, de forma planejada, a serem consumidas em um período de 24 meses, podendo ser renovado até o limite da lei, nos quantitativos e condições do edital.

2.12. Justificativa da Solução Escolhida

2.12.1. O objetivo desta contratação é:

2.12.2. Garantir a confidencialidade, integridade, autenticidade e disponibilidade das informações;

2.12.3. Manter a privacidade do informante e o sigilo das informações prestadas, conforme previsto na Lei n.5534, de 14.11.68;

2.12.4. Permitir que as atividades desempenhadas na Instituição tratem as informações e estudos de natureza estatística, geográfica, cartográfica, demográfica e administrativa com a devida segurança para garantir a legalidade de suas ações;

2.12.5. Permitir maior transparência e autonomia na análise de eventuais vulnerabilidades encontradas na rede e nos Sistemas utilizados pelo IBGE, através da checagem do nível de segurança do IBGE;

2.12.6. Análise geral do ambiente do IBGE quanto a segurança da informação para identificar, mapear, documentar, controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica do IBGE;

2.12.7. Revisão e elaboração de um conjunto de documentos para a atualização constante da Política de Segurança da Informação do IBGE;

2.12.8. Formalizar os procedimentos e instruções para configuração de ativos de TI, de forma a padronizar e orientar os técnicos, bem como definir os responsáveis por sua atualização;

2.12.9. Ajustar a cultura de segurança da informação dentro do IBGE, abordando conceitos de boas práticas e a política e normas de segurança em vigor;

2.12.10. Contratação de empresa para prestação de serviços gerenciados de segurança;

2.12.11. Atuar na infraestrutura de serviços de informática do IBGE para otimização e atualização dos serviços;

2.12.12. Monitorar externa e internamente as aplicações web, servidores, virtualizadores e rede de forma proativa e reativa (com anuência do IBGE) no ambiente internet e intranet da instituição, bem como monitoramento constante de fóruns, grupos ativistas e de crackers, além de movimentações de ataques cibernéticos realizados por grupos articulados.

2.13 Metodologia utilizada para estimativa dos quantitativos:

2.13.1 A estimativa dos quantitativos apresentados neste processo foi construída com base em análise técnica fundamentada principalmente na demanda real observada no contrato anterior, cujo comportamento operacional se manteve estável ao longo do período analisado. Os volumes de consumo desse contrato, amplamente documentados em relatórios periódicos, dashboards de segurança, registros de incidentes e estatísticas operacionais elaborados pela Administração, constituem a melhor referência disponível para dimensionamento da necessidade atual.

2.13.2 A metodologia utilizada para a estimativa consistiu na consolidação dos dados históricos provenientes do ambiente de produção, especialmente aqueles relacionados ao número de alertas processados, incidentes tratados, chamados registrados nas plataformas internas da Central de Atendimento e via Correio Eletrônico quando a demanda é sigilosa, além da volumetria de eventos monitorados pelo SIEM. Esses dados foram obtidos diretamente dos documentos já existentes no IBGE, tais como relatórios mensais de operação, registros de desempenho e evidências extraídas das ferramentas corporativas, os quais refletem com precisão o comportamento da demanda típica do serviço dos itens a serem adquiridos.

2.13.3 Para fins de conformidade com o art. 15 da IN SGD/ME nº 94/2022, esclarece-se que a estimativa apresentada considerou séries históricas consolidadas do órgão, bem como evidências documentais que registram o consumo efetivo do serviço ao longo do contrato anterior. Embora os quantitativos tenham sido apresentados de forma sintética nos artefatos, toda a fundamentação utilizada está respaldada nos documentos oficiais já existentes no IBGE, que foram expressamente considerados pela equipe técnica na formação da estimativa. Assim, a metodologia adotada incorpora dados verificados, critérios objetivamente mensuráveis e amparo documental suficiente para atender às exigências normativas aplicáveis.

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

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

3.2. A solução de TIC consiste em serviço técnico especializado em gerenciamento de segurança da informação (MSS - Managed Security Services), que deve ser provido através de **Centro de Operações de Segurança (Security Operation Center – SOC) remoto 24x7**. Fazem parte deste serviço a gestão e varredura de vulnerabilidades, teste de invasão, monitoração da marca, análise e monitoração de incidentes, prevenção e resposta a incidentes e análise de causa raiz, conforme descrito neste Termo de Referência.

3.3. Além da operação e suporte das ferramentas entregues como objeto deste contrato, a CONTRATADA deverá atuar nas soluções de segurança da informação da CONTRATANTE, fazendo recomendações das melhores práticas de segurança, provenientes de análises globais e melhorias na proteção do ambiente.

3.4 Bens e serviços que compõem a solução:

GRUPO	ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	Unidade de Medida	Qtd
1	1	Gestão de Riscos - Processo integrado envolvendo a Gestão de Vulnerabilidades, Gestão de Riscos, Compliance e Monitoração de Marca CATSER: 27014	Unidade (mês)	24
	2	Gestão de Incidentes - Processo integrado envolvendo a Análise de Incidentes Globais e o Monitoramento de Incidentes CATSER: 27014	Unidade (mês)	24
	3	Resposta aos Incidentes - Processo integrado envolvendo a prevenção, bloqueio e resposta aos incidentes, bem como a análise de sua causa raiz CATSER: 27014	Unidade (mês)	24

3. 5. Cabe ressaltar que o valor unitário máximo deverá ser equivalente a um mês de prestação de serviço.

3.6 Classificação dos serviços:

3.6.1 Trata-se de serviço comum de caráter continuado sem fornecimento de mão de obra em regime de dedicação exclusiva, a ser contratado mediante licitação, na modalidade pregão, em sua forma eletrônica. Os serviços pleiteados serão prestados de forma contínua, pois, pela sua essencialidade, visam atender à necessidade pública de forma permanente e contínua, por mais de um exercício financeiro, assegurando a integridade do patrimônio público e o funcionamento das atividades finalísticas do IBGE, de modo que sua interrupção compromete a prestação do serviço público e o cumprimento da missão institucional

3.6.2 Os serviços a serem contratados enquadram-se nos pressupostos do Decreto nº 9.507, de 21 de setembro de 2018, não se constituindo em quaisquer das atividades previstas no art. 3º do aludido decreto, cuja execução indireta é vedada.

3.6.3 A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração Contratante, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta

3.6.4 O serviço de SOC (Security Operations Center) é caracterizado como um serviço de monitoramento e gestão de segurança cibernética, que envolve operação contínua de infraestrutura de segurança, análise de eventos e resposta a incidentes. Esse tipo de serviço se enquadra como operação de infraestrutura de TIC com foco em segurança.

3.6.5 Trata-se de uma única Solução de TIC, qual seja, o serviço gerenciado de segurança da informação, sendo um único grupo, composto por três itens, com pagamentos fixos mensais.

3.6.6 De acordo com o art. 8º, § 2º, da IN SGD/ME nº 94/2022, foram respeitadas as normas específicas para contratação dos objetos descritos no Anexo I da mesma IN, enquadrando-se o escopo exclusivamente em serviços de monitoramento de segurança da informação operados de forma ininterrupta (SOC 24x7).

3.6.7 Informe-se que o presente Termo de Referência está em conformidade com o modelo de contratação de serviços de tecnologia da informação da Secretaria de Governo Digital do Ministério da Economia, e de acordo com as orientações daquele Ministério (IN-94/2022 e IN-65/2021, modelo de setembro/2025).

3.5.8 O IBGE se orientou na composição da pesquisa de preços nos termos da Instrução Normativa Seges/ME nº 65, de 2021.

3.7 Considerações gerais (descrição):

3.7.1. Modelo de atuação:

3.7.1.1 A fim de garantir a qualidade da entrega do objeto como um todo, os itens desta contratação devem possuir o seguinte modelo de atuação:

3.7.1.1.1 Tal serviço deve ser provido através de Centro de Operações de Segurança (Security Operation Center – SOC 24x7, de forma remota, atendendo ao descrito neste Termo de Referência.

3.7.1.1.2 Algumas atividades, após comum acordo com a CONTRATANTE, poderão ser realizadas mediante atendimento presencial ou virtual (exceto Pentest Físico) em uma das unidades localizadas no município do Rio de Janeiro ou São Paulo, em até 24 horas ao comunicado da CONTRATANTE:

3.7.1.1.2.1 Migração de versionamento dos equipamentos gerenciados;

3.7.1.1.2.2 Necessidade de modernização dos equipamentos gerenciados;

3.7.1.1.2.3 Incidentes massivos ou desastres;

3.7.1.1.2.4 Pentestes físicos (somente presencial);

3.7.1.1.2.5 Inacessibilidade dos equipamentos gerenciados.

3.7.1.2 Seguem os endereços das unidades RJ e SP:

Localidade	Endereço
Rio de Janeiro	Rua General Canabarro, 706, Maracanã, Rio de Janeiro - RJ. CEP 20271-205
São Paulo	Rua Urussuí, 93, ITAIM BIBI, São Paulo - SP. CEP 04542050

3.7.1.3 Além da operação e suporte das ferramentas entregues como objeto deste contrato, a CONTRATADA deverá atuar nas soluções de segurança da informação da CONTRATANTE fazendo recomendações das melhores práticas de segurança, provenientes de análises globais, e melhorias na proteção do ambiente.

3.7.1.3 Nos Anexos I-A , I-B e I-E deste Termo de Referência foram apresentados os itens que compõem o parque tecnológico do IBGE, alvos desta licitação.

3.8 Bens e serviços que compõem a Solução

3.8.1 Garantia de nível de serviço.

3.8.2 Transferência de conhecimento

3.8.3 Disponibilidade dos serviços.

3.8.4 Demais itens apresentados no Anexo I-A Especificação Técnica

4. REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio:

4.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:

4.1.1. Os serviços objeto desta contratação serão diariamente, ampla, irrestrita e rigorosamente fiscalizados por servidores do quadro do IBGE, sendo para este fim designados e denominados Gestores e Fiscais. A contratada obriga-se a prestar todos os esclarecimentos necessários que lhe forem solicitados para a devida validação de serviços executados, dentro do horário de expediente e através de seu preposto, se for o caso;;

4.1.2. Os serviços deverão ser executados sem impacto na utilização do ambiente de TI do IBGE;

4.1.3. Os serviços deverão obedecer aos Níveis Mínimos de Serviço definidos no item 7.4 deste Termo de Referência.

4.1.4 Os serviços devem ser realizados em alinhamento com as arquiteturas tecnológicas da Contratante e nos sistemas já implantados no ambiente do IBGE.

Requisitos de Capacitação

4.2. Não faz parte do escopo da contratação a realização de capacitação técnica na utilização dos recursos relacionados ao objeto da presente contratação;

4.3. A contratada deverá disponibilizar documentação técnica completa e atualizada, incluindo manuais de operação, guias de configuração e procedimentos de suporte.

Requisitos Legais

4.4. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133, de 2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

Requisitos de Manutenção

4.5. Devido às características da solução, há necessidade de realização de manutenções (**corretivas/preventivas/adaptativa/evolutiva**) pela Contratada, visando à manutenção da disponibilidade da solução e ao aperfeiçoamento de suas funcionalidades;

Requisitos Temporais

4.6. Os serviços devem ser prestados no prazo máximo de **30 (trinta)** dias corridos a contar do recebimento da abertura da Ordem de Serviço (OS), emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante;

4.7. 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.

4.8. 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.

4.9. Na execução dos serviços, deverão ser observados os seguintes prazos:

Atividade, Tarefa ou Serviço	Prazo máximo de início de atendimento	Prazo máximo de solução de problema
Monitoramento contínuo (24x7)	Imediato (serviço ativo)	Não se aplica
Detecção de incidente	Imediato após ocorrência	Não se aplica
Classificação e registro do incidente	Até 1 (uma) horas após detecção	Não se aplica
Resposta inicial ao incidente crítico	Até 1 (uma) após registro	Até 4 (quatro) horas após registro
Resposta a incidente de média gravidade	Até 2 (duas) horas após registro	Até 8 (oito) horas após registro
Resposta a incidente de baixa gravidade	Até 4 (quatro) horas após registro	Até 24 (vinte e quatro) horas após registro

4.9.1. Em casos excepcionais, quando a solução demandar ações externas ou dependências de terceiros, os prazos poderão ser ajustados mediante justificativa técnica e autorização da Contratante.

Requisitos de Segurança e Privacidade

4.10. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação do Contratante, do IBGE (POSIC) de modo a atuar em concordância com as práticas da Instituição. A POSIC é um documento público que pode ser consultado em https://www.ibge.gov.br/np_download/novoportal/documentos_institucionais/Politica_de_Seguranca_da_Informacao_e_Comunicacoes_2023.pdf.

4.10.1. Não será permitida a retirada de qualquer informação ou documento relativo à base de dados de conhecimento existente no IBGE, sob pena de ser considerada quebra de sigilo, com as consequências previstas neste Termo de Referência, no Edital e no Contrato.

4.10.2. A CONTRATADA responderá por qualquer demanda em relação aos direitos patrimoniais dos seus empregados, não havendo qualquer responsabilidade da contratante e, no caso eventual de imputação de responsabilidade ao IBGE, na via judicial, a CONTRATADA arcará com o pagamento dos valores.

4.10.3. A Contratada deverá assinar TERMO DE COMPROMISSO DE MANUTENÇÃO DO SIGILO e o TERMO DE CIÊNCIA para a prestação dos serviços, conforme modelos nos Anexos I-C e I-D.

4.10.4. Promover o afastamento, no prazo máximo de 24 (vinte e quatro) horas após o recebimento da notificação, de qualquer dos seus funcionários que não correspondam aos critérios de confiança ou que perturbe a ação da equipe de fiscalização do CONTRATANTE.

4.10.5. Todas as informações coletadas durante a execução desse contrato, somente poderão ser divulgadas à terceiros após a aprovação formal do IBGE.

4.10.6. Todos os participantes deste contrato só podem iniciar o trabalho no IBGE com o termo de sigilo do IBGE assinado.

Requisitos Sociais, Ambientais e Culturais

4.11. Os serviços devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

4.11.1. É recomendado que a empresa contratada siga e pratique as diretrizes sobre Responsabilidade Social apresentadas na ABNT-ISO 26000. A CONTRATADA deve adotar posturas, comportamentos e ações que promovam o bem-estar de seus públicos interno e externo, de forma a atestar sua boa prática empresarial:

Requisitos da Arquitetura Tecnológica

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

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

Requisitos de Projeto e de Implementação

4.14. Os serviços deverão observar integralmente os requisitos de projeto e de implementação descritos a seguir:

4.14.1. Arquitetura e Escopo do Serviço

O projeto deverá contemplar uma arquitetura escalável, segura e de alta disponibilidade, capaz de monitorar, detectar, analisar e responder a incidentes de segurança em tempo real, abrangendo todos os ativos de TI definidos no escopo contratual.

4.14.2. Integração com Ambientes Existentes

A solução deverá ser compatível e integrável com os sistemas, ferramentas e infraestrutura já existentes na organização, incluindo, mas não se limitando a, firewalls, WAFs, antivírus, SIEMs, sistemas operacionais e aplicações críticas.

4.14.3 Monitoramento Contínuo (24x7x365)

O SOC deverá operar em regime ininterrupto, com monitoramento contínuo de eventos de segurança, geração de alertas e resposta a incidentes, conforme níveis de criticidade previamente definidos.

4.14.4. Procedimentos de Resposta a Incidentes

Deverão ser definidos e implementados procedimentos formais de resposta a incidentes, com base em boas práticas de mercado (ex.: NIST, ISO/IEC 27035), incluindo comunicação, contenção, erradicação, recuperação e lições aprendidas.

4.14.5. Relatórios e Indicadores de Desempenho

A contratada deverá fornecer relatórios periódicos contendo indicadores de desempenho (KPIs), métricas de segurança, eventos relevantes e recomendações de melhoria contínua.

4.14.6. Confidencialidade e Conformidade Legal

Todos os serviços deverão observar rigorosamente os requisitos legais e normativos aplicáveis, incluindo a LGPD, garantindo a confidencialidade, integridade e disponibilidade das informações tratadas.

Requisitos de Implantação

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

4.15.1. Os serviços estão detalhados no Anexo I-A deste Termo de Referência. Seguem informações importantes para o dimensionamento onde a demanda do órgão tem como base as seguintes características:

4.15.1.1 Modelo de atuação:

4.15.1.1.1 O serviço deve ser provido através de Centro de Operações de Segurança (Security Operation Center – SOC) remoto 24x7;

4.15.1.1.2 Algumas atividades, após comum acordo com a CONTRATANTE, poderão ser realizadas mediante atendimento presencial ou virtual (exceto Pentest Físico) em uma das unidades localizadas no município do Rio de Janeiro ou São Paulo, em até 24 horas ao comunicado da CONTRATANTE:

4.15.1.1.2.1 Migração de versionamento dos equipamentos gerenciados;

4.15.1.1.2.2 Necessidade de modernização dos equipamentos gerenciados;

4.15.1.1.2.3 Incidentes massivos ou desastres;

4.15.1.1.2.4 Pentestes físicos (somente presencial);

4.15.1.1.2.5 Inaccessibilidade dos equipamentos gerenciados.

4.15.2 Além da operação e suporte das ferramentas entregues como objeto deste contrato, a CONTRATADA deverá atuar nas soluções de segurança da informação da CONTRATANTE fazendo recomendações das melhores práticas de segurança, provenientes de análises globais, e melhorias na proteção do ambiente. Visão do parque institucional do IBGE disponível em:

https://www.ibge.gov.br/np_download/novoportal/documentos_institucionais/PDTI_2023_2024.pdf.

4.15.3 A contratada deverá levar em consideração:

4.15.3.1 Entrega das ferramentas conforme indicado no Anexo I-A deste Termo de Referência, bem como a gerência dos serviços, entrega de relatórios, canais de comunicação, a forma de prestação do serviço e demais especificações deste Termo de Referência e seus anexos.

4.15.4 Descrição do ambiente de TIC do IBGE:

4.15.4.1 Nos Anexos I-A, I-B e I-E deste Termo de Referência foram apresentados os itens que compõem o parque tecnológico do IBGE, atinentes a esta contratação.

4.15.4.2 A descrição completa do parque tecnológico da Instituição pode ser consultada no documento público "Plano Diretor de Tecnologia da Informação e Comunicação – PDTI, disponível em https://www.ibge.gov.br/np_download/novoportal/documentos_institucionais/PDTI_2023_2024.pdf.

4.15.5 Sistemas Computacionais:

4.15.5.1. Os recursos em tecnologia da informação utilizados no IBGE compreendem computadores com diferentes capacidades de processamento e armazenamento, desde desktops e notebooks de uso geral a supercomputadores e estações servidoras com configuração específica para atender requisitos de missões e operações científicas de alto nível de complexidade. De maneira geral:

4.15.5.1.1 O parque computacional do IBGE é heterogêneo, dadas as compras de diferentes padrões de equipamentos ao longo dos anos;

4.15.5.1.2 O parque computacional é distribuído geograficamente nas diversas unidades do IBGE, tendo o seu DataCenter central no Rio de Janeiro e o secundário em São Paulo;

4.15.5.1.3 Confidencialidade, integridade e autenticidade dos dados armazenados e processados no ambiente computacional do IBGE são de importância fundamental para a missão do Instituto, sendo assim é necessária a implementação gradual dos controles preconizados pelas normas da família ISO/IEC NBR 27000;

4.15.5.1.4 O plano para renovação anual de parte do parque computacional do IBGE, conforme previsto no PDTI, objetiva a padronização deste parque a partir de 5 anos;

4.15.5.1.5 A definição das especificações padronizadas de equipamentos é aplicável a todas as unidades do IBGE e as aquisições estão centralizadas no CTIC (Comitê de Tecnologia da Informação e Comunicações do IBGE);

4.15.5.1.6 O IBGE dispõe de sistemas computacionais de uso específico para atendimento das missões específicas das áreas fim do instituto;

4.15.5.1.7 Grupos específicos de especialistas são mantidos para suporte em supercomputadores utilizados em área-fim;

4.15.5.1.8 Detalhes e a descrição básica do parque computacional instalado serão obtidas por ocasião da vistoria virtual, que pode ser agendada pelos e-mails licitacoes@ibge.gov.br e aquisicoestic@ibge.gov.br.

Requisitos de Garantia e Manutenção

4.17. O prazo de garantia contratual dos serviços, complementar à garantia legal, será equivalente à vigência do contrato, ou seja, será de, no mínimo, 24 (vinte e quatro) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

Requisitos de Experiência Profissional

4.18. Os serviços Gerenciados de Segurança da Informação, conforme descritos neste documento, deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços;

Requisitos de Formação da Equipe

4.21. Os serviços deverão ser prestados por técnicos devidamente capacitados, de acordo com os critérios estabelecidos a seguir:

4.21.1. A fim de garantir a prestação do serviço em conformidade com o framework ITIL, a CONTRATADA deve possuir ao menos um profissional com a certificação ITIL Foundation;

4.21.2 A fim de garantir o conhecimento generalista em Segurança da Informação, a CONTRATADA deve possuir ao menos um profissional com a certificação CISSP ou CISM;

4.21.3 A fim de garantir o conhecimento técnico em Segurança da Informação, a CONTRATADA deve possuir ao menos um profissional com a certificação Security+;

4.21.4 A fim de garantir a existência de profissional com experiência de hacker ético, fundamental em momentos de crise de segurança, a CONTRATADA deve possuir ao menos um profissional com a certificação CEH, OSCP ou equivalente.

4.21.5 A empresa contratada deverá possuir certificação ISO/IEC 27001 durante toda a vigência do contrato, emitida em nome da CONTRATADA por organização independente acreditada por autoridade globalmente reconhecida.

4.21.6 A CONTRATADA deverá apresentar, em até 5 dias antes da assinatura do contrato, a comprovação da exigência de certificação listadas do itens 4.21.1 a 4.21.6.

Requisitos de Metodologia de Trabalho

4.24. A execução dos serviços está condicionada ao recebimento pelo Contratado de Ordem de Serviço (OS) emitida pela Contratante.

4.25. A OS indicará o serviço, a quantidade e a localidade na qual os deverão ser prestados.

4.26. O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana de maneira eletrônica (portal, e-mail, sistema de chamados) e 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana por via telefônica.

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

Requisitos de Segurança da Informação e Privacidade

4.29. O Contratado deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

4.30. A solução deverá:

4.30.1 Atender aos princípios e procedimentos elencados na Política de Segurança da Informação do Contratante;

4.30.1 A Contratada deve tomar conhecimento da Política de Segurança da Informação e Comunicações no IBGE (POSIC) de modo a atuar em concordância com as práticas da Instituição. A POSIC é um documento público que pode ser consultado em https://www.ibge.gov.br/np_download/novoportal/documentos_institucionais/Politica_de_Seguranca_da_Informacao_e_Comunicacoes_2023.pdf.

4.30.2 Não será permitida a retirada de qualquer informação ou documento relativo a base de dados de conhecimento existente no IBGE, sob pena de ser considerada quebra de sigilo, com as consequências previstas neste Termo de Referência, no Edital e no Contrato;

4.30.3 A CONTRATADA responderá por qualquer demanda em relação aos direitos patrimoniais dos seus empregados, não havendo qualquer responsabilidade da contratante e, no caso eventual de imputação de responsabilidade ao IBGE, na via judicial, a CONTRATADA arcará com o pagamento dos valores.

4.30.4 A Contratada deverá assinar Termo de Compromisso e de Ciência para a prestação dos serviços, conforme modelos nos Anexos I-B e I-C.

4.30.5 Promover o afastamento, no prazo máximo de 24 (vinte e quatro) horas após o recebimento da notificação, de qualquer dos seus funcionários que não correspondam aos critérios de confiança ou que perturbe a ação da equipe de fiscalização do CONTRATANTE.

4.30.6 A CONTRATADA comprometer-se-á a preservar os dados da CONTRATANTE contra acessos indevidos e abster-se-á de replicar ou realizar cópias de segurança (backups) destes dados fora de ambientes de computação em nuvem, devendo informar imediatamente e formalmente à CONTRATANTE qualquer tentativa, inclusive por meios judiciais, de acesso por parte de outra nação a estes dados.

4.30.7 É vedado o tratamento em ambiente de nuvem de informações não autorizadas pela CONTRATANTE.

4.30.8 É vedado acesso aos dados hospedados na infraestrutura de nuvem à CONTRATADA ou ao provedor, sem prévia e formal autorização por parte da CONTRATANTE. Salvo nas necessidades da contratante para execução dos serviços e processo de prestação de contas e faturamento.

4.30.9 É vedado o uso de informações do CONTRATANTE pelo provedor de serviço de nuvem para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não autorizado.

4.30.10 Deverá ser atendida a Instrução Normativa GSI/PR nº 05/2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.

4.30.11 A política de segurança da informação do provedor de serviço de nuvem deverá estar em conformidade com a legislação brasileira.

Vistoria

4.31. Não há necessidade de realização de avaliação prévia do local de execução dos serviços.

Sustentabilidade

4.40. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

4.40.1. A empresa deverá estar em conformidade com a Instrução Normativa nº 01, de 19 de janeiro de 2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional, aplicando, no que couber, as disposições do Art. 6º aos serviços objeto deste documento;

Indicação de marcas ou modelos

4.41 A presente contratação não exige a indicação de marcas ou modelos específicos, conforme previsto no Art. 41, inciso I, da Lei nº 14.133/2021. Entretanto, a descrição técnica detalhada do objeto, bem como os anexos que apresentam o parque computacional existente, já estabelecem de forma clara e objetiva que:

4.41.1 As condições de funcionamento esperadas pela Administração;

4.41.2 Os requisitos mínimos de desempenho, compatibilidade e integração com o ambiente tecnológico atual;

4.42 As características técnicas essenciais para garantir a plena execução do objeto contratado.

Da vedação de utilização de marca/produto na execução do serviço

4.43 Não se aplica para esta contratação.

Da exigência de carta de solidariedade

4.44 Não será exigida carta de solidariedade.

Subcontratação

4.45. É permitida a subcontratação parcial do objeto, até o limite de **30%** (trinta por cento) do valor total do contrato, nas seguintes condições:

4.46. É vedada a subcontratação completa ou da parcela principal da obrigação, abaixo discriminada:

4.46.1. Monitoramento contínuo (24x7) do ambiente;

4.46.2. Detecção e análise de incidentes de segurança; e

4.46.3. Resposta a incidentes críticos e gestão de vulnerabilidades.

4.47. Poderão ser subcontratadas as seguintes parcelas do objeto:

4.47.1. Serviços de suporte técnico especializado para tecnologias específicas (ex.: gestão de vulnerabilidades, monitoramento de marca, SIEM);

4.47.2. Serviços de atualização de ferramentas ou integração com sistemas legados; e

4.47.3. Serviços de infraestrutura em nuvem ou datacenter certificado para hospedagem segura.

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

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

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

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

Da exigência de amostra

4.52 Não se aplica para esta contratação.

Garantia da contratação

4.53. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, com validade durante a execução do contrato e 90 (noventa) dias após término da vigência contratual, podendo o Contratado optar pela caução em dinheiro ou em títulos da dívida pública, seguro-garantia, fiança bancária ou título de capitalização, em valor correspondente a **5% (cinco por cento)** do valor anual da contratação.

4.54. Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.

4.54.1. A apólice de seguro-garantia permanecerá em vigor mesmo que o Contratado não pague o prêmio nas datas convencionadas.

4.54.2. Caso o adjudicatário não apresente a apólice de seguro de garantia antes da assinatura do contrato, ocorrerá a preclusão do direito de escolha dessa modalidade de garantia.

4.54.3. A apólice de seguro-garantia deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.

4.54.4. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvados os períodos de suspensão contratual.

4.54.5. Caso o adjudicatário não opte pelo seguro-garantia ou não apresente a apólice de seguro de garantia antes da assinatura do contrato, deverá apresentar, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contado da assinatura do contrato, comprovante de prestação de garantia nas modalidades de caução em dinheiro ou títulos da dívida pública, fiança bancária ou títulos de capitalização.

4.55. Caso seja a garantia em dinheiro a modalidade de garantia escolhida pelo Contratado, deverá ser efetuada em favor do Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

4.56. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério competente.

4.57. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

4.58. Na hipótese de opção pelo título de capitalização, a garantia deverá ser custeada por pagamento único, com resgate pelo valor total, sob a modalidade de instrumento de garantia, emitido por sociedades de capitalização regulamente constituídas e autorizadas pelo Governo Federal.

4.58.1. O título de capitalização deverá ser apresentado ao Contratante juntamente com as condições gerais e o número do processo administrativo sob o qual o plano de capitalização foi aprovado pela Susep (art. 8º, III, da Circular SUSEP nº 656, de 11 de março de 2022).

4.59. A garantia assegurará, qualquer que seja a modalidade escolhida, sob pena de não aceitação, o pagamento de:

4.59.1. prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

4.59.2. multas moratórias e punitivas aplicadas pela Administração à contratada; e

4.59.3. obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo Contratado.

4.60. Em caso de seguro-garantia, a apólice deverá ter cobertura para pagamento direto ao empregado após decisão definitiva em processo administrativo que apure montante líquido e certo a ele devido em razão de inadimplência do Contratado, independentemente de trânsito em julgado de decisão judicial.

4.61. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, contado da data de assinatura do termo aditivo ou da emissão do apostilamento, seguindo os mesmos parâmetros utilizados quando da contratação.

4.62. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o Contratado ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

4.63. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o Contratado obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contados da data em que for notificada.

4.64. O Contratante executará a garantia na forma prevista na legislação que rege a matéria.

4.64.1. O emitente da garantia ofertada pelo Contratado deverá ser notificado pelo Contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

4.64.2. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep nº 662, de 11 de abril de 2022.

4.65. Extinguir-se-á a garantia com a restituição da carta fiança, autorização para a liberação de importâncias depositadas em dinheiro a título de garantia ou anuência ao resgate do título de capitalização, acompanhada de declaração do Contratante, mediante termo circunstanciado, de que o Contratado cumpriu todas as cláusulas do contrato.

4.65.1. A extinção da garantia na modalidade seguro-garantia observará a regulamentação da Susep.

4.65.2. A Administração deverá apurar se há alguma pendência contratual antes do término da vigência da apólice.

4.66. A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

4.67. O Contratado autoriza o Contratante a reter, a qualquer tempo, a garantia, na forma prevista neste Termo de Referência.

4.68. O garantidor não é parte para figurar em processo administrativo instaurado pelo Contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

4.69. A garantia de execução é independente de eventual garantia do produto ou serviço prevista neste Termo de Referência.

Instalação de escritório

4.70 Não se aplica a esta contratação.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

- 5.1.1. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;
- 5.1.2. encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;
- 5.1.3. receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
- 5.1.4. aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;
- 5.1.5. liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;
- 5.1.6. comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;
- 5.1.7. definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do contratado, com base em pesquisas de mercado, quando aplicável;
- 5.1.8. prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

5.2. São obrigações do CONTRATADO:

- 5.2.1. indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;
- 5.2.2. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;
- 5.2.3. reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;
- 5.2.4. propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;
- 5.2.5. manter, durante toda a execução do contrato, as mesmas condições da habilitação;
- 5.2.6. quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;
- 5.2.7. quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;
- 5.2.8. ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

5.2.9. fazer a transição contratual, quando for o caso.

5.3. São obrigações do órgão gerenciador do registro de preços:

5.3.1. efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;

5.3.2. conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

5.3.3. definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

5.3.4. as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e

5.3.5. definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;

5.3.6. definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

5.3.7. a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;

5.3.8. as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pelo contratado; e

5.3.9. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no inciso III, alínea "c", item 2 do art. 17 da Instrução Normativa SGS/ME nº 94, de 2022, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

6. MODELO DE EXECUÇÃO DO OBJETO

6.1. A execução do objeto seguirá a seguinte dinâmica:

6.1.1. Início da execução do objeto: a partir da data da assinatura do contrato;

6.1.2. Descrição detalhada dos métodos, rotinas, etapas, tecnologias procedimentos, frequência e periodicidade de execução do trabalho:

6.1.2.1 A fim de garantir a qualidade da entrega do objeto como um todo, os itens desta contratação devem possuir o seguinte modelo de atuação:

6.1.2.2 O serviço deve ser provido através de Centro de Operações de Segurança (Security Operation Center – SOC 24x7, de forma remota, atendendo ao descrito neste Termo de Referência.

6.1.2.3 Algumas atividades, após comum acordo com a CONTRATANTE, poderão ser realizadas mediante atendimento presencial ou virtual (exceto Pentest Físico) em uma das unidades localizadas no município do Rio de Janeiro ou São Paulo, em até 24 horas ao comunicado da CONTRATANTE:

6.1.2.3.1 Migração de versionamento dos equipamentos gerenciados;

6.1.2.3.2 Necessidade de modernização dos equipamentos gerenciados;

6.1.2.3.3 Incidentes massivos ou desastres;

6.1.2.3.4 Pentestes físicos (somente presencial);

6.1.2.3.5 Inacessibilidade dos equipamentos gerenciados.

6.1.3. O endereço das unidades do RJ e SP podem ser encontradas no item 3.7.1.2 deste documento.

6.1.4. Além da operação e suporte das ferramentas entregues como objeto deste contrato, a CONTRATADA deverá atuar nas soluções de segurança da informação da CONTRATANTE fazendo recomendações das melhores práticas de segurança, provenientes de análises globais, e melhorias na proteção do ambiente. Visão do parque institucional do IBGE disponível em:

https://www.ibge.gov.br/np_download/novoportal/documentos_institucionais/PDTI_2023_2024.pdf .

6.1.3. O cronograma deverá contemplar todas as fases da contratação, conforme abaixo:

6.1.4. Etapas e Períodos:

Etapas	Período / Condição
1. Planejamento e Kick-off	Até 10 dias após assinatura do contrato
2. Levantamento e análise inicial	Até 20 dias após o Kick-off
3. Implantação da solução SOC	Até 45 dias após conclusão da análise inicial
4. Testes e validação operacional	Até 15 dias após implantação
5. Início da operação assistida	Até 10 dias após validação
6. Entrega da documentação final	Até 5 dias após término da operação assistida

6.2. Os serviços serão prestados no seguinte endereço: O endereço das unidades do RJ e SP podem ser encontrados no item 3.7.1.2 deste documento.

6.3. Os serviços serão prestados no seguinte horário: Os serviços serão prestados em regime contínuo, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, incluindo feriados nacionais, garantindo monitoramento e resposta a incidentes em tempo real.

Rotinas a serem cumpridas

6.3.1. A execução contratual observará as rotinas

6.3.1.1 **Monitoramento contínuo** – Diária (24x7)

6.3.1.2 **Análise e correlação de alertas** – Diária

6.3.1.3 **Resposta a incidentes** – Sempre que ocorrer incidente

6.3.1.4 **Gestão de vulnerabilidades** – Semanal

6.3.1.5 **Geração de relatórios** – Semanal e Mensal

6.3.1.6 **Reuniões de alinhamento** – Semanais e Mensais

Materiais a serem disponibilizados

6.4. Para a perfeita execução dos serviços, o Contratado deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas neste documento e qualidades a seguir estabelecidas, promovendo sua substituição quando necessário e garantindo conformidade com normas de segurança da informação e a Lei Geral de Proteção de Dados (LGPD):

6.4.1. **Equipamentos e infraestrutura tecnológica:**

6.4.1.1 Recursos em nuvem para operação do SOC;

6.4.1.2 Sistema SIEM (Security Information and Event Management) licenciado e atualizado;

6.4.1.3 Ferramentas para análise de logs, correlação de eventos e gestão de incidentes;

6.4.1.4 Solução para monitoramento de vulnerabilidades e ativos licenciado e atualizado;

6.4.1.5 Solução para acompanhamento de riscos licenciado e atualizado;

6.4.1.6 Solução para monitoramento de marca licenciado e atualizado.

6.4.2. **Materiais de apoio e documentação:**

6.4.2.1 Manuais técnicos e guias de operação atualizados;

6.4.2.2 Documentação dos procedimentos de resposta a incidentes;

6.4.2.3 Relatórios periódicos (semanal e mensal) em formato digital; e

6.4.3. **Softwares e recursos de segurança:**

6.4.3.1 Licenças válidas para todos os componentes da solução;

6.4.3.2 Ferramentas de inteligência contra ameaças (Threat Intelligence) integradas;

6.4.3.3 Painéis de visualização e relatórios automatizados.

Formas de transferência de conhecimento

6.6. A transferência do conhecimento deverá ser realizada observando-se o que segue:

6.6.1. Documentação técnica completa:

6.6.1.1 A Contratada deverá entregar manuais, guias de operação, procedimentos de resposta a incidentes e relatórios de configuração, em formato digital, atualizados e compatíveis com as práticas de segurança da informação.

6.6.2. Sessões de treinamento e capacitação:

6.6.2.1 Deverão ser realizadas sessões presenciais ou remotas para a equipe designada pela Administração, com carga horária mínima de 16 horas, abordando operação da solução, análise de alertas, geração de relatórios e boas práticas de segurança.; e

6.6.3. Transferência prática e acompanhamento

6.6.3.1 Durante a fase de operação assistida, a Contratada deverá garantir acompanhamento técnico e orientação prática, permitindo que a equipe interna adquira autonomia na utilização dos recursos contratados.

Procedimentos de transição e finalização do contrato

6.8. Os procedimentos de transição e finalização do contrato constituem-se das seguintes etapas:

6.8.1. Entrega da documentação final:

6.8.1.1 A Contratada deverá entregar toda a documentação técnica atualizada, incluindo relatórios finais, inventário de ativos monitorados, configurações aplicadas e histórico de incidentes.

6.8.2. Transferência de conhecimento e credenciais:

6.8.2.1 Deverá ocorrer a transferência segura de credenciais, chaves de acesso, scripts e demais artefatos necessários para continuidade das operações pela Administração ou nova contratada.

6.8.3. Apoio à transição:

6.8.3.1 A Contratada deverá prestar suporte técnico por um período mínimo de 30 dias após o término do contrato, para garantir a migração segura e sem interrupções, incluindo reuniões de alinhamento e esclarecimento de dúvidas.

Quantidade mínima de serviços para comparação e controle

6.10. Cada OS conterá o volume de serviços demandados, incluindo a sua localização e o prazo, conforme modelo descrito no [Anexo I-G].

Mecanismos formais de comunicação

6.11. São definidos como mecanismos formais de comunicação, entre a Contratante e o Contratado, os seguintes:

- I) Ordem de Serviço;
- II) Ata de Reunião;
- III) Ofício;
- IV) Sistema de abertura de chamados;
- V) E-mails e Cartas;
- VI) Relatórios periódicos.

Manutenção de Sigilo e Normas de Segurança

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

6.13. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se nos ANEXOS I-C e I-D.

7. MODELO DE GESTÃO DO CONTRATO

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

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

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

7.4. O órgão ou entidade poderá convocar o preposto da empresa para adoção de providências que devam ser cumpridas de imediato.

Preposto

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

7.6. O Contratado não necessitará manter preposto da empresa no local da execução do objeto durante o período descrito neste Termo de Referência.

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

Reunião Inicial

7.8. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

7.9. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 5 (dias) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

7.10. A pauta desta reunião observará, pelo menos:

7.10.1. Presença do representante legal da contratada, que apresentará o seu preposto;

7.10.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

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

7.10.4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

Rotinas de Fiscalização

7.11. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

Fiscalização Técnica

7.12. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

7.13. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

7.14. Identificada qualquer inexistência ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

7.15. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

7.16. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato.

7.17. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual.

7.18. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade do Contratado, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade do Contratante ou de seus agentes, gestores e fiscais, de conformidade.

Fiscalização Administrativa

7.20. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

7.21. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

Gestor do Contrato

- 7.22. Cabe ao gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022:
- 7.22.1.. coordenar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.
 - 7.22.2. acompanhar os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.
 - 7.22.3. acompanhar a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotar os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.
 - 7.22.4. emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.
 - 7.22.5. tomar providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.
 - 7.22.6. elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.
 - 7.22.7. enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, com a indicação expressa de que o valor da Nota Fiscal emitida pela contratada confere com o valor dimensionado pela fiscalização e gestão no recebimento definitivo do serviço.
 - 7.22.8. receber e dar encaminhamento imediato:
 - 7.22.8.1. às denúncias de discriminação, violência e assédio no ambiente de trabalho, conforme o art. 2º, inciso III, do Decreto n.º 12.174/2024;
 - 7.22.8.2. à notificação formal de que a empresa contratada está descumprindo suas obrigações trabalhistas, enviada pelo trabalhador, sindicato, Ministério do Trabalho, Ministério Público, Defensoria Pública ou por qualquer outro meio idôneo.

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

- 8.1. A avaliação da execução do objeto utilizará o [Instrumento de Medição de Resultado (IMR)], conforme o disposto nesta seção.
- 8.1.1. NÍVEIS MÍNIMOS DE SERVIÇO
- 8.1.1.1. Classificação da criticidade dos serviços e percentual de glosa no caso de não atendimento dos prazos indicados a seguir:

Criticidade	Prazos
-------------	--------

Baixa	Início de atendimento em até 08 (oito) horas
Média	Início de atendimento em até 04 (quatro) horas
Alta	Início de atendimento em até 01 (uma) hora

8.1.1.2. A descrição das atividades e suas respectivas criticidades estão indicadas no anexo I-A deste Termo de Referência (Especificação Técnica).

Criticidade Descrição do impacto		Percentual de desconto na fatura mensal
Baixa	Baixo risco - incidentes de baixo impacto no funcionamento das atividades principais do IBGE. Têm impactos apenas localizados.	5% do valor mensal do item
Média	Médio risco - incidentes referentes a problemas que afetam atividades críticas para o usuário do IBGE, sem causar interrupção do serviço, mas afetando significativamente seu desempenho.	10% do valor mensal do item
Alta	Alto risco - o incidente tem consequências sérias para transações de negócio do IBGE ou impede que as tarefas críticas sejam realizadas para todo o IBGE	20% do valor mensal do item

8.1.1.3. Se em um determinado mês ocorrer a possibilidade de aplicação de desconto por mais de um nível mínimo de serviço não atendido, será aplicado o critério de maior desconto, por item.

8.1.1.4. O Total de descontos não poderá extrapolar 30% da fatura global.

8.1.1.5. Os descontos serão efetuados quando da emissão da fatura do respectivo pedido.

8.1.1.6. O IBGE comunicará formalmente a CONTRATADA, via e-mail, o percentual de NMS a ser aplicado.

8.1.1.7. Os atrasos de qualquer natureza deverão ser justificados formalmente ao CONTRATANTE.

8.1.1.8. Os Acordos de Níveis de Serviços – SLA (ou NMS) poderão ser aplicados cumulativamente por item do objeto, obedecendo ao critério de aplicação de maior desconto, conforme indicado no item 8.1.1.3 acima.

8.1.2. RELATÓRIO TÉCNICO MENSAL DE ATIVIDADES

8.1.2.1. Visando sempre a transparência e o acompanhamento dos serviços executados, a medição dos serviços prestados se dará através do aceite a Contratada nos relatórios gerenciais mensais entregues pela contratada, conforme serviços previstos pelo Termo de Referência.

8.1.2.2. PAGAMENTO E PROCEDIMENTOS PRA RETENÇÃO E GLOSA:

8.1.2.3. Descontos pela Reincidência de descumprimento dos níveis de serviço por serviços não entregues, são calculados de acordo com a tabela a seguir:

Número de Glosas no mesmo indicador	Percentual de desconto a ser aplicado no valor mensal apurado relativo a complexidade reincidente pelo não atendimento do indicador da mesma, por meses consecutivos ou não
Até 2	0%

3	1%
4	2%
5	3%
6	4%
7	6%
8	8%
9 ou mais	10%

8.1.2.4. Se em um determinado mês ocorrer a possibilidade de aplicação de desconto pela reincidência de glosa e também pelo não cumprimento do nível de serviço, serão aplicados os critérios concomitantemente

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

8.2.1. não produziu os resultados acordados,

8.2.2. deixou de executar, ou não executou com a qualidade mínima exigida as atividades contratadas; ou

8.2.3. deixou de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou os utilizou com qualidade ou quantidade inferior à demandada.

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

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

8.4.1. Disponibilidade e continuidade do serviço:

Verificação do funcionamento ininterrupto do SOC remoto 24x7, conforme os níveis de serviço (SLA) estabelecidos no contrato, incluindo tempo de resposta, tempo de resolução e cobertura de monitoramento.

8.4.2. Qualidade técnica dos serviços prestados:

Avaliação da conformidade dos serviços com os padrões técnicos exigidos, incluindo a emissão de relatórios de segurança, alertas, análises de incidentes e recomendações de mitigação, conforme previsto no plano de trabalho.

Recebimento

8.5. Os serviços serão recebidos provisoriamente, no prazo de 7 (dias) dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo.

8.6. O prazo para recebimento provisório será contado do recebimento de comunicação de cobrança oriunda do Contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

8.7. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico.

8.8. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo.

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

8.10. Para efeito de recebimento provisório, será considerado para fins de faturamento o período **mensal** (a cada mês de efetiva prestação dos serviços).

8.11. Ao final de cada período/evento de faturamento:

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

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

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

8.14. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no recebimento provisório.

8.15. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

8.16. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

8.17. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

8.18. Os serviços serão recebidos definitivamente no prazo de 10 (dias) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

8.18.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento.

8.18.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando ao Contratado, por escrito, as respectivas correções;

8.18.3. Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

8.18.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

8.18.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

8.19. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal quanto à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

8.20. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo Contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

8.21. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

Procedimentos de Teste e Inspeção

8.22 Não se aplica a esta contratação.

Liquidação

8.23. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §3º da Instrução Normativa SEGES/ME nº 77/2022.

8.24. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, nos casos de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

8.25. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

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

8.26. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante.

8.27. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133/2021.

8.28. A Administração deverá realizar consulta ao SICAF para:

- 8.28.1. verificar a manutenção das condições de habilitação exigidas;
- 8.28.2. Identificar possível razão que impeça a participação em licitação/contratação no âmbito do órgão ou entidade, tais como a proibição de contratar com a Administração ou com o Poder Público, bem como ocorrências impeditivas indiretas.

8.29. Constatando-se, junto ao SICAF, a situação de irregularidade do Contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do Contratante.

8.30. Não havendo regularização ou sendo a defesa considerada improcedente, o Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do Contratado, bem como quanto

à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

8.31. Persistindo a irregularidade, o Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao Contratado a ampla defesa.

8.32. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o Contratado não regularize sua situação junto ao SICAF.

Prazo de pagamento

8.33. O pagamento será efetuado no prazo máximo de até dez dias úteis, contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

8.34. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA de correção monetária.

Forma de pagamento

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

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

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

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

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

Reajuste

8.39. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em 04/03/2026.

8.40. Após o interregno de um ano, e independentemente de pedido do Contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo Contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

8.42. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o Contratante pagará ao Contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

8.43. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

8.44. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

8.45. 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.

8.46. O reajuste será realizado por apostilamento.

Cessão de Crédito

8.47. As cessões de crédito dependerão de prévia aprovação do Contratante.

8.47.1. A eficácia da cessão de crédito, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

8.47.2. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do Contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, nos termos do Parecer JL-01, de 18 de maio de 2020.

8.47.3. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração.

8.47.4. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do Contratado.

8.48. O disposto nesta seção não afeta as operações de crédito de que trata a Instrução Normativa SEGES/MGI nº 82, de 21 de fevereiro de 2025, as quais ficam por esta regidas.

9. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO

9.1. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela contratante, conforme a tabela descrita nos Níveis Mínimos de Serviço, item 8 deste documento.

9.2. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que p contratado:

9.2.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

9.2.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

9.3. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

a) der causa à inexecução parcial do contrato;

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

c) der causa à inexecução total do contrato;

d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

- f) praticar ato fraudulento na execução do contrato;
- g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

9.4. Serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções:

- 9.4.1. Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;
- 9.4.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave;
- 9.4.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

9.4.4. Multa:

9.4.4.1. *Moratória, para as infrações descritas no item “d”, de 0,5% (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 15 (quinze) dias.*

9.4.4.2. *Moratória de 0,07% (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia;*

9.4.4.2.1. *O atraso superior a 25 (vinte e cinco) dias para apresentação, suplementação ou reposição da garantia autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.*

9.4.4.3. *Compensatória, para as infrações descritas acima alíneas “e” a “h” de 10% (dez por cento) a 30% (trinta por cento) do valor da contratação.*

9.4.4.4. *Compensatória, para a inexecução total do contrato prevista acima na alínea “c”, de 10% (dez por cento) a 30% (trinta por cento) do valor da contratação.*

9.4.4.5. *Compensatória, para a infração descrita acima na alínea “b”, de 15% (quinze por cento) a 20% (vinte por cento) do valor da contratação.*

9.4.4.6. *Compensatória, em substituição à multa moratória para a infração descrita acima na alínea “d”, de 1% (um por cento) a 20% (vinte por cento) do valor da contratação.*

9.4.4.7. *Compensatória, para a infração descrita acima na alínea “a”, de 1% (um por cento) a 20% (vinte por cento) do valor da contratação.*

9.5. A aplicação das sanções previstas neste Termo de Referência não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.

9.6. Todas as sanções previstas neste Termo de Referência poderão ser aplicadas cumulativamente com a multa.

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

9.8. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

9.9. A multa poderá ser recolhida administrativamente no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

9.10. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

9.10.1. Para a garantia da ampla defesa e contraditório, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como os cadastrados pela empresa no SICAF.

9.10.2. Os endereços de e-mail informados na proposta comercial e/ou cadastrados no SICAF serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

9.11. Na aplicação das sanções serão considerados:

9.11.1. a natureza e a gravidade da infração cometida;

9.11.2. as peculiaridades do caso concreto;

9.11.3. as circunstâncias agravantes ou atenuantes;

9.11.4. os danos que dela provierem para o Contratante; e

9.11.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

9.12. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

9.13. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Termo de Referência ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

9.14. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal.

9.14.1. As penalidades serão obrigatoriamente registradas no SICAF.

9.15. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021.

9.16. Os débitos do Contratado para com a Administração Contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o Contratado possua com o mesmo órgão ora Contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

Forma de seleção e critério de julgamento da proposta

10.1. 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.

Regime de Execução

10.2. O regime de execução do contrato será por empreitada por preço global. Essa escolha justifica-se pela natureza do serviço de Security Operations Center (SOC remoto 24x7), que exige a disponibilidade contínua de infraestrutura e de equipe especializada, independentemente da quantidade exata de incidentes, que é imprevisível. Assim, a remuneração por parcelas fixas mensais garante previsibilidade orçamentária à Administração, transfere o risco da variação de demanda para a contratada e atrela o pagamento estritamente à qualidade do resultado e ao cumprimento dos Acordos de Nível de Serviço (IMR/SLA), e não ao volume individual de chamados.

Exigências de habilitação

10.3. Para fins de habilitação, deverá o interessado comprovar os seguintes requisitos:

Habilitação jurídica

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

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

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

10.7. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

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

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

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

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

10.12. Consórcio de empresas: contrato de consórcio devidamente arquivado no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis (art. 279 da Lei nº 6.404, de 15 de dezembro de 1976) ou compromisso público ou particular de constituição, subscrito pelos consorciados, com a indicação da empresa líder, responsável por sua representação perante a Administração (art. 15, caput, I e II, da Lei nº 14.133, de 2021).

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

Habilitação fiscal, social e trabalhista

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

- 10.15. 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.
- 10.16. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);
- 10.17. 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;
- 10.18. Prova de inscrição no cadastro de contribuintes Distrital ou Municipal relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
- 10.19. Prova de regularidade com a Fazenda Distrital ou Municipal do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;
- 10.20. Caso o fornecedor seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.
- 10.21. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

- 10.22. certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do interessado, caso se trate de pessoa física, desde que admitida a sua participação na licitação/contratação, ou de sociedade simples;
- 10.23. certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;
- 10.24. balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis já exigíveis e apresentados na forma da lei, comprovando, índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um), obtidos por meio da 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

10.25. Caso a empresa apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido, para fins de habilitação, **[patrimônio líquido mínimo]** de 10% (dez por cento) do valor total estimado da contratação para o período de doze meses – aplicável para o contrato de serviço continuado.

10.26. Os indicadores fixados acima deverão ser atingidos em cada um dos dois últimos exercícios sociais, sob pena de inabilitação;

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

10.28. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

10.29. O atendimento dos índices econômicos previstos neste termo de referência deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

10.29.1 se a apresentação de declaração de índices econômicos firmada por contador como mecanismo de garantia da fidedignidade da situação patrimonial da licitante. Dada a materialidade da contratação, tal exigência busca resguardar a Administração Pública, assegurando que a empresa selecionada possua a solidez necessária para o cumprimento integral das obrigações assumidas.

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

Qualificação Técnica

10.31. Declaração de que o fornecedor tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da contratação.

10.31.1. Essa declaração poderá ser substituída por declaração formal assinada pelo responsável técnico do interessado acerca do conhecimento pleno das condições e peculiaridades da contratação.

Qualificação Técnico

10.32. Comprovação de aptidão para execução de serviço similar, de complexidade tecnológica e operacional equivalente ou superior à do objeto desta contratação, ou do item pertinente, por meio da apresentação de certidões ou atestados emitidos por pessoas jurídicas de direito público ou privado, ou pelo conselho profissional competente, quando for o caso .

10.32.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contrato(s) executado(s) com as seguintes características mínimas:

10.32.1.1. contrato(s) que comprove(m) a experiência mínima de 3 (três) anos do fornecedor na prestação dos serviços, em períodos sucessivos ou não, sendo aceito o somatório de atestados de períodos diferentes;

10.32.1.2. Os serviços comprovados deverão incluir, no mínimo:

10.32.1.2.1 Monitoramento contínuo de eventos de segurança (24x7);

10.32.1.2.2 Análise e correlação de alertas utilizando plataforma SIEM;

10.32.1.2.3 Resposta a incidentes de segurança conforme boas práticas (ex.: NIST, ISO 27035);

10.32.1.2.4 Emissão de relatórios periódicos (mensais ou semanais);

10.32.1.2.5 Atendimento remoto e/ou presencial conforme demanda.

10.32.2 Serão admitidos, para fins de comprovação de quantitativo mínimo de serviço, a apresentação e o somatório de diferentes atestados de serviços executados de forma concomitante.

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

10.32.4. 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 do Contratante e local em que foram prestados os serviços, entre outros documentos.

10.32.5. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

10.33. Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras quando acompanhados de tradução para o português, salvo se comprovada a inidoneidade da entidade emissora.

10.34. A apresentação, pelo fornecedor, de certidões ou atestados de desempenho anterior emitido em favor de consórcio do qual tenha feito parte será admitida, desde que atendidos os requisitos do art. 67, §§ 10 e 11, da Lei nº 14.133/2021 e regulamentos sobre o tema.

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

Disposições gerais sobre habilitação

10.46. Quando permitida a participação na licitação/contratação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

10.47. Na hipótese de o fornecedor ser empresa estrangeira que não funcione no País, para assinatura do contrato ou da ata de registro de preços ou do aceite do instrumento equivalente, 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.

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

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

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

Documentação complementar para cooperativas

10.51. Caso admitida a participação de cooperativas, será exigida a seguinte documentação complementar:

10.51.1. . A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;

10.51.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

10.51.3. A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;

10.51.4. O registro previsto na Lei n. 5.764, de 1971, art. 107;

10.51.5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato;

10.51.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa:

10.51.1. ata de fundação;

10.51.2. estatuto social com a ata da assembleia que o aprovou;

10.51.3. regimento dos fundos instituídos pelos cooperados, com a ata da assembleia;

10.51.4. editais de convocação das três últimas assembleias gerais extraordinárias;

10.51.5. três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais;

10.51.6. ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da contratação; e

10.51.7. última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador .

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado total da contratação, que é o máximo aceitável, é de **R\$ 6.927.887,52 (Seis milhões, novecentos e vinte e sete mil, oitocentos e oitenta e sete reais e cinquenta e dois centavos)**, conforme custos unitários apostos na **tabela contida no item 1.1 deste termo de referência**.

12. ADEQUAÇÃO ORÇAMENTÁRIA

12.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

12.2. A contratação será atendida pela seguinte dotação:

I) Gestão/unidade: 114601;

II) Fonte de recursos: NACIONAL;

III) Programa de trabalho: 225271, 225270 e 225273;

IV) Elemento de despesa: 33904011; e

V) Plano interno: CENSO2020, 12CensoAgro e 1CensoPSR

12.3. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

13. DISPOSIÇÕES FINAIS

13.1. As informações contidas neste Termo de Referência não são classificadas como sigilosas

Integrante Requisitante Flavia Marinho de Lima Analista de Plan. e Gestão Matrícula/SIAPE: 1921901	Integrante Técnico Jussara Roberta de Freitas Silva Analista de Plan. e Gestão Matrícula/SIAPE: 2126098	Integrante Administrativo Antonio Agra Lopes Neto Analista de Plan. e Gestão Matrícula/SIAPE: 1788268
---	--	--

Autoridade Máxima da Área de TIC
Marcos Vinicius Ferreira Mazoni Matrícula/SIAPE: 1572698 Diretor de Tecnologia da Informação

Aprovo,

Autoridade Competente
Marcos Vinicius Ferreira Mazoni Matrícula/SIAPE: 1572698 Diretor de Tecnologia da Informação

14. Responsáveis

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

JUSSARA ROBERTA DE FREITAS SILVA

Equipe de apoio

ANTONIO AGRA LOPES NETO

Equipe de apoio

FLAVIA MARINHO DE LIMA

Equipe de apoio

MARCOS VINICIUS FERREIRA MAZONI

Autoridade competente

Lista de Anexos

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

- Anexo I - TR_Servico Gerenc Seguranca 24x7_Anexos_V3.pdf (891.84 KB)

ANEXO I-A – ESPECIFICAÇÃO TÉCNICA**1. SERVIÇOS PARA O ITEM 1****1.1. Gestão de Vulnerabilidades**

- 1.1.1. A atividade de Gestão de Vulnerabilidades poderá ser realizada in loco ou remotamente, conforme determinação do IBGE, e terá como objetivo principal a análise geral do ambiente do IBGE quanto a segurança da informação para identificar, mapear, documentar, controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica do IBGE, bem como apresentar recomendações de melhorias e/ou correções das vulnerabilidades identificadas durante os testes.
- 1.1.2. Fazem parte do processo de gestão de vulnerabilidades as fases de Varredura de vulnerabilidades, Teste de Invasão, Alerta de Vulnerabilidades e Controle das vulnerabilidades. Estas fases devem atuar de forma integrada com o objetivo de proverem informações suficientes para uma proteção mais eficaz do ambiente da contratada.
- 1.1.3. A periodicidade da execução das fases supracitadas dentro da vigência contratual de 24 meses deverá seguir as exigências da tabela abaixo, bem como está definida a criticidade das atividades, para aplicação dos níveis mínimos de serviço :

FASE	PERIODICIDADE	TOTAL DE EXECUÇÕES NO CONTRATO	CRITICIDADE (Conforme item 7.4 do termo de referência - NMS)
Varredura de vulnerabilidades (Interno)	Mensal	24	BAIXA
Teste de invasão (Externo)	Trimestral	8	BAIXA
Alerta de vulnerabilidades	Semanal	106	MÉDIA
Controle de vulnerabilidades	Diária	730	BAIXA

1.1.4. Características gerais.

- 1.1.4.1. Deverá ser considerado um total de 2100 IPs para o monitoramento de vulnerabilidades e 99 URLs para aplicações.
- 1.1.4.2. A empresa contratada deverá entregar ao gestor do contrato, ou técnico indicado por ele, todo detalhamento dos testes, sejam manuais ou automatizados, a serem realizados, desde os ativos a serem testados, qual procedimento adotado, ferramentas utilizadas, entre outras informações que possam ser solicitadas.
- 1.1.4.3. Os testes de infraestrutura só poderão acontecer mediante autorização do gestor

técnico do contrato, ou técnico indicado por ele, com anuência da DTI – Diretoria de Tecnologia da Informação.

- 1.1.4.4. Os testes de sistemas só poderão acontecer mediante autorização do gestor técnico do contrato, ou técnico indicado por ele, com anuência da área técnica responsável pela sustentação em produção do sistema do escopo.
- 1.1.4.5. Todos os testes a serem realizados deverão ser precedidos de caderno de testes, contendo todo o detalhamento das ações a serem executadas, possíveis comprometimentos, possíveis ações de contorno, dentre outras informações que se julguem necessárias para garantia da segurança e do sigilo das informações do IBGE.
- 1.1.4.6. Todas as fases dos testes serão acompanhadas e supervisionadas a critério da CONTRATANTE.
- 1.1.4.7. Quaisquer atividades que possam comprometer ou prejudicar algum ambiente ou ativo deverão ser reportadas, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos.
- 1.1.4.8. O Responsável Técnico deverá estar presente, no mínimo, 1 (um) dia por semana nas dependências do CONTRATANTE ou virtualmente para efetuar o acompanhamento dos serviços e repassar as informações para o CONTRATANTE, durante a execução dos Testes de Invasão;

1.1.5. Varredura de vulnerabilidades

- 1.1.5.1. Deverá ser realizada mensalmente uma varredura interna de vulnerabilidades no escopo descrito abaixo;
- 1.1.5.2. A varredura de vulnerabilidades do ambiente de TI deve considerar até 2100 (dois mil e cem) endereços IPs e 99 (noventa e nove) Aplicações Web definidos pelo IBGE, devendo considerar as seguintes etapas:
 - 1.1.5.2.1.1. Levantamento de todos os ativos da infraestrutura de TIC que deverão ser alvo da varredura. Para cada ativo, deverão ser levantados além das informações básicas, as informações de criticidade do ativo no ambiente e as informações das janelas de manutenção e mudança caso seja necessário aplicar patch e/ou correções;
 - 1.1.5.2.1.2. Execução da varredura de vulnerabilidades;
 - 1.1.5.2.1.3. Análise dos resultados e priorização das vulnerabilidades;
 - 1.1.5.2.1.4. Elaboração e entrega de um Plano de Remediação considerando a criticidade da vulnerabilidade identificada e, também, os critérios definidos na fase de Levantamento de Ativos.
 - 1.1.5.2.1.5. Para toda vulnerabilidade encontrada, a CONTRATADA deverá descrever de forma detalhada as ações para correção. Caso precise ter acesso as configurações dos ativos de tecnologia ou o código fonte para propor as soluções de correção, a Contratada deverá justificar a necessidade, ficando a cargo do IBGE decidir pela liberação;
 - 1.1.5.2.1.6. Deve ser também apresentado a Matriz de Risco das vulnerabilidades detectadas e o grau de maturidade do IBGE em cada item analisado.

1.1.6. Para realização da varredura de vulnerabilidades deve ser entregue uma ferramenta

com as seguintes características:

- 1.1.6.1. Necessidades gerais:
 - 1.1.6.1.1. A solução de varredura de vulnerabilidades deverá ser fornecida como Software como Serviço (SaaS), hospedada em infraestrutura de nuvem que atenda aos requisitos legais de proteção de dados e segurança da informação, conforme a Lei Geral de Proteção de Dados (LGPD) e demais normativas aplicáveis. Preferencialmente, os dados devem ser armazenados em data centers localizados no Brasil, conforme diretrizes da Portaria SGD/MGI nº 5.950/2023.
 - 1.1.6.1.2. Caso seja necessário serem instalados coletores na modalidade on-premises (uso interno), este deve ser compatível com sistemas de virtualização VMWare e Microsoft HyperV, devendo também ser fornecido todo o licenciamento referente a banco de dados, aplicações e softwares necessários para seu funcionamento.
 - 1.1.6.1.3. Caso seja necessária a instalação de coletores na modalidade on-premises (uso interno), a solução deverá adotar as melhores práticas de segurança da informação para comunicação entre os componentes da ferramenta, incluindo, mas não se limitando a:
 - 1.1.6.1.3.1. Utilização de protocolos seguros e atualizados (como TLS 1.2 ou superior) para transmissão de dados;
 - 1.1.6.1.3.2. Autenticação mútua entre os coletores e os servidores centrais, preferencialmente com uso de certificados digitais;
 - 1.1.6.1.3.3. Criptografia de dados em trânsito e, quando aplicável, em repouso;
 - 1.1.6.1.3.4. Segmentação de rede e restrição de acesso por meio de listas de controle ou grupos de segurança;
 - 1.1.6.1.3.5. Monitoramento contínuo e registro de logs de comunicação para fins de auditoria e resposta a incidentes;
 - 1.1.6.1.3.6. Compatibilidade com ambientes híbridos e respeito às políticas de segurança da organização contratante.
 - 1.1.6.1.4. A solução deve ser integrada e fornecida por um único fabricante, podendo incluir componentes de terceiros desde que devidamente homologados e certificados pelo fabricante principal, respeitando os princípios da interoperabilidade e segurança.
 - 1.1.6.1.5. A solução deverá possuir no mínimo duas certificações reconhecidas internacionalmente relacionadas à segurança da informação e privacidade, tais como:
 - 1.1.6.1.6. Cloud Security Alliance (CSA) STAR;
 - 1.1.6.1.7. ISO/IEC 27001;
 - 1.1.6.1.8. ISO/IEC 27017 ou 27018;
 - 1.1.6.1.9. SOC 2 Type II;
 - 1.1.6.1.10. Certificações equivalentes que comprovem conformidade com boas práticas de segurança e privacidade.
 - 1.1.6.1.11. A plataforma SaaS deverá garantir alta disponibilidade, com operação contínua 24x7x365 e SLA mínimo de 99%, conforme padrões de mercado e requisitos de continuidade de serviço público.
 - 1.1.6.1.12. O ofertante deve oferecer manutenção e atualização constante da plataforma durante todo o período de vigência do contrato de serviço.
 - 1.1.6.1.13. As atualizações de serviço devem ser transparentes para o administrador da solução,

sem afetar nenhum dos dados armazenados ou serviços fornecidos.

- 1.1.6.1.14. Todas as comunicações entre componentes, transferência de dados e sincronização da solução devem ser criptografadas de ponta a ponta, fazendo uso de no mínimo TLS 1.2, certificados assinados com RSA 2048 bits e algoritmo de assinatura SHA256.
- 1.1.6.1.15. Certificados utilizados devem ser emitidos por Autoridades Certificadoras confiáveis, conforme cadeia de confiança reconhecida internacionalmente.
- 1.1.6.1.16. A solução deve permitir criação de usuários distintos.
- 1.1.6.1.17. Deve permitir separação de funções e permissões na console.
- 1.1.6.1.18. A console deve ser acessível a partir de, pelo menos, um dos navegadores comerciais dentre Google Chrome, Microsoft Edge e Mozilla Firefox.
- 1.1.6.1.19. Realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance) e indícios e padrões de códigos maliciosos conhecidos (malware);
- 1.1.6.1.20. Possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;
- 1.1.6.1.21. Suportar varreduras de dispositivos de IoT;
- 1.1.6.1.22. Ter a capacidade de adicionar etiquetas (tags) aos ativos de maneira automática, manual e através de regras com parâmetros específicos;
- 1.1.6.1.23. Atribuir uma severidade a todas as vulnerabilidades identificadas com base na pontuação do CVSS (Common Vulnerability Scoring System), preferencialmente utilizando a versão mais atualizada;
- 1.1.6.1.24. Calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança, sistema e conformidade, bem como hierarquias e prioridades;
- 1.1.6.1.25. Possuir assinaturas intrusivas e a possibilidade de inseri-las ou não nas varreduras, buscando maior efetividade nos testes.
- 1.1.6.1.26. Fornecer criptografia de ponta a ponta dos dados de vulnerabilidade;
- 1.1.6.1.27. Possuir a capacidade de criar um inventário do ambiente coletando e alimentando continuamente os dados do sistema, conformidade e segurança dos ativos de TI;
- 1.1.6.1.28. Possuir um sistema de busca do inventário com no mínimos as seguintes características:
 - 1.1.6.1.28.1. Por sistema operacional;
 - 1.1.6.1.28.2. Por fabricante do hardware;
 - 1.1.6.1.28.3. Por um determinado software instalado;
 - 1.1.6.1.28.4. Por Ativos impactados por uma determinada vulnerabilidade;
- 1.1.6.1.29. Fornecer gerenciamento de fluxo de trabalho de correção com base em políticas com criação e atribuição automática de registro de problema.
- 1.1.6.1.30. Possuir um sistema de pontuação e priorização das vulnerabilidades;
- 1.1.6.1.31. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
 - 1.1.6.1.31.1. CVSSv3 Impact Score;
 - 1.1.6.1.31.2. Idade da Vulnerabilidade;

- 1.1.6.1.31.3. Número de produtos afetados pela vulnerabilidade;
- 1.1.6.1.31.4. Intensidade baseada no Número e Frequência de ameaças que utilizaram a vulnerabilidade ao longo do tempo;
- 1.1.6.1.32. Fazer a correlação em tempo real de ameaças ativas contra suas vulnerabilidades, incluindo feeds de inteligência de ameaças ao vivo
- 1.1.6.1.33. Suportar análise de vulnerabilidades de ambientes ativos utilizados em ambiente de automação;
- 1.1.6.1.34. Possuir uma API abrangente para automação de processos e integração com aplicações terceiras, sendo disponibilizada a documentação técnica para uso;
- 1.1.6.1.35. Permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;
- 1.1.6.1.36. Produzir relatórios nos seguintes formatos: PDF, CSV e HTML;
- 1.1.6.1.37. Deve ser possível determinar em tempo real quais portas estão abertas em determinado ativo;
- 1.1.6.1.38. Realizar em tempo real a descoberta de novos ativos para no mínimo:
 - 1.1.6.1.38.1. Bancos de dados;
 - 1.1.6.1.38.2. Hypervisors;
 - 1.1.6.1.38.3. Dispositivos móveis;
 - 1.1.6.1.38.4. Dispositivos de rede;
 - 1.1.6.1.38.5. Servidores físicos e virtuais;
 - 1.1.6.1.38.6. Aplicações;
- 1.1.6.1.39. Realizar em tempo real a identificação de informações sensíveis no tráfego de rede do ambiente;
- 1.1.6.1.40. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede em tempo real sem a necessidade de um agente:
 - 1.1.6.1.40.1. Caso seja necessário serem instalados coletores na modalidade on-premises (uso interno), este deve ser compatível com sistemas de virtualização VMWare e Microsoft HyperV, devendo também ser fornecido todo o licenciamento referente a banco de dados, aplicações e softwares necessários para seu funcionamento.
- 1.1.6.1.41. A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.
- 1.1.6.2. Deve possuir configuração de segurança e acesso restrito à console, atendendo aos seguintes itens:
 - 1.1.6.2.1. Suportar autenticação de dois fatores para os usuários e login.
 - 1.1.6.2.2. Suportar a configuração de segurança de senha e personalizar a política de segurança para a configuração de gerenciamento de senha:
 - 1.1.6.2.2.1. Idade e validade da senha;
 - 1.1.6.2.2.2. Conta de usuário bloqueada após o número de login com falha;
 - 1.1.6.2.2.3. Comprimento mínimo da senha;

- 1.1.6.2.2.4. Complexidade de senha, caracteres alfanuméricos e numéricos a serem usados;
- 1.1.6.2.2.5. Forçar alteração de senha no login inicial;
- 1.1.6.2.2.6. Notificação para senha expirada antes do número de dias.
- 1.1.6.2.3. Executar relatórios manuais e periódicos de acordo com a frequência estabelecida pelo administrador;
- 1.1.6.2.4. Permitir a criação de relatórios baseado nos seguintes alvos: Todos os ativos existentes e alvos específicos;
- 1.1.6.2.5. Suportar a criação de relatórios criptografados (protegidos por senha configurável);
- 1.1.6.2.6. Suportar o envio automático de relatórios para destinatários específicos;
- 1.1.6.2.7. Ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
- 1.1.6.2.8. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
- 1.1.6.2.9. Fornecer relatórios de correção: tendência de ticket por grupo de ativos, usuário e vulnerabilidade
- 1.1.6.2.10. Permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas
- 1.1.6.2.11. Permitir a coleta de informações detalhadas sobre o ativo gerenciado, deve detalhar pelo menos os seguintes dados para cada ativo:
 - 1.1.6.2.11.1. Serviços em execução
 - 1.1.6.2.11.2. Software instalado
 - 1.1.6.2.11.3. Usuários
 - 1.1.6.2.11.4. Portas abertas
 - 1.1.6.2.11.5. Nome do host
 - 1.1.6.2.11.6. FQDN
 - 1.1.6.2.11.7. IP v4 / v6
 - 1.1.6.2.11.8. Endereço MAC
 - 1.1.6.2.11.9. Processador
 - 1.1.6.2.11.10. Memória
 - 1.1.6.2.11.11. Volumes de disco
 - 1.1.6.2.11.12. BIOS
- 1.1.6.2.12. Classificar automaticamente os ativos por famílias de tecnologia, tipo de dispositivo, tipo de plataforma e fabricante.
- 1.1.6.2.13. Normalizar automaticamente os nomes dos fabricantes de HW e SW com seus dados relevantes, como o nome dos aplicativos e versões, para facilitar sua posterior busca na solução.
- 1.1.6.2.14. A solução deverá possuir funcionalidade de etiquetagem (tags) de ativos, com o objetivo de facilitar a organização, identificação e agrupamento dos ativos conforme critérios definidos pela organização contratante.

- 1.1.6.2.15. É desejável que a ferramenta permita a criação e aplicação de tags com base em múltiplos parâmetros, incluindo, mas não se limitando a:
 - 1.1.6.2.15.1. Etiquetagem manual ou estática;
 - 1.1.6.2.15.2. Palavras-chave associadas aos ativos;
 - 1.1.6.2.15.3. Endereços IP e intervalos de IP;
 - 1.1.6.2.15.4. Segmentos de rede;
 - 1.1.6.2.15.5. Portas abertas detectadas;
 - 1.1.6.2.15.6. Identificadores de vulnerabilidades específicas;
 - 1.1.6.2.15.7. Expressões regulares (Regex);
 - 1.1.6.2.15.8. Scripts customizados, como scriptlets em linguagens compatíveis com a solução (ex.: Groovy, Python, etc.), não sendo exigido suporte exclusivo a uma linguagem específica.
- 1.1.6.2.16. A solução proposta deve possuir a capacidade de obter e exibir informações sobre os ciclos de vida de hardware / software (EOL / EOS).
- 1.1.6.2.17. A solução deve permitir identificar o tipo de licenças associadas ao software instalado, classificando-as como comercial, open source e outros tipos de licenciamento.
- 1.1.6.2.18. A solução deve permitir a detecção de software não autorizado e permitir sua desinstalação em plataformas Microsoft Windows.
- 1.1.6.2.19. A solução deve permitir detectar hardwares e softwares desatualizados, sem suporte do fabricante - em final de vida útil.
- 1.1.6.2.20. A solução deve permitir atribuir criticidade ao ativo para priorizá-lo durante o processo de gerenciamento.
- 1.1.6.2.21. Possuir relatórios pré configurados com as seguintes informações:
 - 1.1.6.2.21.1. Hosts verificados sem credenciais;
 - 1.1.6.2.21.2. Top 100 Vulnerabilidades mais críticas;
 - 1.1.6.2.21.3. Top 10 Hosts infectados por Malwares;
 - 1.1.6.2.21.4. Hosts exploráveis por Malwares;
 - 1.1.6.2.21.5. Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
 - 1.1.6.2.21.6. Vulnerabilidades críticas e exploráveis;
 - 1.1.6.2.21.7. Máquinas com vulnerabilidades que podem ser exploradas;
- 1.1.6.2.22. Possuir dashboards customizáveis onde o administrador pode deletar, editar ou criar painéis de acordo com a necessidade;
- 1.1.6.2.23. Inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.
- 1.1.6.2.24. Possuir integração nativa do mesmo fabricante ou com terceiros, a solução de gestão de patches;
- 1.1.6.3. Características específicas da funcionalidade de gestão de vulnerabilidade e varreduras de ativos:
 - 1.1.6.3.1. Realizar varreduras (scans) de vulnerabilidades, de acordo com os somatórios de

endereços IP licenciados;

- 1.1.6.3.2. Permitir a instalação e distribuição de no mínimo 5 scanners no ambiente;
- 1.1.6.3.3. Permitir a configuração de vários painéis e widgets;
- 1.1.6.3.4. Medir e reportar ameaças;
- 1.1.6.3.5. Visualizar ameaças críticas no ambiente da rede corporativa;
- 1.1.6.3.6. Realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como appliances virtuais;
- 1.1.6.3.7. Suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;
- 1.1.6.3.8. Fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de configurações e vulnerabilidades;
- 1.1.6.3.9. Incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia;
- 1.1.6.3.10. No caso onde uma atividade de varredura seja interrompida por invadir o período não permitido, o mesmo deve ser reiniciado de onde parou;
- 1.1.6.3.11. Ser configurável para permitir a otimização das configurações de varredura;
- 1.1.6.3.12. Permitir a utilização de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux, para varreduras autenticadas;
- 1.1.6.3.13. Informar a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
- 1.1.6.3.14. Realizar pesquisas de dados confidenciais;
- 1.1.6.3.15. Conter a funcionalidade de gestão de vulnerabilidade de aplicativos Web.
- 1.1.6.3.16. Realizar varreduras de vulnerabilidades em aplicações Web, cobrindo no mínimo, mas não limitando-se a base de ameaças apontadas pelo OWASP Top 10;
- 1.1.6.3.17. Analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;
- 1.1.6.3.18. Executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);
- 1.1.6.3.19. Avaliar no mínimo os padrões de segurança OWASP Top 10, CWE e WASC;
- 1.1.6.3.20. Identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal;
- 1.1.6.3.21. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os elementos JSON e XML;
- 1.1.6.3.22. Permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;
- 1.1.6.3.23. Realizar testes/varreduras em aplicações separadas, simultaneamente
- 1.1.6.3.24. Suportar override de DNS para os testes de aplicações web
- 1.1.6.3.25. Oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada antes no aplicativo Web.

- 1.1.6.3.26. Excluir determinadas URLs da varredura através de expressões regulares;
- 1.1.6.3.27. Instituir no mínimo os seguintes limites:
 - 1.1.6.3.27.1. Número máximo de URLs para crawl e navegação;
 - 1.1.6.3.27.2. Número máximo de diretórios para varreduras;
 - 1.1.6.3.27.3. Tempo máximo para a varredura;
 - 1.1.6.3.27.4. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;
 - 1.1.6.3.27.5. Número máximo de requisições HTTP por segundo;
- 1.1.6.3.28. Agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
- 1.1.6.3.29. Suportar o envio de notificações por email;
- 1.1.6.3.30. Ser compatível com avaliação de web services REST e SOAP;
- 1.1.6.3.31. Suportar os seguintes esquemas de autenticação:
 - 1.1.6.3.31.1. Autenticação Básica (Digest);
 - 1.1.6.3.31.2. NTLM;
 - 1.1.6.3.31.3. Autenticação de Cookies;
 - 1.1.6.3.31.4. Autenticação através de Selenium;
- 1.1.6.3.32. Importar scripts de autenticação selenium previamente configurados pelo usuário;
- 1.1.6.3.33. Exibir os resultados das varreduras de forma temporal para acompanhamento de correções e introdução de novas vulnerabilidades;
- 1.1.6.3.34. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
- 1.1.6.3.35. Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências;
- 1.1.6.3.36. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;
- 1.1.6.3.37. Serviço de Detecção de Malware em aplicativos Web
- 1.1.6.3.38. Ter a capacidade de varrer e identificar infecções por malware nas propriedades da web
- 1.1.6.3.39. Suportar capacidade de detecção de malware de dia zero.
- 1.1.6.3.40. Fornecer uma visão abrangente da atividade de verificação, páginas infectadas e tendências de infecção por malware.
- 1.1.6.3.41. Fornecer um relatório interativo com análise poderosa e distribuição segura dos resultados da verificação.
- 1.1.6.3.42. Fornecer relatórios de resumo e resumo do site que podem ser exportados para o formato HTML e PDF.
- 1.1.6.3.43. Realizar varreduras nos seguintes componentes:
 - 1.1.6.3.43.1. AngularJS, Apache, Apache Tomcat, Apache Tomcat JK connector, Apache Spark e Apache Struts;
 - 1.1.6.3.43.2. Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI

- 1.1.6.3.43.3. JBoss AS e WildFly
- 1.1.6.4. Características específicas da funcionalidade de gestão de vulnerabilidade com a políticas de conformidade
 - 1.1.6.4.1. Fornecer um console interativo e centralizado para especificar os padrões de linha de base necessários para diferentes conjuntos de hosts. Os grupos de ativos devem ser compartilhados em toda a plataforma, portanto, os hosts descobertos e categorizados pela função de negócios no Gerenciamento de vulnerabilidades podem ter automaticamente as políticas de proteção adequadas avaliadas no Conformidade de política ;
 - 1.1.6.4.2. Permitir ao usuário final utilizar biblioteca integrada de políticas amplamente utilizadas.
 - 1.1.6.4.3. Usar um host previamente escaneado como uma “imagem dourada”;
 - 1.1.6.4.4. Permitir criar políticas personalizadas através de um editor interativo baseado na web;
 - 1.1.6.4.5. Permitir interativamente escolher quais configurações devem ser monitoradas;
 - 1.1.6.4.6. Permitir que o usuário final teste os controles imediatamente sem redigitar ou relatar;
 - 1.1.6.4.7. Ter uma biblioteca rica de controles para sistemas operacionais, dispositivos de rede, bancos de dados e aplicativos;
 - 1.1.6.4.8. A solução deve incluir indicadores de ameaças em tempo real que ajudam a avaliar e priorizar as vulnerabilidades detectadas, categorizados da seguinte forma:
 - 1.1.6.4.8.1. Dia Zero: vulnerabilidades para as quais não há patch disponível e para as quais um ataque ativo foi observado.
 - 1.1.6.4.8.2. Exploração pública: Vulnerabilidades cujo mecanismo de exploração é conhecido, para o qual existe um código de exploração e está disponível publicamente.
 - 1.1.6.4.8.3. Ataques ativos: vulnerabilidades que estão sendo atacadas ativamente.
 - 1.1.6.4.8.4. Movimento lateral: vulnerabilidades que permitem ao invasor espalhar o ataque amplamente pela rede violada.
 - 1.1.6.4.8.5. Fácil exploração: vulnerabilidades que podem ser facilmente exploradas, exigindo poucas habilidades e pouco conhecimento
 - 1.1.6.4.8.6. Perda de dados: vulnerabilidades cuja exploração causará perda massiva de dados
 - 1.1.6.4.8.7. Negação de serviço: vulnerabilidades cuja carga útil pode sobrecarregar - impedir que sistemas comprometidos estejam permanentemente - temporariamente disponíveis.
 - 1.1.6.4.8.8. No Patch: Vulnerabilidades para as quais não há solução do provedor
 - 1.1.6.4.8.9. Malware: vulnerabilidades associadas a infecções por malware
 - 1.1.6.4.8.10. Kit de exploração: vulnerabilidades para as quais um kit de exploração está disponível
 - 1.1.6.4.9. Monitorar a integridade dos arquivos e observar mudanças.
 - 1.1.6.4.10. Permitir a configuração de controles personalizados sem escrever código ou scripts.

- 1.1.6.4.11. Ter o recurso "Scan Anywhere" em um único console.
- 1.1.6.4.12. Permitir a verificação sob demanda ou em um cronograma;
- 1.1.6.4.13. Avaliar detalhadamente através de varreduras autenticadas;
- 1.1.6.4.14. Gerenciar exceções por meio de um processo de aprovações documentadas;
- 1.1.6.4.15. A solução proposta deve fornecer um workflow de correção baseado em políticas de criação e atribuição, re-atribuindo tickets de acordo com as condições definidas pelo administrador da solução através de políticas ou manualmente.
- 1.1.6.4.16. A solução deve permitir a criação de tickets com status aberto, fechado, ignorado, com base nos seguintes critérios:
 - 1.1.6.4.16.1. Host(s) a quem a regra se aplica;
 - 1.1.6.4.16.2. Vulnerabilidade (s) a que a regra se aplica;
 - 1.1.6.4.16.3. Usuário atribuído;
 - 1.1.6.4.16.4. Data de criação – expiração;
 - 1.1.6.4.16.5. Mudança de estado.
- 1.1.6.4.17. A solução deve permitir a criação de tickets de correção automaticamente a partir do resultado de uma varredura de vulnerabilidade - com base nas informações de um host específico e também manualmente por um administrador de solução.
- 1.1.6.4.18. Permitir a personalização de relatórios abrangentes, como por exemplo, documentar o progresso de TI em relação à correção das vulnerabilidades, informar as prioridades a serem corrigidas ou fomentar gerentes e auditores com o histórico das análises realizadas.
- 1.1.6.4.19. Permitir a geração de relatórios a qualquer momento, em qualquer lugar - sem redigitalizar
- 1.1.6.4.20. Comparar taxas de conformidade entre políticas, tecnologias e ativos
- 1.1.6.4.21. Disponibilizar histórico das varreduras realizadas com as respectivas políticas, assim como o andamento das correções efetuadas
- 1.1.6.4.22. Criar relatórios diferentes para diferentes públicos
- 1.1.6.4.23. Permitir o gerenciamento de risco e conformidade orientado a dados
- 1.1.6.4.24. Compartilhar dados com sistemas de gestão de risco e outros aplicativos corporativos
- 1.1.6.4.25. Agentes:
 - 1.1.6.4.25.1. A solução proposta deve oferecer um agente de baixo impacto nos sistemas operacionais onde está instalado e no consumo de largura de banda que utilizará na rede.
 - 1.1.6.4.25.2. A solução deve ser instalada em servidores, estações de trabalho, e máquinas virtuais, suportando sua implantação em rede local, em rede doméstica e na nuvem.
 - 1.1.6.4.25.3. A solução deve oferecer suporte para sua implantação em pelo menos os seguintes sistemas operacionais:
 - 1.1.6.4.25.3.1. Windows Server 2019 e posterior (x86, x64)
 - 1.1.6.4.25.3.2. CentOS 7.x (x64), 8.x (x64)

- 1.1.6.4.25.4. Red Hat Enterprise Linux (RHEL)
- 1.1.6.4.25.5. O agente da solução deve se atualizar automaticamente e gerir as suas atualizações automaticamente.
- 1.1.6.4.25.6. A solução deve suportar plataformas de nuvem AWS, GCP, Azure.
- 1.1.6.4.25.7. A solução deve ser capaz de coletar informações sobre o inventário de ativos.
- 1.1.6.4.25.8. A solução deve prover nativamente um dispositivo capaz de concentrar requisições dos agentes para encaminhamento a console de gerenciamento de forma a evitar a conexão direta de agentes com a plataforma.
- 1.1.6.4.25.9. O agente de gerenciamento deve suportar o uso de proxy.
- 1.1.6.4.25.10. Deve ser possível definir o intervalo de comunicação entre o agente e a console de gerenciamento.
- 1.1.6.4.25.11. Deve ser possível limitar o consumo de CPU e memória do agente.
- 1.1.6.4.25.12. Deve permitir a definição de um período global de inatividade dos agentes
- 1.1.6.4.26. Scanners:
 - 1.1.6.4.26.1. A solução deve permitir o uso de scanners capazes de identificar vulnerabilidades através de varreduras em ranges de IP definidos pelo administrador.
 - 1.1.6.4.26.2. Não deverá haver restrições para instalação de scanners virtuais no ambiente.
 - 1.1.6.4.26.3. Deve ser permitido o uso de scanners externos, sem necessidade de instalação, em nuvem própria do fabricante para varreduras de ativos publicados na internet.
 - 1.1.6.4.26.4. Os scanners virtuais devem suportar pelo menos um dos hypervisors abaixo:
 - 1.1.6.4.26.4.1. Hyper-V
 - 1.1.6.4.26.4.2. VMWare
 - 1.1.6.4.26.5. Os Scanners devem suportar a varredura de ambientes em nuvem para pelo menos os seguintes provedores:
 - 1.1.6.4.26.5.1. Azure
 - 1.1.6.4.26.5.2. AWS
 - 1.1.6.4.26.5.3. Google Cloud Platform
 - 1.1.6.4.26.5.4. Oracle
 - 1.1.6.4.26.6. Os scanners devem reportar vulnerabilidades para a console, permitindo uma visão consolidada das vulnerabilidades.
 - 1.1.6.4.26.7. Deve ser permitido o agendamento de varreduras para máquinas que possuam uma determinada versão de banco de dados em execução.
 - 1.1.6.4.26.8. Deve ser permitido a varredura sob demanda para um ou mais ativos de rede.
 - 1.1.6.4.26.9. O mesmo scanner deve ser capaz de varrer por falhas de conformidade e também por vulnerabilidades.
 - 1.1.6.4.26.10. O scanner deverá consolidar vulnerabilidades encontradas em um ativo que possua agente instalado.

- 1.1.6.4.26.11. A solução deve permitir a configuração do tipo de varredura a ser realizada, permitindo pelo menos definir as seguintes configurações ao defini-la:
- 1.1.6.4.26.12. Configuração de quantidades de portas TCP/UDP a serem validadas.
- 1.1.6.4.26.13. Consumo de largura de banda e recursos (alto, médio, baixo).
- 1.1.6.4.26.14. Digitalize para dispositivos que não suportam ping - traceroute.
- 1.1.6.4.26.15. Detecção de balanceadores de carga.
- 1.1.6.4.26.16. Configuração de força bruta para usar em senhas.
- 1.1.6.4.26.17. Uso de um cabeçalho HTTP personalizado.
- 1.1.6.4.26.18. Ignorar pacotes.
- 1.1.6.4.26.19. Instalação de agente temporário para validação de registro local.
- 1.1.6.4.27. Categorização e Gestão de Ativos Tecnológicos
 - 1.1.6.4.28. Para realização da Categorização e Gestão dos ativos tecnológicos deve ser entregue uma ferramenta com as seguintes características:
 - 1.1.6.4.29. A solução deve identificar e inventariar automaticamente todos os ativos conectados à rede, incluindo servidores, estações de trabalho, dispositivos de rede e ativos em nuvem.
 - 1.1.6.4.30. A solução deve identificar e inventariar automaticamente todos os ativos conectados à rede, incluindo servidores, estações de trabalho, dispositivos de rede e ativos em nuvem.
 - 1.1.6.4.31. A solução deve ser capaz de detectar ativos não gerenciados e fornecer mecanismos para sua categorização e monitoramento contínuo.
 - 1.1.6.4.32. A solução deve correlacionar ativos descobertos com informações de segurança, permitindo a análise de riscos e priorização de ações corretivas.
 - 1.1.6.4.33. A solução deve possuir integração via API para permitir a exportação e análise de dados em sistemas de terceiros, como SIEM, ITSM e CMDBs.
 - 1.1.6.4.34. A documentação da API da solução deverá ter acesso público através de website ou documentação do próprio fabricante.
 - 1.1.6.4.35. A console de administração deverá possuir controle de acesso, no mínimo permitindo usuários com capacidade de somente visualizar as informações e usuários com capacidade de administrar os ativos e configurar políticas.
 - 1.1.6.4.36. A solução deve permitir a descoberta de ativos em tempo real, utilizando múltiplos métodos, incluindo varreduras ativas, passivas e agentes instalados nos dispositivos.
 - 1.1.6.4.37. A solução deve ser capaz de identificar softwares instalados em cada ativo e correlacioná-los com vulnerabilidades conhecidas, permitindo a gestão de riscos com base em ameaças reais.
 - 1.1.6.4.38. A solução deve possibilitar a criação de relatórios personalizados sobre o inventário de ativos, incluindo estado de conformidade e nível de risco associado.

- 1.1.6.4.39. A solução deve permitir a categorização dos ativos por tipo, localização, sistema operacional, uso e outras características personalizáveis.
- 1.1.6.4.40. A solução deve ser capaz de identificar mudanças nos ativos, alertando sobre novos dispositivos conectados à rede, remoção de dispositivos e alterações na configuração de hardware ou software.
- 1.1.6.4.41. A solução deve integrar-se com outras ferramentas para ampliar as capacidades de análise e correção de vulnerabilidades nos ativos gerenciados.
- 1.1.6.4.42. A solução deve permitir a visualização dos ativos por meio de dashboards interativos, facilitando a análise e a tomada de decisão.
- 1.1.6.4.43. A solução deve suportar a aplicação de políticas de segurança e conformidade para avaliar continuamente os ativos contra padrões predefinidos.
- 1.1.6.4.44. A solução deve permitir a configuração de alertas automatizados para notificações sobre novos ativos, ativos fora de conformidade ou mudanças na infraestrutura.
- 1.1.6.4.45. A solução deve possibilitar a segmentação dos ativos em grupos para melhor gerenciamento e aplicação de políticas específicas.
- 1.1.6.4.46. A solução deve permitir auditoria detalhada das ações realizadas dentro da ferramenta, garantindo rastreabilidade e conformidade com normativas.
- 1.1.6.4.47. A solução deve permitir a customização dos critérios de risco dos ativos, permitindo que a organização adapte a análise de segurança conforme suas necessidades.
- 1.1.6.4.48. A solução deve suportar a criação de inventários automatizados e relatórios programados para distribuição periódica aos responsáveis pela segurança.
- 1.1.6.4.49. A solução deve permitir integração com serviços de nuvem pública, como AWS, Azure e Google Cloud, para descoberta e gerenciamento de ativos em ambientes híbridos.
- 1.1.6.4.50. A solução proposta deve possuir a capacidade de obter e exibir informações sobre os ciclos de vida de hardware / software (EOL / EOS)
- 1.1.6.4.51. A solução deve permitir identificar o tipo de licenças associadas ao software instalado, classificando-as como comercial, open source e outros tipos de licenciamento.
- 1.1.6.4.52. A solução deve permitir a detecção de software não autorizado e permitir sua desinstalação em plataformas Microsoft Windows.
- 1.1.6.4.53. A solução deve permitir detectar hardwares e softwares desatualizados, sem suporte do fabricante - em final de vida útil.
- 1.1.6.4.54. A solução deve permitir atribuir criticidade ao ativo para priorizá-lo durante o processo de gerenciamento.

- 1.1.6.4.55. A solução proposta permitirá a coleta de informações detalhadas sobre o ativo gerenciado, devendo detalhar pelo menos os seguintes dados para cada ativo:
 - 1.1.6.4.55.1. Serviços em execução
 - 1.1.6.4.55.2. Software instalado
 - 1.1.6.4.55.3. Usuários
 - 1.1.6.4.55.4. Portas abertas
 - 1.1.6.4.55.5. Nome do host
 - 1.1.6.4.55.6. FQDN
 - 1.1.6.4.55.7. IP v4 / v6
 - 1.1.6.4.55.8. Endereço MAC
 - 1.1.6.4.55.9. Processador
 - 1.1.6.4.55.10. Memória
 - 1.1.6.4.55.11. Volumes de disco
 - 1.1.6.4.55.12. BIOS
- 1.1.6.4.56. A solução deve classificar automaticamente os ativos por famílias de tecnologia, tipo de dispositivo, tipo de plataforma e fabricante.
- 1.1.6.4.57. A solução deve normalizar automaticamente os nomes dos fabricantes de hardware e software com seus dados relevantes, como o nome dos aplicativos e versões, para facilitar sua posterior busca na solução.
- 1.1.6.4.58. A solução deve possuir a habilidade de etiquetagem (tags) de ativos para facilitar a identificação, deve permitir a geração de tags, pelo menos, usando os seguintes parâmetros:
 - 1.1.6.4.58.1. Palavras-chave
 - 1.1.6.4.58.2. Endereço IP e intervalos de IP
 - 1.1.6.4.58.3. Segmento de rede
 - 1.1.6.4.58.4. Portas abertas
- 1.1.6.5. Informações de inventário considerando, no mínimo:
 - 1.1.6.5.1.1. Sistema operacional,
 - 1.1.6.5.1.2. Presença ou ausência de determinado software instalado ou serviço em execução.
 - 1.1.6.5.1.3. Última localização geográfica detectada incluindo cidade e país
 - 1.1.6.5.1.4. Regex
 - 1.1.6.5.2. A solução deve permitir agrupamento manual a critério do administrador da solução.
 - 1.1.6.5.3. A solução deve permitir atribuir criticidade ao ativo para priorizá-lo durante o processo de gerenciamento.

- 1.1.6.5.4. Deve permitir criação de dashboards personalizados que sejam capazes de trazer as seguintes informações sobre os ativos:
 - 1.1.6.5.4.1. Categorias de softwares instalados nos ativos
 - 1.1.6.5.4.2. Hosts que executam máquinas virtuais
 - 1.1.6.5.4.3. Sistemas operacionais utilizados
 - 1.1.6.5.4.4. Serviços e portas TCP ou UDP abertas
 - 1.1.6.5.4.5. Softwares de segurança instalados
 - 1.1.6.5.4.6. Memória total utilizada
 - 1.1.6.5.4.7. Quantidade de processadores
 - 1.1.6.5.4.8. Quantidade de armazenamento disponível
- 1.1.6.5.5. A solução deve permitir uma interface de busca de ativos que utilize sintaxe lógica baseada, no mínimo, nos critérios abaixo:
 - 1.1.6.5.5.1. Fabricante de hardware
 - 1.1.6.5.5.2. Último usuário logado
 - 1.1.6.5.5.3. Categoria de software instalado
- 1.1.6.5.6. A solução deve permitir a visualização de quantidade de máquinas com um determinado software instalado.
- 1.1.6.5.7. Deve permitir visibilidade a respeito de hosts que executam containers e containers em execução.
- 1.1.6.5.8. Além de workstations e servidores, a solução deve permitir visibilidade a respeito de ativos tais como switches, roteadores, firewalls, impressoras, etc.
- 1.1.6.6. Gestão de Vulnerabilidade, Detecção e Resposta
 - 1.1.6.6.1. A solução deve permitir descobrir, avaliar, priorizar e auxiliar na correção de vulnerabilidades e configurações em toda a infraestrutura de rede, incluindo estações de trabalho, servidores, dispositivos de rede, dispositivos de telecomunicações e dispositivos de segurança, hypervisors, máquinas virtuais, proporcionando através de única interface para o administrador via um portal web para gerenciamento de todos os ativos, permitindo o gerenciamento centralizado de todos os componentes da solução a partir de um único ponto, sem a necessidade de incorrer em consoles ou componentes adicionais fora dele para a administração dos serviços oferecidos.
 - 1.1.6.6.2. A solução deve ser licenciada por Asset (IP - HOST) para ativos de infraestrutura.
 - 1.1.6.6.3. A solução deve ser licenciada por URLs para varreduras de aplicação web.
 - 1.1.6.6.4. A solução deve permitir varreduras de vulnerabilidade com base em:
 - 1.1.6.6.4.1. Sistemas Operacionais
 - 1.1.6.6.4.2. Serviços WEB
 - 1.1.6.6.4.3. Portas TCP e UDP
 - 1.1.6.6.4.4. Serviços
 - 1.1.6.6.4.5. Aplicações

- 1.1.6.6.4.6. Bancos de dados
- 1.1.6.6.4.7. Dispositivos de rede como switches, roteadores e balanceadores de carga
- 1.1.6.6.5. No mínimo, a ferramenta deve abranger os seguintes sistemas operacionais, bancos de dados e aplicativos:
 - 1.1.6.6.5.1. Microsoft Windows
 - 1.1.6.6.5.2. LINUX
 - 1.1.6.6.5.3. Mac OS X
 - 1.1.6.6.5.4. VMware
- 1.1.6.6.6. Detectar e analisar vulnerabilidades nas principais versões de Bancos de Dados, pelo menos:
 - 1.1.6.6.6.1. Microsoft SQL Server
 - 1.1.6.6.6.2. MySQL
 - 1.1.6.6.6.3. Oracle
 - 1.1.6.6.6.4. PostgreSQL
 - 1.1.6.6.6.5. Detectar e analisar vulnerabilidades em plataformas WEB, pelo menos:
 - 1.1.6.6.6.6. IIS
 - 1.1.6.6.6.7. Apache Tomcat
- 1.1.6.6.7. Detectar e analisar vulnerabilidades em portas e serviços TCP e UDP
- 1.1.6.6.8. Detectar vulnerabilidades em pelo menos os seguintes aplicativos ou plataformas:
 - 1.1.6.6.8.1. Adobe
 - 1.1.6.6.8.2. Apple
 - 1.1.6.6.8.3. HP
 - 1.1.6.6.8.4. McAfee
 - 1.1.6.6.8.5. Microsoft
 - 1.1.6.6.8.6. Oracle
 - 1.1.6.6.8.7. Oracle Java
 - 1.1.6.6.8.8. VMware
 - 1.1.6.6.8.9. Linux
- 1.1.6.6.9. Permitir a descoberta de vulnerabilidades na rede, oferecendo as seguintes alternativas de varredura:
 - 1.1.6.6.10. Varredura ativa de rede não autenticada
 - 1.1.6.6.11. Varredura ativa de rede autenticada
- 1.1.6.7. Varreduras externas
 - 1.1.6.7.1.1. O mecanismo de varredura deve ter uma taxa de precisão de detecção de vulnerabilidade de 99,99966% durante os últimos 10 anos.
 - 1.1.6.7.1.2. A base de conhecimento de vulnerabilidade deve ser atualizada no mínimo semanalmente, garantindo a incorporação de pelo menos 20 CVEs a ela e deve

- ter pelo menos uma base de conhecimento de 35.000 CVEs relacionados incluindo tecnologias legadas e atuais.
- 1.1.6.7.1.3. A solução deve oferecer suporte ao padrão da indústria para pontuação de vulnerabilidade do Common Vulnerability Scoring System (CVSS)
 - 1.1.6.7.1.4. A solução deve oferecer suporte ao padrão da indústria para adicionar detecções personalizadas usando Open Vulnerability Assessment Language (OVAL).
 - 1.1.6.7.1.5. A solução deve permitir vincular as vulnerabilidades detectadas e indicar sua relação com ameaças como Vírus, Trojan e Malware.
 - 1.1.6.7.1.6. A solução deve ser capaz de indicar explorações disponíveis e códigos disponíveis para uma vulnerabilidade, quando aplicável
 - 1.1.6.7.1.7. O banco de dados deve relacionar a maioria das vulnerabilidades ao CVE e Bugtraq.
 - 1.1.6.7.1.8. A solução deve oferecer suporte à integração para autenticação por ferramentas de cofres de senha com ao menos uma das seguintes fabricantes, Delinea, CyberArk, BeyondTrust
 - 1.1.6.7.1.9. A solução deve permitir buscas interativas de vulnerabilidade utilizando filtros como severidade, categoria, sistema operacional, status, classificação do CVSS, CVE ou KB.
 - 1.1.6.7.1.10. A solução deve permitir a utilização de operadores lógicos na busca de vulnerabilidades para que seja possível encontrar, no mínimo, as seguintes informações:
 - 1.1.6.7.1.10.1. Vulnerabilidades associadas a ransomware e que possuem patches disponíveis
 - 1.1.6.7.1.10.2. Vulnerabilidades detectadas em um segmento de rede
 - 1.1.6.7.1.10.3. Vulnerabilidades detectadas em serviços específicos
 - 1.1.6.7.1.10.4. Vulnerabilidades detectadas por um usuário específico
 - 1.1.6.7.1.10.5. Vulnerabilidades detectadas em hardware específico
 - 1.1.6.7.1.10.6. A busca de vulnerabilidades deve permitir agrupamento para mostrar, no mínimo, as seguintes visualizações:
 - 1.1.6.7.1.10.7. Quantidade de ocorrências de uma mesma vulnerabilidade
 - 1.1.6.7.1.10.8. Quantidade de vulnerabilidades por sistema operacional
 - 1.1.6.7.1.10.9. Quantidade de vulnerabilidades por host
 - 1.1.6.7.1.10.10. Quantidade de vulnerabilidades por Exploit disponível
 - 1.1.6.7.1.10.11. Quantidade de vulnerabilidades por produto/software vulnerável
 - 1.1.6.7.1.11. A solução deve permitir exportar buscas e filtros criados para um dashboard
 - 1.1.6.7.1.12. A solução deve permitir salvar filtros criados em buscas para reutilização
 - 1.1.6.7.1.13. Deve mostrar dashboards que apresentem variação histórica de vulnerabilidades novas, corrigidas, reabertas

- 1.1.6.7.1.14. Deve permitir mostrar dashboards que contenham quantidades de vulnerabilidades associadas a ransomware, que contém exploits públicos e que permitem exploração sem autenticação
- 1.1.6.7.1.15. Deve mostrar dashboards que mostrem o racional de vulnerabilidades que podem ser corrigidas através de patches
- 1.1.6.7.1.16. Deve mostrar patches faltantes em sistemas operacionais independente da relação com uma vulnerabilidade existente
- 1.1.6.8. Gestão de Configuração
 - 1.1.6.8.1. A solução deve permitir a avaliação e o relatório de problemas de configuração, com base nas referências do padrão da indústria do Centro de Segurança da Internet (CIS).
 - 1.1.6.8.2. O fabricante deve ser oficialmente certificado pelo CIS para fornecer este nível de controles.
 - 1.1.6.8.3. A solução deve oferecer avaliação de configuração com base no benchmark CIS padrão da indústria, cobrindo esta funcionalidade nas seguintes categorias:
 - 1.1.6.8.3.1. Sistemas operacionais
 - 1.1.6.8.3.2. Software de servidor
 - 1.1.6.8.3.3. Provedores de nuvem
 - 1.1.6.8.3.4. Dispositivos de rede
 - 1.1.6.8.3.5. Software de desktop
 - 1.1.6.8.4. A solução deve suportar detecção de falhas de conformidades através de varreduras autenticadas ou através de agente instalado diretamente no ativo monitorado.
 - 1.1.6.8.5. A solução deve permitir que os administradores recebam informação de conformidade de sistemas operacionais Windows e Linux, mesmo que não estejam conectados à rede corporativa.
 - 1.1.6.8.6. A solução deve permitir a avaliação de certificados digitais (internos e externos) e configurações de TLS em busca de problemas e vulnerabilidades, resultando em diferentes graus de conformidade de acordo com os resultados da avaliação de seu emissor, prazo de validade, tipo de certificado, robustez do o algoritmo e o conjunto de criptografia usados.
- 1.1.6.9. Detecção e priorização de ameaças
 - 1.1.6.9.1. A solução proposta deve permitir enviar alertas em tempo real sobre irregularidades na rede, identificar ameaças e monitorar mudanças inesperadas que ocorram.
 - 1.1.6.9.2. A solução deve permitir enviar notificações para usuários específicos e grupos de usuários para o perfil de monitoramento ou perfis de monitoramento múltiplos.
 - 1.1.6.9.3. A solução deve permitir a personalização do perfil de monitoramento associado a uma lista específica de critérios.
 - 1.1.6.9.4. A solução deve permitir que os alertas sejam personalizados para uma ampla variedade de condições que afetam sistemas, certificados, vulnerabilidades, portas, serviços e software. Cada regra deve permitir que seja configurada para detectar mudanças gerais comuns - para se ajustar a circunstâncias muito específicas.
 - 1.1.6.9.5. A solução deve permitir a atribuição de destinatários diferentes para cada alerta.

- 1.1.6.9.6. A solução deve enviar alertas de monitoramento sobre vulnerabilidades, configurações incorretas e outros parâmetros definidos pelo administrador da solução, incluindo:
 - 1.1.6.9.6.1. Ativos com sistemas operacionais não aprovados
 - 1.1.6.9.6.2. Certificados expirados ou expirando
 - 1.1.6.9.6.3. Portas abertas
 - 1.1.6.9.6.4. Vulnerabilidades graves
 - 1.1.6.9.6.5. Tickets de correção abertos, resolvidos e fechados
 - 1.1.6.9.6.6. Software não aprovado
- 1.1.6.9.7. A solução proposta deve fornecer fontes de inteligência de ameaças em tempo real e técnicas de aprendizado de máquina para fornecer controle de administrador sobre a evolução das ameaças relacionadas a vulnerabilidades encontradas nos ativos da organização e identificar quais corrigir primeiro.
- 1.1.6.9.8. A solução deve permitir consultas ad-hoc com múltiplas variáveis e critérios, como classe de ativo, tipo de vulnerabilidade, indicadores de ameaça em tempo real, etiqueta de ativo e sistema operacional, de modo que, por exemplo, seja possível pesquisar todas as vulnerabilidades que tenham um alta classificação de gravidade, são fáceis de explorar e foram lançados na semana passada.
- 1.1.6.9.9. A solução deve permitir que se faça uma correlação em tempo real das ameaças ativas contra as vulnerabilidades detectadas nos ativos corporativos.
- 1.1.6.9.10. A solução deve incluir indicadores de ameaças em tempo real que ajudem a avaliar e priorizar as vulnerabilidades detectadas, categorizados da seguinte forma:
 - 1.1.6.9.10.1. Vulnerabilidades para as quais não há patch disponível e para as quais um ataque ativo foi observado.
 - 1.1.6.9.10.2. Vulnerabilidades cujo mecanismo de exploração é conhecido, para o qual existe um código de exploração e está disponível publicamente.
 - 1.1.6.9.10.3. Vulnerabilidades que estão sendo ativamente utilizadas como fonte de ataques.
 - 1.1.6.9.10.4. Vulnerabilidades que permitem ao invasor espalhar o ataque amplamente pela rede violada.
 - 1.1.6.9.10.5. Vulnerabilidades que podem ser facilmente exploradas, exigindo poucas habilidades e pouco conhecimento.
 - 1.1.6.9.10.6. Vulnerabilidades cuja exploração causará perda massiva de dados.
 - 1.1.6.9.10.7. Vulnerabilidades cuja carga útil pode sobrecarregar ou impedir que sistemas comprometidos estejam permanentemente ou temporariamente disponíveis.
 - 1.1.6.9.10.8. Vulnerabilidades para as quais não há correção do provedor.
 - 1.1.6.9.10.9. Vulnerabilidades associadas a infecções por malware.
- 1.1.6.9.11. A solução deve atribuir uma pontuação a cada vulnerabilidade de forma contextual de forma a quantificar o risco associado a esta vulnerabilidade.
- 1.1.6.9.12. Os fatores de risco devem considerar pelo menos os fatores abaixo:
 - 1.1.6.9.12.1. Malwares associados
 - 1.1.6.9.12.2. Atores maliciosos associados

- 1.1.6.9.12.3. Possibilidade de remediação
- 1.1.6.9.13. A solução proposta deve fornecer um workflow de correção baseado em políticas de criação e atribuição, atribuindo tickets de acordo com as condições definidas pelo administrador da solução através de políticas ou manualmente.
- 1.1.6.9.14. A solução deve permitir a criação de tickets com status aberto, fechado, ignorado, com base nos seguintes critérios:
 - 1.1.6.9.14.1. Host(s) a quem a regra se aplica
 - 1.1.6.9.14.2. Vulnerabilidade(s) a que a regra se aplica
 - 1.1.6.9.14.3. Usuário atribuído
 - 1.1.6.9.14.4. Data de criação ou expiração
 - 1.1.6.9.14.5. Mudança de estado
- 1.1.6.9.15. A solução deve permitir a criação de tickets de correção automaticamente a partir do resultado de uma varredura de vulnerabilidade, com base nas informações de um host específico e também manualmente por um administrador de solução.
- 1.1.7. Gestão de Patches
 - 1.1.8. A solução proposta deve correlacionar vulnerabilidades e patches automaticamente para os hosts do IBGE contabilizando até 2100 servidores (dois mil e duzentos e dez servidores).
 - 1.1.9. A solução deve mapear automaticamente os patches com CVEs associados às vulnerabilidades detectadas.
 - 1.1.10. Deve mostrar patches faltantes mesmo que não exista correlação com uma vulnerabilidade existente
 - 1.1.11. A solução de Gestão de Patches deve ser do mesmo fabricante da solução de Gestão de Vulnerabilidades compartilhando a mesma console de gestão das soluções.
 - 1.1.12. Deve mostrar patches faltantes para no mínimo as seguintes categorias:
 - 1.1.12.1. Navegadores
 - 1.1.12.2. Ferramentas de compressão de arquivos
 - 1.1.12.3. Visualizadores de PDF
 - 1.1.12.4. Sistemas operacionais
 - 1.1.13. A solução deve permitir aplicação de patches de segurança para, no mínimo, as plataformas abaixo:
 - 1.1.13.1. Windows Server 2019 e posterior
 - 1.1.13.2. CentOS 7.x e 8.x
 - 1.1.13.3. Red Hat Enterprise Linux (RHEL)
 - 1.1.14. A solução deve possuir um catálogo com no mínimo 35.000 patches e permitir aplicação de patches para, no mínimo, os produtos abaixo:
 - 1.1.15. 7-Zip
 - 1.1.16. Acro Software CutePDF Writer
 - 1.1.17. AdoptOpenJDK JDK

- 1.1.18. AdoptOpenJDK JRE
- 1.1.19. Adobe Acrobat
- 1.1.20. Adobe Flash
- 1.1.21. Adobe Reader
- 1.1.22. Adobe Shockwave
- 1.1.23. AIMP DevTeam AIMP
- 1.1.24. Amazon Correo
- 1.1.25. Apache Software Foundaon Tomcat
- 1.1.26. Apple iCloud
- 1.1.27. Apple iTunes
- 1.1.28. Apple Mobile Device Support
- 1.1.29. Apple Software Update
- 1.1.30. Atlassian HipChat
- 1.1.31. Sourcetree
- 1.1.32. Audacity
- 1.1.33. Azul Zulu JDK
- 1.1.34. Azul Zulu JRE
- 1.1.35. Bandicam Company Bandicut
- 1.1.36. Blue Jeans
- 1.1.37. Blue Jeans Outlook Addin
- 1.1.38. Barco ClickShare
- 1.1.39. Botkind Allway Sync
- 1.1.40. Box Drive
- 1.1.41. Box Edit
- 1.1.42. Box Sync
- 1.1.43. CDBurnerXP
- 1.1.44. Cisco Jabber
- 1.1.45. Cisco WebEx Teams
- 1.1.46. Citrix GoToMeeng
- 1.1.47. Citrix Receiver
- 1.1.48. Citrix Workspace App
- 1.1.49. Code4ward.net Royal Applications
- 1.1.50. CoreFTP
- 1.1.51. Corel WinDVD Pro
- 1.1.52. dotPDN LLC Paint.NET

- 1.1.53. Dropbox
- 1.1.54. Evernote
- 1.1.55. FileZilla
- 1.1.56. Foxit PhantomPDF
- 1.1.57. Foxit Reader
- 1.1.58. Gimp
- 1.1.59. GIT
- 1.1.60. GlavSo TightVNC
- 1.1.61. Chrome
- 1.1.62. Google Drive
- 1.1.63. Google Desktop
- 1.1.64. Google Drive File Stream
- 1.1.65. Google Earth Pro
- 1.1.66. Gretech GOM Player
- 1.1.67. Inkscape
- 1.1.68. IrfanView
- 1.1.69. Jabra Direct
- 1.1.70. JAM Software TreeSizeFree
- 1.1.71. Juraj Simlovic TED Notepad
- 1.1.72. KeePass
- 1.1.73. LibreOffice
- 1.1.74. Lightning ImgBurn
- 1.1.75. LogMeIn
- 1.1.76. Malwarebytes An-Malware Home
- 1.1.77. Microsoft .Net
- 1.1.78. Microsoft .Net Core
- 1.1.79. AnXSS
- 1.1.80. Azure Site Recovery Provider
- 1.1.81. Azure Informaon Protecon Client
- 1.1.82. BizTalk Server
- 1.1.83. Business Contact Manager
- 1.1.84. CAPICOM
- 1.1.85. Microsoft Commerce Server
- 1.1.86. Microsoft Content Management Server
- 1.1.87. Windows Defender

- 1.1.88. Microsoft Digital Image
- 1.1.89. DirectX
- 1.1.90. Microsoft Dynamics
- 1.1.91. Microsoft Edge
- 1.1.92. Microsoft Enhanced Migration Experience Toolkit
- 1.1.93. Exchange Server
- 1.1.94. Exchange System Manager
- 1.1.95. Microsoft Expression
- 1.1.96. Forefront Server
- 1.1.97. Front Page Server
- 1.1.98. Host Integration Server
- 1.1.99. Microsoft Identity Manager
- 1.1.100. Internet Explorer
- 1.1.101. Internet Information Server
- 1.1.102. ISA Server
- 1.1.103. Microsoft Journal Viewer
- 1.1.104. Live Meeting
- 1.1.105. Live Messenger
- 1.1.106. Skype for Business Server
- 1.1.107. MDAC
- 1.1.108. Microsoft Mouse and Keyboard Center
- 1.1.109. Microsoft Step By Step Interactive Training
- 1.1.110. Mscomctl
- 1.1.111. MSN Messenger
- 1.1.112. MSXML
- 1.1.113. Office Communicator 2005
- 1.1.114. Office Web Components XP
- 1.1.115. Producer for PowerPoint 1.1
- 1.1.116. Small Business Accounting 2006
- 1.1.117. Works 6-9 Converter
- 1.1.118. Office Communicator 2007
- 1.1.119. Office Communications Server 2007 R2
- 1.1.120. Office Communicator 2007 R2
- 1.1.121. Producer for PowerPoint 2003
- 1.1.122. Suíte Office nas versões 2000, 2002, 2003, 2007, 2010, 2013, 2016
- 4.3.8.6.112. System Center Operations Manager

- 1.1.123. Microsoft SQL Server nas versões 2005, 2008, 2008 R2, 2012, 2014, 2016, 2017, 2019 4.3.8.6.114. SQL Management Studio
- 1.1.124. Microsoft Visual Studio
- 1.1.125. Windows Server 2012, 2016, 2019
- 1.1.126. A solução deve permitir a criação de dashboards para acompanhamento de aplicação de patches.
- 1.1.127. Os Dashboards devem permitir inclusão de filtros personalizados para incluir, no mínimo, os requisitos abaixo:
 - 1.1.127.1. Ativos que não possuem patches de segurança instalados ;
 - 1.1.127.2. Ativos pendentes de boot para aplicação de patches ;
 - 1.1.127.3. Patches faltantes por fabricante ;
 - 1.1.127.4. Status de aplicação de patches ;
 - 1.1.127.5. Patches faltantes por severidade ;
- 1.1.128. A solução deve permitir mostrar em um mesmo dashboard a quantidade de Ativos que possuem um software instalado e quantidade de patches relevantes a esse mesmo software
- 1.1.129. A solução deve conter uma lista de produtos e softwares priorizados, permitindo visualizar patches relevantes a esses produtos
- 1.1.130. A solução deve permitir a criação de tarefas de instalação a partir de produtos e softwares priorizados
- 1.1.131. A solução deve oferecer uma interface que permita buscas com uma sintaxe lógica para visualizar detalhes de um patch específico
- 1.1.132. As buscas devem considerar, no mínimo, os filtros abaixo:
 - 1.1.132.1. Fabricante da aplicação ou software
 - 1.1.132.2. Patches que corrigem falhas de segurança
 - 1.1.132.3. Patches de sistema operacional ou aplicações
 - 1.1.132.4. Severidade do fabricante
 - 1.1.132.5. Número do KB ou boletim
 - 1.1.132.6. CVE associado
- 1.1.133. A solução deve ser capaz de apresentar informações de patches que já consideram e resolvem correções anteriores
- 1.1.134. A solução deve apontar vulnerabilidades resolvidas por um determinado patch
- 1.1.135. A solução deve apontar todas as versões da aplicação que são afetadas e precisam de correção
- 1.1.136. A solução deve conter referências do fabricante do software ou sistema operacional contendo descrição dos patches disponíveis
- 1.1.137. Deve ser possível visualizar agentes, último status de comunicação, a quantidade de patches aplicados e faltantes
- 1.1.138. Deve ser possível definir o intervalo em horas para verificação de patches e reporte à console

- 1.1.139. A solução deve suportar tarefas de instalação e remoção dos patches
- 1.1.140. A solução deve permitir a execução de scripts personalizados durante a tarefa de instalação de patches
- 1.1.141. Deve ser possível executar scripts Powershell antes e depois da instalação de correções
- 1.1.142. A solução deve permitir instalação de softwares através de scripts
- 1.1.143. A tarefa de aplicação de patches deve permitir alteração de chaves de registro
- 1.1.144. A tarefa de aplicação de correções deve permitir selecionar manualmente os patches a serem aplicados ou através de um filtro de seleção que considere, no mínimo, severidade do patch, fabricante, associação a uma vulnerabilidade, associação a riscos de segurança
- 1.1.145. Deve ser possível restringir a aplicação de patches a um grupo de máquinas baseados em ranges de IP, software instalado, portas abertas, serviços em execução
- 1.1.146. Deve ser possível o agendamento de execução de tarefas de patch de forma imediata
- 1.1.147. Deve ser possível agendar a execução de tarefas de patch em um horário específico com recorrência diária, semanal ou mensal
- 1.1.148. Deve ser possível agendar a execução de tarefas de patch com agendamento a partir do Patch Tuesday, da Microsoft, de forma automática
- 1.1.149. Deve ser possível configurar uma janela de tempo máximo para execução de patches em intervalo de horas ou minutos
- 1.1.150. A solução deve permitir customização de mensagens para o usuário antes, durante e após a aplicação de patches
- 1.1.151. Deve permitir o download de patches antes do início da tarefa, de forma a otimizar o processo de instalação
- 1.1.152. A solução deve permitir a supressão do reinício do sistema operacional, forçá-la ou permitir que o usuário reinicie o sistema, caso o patch aplicado exija o reinício.
- 1.1.153. A solução deve permitir colocar em quarentena ativos em risco para evitar exploração.
- 1.1.154. A solução deverá isolar dispositivos da rede e ainda permitir o controle e a aplicação de patches remotos via a própria solução e outros recursos autorizados usando tecnologia de agente em nuvem.
- 1.1.155. A solução deverá disponibilizar ações de correção de vulnerabilidades não corrigidas e fornecer mitigações alternativas onde a correção pode causar interrupções.
- 1.1.156. Deve ser possível restringir o licenciamento a um determinado grupo de máquinas baseado em critérios como sistema operacional, presença de softwares instalados e ranges de IPs
- 1.1.157. A solução deve conter a inteligência de filtrar automaticamente, sem intervenção, quais Ativos receberão os patches selecionados na tarefa de patch considerando a arquitetura do sistema operacional e também a pré-existência de determinada aplicação, evitando assim instalações indesejadas;

- 1.1.158. Deve ser possível gerar relatórios a partir do catálogo de patches a serem aplicados considerando filtros dos patches e dos Ativos;
- 1.1.159. O catálogo de patches a serem aplicados deve filtrar de forma simples quais são os patches que precisam ser instalados e exibir somente as últimas versões disponíveis de cada um deles, considerando a obsolescência de versões antigas;
- 1.1.160. Deve ser possível visualizar, pela interface, o status de instalação de cada uma das tarefas de patch criadas;
- 1.1.161. O status individual de cada tarefa de patch deve mostrar quais patches foram instalados com sucesso, as quais falharam e quais não foram instalados por não serem necessários;
- 1.1.162. A solução deve exibir, para os patches que não foram instalados com sucesso, qual o motivo do erro;
- 1.1.163. Deve ser possível gerar um relatório CSV para uma tarefa de patch específica, com a finalidade de validar seu progresso e situação final de execução;
- 1.1.164. A solução deve possuir controle de acesso no modelo Role Based Access Control, para que sejam definidos no mínimo dois perfis de usuários caso seja necessário, sendo um deles, necessariamente, incapaz de iniciar uma tarefa de execução de patch;
- 1.1.165. A solução deve possuir uma interface de API para permitir automatização com no mínimo as seguintes funções:
 - 1.1.165.1. Criação de tarefa de patch;
 - 1.1.165.2. Listagem de Ativos;
 - 1.1.165.3. Listagem de patches;
 - 1.1.165.4. Listagem de tarefas de patch;
 - 1.1.165.5. Criação e geração de relatórios.
- 1.1.166. Varreduras dinâmicas de aplicações WEB e API's :
 - 1.1.166.1. A ferramenta deverá ser dimensionada para atender até 99 aplicações web;
 - 1.1.166.2. A ferramenta de varreduras dinâmicas de vulnerabilidades em aplicações web e API's deve ser do mesmo fabricante da solução de Gestão de Vulnerabilidades compartilhando a mesma console de gestão das soluções.
 - 1.1.166.3. A solução proposta deve habilitar varreduras profundas dinâmicas para descobrir e catalogar todos os aplicativos da web e APIs na rede corporativa externa, redes corporativas internas e instâncias de nuvem.
 - 1.1.166.4. A solução deve permitir varreduras autenticadas, complexas e progressivas.
 - 1.1.166.5. A solução deve suportar varreduras programadas de serviços SOAP e REST API.
 - 1.1.166.6. A solução deve contar com API e integração com Jenkins para automação em ambiente de CI / CD.
 - 1.1.166.7. A solução deve detectar, identificar, avaliar, rastrear os 10 principais riscos OWASP (Top 10), como injeção de SQL, Cross-site script (XSS), XML External Entity (XXE), autenticação interrompida e configurações incorretas, também ameaças de WASC, vulnerabilidades CWE e CVEs associados em aplicações da web.

- 1.1.166.8. A solução deve suportar a capacidade de re-testar uma vulnerabilidade específica que foi detectada anteriormente na aplicação web.
- 1.1.166.9. A solução deve ter capacidade de encontrar aplicações web aprovadas e não aprovadas em sua rede, gerando um processo contínuo de catalogação e descoberta de aplicações web.
- 1.1.166.10. A solução deve gerar tags para facilitar a localização e o uso de ativos de aplicações web encontrados.
- 1.1.166.11. A solução deve permitir que se faça a varredura de grandes aplicações da web usando um mecanismo de varredura progressiva, que deve permitir a varredura em estágios incrementais e evitar quaisquer restrições que possam surgir ao tentar fazer a varredura de um aplicativo de uma vez.
- 1.1.166.12. A solução deve definir a hora exata de início e duração das verificações.
- 1.1.166.13. A solução deve permitir gerenciar várias varreduras de aplicações web, combinando vários scanners para acelerar o processo e obter resultados mais rapidamente.
- 1.1.166.14. A solução deve permitir integração nativa ou por meio de conectores, APIs ou outros mecanismos compatíveis com pelo menos uma ferramenta de Web Application Firewall (WAF) amplamente utilizada no mercado, tais como F5, Fortinet, Imperva, Citrix NetScaler ou equivalente, desde que compatível com a infraestrutura tecnológica da contratante;
- 1.1.166.15. A solução deve permitir a consolidação de dados de varredura automatizada com dados provenientes de ferramentas de avaliação manual de vulnerabilidades, como Burp Suite, Bugcrowd ou equivalentes, de forma a proporcionar uma visão unificada das vulnerabilidades identificadas em aplicações web;
- 1.1.166.16. A solução deve fornecer relatórios resumidos e de varredura do site que podem ser exportados para os formatos HTML e PDF.
- 1.1.166.17. A solução deve oferecer suporte à criação de escopos e funções definidos pelo usuário e permitir que as permissões apropriadas sejam atribuídas a cada função.
- 1.1.167. Relatórios e dashboards:
 - 1.1.167.1. A solução proposta deve permitir administração centralizada via interface gráfica WEB usando HTTPS.
 - 1.1.167.2. A solução deve possibilitar o acesso a console de todos os componentes do serviço a partir de um único ponto.
 - 1.1.167.3. A solução deve permitir a definição de diferentes perfis de usuários e funções para administração.
 - 1.1.167.4. A solução deve fornecer controles de acesso de usuário hierárquicos e baseados em funções que permitam a delegação de responsabilidades para refletir a estrutura organizacional.
 - 1.1.167.5. A solução deve permitir o acesso de um usuário autorizado de qualquer local.
 - 1.1.167.6. A solução deve suportar integração com uma biblioteca API XML extensível.
 - 1.1.167.7. A solução deve suportar autenticação de dois fatores para login de usuários.
 - 1.1.167.8. A solução deve suportar configurações de segurança de senha.
 - 1.1.167.9. A solução deve suportar personalizar a política de segurança para configurações de gerenciamento de senha, por:

- 1.1.167.10. Idade e expiração da senha.
- 1.1.167.11. Conta do usuário bloqueada após uma série de logins com falha.
- 1.1.167.12. Comprimento mínimo da senha.
- 1.1.167.13. Complexidade da senha, caracteres alfanuméricos e numéricos a serem usados.
- 1.1.167.14. Forçar mudança de senha no login inicial
- 1.1.167.15. A solução deve permitir a configuração de notificações de expiração de senha com antecedência mínima parametrizável, de forma a alertar os usuários com vários dias de antecedência, conforme política de segurança da contratante.
- 1.1.167.16. A solução deve suportar a capacidade de restringir o acesso apenas a partir da rede interna da empresa.
- 1.1.167.17. A solução deve suportar a capacidade de rastrear a atividade do usuário por nome da conta do usuário, data, ação e informações sobre a ação.
- 1.1.167.18. A solução deve suportar a capacidade de distribuir relatórios em PDF com segurança por meio de uma senha e um número restrito de download de relatórios por meio do link.
- 1.1.167.19. A solução deve suportar acesso por SSO (Single Sign-on) usando SAML 2.0.
- 1.1.167.20. A solução deve permitir o controle de alterações com trilhas de auditoria à prova de violação.
- 1.1.167.21. A solução proposta deve gerar relatórios por IPs, Grupo e Tags
- 1.1.167.22. A solução deve permitir a geração de relatórios de qualquer IP - Host previamente verificado.
- 1.1.167.23. A solução deve permitir agendar relatórios diários, semanais, mensais e sob demanda.
- 1.1.167.24. A solução deve permitir o envio de notificações por e-mail sempre que um relatório estiver disponível para o administrador da solução, usuários específicos e perfis diferentes criados na ferramenta.
- 1.1.167.25. A solução deve permitir pelo menos os seguintes tipos de relatórios:
 - 1.1.167.25.1. Relatório de correção
 - 1.1.167.25.2. Relatório de vulnerabilidades altamente críticas
 - 1.1.167.25.3. Relatório Executivo
 - 1.1.167.25.4. Relatório de autenticação
 - 1.1.167.25.5. Relatório de conformidade normativa e regulatória
 - 1.1.167.25.6. Relatório de remediação
- 1.1.167.26. A solução deve fornecer relatórios de correção por grupo de ativos, usuário e vulnerabilidade.
- 1.1.167.27. A solução deve permitir a criação de relatórios baseados em IPv4, endereços IPv6, nome do host, grupo de ativos e rótulos personalizados pelo administrador.
- 1.1.167.28. A solução deve permitir relatórios com cálculo de risco de segurança, permitindo um cálculo de risco global para todos os ativos incluídos no relatório.

- 1.1.167.29. A solução deve permitir relatórios que possibilitem o cálculo do risco do negócio, utilizando como base para o cálculo do risco de impacto ao negócio e do risco de segurança dos ativos incluídos no relatório.
- 1.1.167.30. A solução deve permitir relatar as descobertas com base no status das vulnerabilidades detectadas e seu status, conforme lista abaixo:
 - 1.1.167.30.1. Novo
 - 1.1.167.30.2. Resolvido
 - 1.1.167.30.3. Reaberto
 - 1.1.167.30.4. Ativo
- 1.1.167.31. A solução deve permitir relatórios que incluam vulnerabilidades com base na data de publicação.
- 1.1.167.32. A solução deve permitir incluir e excluir kernels Linux detectados na varredura de vulnerabilidade e que não estejam em execução.
- 1.1.167.33. A solução deve permitir a exclusão de vulnerabilidades encontradas em uma porta ou serviço que não esteja em execução.
- 1.1.167.34. A solução deve permitir excluir vulnerabilidades que não sejam exploráveis devido à configuração do sistema ou plataforma onde foi detectada.
- 1.1.167.35. A solução deve permitir a exclusão de patches da Microsoft que foram substituídos por um novo patch ou um patch cumulativo do mesmo fabricante.
- 1.1.167.36. A solução deve fornecer relatórios automatizados de tendências e diferenciais.
- 1.1.167.37. A solução deve fornecer várias opções de distribuição de relatórios, incluindo PDF criptografado.
- 1.1.167.38. A solução deve dar suporte à personalização do modelo de relatório conforme necessário.
- 1.1.167.39. A solução deve permitir a exportação de relatórios para os formatos HTML, MHT, PDF, DOC, CSV e XML
- 1.1.167.40. A solução deve permitir que relatórios sejam apresentados em tabelas e gráficos com as ocorrências ocorridas, permitindo a customização detalhada de cada relatório.
- 1.1.167.41. A solução deve permitir em seus relatórios comparar o nível de conformidade entre políticas, tecnologias e ativos.
- 1.1.167.42. A solução deve possuir um painel que, por padrão, permite que você veja as tendências de vulnerabilidades por gravidade, plataforma, idade e status de remediação.
- 1.1.167.43. A solução deve permitir a customização dos painéis fazendo uso de qualquer um dos dados disponíveis associados aos ativos varridos para selecionar diferentes tipos de gráficos, tabelas e visualizações sobre a priorização de vulnerabilidades.
- 1.1.167.44. A solução deve fornecer painéis executivos personalizáveis com uma visão unificada de todos os componentes da solução.
- 1.1.167.45. Deve ser possível criar dashboards que mostrem a pontuação de risco global de ativos e sua variação ao longo do tempo.

1.1. Teste de Invasão

1.1.1. Escopo

- 1.1.1.1. Os Testes de Invasão deverão contemplar tanto a infraestrutura quanto as aplicações, devendo ser realizados a partir do ambiente interno e externo a cada três meses.
- 1.1.1.2. O teste de Infraestrutura avaliará a possibilidade de exploração e comprometimento para até 254 (duzentos e cinquenta e quatro) endereços IPs, definidos pelo IBGE.
- 1.1.1.3. O teste de aplicações web avaliará a possibilidade de exploração e comprometimento de até 50 (cinquenta) aplicações web definidas pelo IBGE, podendo ocorrer retestes caso necessário;
- 1.1.1.3.1. O teste de aplicações web avaliará a possibilidade de exploração considerando as prerrogativas abaixo, onde deverão ser realizados minimamente, as seguintes verificações:
 - 1.1.1.3.1.1. “Cross Site Scripting (XSS)”;
 - 1.1.1.3.1.2. “Injeção de Código”;
 - 1.1.1.3.1.3. “Inclusão Remota de Arquivos (RFI)”;
 - 1.1.1.3.1.4. Deverão ser realizados mapeamentos e sondagens, com o objetivo de identificar possíveis vetores de entradas de ataques;
 - 1.1.1.3.1.5. “Referência Direta a Objetos”.
 - 1.1.1.3.1.6. “Vazamento de informações”, onde deve ser verificada a exposição inadvertida de informações sobre a aplicação e o servidor que a hospeda.
 - 1.1.1.3.1.7. “Gerenciamento de Sessões”.
 - 1.1.1.3.1.8. Pelo menos, as vulnerabilidades dos últimos dois relatórios OWASP Top 10.
- 1.1.1.3.2. Caso necessário, devem ser criados ataques customizados baseados na arquitetura das aplicações.
- 1.1.1.4. Serviço de Auditoria de Segurança em Códigos Fonte de Aplicações
 - 1.1.1.4.1. Para a realização das auditorias o IBGE disponibilizará, quando permitido, o código-fonte da aplicação a ser auditada, que deverá ser mantida sob sigilo pela CONTRATADA.
 - 1.1.1.4.2. A auditoria de códigos-fonte visa avaliar, dentre outros itens, os seguintes conceitos:
 - 1.1.1.4.2.1. Avaliação do fluxo de informações indo desde a arquitetura física (ex: fluxo de informações entre camadas web, camadas de aplicação e bancos de dados) até o fluxo de informações entre os módulos - variáveis e parâmetros.
 - 1.1.1.4.2.2. Avaliação das lógicas de negócio requisitadas e implementadas. Detecção de possíveis fraudes internas ou vulnerabilidades na implementação das lógicas de negócio.
 - 1.1.1.4.2.3. Avaliação da utilização das APIs e construtos da linguagem de programação apontamento dos locais no código onde é feito uso inseguro das bibliotecas do sistema, dos elementos da linguagem de programação e recomendações de correção classificadas por risco e custo.

- 1.1.1.4.2.4. Avaliação da exposição do código-fonte e das regras de negócio para entidades externas apontando os aspectos do código que estariam mais sujeitos a permitir o vazamento de segredos.
- 1.1.1.5. Uma vez que o objetivo destes testes é garantir a segurança do ambiente, e não comprovar a existência de brechas, deverá ser utilizada a “Técnica da caixa branca”, onde o avaliador terá acesso irrestrito a qualquer informação que possa ser relevante ao teste;
- 1.1.1.6. As atividades utilizadas para a execução dos testes não se resumirão apenas ao uso de ferramentas, devendo incluir também procedimentos e técnicas com interação humana e não oferecidos por ferramentas conhecidas
- 1.1.1.7. Os Testes de Invasão envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos e informações do IBGE, e devem observar orientações e técnicas emanadas por padrões internacionais ou equivalente apresentados pela empresa CONTRATADA, caso possua, em seu portfólio, normativos que complementem os demonstrados abaixo:
 - 1.1.1.7.1. OSSTMM 3 (The Open Source Security Testing Methodology Manual: at least those three channels PHYSSEC, SPECSEC, COMSEC or/and any new one which will be defined);
 - 1.1.1.7.2. ISSAF/PTF (Information Systems Security Assessment Framework);
 - 1.1.1.7.3. NIST Special Publication 800-115 (Technical Guide to Information Security Testing and assessment);
 - 1.1.1.7.4. NIST Special Publication 800-42 (Guideline on Network Security Testing)
 - 1.1.1.7.4.1. OWASP TESTING GUIDE 3.0 – The Open Web Application Security Project.
 - 1.1.1.7.4.2. PCI DSS (Payment Card Industry Data Security Standard)
 - 1.1.1.7.4.3. PCI SSC Information Supplement
 - 1.1.1.7.4.4. PTES (Penetration Testinf Execution Standard)
- 1.1.1.8. **Considerações gerais**
 - 1.1.1.8.1. Os alvos dos testes a serem efetuados, assim como suas condições serão definidos em reunião prévia entre a CONTRATADA e o IBGE;
 - 1.1.1.8.2. Todas as fases (ciclos) dos “Testes de Invasão” poderão ser acompanhadas e supervisionadas a qualquer momento pelo IBGE;
 - 1.1.1.8.3. A CONTRATADA não deverá alterar a integridade das informações, ou seja, não deve alterar informações dos servidores e sistemas que possam comprometer os serviços do IBGE;
 - 1.1.1.8.4. Cada fase deve ser feita durante o período que não comprometa processamento da CONTRATANTE e que as agências estejam fechadas sendo feita em no máximo 2 dias corridos no total;
 - 1.1.1.8.5. Os testes e avaliações poderão ser interrompidos por solicitação expressa do IBGE a qualquer momento;
 - 1.1.1.8.6. Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo deverá ser imediatamente reportada ao IBGE, haja vista a necessidade do IBGE de manter a disponibilidade dos seus ambientes, ativos e serviços;

- 1.1.1.8.7. Deve ser comunicado ao IBGE, e devidamente documentado, o andamento da análise/teste, especialmente se identificada uma situação crítica.
- 1.1.1.8.8. Cada teste de invasão deverá obedecer às seguintes fases:
 - 1.1.1.8.8.1. Planejamento;
 - 1.1.1.8.8.2. Descoberta;
 - 1.1.1.8.8.3. Ataque;
 - 1.1.1.8.8.4. Relatório de Teste de Invasão;
 - 1.1.1.8.8.5. Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste;
 - 1.1.1.8.8.6. Reavaliação, novo teste pós remediação (RETESTE);
 - 1.1.1.8.8.7. Relatório final do Teste de Invasão;
 - 1.1.1.8.8.8. Maturidade do IBGE e Matriz de risco.
- 1.1.1.9. **Planejamento:**
 - 1.1.1.9.1. Todas as premissas, processos, atividades descritas, inclusive os cronogramas serão detalhados e apresentados na fase de planejamento para os tipos de teste de penetração a seguir:
 - 1.1.1.9.1.1. PENTEST DE REDE: Este teste é focado em recursos de rede, onde o escopo é definido em termos de endereços IP e intervalos de rede. Os testes de rede externa também podem ter o escopo definido em termos de nomes de domínio (o avaliador precisa descobrir os endereços de rede associados a esses domínios como parte do teste).
 - 1.1.1.9.1.2. PENTEST DE APLICAÇÃO: Este teste é focado em aplicação, geralmente aplicação web, mobile e cliente/servidor. Os avaliadores se concentrarão em encontrar e explorar vulnerabilidades somente nessa aplicação.
 - 1.1.1.9.1.3. PENTEST DE REDE SEM FIO: Este teste é semelhante a um pentest de rede, mas o escopo é definido por redes sem fio, tanto faz se especificadas diretamente pelos identificadores de conjunto de serviços (SSIDs) e localização física ou apenas por localização (por exemplo, "qualquer rede sem fio em nosso Prédio de escritórios principais").
 - 1.1.1.9.1.4. PENTEST DE ACESSO REMOTO: este teste é semelhante a pentest de rede, mas o escopo é definido em pontos específicos de acesso à rede corporativa (como VPN de acesso remoto de funcionários ou VPN B2B)
 - 1.1.1.9.1.5. PENTEST DE ENGENHARIA SOCIAL: quando os testes incluem a tentativa de enganar as pessoas para fornecer dados confidenciais ou privilégios de acesso ao avaliador, os tipos de truques a serem executados (como golpes de telefone, tentativas de phishing ou acesso físico) e alvos autorizados (como pessoas que podem ser alvo do teste, incluindo executivos, agentes do call center ou qualquer pessoa no escritório principal) são parte da definição do escopo.
 - 1.1.1.9.1.6. TESTE FÍSICO OU DE INSTALAÇÕES: estes testes abrangem controles de segurança física, como controle de acesso a instalações e recursos de TI. Um teste típico de segurança física pode incluir acesso a um centro de dados e acesso direto aos racks dos servidores. Também pode ser focado em ambientes de escritório, verificando a disponibilidade de informações confidenciais em

papel ou acesso a desktops e laptops dos usuários.

1.1.1.9.2. Deverá ser elaborado o “PLANO DE TESTE DE PENETRAÇÃO”, para cada teste ou reavaliação, contemplando as informações de PLANEJAMENTO do teste, tais como:

1.1.1.9.2.1. Objetivos, premissas e escopo do teste, datas e horas dos testes, realizações, metodologias, vulnerabilidades encontradas, categorização e severidade das vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades, apresentação das evidências apuradas, fontes de pesquisa, referências e ferramentas utilizadas.

1.1.1.9.3. Também na fase de planejamento, deverão ser atendidas e apresentadas, no mínimo, as seguintes informações:

1.1.1.9.3.1. Detalhes da infraestrutura alvo dos testes de invasão;

1.1.1.9.3.2. Equipamentos e recursos demandados para este teste;

1.1.1.9.3.3. Tipos de ataque que serão realizados;

1.1.1.9.3.4. Prazos (janela de tempo para execução dos testes);

1.1.1.9.3.5. Contato da CONTRATADA (responsáveis para tratamento de questões não abordadas nos testes);

1.1.1.9.4. A CONTRATADA deverá elaborar o “Plano de Teste de Invasão”, para cada teste que será realizado, contemplando as informações de planejamento do teste, tais como: objetivos, premissas e escopo do teste, metodologia de análise de vulnerabilidades, equipe envolvida, prazos do teste, de acordo com as informações abaixo:

1.1.1.9.4.1. O planejamento abrange a definição dos elementos a serem avaliados/testados, bem como a definição dos testes em si e o cronograma de execução. Deve ser realizado previamente, e em conjunto com o IBGE, sendo obrigatória, a autorização formal do IBGE antes da execução.

1.1.1.9.4.2. Deve apresentar todo o detalhamento das análises e testes a serem realizados, desde os ativos que serão testados, procedimentos adotados, técnicas e ferramentas utilizadas, entre outras informações que possam ser relevantes ou solicitadas.

1.1.1.9.4.3. Deve ser demonstrado e explanado a finalidade de cada ferramenta a ser utilizada, para avaliação e autorização prévia do IBGE.

1.1.1.9.4.4. Os testes e avaliações não poderão impactar o pleno funcionamento dos recursos testados, o que deve ser considerado na definição do cronograma. Caso o IBGE entenda que haja algum risco neste sentido, solicitará modificação da metodologia e/ou do cronograma, inclusive podendo requerer a execução em finais de semana, feriados ou fora do horário comercial.

1.1.1.9.4.5. Deverão ocorrer no mínimo 04 (quatro) reuniões de planejamento no IBGE a cada ano, sendo possível por parte do IBGE, solicitar demais reuniões presenciais ou remotas para alinhamento de informações adicionais relativas a esta etapa de planejamento.

1.1.1.9.4.6. Todas as ferramentas e recursos utilizados para a prestação dos serviços são de responsabilidade da CONTRATADA.

1.1.1.10. Descoberta:

- 1.1.1.10.1. O serviço deve contemplar a realização de análise de vulnerabilidade, visando identificar pontos de falha em suas configurações e versões que possam implicar em não atendimento as melhores práticas de segurança estabelecidas pelo mercado, além de identificar possíveis vulnerabilidades presentes em ativos, servidores, aplicações, sistemas, serviços, versões e configurações em produtos atualmente em uso pelo IBGE;
- 1.1.1.10.2. Os endereços IPs externos a serem testados serão definidos pelo IBGE durante a etapa de planejamento. Estes endereços IPs podem não ser todos pertencentes diretamente ao IBGE e, não necessariamente farão parte do mesmo bloco de endereços;
- 1.1.1.10.3. Neste processo é aceito o uso de ferramentas automatizadas de escaneamento próprias e padrões de mercado.
- 1.1.1.10.4. A análise de vulnerabilidade deve considerar as principais vulnerabilidades informadas pelos principais meios de informações até a data de execução da análise, tais como fabricante de softwares, canais de divulgações de vulnerabilidades, além de recomendações aceitas como boas práticas pelo mercado.
- 1.1.1.10.5. O método de análise de vulnerabilidades deve contemplar, no mínimo, não restringindo-se somente a estes, os seguintes itens:
 - 1.1.1.10.5.1. Identificação de pontos de entrada;
 - 1.1.1.10.5.2. Mapeamento todas as portas abertas e serviços;
 - 1.1.1.10.5.3. Descoberta de ativos, servidores, aplicações, sistemas, serviços e configurações;
 - 1.1.1.10.5.4. Identificação versões utilizadas e informar se esta é a versão atualizada;
 - 1.1.1.10.5.5. Testes de configuração;
 - 1.1.1.10.5.6. Testes de vulnerabilidades;
 - 1.1.1.10.5.7. Vetores de acesso;
 - 1.1.1.10.5.8. Vetores de criação;
 - 1.1.1.10.5.9. Vetores de alteração;
 - 1.1.1.10.5.10. Vetores de exclusão;
 - 1.1.1.10.5.11. Vetores de negação de serviço (comprometimento geral/parcial);
 - 1.1.1.10.5.12. Análise de mensagens de erro;
 - 1.1.1.10.5.13. Identificação da vulnerabilidade (de acordo com CVE- <http://cve.mitre.org/>), problema, bug, erro ou item em não conformidade com boas práticas de segurança.
- 1.1.1.10.6. O mapeamento deve ser proativo, identificando as ameaças confirmadas e ameaças potenciais, mapeando o grau do risco e classificando conforme padrões de mercado.
- 1.1.1.10.7. Todos os endereços IPs, ativos, servidores, aplicações, sistemas, serviços, versões e configurações foco da análise, devem ser previamente aprovados pelo IBGE, que pode eventualmente impedir alguns tipos de análises, bem como solicitar análises específicas, com foco de verificar a segurança de determinado ativo.
- 1.1.1.10.8. O resultado da análise deve seguir as seguintes etapas e conter os seguintes itens para análise de vulnerabilidades de infraestrutura:

- 1.1.1.10.8.1. Identificação e explicação do endereço IPs, ativos, servidores, aplicações, sistemas, serviços, versões e configurações encontrados;
- 1.1.1.10.8.2. Identificação de vulnerabilidades;
- 1.1.1.10.8.3. Metodologia utilizada passo-a-passo (descrição do teste);
- 1.1.1.10.8.4. Resultados obtidos (descrição do resultado);
- 1.1.1.10.8.5. Evidência do teste;
- 1.1.1.10.8.6. Classificação e priorização das vulnerabilidades por risco (seguindo o padrão CVSS);
- 1.1.1.10.8.7. Controles mitigatórios aplicáveis;
- 1.1.1.10.8.8. Definição da recomendação técnica para solução.

1.1.1.11. Ataque

- 1.1.1.11.1. Os testes devem incluir pelo menos as seguintes atividades, não se restringindo somente a estas:
 - 1.1.1.11.1.1. Leitura/Alteração/exclusão de configurações;
 - 1.1.1.11.1.2. Fingerprint;
 - 1.1.1.11.1.3. Descoberta da senha de acesso do ativo;
 - 1.1.1.11.1.4. Escalonamento(salto) de acessos, até o ponto máximo possível.
- 1.1.1.11.2. Os testes devem ser feitos nas seguintes camadas:
 - 1.1.1.11.2.1. Aplicação;
 - 1.1.1.11.2.2. Apresentação;
 - 1.1.1.11.2.3. Sessão;
 - 1.1.1.11.2.4. Transporte;
 - 1.1.1.11.2.5. Rede.
- 1.1.1.11.3. Os testes de infraestrutura devem avaliar a possibilidade de exploração, comprometimento e/ou vulnerabilidades de:
 - 1.1.1.11.3.1. Servidores (diversas plataformas);
 - 1.1.1.11.3.2. Serviços (web, ftp, telnet, e-mail, dns, outros);
 - 1.1.1.11.3.3. Ativos de rede (Firewall, Firewall de aplicação, IPS, Switches, Roteadores, Soluções de Balanceamentos, outros).
- 1.1.1.11.4. Nos testes deve ser utilizado a última metodologia disponível OSSTMM, item “Testes de Segurança em Rede de Dados (Capítulo 11 - Data Networks Security Testing)”.
- 1.1.1.11.5. Deve ser imediatamente comunicado ao IBGE cada salto (escalonamento de acesso) de endereços IPs, ativos, servidores, aplicações, sistemas, serviços ou domínios efetuados com sucesso, durante a realização de todos os testes manuais.
- 1.1.1.11.6. Os testes de aplicações web devem englobar baseados na publicação OWASP TESTING GUIDE 3.0 (The Open Web Application Security Project):
 - 1.1.1.11.6.1. Aplicações acessadas via internet ou Intranet;
 - 1.1.1.11.6.2. Portais web disponíveis;

- 1.1.1.11.6.3. Serviços web diversos detectados;
- 1.1.1.11.6.4. Webservices;
- 1.1.1.11.6.5. Sockets.
- 1.1.1.11.7. A critério do IBGE, será definido qual escopo de usuários utilizado em cada teste, podendo ser definidos um ou mais destes critérios para uma mesma aplicação:
 - 1.1.1.11.7.1. Sem credenciais;
 - 1.1.1.11.7.2. Credenciais comuns;
 - 1.1.1.11.7.3. Credenciais de administrador.
- 1.1.1.11.8. Os testes devem contemplar todas as páginas, telas e transações disponíveis na aplicação, incluindo páginas/telas disponíveis para usuários sem credencias, com credencias, páginas/telas de administração, bem como demais existentes.
- 1.1.1.11.9. Os testes em aplicações devem contemplar as seguintes fases e itens em seu planejamento e execução, não se limitando somente a estes:
 - 1.1.1.11.9.1. Coleta de Informações;
 - 1.1.1.11.9.2. Teste de lógica de negócios;
 - 1.1.1.11.9.3. Teste de autenticação;
 - 1.1.1.11.9.4. Gerenciamento de Sessões;
 - 1.1.1.11.9.5. Testes de validação de Dados;
 - 1.1.1.11.9.6. Teste de Web Services;
 - 1.1.1.11.9.7. Negação de Serviço.
- 1.1.1.11.10. Deve incluir os testes listados e descritos nas duas últimas versões do TOPTEN disponibilizadas pela OWASP;
- 1.1.1.11.11. Pentest deve incluir a avaliação funcional de segurança, inspeção de segurança de código fonte e a avaliação de vulnerabilidade, sobre uma aplicação genérica de porte médio em uma ou mais das linguagens abaixo definidas:
 - 1.1.1.11.11.1. Java
 - 1.1.1.11.11.2. C#
 - 1.1.1.11.11.3. C, C++, Objective-C
 - 1.1.1.11.11.4. Python
 - 1.1.1.11.11.5. Power Builder
 - 1.1.1.11.11.6. Perl
 - 1.1.1.11.11.7. Basic, VB, VB.NET, VBScript
 - 1.1.1.11.11.8. HTML5, JavaScript
 - 1.1.1.11.11.9. .NET, ASP
 - 1.1.1.11.11.10. E demais a ser informada na reunião prévia entre a CONTRATADA e o IBGE.
- 1.1.1.11.12. Avaliação funcional de segurança com análise de código e segurança em software que consiste em avaliação automatizada seguida por inspeção manual por amostragem;

1.1.1.11.13. Numa primeira verificação, o analista irá executar um sistema de inspeção automatizada de código fonte. O sistema de Avaliação funcional de segurança com análise de código e segurança em software irá destacar trechos do código que considerar sensíveis. A atividade de inspeção de código tem por objetivo:

- 1.1.1.11.13.1. Indicar código malicioso inserido pelo desenvolvedor;
- 1.1.1.11.13.2. Apontar código inseguro e sugerir melhorias;
- 1.1.1.11.13.3. Identificar vulnerabilidades latentes;
- 1.1.1.11.13.4. Apontar uso de funções do sistema operacional com problemas conhecidos de segurança;
- 1.1.1.11.13.5. Indicar implementações de controles de segurança fora dos padrões e normas.

1.1.1.11.14. Cada ponto fraco identificado é apontado com o código correspondente, descrição do problema e forma de solução.

1.1.1.11.15. Deve ser feita uma análise detalhada e manual do código-fonte do aplicativo. Muitas das vulnerabilidades detectadas em uma análise de código-fonte são semelhantes às vulnerabilidades detectadas durante um Teste de penetração de aplicativo.

1.1.1.11.16. Deve-se personalizar o plano de teste para adequar a tecnologia usada pelo aplicativo.

1.1.1.12. Relatório de Teste de Invasão, maturidade do IBGE e matriz de risco:

1.1.1.12.1. A CONTRATADA deverá elaborar “Relatório de Teste de Invasão/ Maturidade do IBGE e Matriz de risco” para cada teste realizado apresentando todas as informações sobre o mesmo, contemplando no mínimo:

- 1.1.1.12.1.1. Objetivos, premissas e escopo do teste;
- 1.1.1.12.1.2. Metodologia de análise de vulnerabilidades;
- 1.1.1.12.1.3. Descrição das ações realizadas;
- 1.1.1.12.1.4. Vulnerabilidades encontradas;
- 1.1.1.12.1.5. Categorização e severidades vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades;
- 1.1.1.12.1.6. Apresentação das evidências apuradas;
- 1.1.1.12.1.7. Fontes de pesquisa, pontos positivos encontrados, referências e ferramentas utilizadas.

1.1.1.12.2. Deverão ser entregues os relatórios:

- 1.1.1.12.2.1. Relatório Executivo, com considerações e recomendações: Relatório a ser entregue ao final do ciclo, que deverá conter um histórico com a evolução da situação real do ambiente diante das análises e testes aplicados, bem como processo de mitigação e verificações feitas que elenquem as conclusões do trabalho, recomendações referentes às vulnerabilidades identificadas e exploradas resolvidas e não resolvidas, conforme requisitos deste documento.
- 1.1.1.12.2.2. Relatório Detalhado: O relatório deve ser entregue ao final de cada ciclo contendo todos os procedimentos efetuados e seus resultados, com a identificação do problema de segurança, explicação do procedimento detalhado, evidência do teste (incluindo filmagens dos ataques bem sucedidos),

recomendações concretas e detalhadas para aprimoramento e correção das falhas e vulnerabilidades exploradas. Este deve descrever o passo-a-passo de como a vulnerabilidade/falha pode ser explorada, para efeito de validação da solução aplicada por parte do IBGE, e atender itens conforme requisitos deste documento.

- 1.1.1.12.3. Os relatórios deverão ser validados junto ao IBGE, onde poderão ser solicitadas tantas alterações e correções quantas forem necessárias, até que se chegue a uma versão final aceita por ambas as partes.
- 1.1.1.12.4. Não serão aceitos relatórios obtidos diretamente por ferramentas automatizadas utilizadas para a realização dos testes, sem a devida transcrição e contextualização adequada, bem como atendimento de todos os requisitos do edital.
- 1.1.1.12.5. Os relatórios devem ser entregues na língua portuguesa com atendimento aos requisitos do edital.
- 1.1.1.12.6. As entregas devem ser realizadas por meio físico e/ou digital a ser definido pelo IBGE. Se digital disponibilizar: 1 arquivo .doc não protegido contra gravação e 1 arquivo .pdf assinado digitalmente com certificado digital ICP Brasil; e protegido por criptografia que deverá conter no mínimo código hash de cada documento, a fim de garantir integridade destas entregas. A versão digital dos documentos deverá ser assinada digitalmente com certificado digital ICP Brasil.
- 1.1.1.12.7. Para auxiliar na solução para correção das vulnerabilidades identificadas, o relatório deve indicar ao IBGE mais de uma opção de correção para cada item de vulnerabilidade identificado. Estas opções devem ser validadas com IBGE durante a redação dos relatórios, de forma que considerem as peculiaridades do ambiente IBGE, até o aceite final do mesmo.
- 1.1.1.12.8. A CONTRATADA deve fornecer ao IBGE todas as informações necessárias para correção da vulnerabilidade, clarificando eventuais dúvidas durante a vigência de todo o contrato.
- 1.1.1.13. Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste:
 - 1.1.1.13.1. Ao final de ciclo, deve ser realizada uma apresentação detalhada, nas dependências do IBGE no Rio de Janeiro ou remotamente, conforme solicitação do IBGE, com local a ser definido posteriormente, das documentações e conclusões.
- 1.1.1.14. Reavaliação, novo teste após remediação
 - 1.1.1.14.1. A contratada fará novos testes do mesmo tipo, no próximo ciclo, após a correção das vulnerabilidades apontadas no respectivo relatório por parte do IBGE.
- 1.1.1.15. Restrições e Limites
 - 1.1.1.15.1. As janelas de tempo para a execução dos testes serão acordadas entre CONTRATADA e IBGE, priorizando sempre os períodos/horários de menor pico de forma a não impactar no negócio.

Restrição	Exemplo	Razão da Restrição
Tempo de restrição	Teste de intrusão só poderá ser feito durante final de semana ou dia não útil	Reduzir risco de causar impacto durante horas de trabalho normal para assegurar que as atividades do teste sejam

TERMO DE REFERÊNCIA - SERVIÇOS DE TIC - LICITAÇÃO

		controladas e monitoradas devidamente.
Tipo de teste	Não executar teste de engenharia social	Focar na análise dos resultados técnicos somente
	Não executar ataque de força bruta em sistema com autenticação	Evitar problemas de bloqueio de credenciais advindo do ataque de força bruta.
IPs e aplicações	Não executar teste em IPs não especificados no escopo	Evitar ambiente compartilhado
	Teste não deve envolver determinado componente de sistema X	Evitar impacto no negócio com corrupção/interrupção de determinado sistema

1.1.1.15.2. Em caso de problemas durante a execução dos testes de invasão o IBGE acionará a CONTRATADA para manutenções corretivas. Ao acionar a CONTRATADA o IBGE classificará o problema em um dos níveis de criticidade da tabela a seguir. Cada nível de severidade possui diferentes níveis mínimos de serviço, conforme descrito também nas tabelas a seguir:

CLASSIFICAÇÃO DE EVENTOS	
(A) EMERGENCIAL	São consideradas como “Emergência” todas as falhas cujas consequências tenham impactos sobre o serviço, rede , tráfego de dados e sincronismo e/ou recursos de manutenção que exigem ação corretiva imediata (independente da hora do dia ou do dia da semana).
(B) ALTA PRIORIDADE	Situações que podem configurar uma severidade emergencial. São situações potenciais e exigem atenção imediata. São situações potenciais que precedem, em sua maioria, uma situação que pode ser classificada num segundo momento como severidade emergencial.
(C) MÉDIA PRIORIDADE	Problemas que não prejudicam significativamente o funcionamento dos sistemas / serviços. São problemas graves ou perturbações que afetam uma área específica de determinada funcionalidade. Exemplos: degradação de desempenho, perda de funcionalidades.
(D) BAIXA PRIORIDADE E CONSULTA	Consulta geral e problemas secundários que têm um efeito pequeno na funcionalidade do produto. Ex.: Falhas de documentação, falhas no projeto e questionamentos operacionais.

1.1.2. Alerta de vulnerabilidades

1.1.2.1. Deve ser entregue, pelo menos, um relatório semanal descrevendo as novas

vulnerabilidades publicadas por seus respectivos fabricantes, em português. Tal relatório deve conter, ao menos:

- 1.1.2.1.1. Fabricante que publicou a vulnerabilidade;
- 1.1.2.1.2. Produtos envolvidos;
- 1.1.2.1.3. Descrição da vulnerabilidade;
- 1.1.2.1.4. Solução proposta para mitigação ou eliminação da vulnerabilidade.
- 1.1.2.2. Devem estar inclusas as vulnerabilidades de todos os softwares de prateleira existentes no parque da CONTRATANTE (Sistemas Operacionais, Bancos de Dados, Aplicativos de escritório, entre outros).
 - 1.1.2.2.1. A definição de tais softwares deve ser realizada no momento da adoção do serviço.
- 1.1.3. Controle das vulnerabilidades
 - 1.1.3.1. De modo a garantir a redução constante do risco, deverão ser implantadas as seguintes ações:
 - 1.1.3.2. Abertura de chamado no sistema da CONTRATANTE para tratamento de cada vulnerabilidade ou conjunto de vulnerabilidades identificadas e que não estejam no escopo de atuação da CONTRATADA;
 - 1.1.3.3. Acompanhamento da implementação do Plano de Remediação e da correção efetiva da vulnerabilidade identificada;
 - 1.1.3.4. Validação das correções aplicadas e sugeridas pelo Plano de Remediação, incluindo reteste do ativo para validar a efetividade da ação realizada;
 - 1.1.3.5. Atualização diária da lista de vulnerabilidades existentes no parque, considerando as correções aplicadas e as novas vulnerabilidades divulgadas no relatório de alerta de vulnerabilidades.
 - 1.1.3.6. A contratada deverá disponibilizar profissionais para sanar quaisquer dúvidas relativas as vulnerabilidades identificadas, bem como testar novamente as vulnerabilidades corrigidas.
- 1.1.4. GERENCIAMENTO DE RISCOS
 - 1.1.4.1. Quanto ao gerenciamento de riscos a CONTRATADA deverá:
 - 1.1.4.1.1. Estabelecer uma matriz de riscos juntamente com a Administração do IBGE e propor ações de tratamento desses riscos (mitigação, eliminação, transferências, etc);
 - 1.1.4.1.2. Realizar ações de análise de riscos, visando a criação de uma matriz em conformidade com as diretrizes da administração da Contratada;
 - 1.1.4.1.3. Elaborar um documento para que seja avaliado e homologado pela Contratada, contendo minimamente a matriz de riscos, os processos de mitigação e tratamento dos riscos reportados;
 - 1.1.4.1.4. Realizar análises de risco de segurança para cada contratação tecnológica a ser realizada pela CONTRATANTE;
 - 1.1.4.1.5. Acompanhar e realizar ações de cobrança junto aos responsáveis para cada ação definida nos processos de mitigação e tratamento;
 - 1.1.4.1.6. Para que seja possível o adequado gerenciamento de riscos deve ser entregue uma ferramenta com as seguintes características:

- 1.1.4.1.6.1. Administração
 - 1.1.4.1.6.1.1. Possuir módulo único e central de administração do ambiente, com possibilidade de definição de perfis de acesso e permissões para usuários e grupos de usuários;
 - 1.1.4.1.6.1.2. Registrar atividades em trilhas de auditoria;
 - 1.1.4.1.6.1.3. Permitir que o administrador parametrize quais funções do sistema cada usuário terá acesso através de perfis de acesso. Entende-se funções do sistema todos os menus contidos no sistema;
 - 1.1.4.1.6.1.4. Suportar autenticação Single Sign-On (SSO) através do protocolo SAML. O recurso deve ser nativo e ter interface de configuração na própria solução para que o administrador realize as configurações;
 - 1.1.4.1.6.1.5. Permitir a sincronização de usuários com o Active Directory da Microsoft de forma nativa e configurável dentro da própria solução em um ambiente on premise do cliente onde a solução está hospedada em outro servidor, sem necessidade de abertura de portas de firewall entre servidor de aplicação e AD do cliente, garantindo segurança do ambiente do cliente;
 - 1.1.4.1.6.1.6. Permitir realizar testes de sincronização e envio de relatório de sincronização de usuários a cada execução;
 - 1.1.4.1.6.1.7. Possuir interface para gestão e monitoramento da fila de serviços de execução;
 - 1.1.4.1.6.1.8. Possuir interface para monitoramento de notificações enviadas por e-mail;
- 1.1.4.1.6.2. Usabilidade:
 - 1.1.4.1.6.2.1. Permitir utilizar soluções de código aberto como requisitos do sistema, incluindo: servidor web, servidor de aplicação Java, sistema operacional e banco de dados;
 - 1.1.4.1.6.2.2. Ser compatível com os navegadores internet: Google Chrome, Microsoft Internet Explorer;
 - 1.1.4.1.6.2.3. Permitir rodar em ambiente virtualizado;
 - 1.1.4.1.6.2.4. Permitir a configuração do armazenamento de conteúdo (documentos e anexos) de forma visual pelo administrador do sistema, com as opções de armazenamento em banco de dados (campo Blob) ou diretório em rede;
 - 1.1.4.1.6.2.5. Permitir a conversão de conteúdo para o formato PDF;
 - 1.1.4.1.6.2.6. Suportar idiomas padrão UTF8;
 - 1.1.4.1.6.2.7. Suportar o uso de Load balancing tanto na camada de banco de dados, quanto de aplicação, permitindo que a carga do sistema seja distribuída entre dois ou mais nós da solução;
 - 1.1.4.1.6.2.8. Possuir visualizador nativo HTML 5 para PDF sem a necessidade de instalação de softwares adicionais para visualização nas estações clientes.
- 1.1.4.1.6.3. Requisitos do sistema
 - 1.1.4.1.6.3.1. Permitir utilizar soluções de código aberto como requisitos do sistema, incluindo: servidor web, servidor de aplicação Java, sistema operacional e banco de dados;
 - 1.1.4.1.6.3.2. Ser compatível com os navegadores internet: Google Chrome, Microsoft Internet Explorer;

- 1.1.4.1.6.3.3. Permitir rodar em ambiente virtualizado;
- 1.1.4.1.6.3.4. Permitir a configuração do armazenamento de conteúdo (documentos e anexos) de forma visual pelo administrador do sistema, com as opções de armazenamento em banco de dados (campo Blob) ou diretório em rede;
- 1.1.4.1.6.3.5. Permitir a conversão de conteúdo para o formato PDF;
- 1.1.4.1.6.3.6. Suportar idiomas padrão UTF8;
- 1.1.4.1.6.3.7. Suportar o uso de Load balancing tanto na camada de banco de dados, quanto de aplicação, permitindo que a carga do sistema seja distribuída entre dois ou mais nós da solução;
- 1.1.4.1.6.3.8. Possuir visualizador nativo HTML 5 para PDF sem a necessidade de instalação de softwares adicionais para visualização nas estações clientes.
- 1.1.4.1.6.4. Segurança:
 - 1.1.4.1.6.4.1. Realizar comunicação segura entre os diferentes componentes da solução e com a estação de trabalho usando padrões de criptografia e protocolos, ambos não proprietários (ex: SSL);
 - 1.1.4.1.6.4.2. Deve possuir controle de acesso por identificação e senha, com cadastro de usuários, grupos e transações, onde as permissões para cada uma das transações possam ser dadas diretamente ao usuário ou implicitamente através de um grupo do qual ele faça parte;
 - 1.1.4.1.6.4.3. Registrar os acessos efetuados por todos os usuários em um arquivo de log, para fins de auditoria e elaboração de relatórios gerenciais. Esses dados serão acessíveis apenas por um grupo determinado de usuários autorizados, contendo no mínimo os seguintes dados: usuário, data, hora, transação realizada;
 - 1.1.4.1.6.4.4. A ferramenta deve prover mecanismos de segregação de usuários através de nível de atuação (usuários, gerentes de projeto, consultor do escritório de projetos, suporte, administração);
 - 1.1.4.1.6.4.5. A ferramenta deve possuir mecanismos para restringir as operações no sistema conforme o perfil dos usuários;
 - 1.1.4.1.6.4.6. A ferramenta deve possibilitar o controle de restrições de acesso por usuário e por grupo de usuários;
 - 1.1.4.1.6.4.7. A ferramenta deve manter registro das alterações feitas nos dados e documentos com data, hora e usuário;
 - 1.1.4.1.6.4.8. A ferramenta deve possibilitar registro e consulta a dados estatísticos sobre acesso de usuários como acesso simultâneo, tempo de logon, origem do acesso;
 - 1.1.4.1.6.4.9. Todas as senhas de usuários devem ser armazenadas utilizando algoritmos de criptografia salted hash;
 - 1.1.4.1.6.4.10. A solução deve permitir a configuração e autenticação em mais de um domínio para a mesma instância, de forma que em um mesmo ambiente, seja possível se autenticar através de Single Sign-On (SSO) em diferentes domínios, não necessitando que os mesmos estejam integrados entre si, sem qualquer necessidade de parametrização via arquivo de configuração ou customização do produto.

- 1.1.4.1.6.5. Gestão de riscos
 - 1.1.4.1.6.5.1. Permitir a definição da metodologia de avaliação de pontuação do risco em qualquer nível da organização;
 - 1.1.4.1.6.5.2. Permitir diversos métodos para a avaliação de risco, tais como: matriz; critérios quantitativos; mais de um critério quantitativos para gerar os eixos da matriz, e; critérios qualitativos;
 - 1.1.4.1.6.5.3. Classificar os riscos de acordo com a severidade para a organização e com a probabilidade da ocorrência no processo;
 - 1.1.4.1.6.5.4. Permitir a avaliação periódica do risco, monitorando a sua evolução analiticamente e graficamente;
 - 1.1.4.1.6.5.5. Permitir a criação de modelos (template) de plano de riscos, para facilitar a replicação de estruturas similares nas organizações;
 - 1.1.4.1.6.5.6. Permitir uma abordagem estratégica na identificação dos principais objetivos da organização e dos riscos existentes para o alcance desses objetivos;
 - 1.1.4.1.6.5.7. Permitir que os riscos possam ser facilmente identificados e associados a um processo;
 - 1.1.4.1.6.5.8. Permitir a criação de bibliotecas de riscos, ou seja, que os nomes dos riscos e tipos de riscos sejam armazenados em um repositório único, garantindo um conjunto de riscos padronizados para a organização;
 - 1.1.4.1.6.5.9. Permitir a definição de equipes responsáveis pela avaliação;
 - 1.1.4.1.6.5.10. Manter o cadastro e acompanhamento das alterações (revisão) dos objetos e dos planos de risco;
 - 1.1.4.1.6.5.11. Permitir a definição do custo dos controles e o valor do impacto ou ganho do risco possibilitando a realização de análises quantitativas do risco;
 - 1.1.4.1.6.5.12. Permitir a abertura de eventos (incidentes, problemas, workflows) caso as consequências do risco superem o esperado, possibilitando a identificação das causas, análise da causa, criação de planos de ação e verificação da eficácia. Estes registros devem ser mantidos para histórico e entrada da nova avaliação do risco futuramente;
 - 1.1.4.1.6.5.13. Possibilitar a abertura de um workflow específico caso a avaliação do risco esteja acima do esperado;
 - 1.1.4.1.6.5.14. Possibilitar a aprovação do plano de riscos ao final do planejamento e a revalidação dentro de frequência pré-estabelecida;
 - 1.1.4.1.6.5.15. Permitir que os riscos possam ser associados a mais de um processo, porém, que sejam analisados e documentados individualmente para cada processo;
 - 1.1.4.1.6.5.16. Permitir a avaliação considerando o risco potencial, o risco inerente e o risco residual;
 - 1.1.4.1.6.5.17. Permitir o cálculo automático do risco residual;
 - 1.1.4.1.6.5.18. Permitir a associação de anexos e documentos controlados ao Risco;
 - 1.1.4.1.6.5.19. Executar as avaliações de maneira on-line;
 - 1.1.4.1.6.5.20. Permitir a análise de risco dos processos mapeados;
 - 1.1.4.1.6.5.21. Apresentar graficamente, no fluxograma do processo, as atividades que

possuem riscos associados;

- 1.1.4.1.6.5.22. Mapear os processos e modelar todas as atividades relacionadas;
- 1.1.4.1.6.5.23. Permitir a análise de risco dos ativos;
- 1.1.4.1.6.5.24. Permitir a gestão dos riscos relacionados ao planejamento estratégico (Scorecard);
- 1.1.4.1.6.5.25. Definir o Scorecard corporativo com todos os seus elementos (perspectivas, objetivos e indicadores);
- 1.1.4.1.6.5.26. Permitir a habilidade de desenvolver ou adotar um framework para a gestão de riscos (COSO ERM, ISSO 31000, OCEG ou outros frameworks similares);
- 1.1.4.1.6.5.27. Mapear os riscos operacionais de acordo com framework COSO;
- 1.1.4.1.6.5.28. Permitir a associação de tratamentos e planos de ação no momento da criação da análise de risco;
- 1.1.4.1.6.5.29. Permitir a associação de controles aos riscos durante o cadastro, facilitando a utilização posterior;
- 1.1.4.1.6.5.30. Apresentar o histórico das avaliações do risco atualizado conforme última versão do método de avaliação;
- 1.1.4.1.6.5.31. Oferecer método de avaliação para a definição do nível do risco. Critérios quantitativos podem ser informados para a obtenção do resultado;
- 1.1.4.1.6.5.32. Personalizar as colunas para serem visualizadas na estrutura do plano de risco e controle;
- 1.1.4.1.6.5.33. Permitir a visualização da Matriz de Risco de todos os riscos de um plano de risco;
- 1.1.4.1.6.5.34. Permitir a visualização da Matriz de Risco agrupando quantitativamente as avaliações dos riscos;
- 1.1.4.1.6.5.35. Permitir a associações do risco no momento que está cadastrando um evento, ou seja, um incidente, problema ou workflow;
- 1.1.4.1.6.5.36. Permitir registrar uma justificativa, anexo ou documento para cada resultado da avaliação do risco;
- 1.1.4.1.6.5.37. Permitir associar causas, consequências, fontes de risco e melhores práticas ao risco;
- 1.1.4.1.6.5.38. Permitir criar e gerenciar KRI (Indicadores chave de risco), com geração de eventos casos do KRI estejam fora dos valores aceitáveis;
- 1.1.4.1.6.5.39. Permitir enviar e-mail a aprovação da avaliação do risco;
- 1.1.4.1.6.5.40. Permitir solicitar a avaliação de risco para o responsável no momento da Auditoria.
- 1.1.4.1.6.6. Problemas e tratamento
 - 1.1.4.1.6.6.1. Permitir identificar problemas nas atividades de controle;
 - 1.1.4.1.6.6.2. Permitir identificar problemas na avaliação do risco;
 - 1.1.4.1.6.6.3. Permitir associar prioridade aos problemas;
 - 1.1.4.1.6.6.4. Permitir definir responsáveis aos problemas;

- 1.1.4.1.6.6.5. Permitir monitorar prazos de planejamento e de execução;
- 1.1.4.1.6.6.6. Permitir enviar e-mail automaticamente para o responsável assim que uma ocorrência for registrada;
- 1.1.4.1.6.6.7. Permitir criar e monitorar múltiplos planos de ação para cada problema;
- 1.1.4.1.6.6.8. Permitir que os responsáveis pelos planos de ação possam ser diferentes dos responsáveis pelo problema;
- 1.1.4.1.6.6.9. Permitir que os planos de ação sejam revisados e aprovados por um usuário específico ou pelo responsável pelo problema;
- 1.1.4.1.6.6.10. Permitir que a situação de execução dos planos de ação seja monitorada;
- 1.1.4.1.6.6.11. Permitir que as notificações por e-mail possam ser definidas pelos usuários;
- 1.1.4.1.6.6.12. Permitir que o gestor tenha fácil acesso a todos os problemas e planos de ação de sua área de responsabilidade;
- 1.1.4.1.6.6.13. Permitir que trilhas de auditoria para qualquer alteração nas atividades e prazos relacionados aos problemas e planos de ação façam parte do sistema;
- 1.1.4.1.6.6.14. Permitir a análise de causa e de tendência;
- 1.1.4.1.6.6.15. Permitir a personalização da resposta ao risco;
- 1.1.4.1.6.6.16. Permitir a criação ou a associação de um ou mais planos de ação para cada tratamento do risco;
- 1.1.4.1.6.6.17. A solução deverá permitir a gestão estruturada de iniciativas relacionadas à segurança da informação, como planejamentos de correção de vulnerabilidades, auditorias e projetos de conformidade, com base nas boas práticas de gerenciamento de projetos descritas no PMBOK Guide, Se integrando e oferecendo funcionalidades compatíveis com práticas de gestão de projetos, como:
 - 1.1.4.1.6.6.17.1. Definição de escopo e objetivos;
 - 1.1.4.1.6.6.17.2. Planejamento de recursos e prazos;
 - 1.1.4.1.6.6.17.3. Monitoramento de progresso e riscos;
 - 1.1.4.1.6.6.17.4. Geração de relatórios gerenciais.
- 1.1.4.1.6.6.18. Permitir definir um tratamento para uma avaliação de risco e associar um plano de ação para este tratamento.
- 1.1.4.1.6.7. Consultas e relatórios:
 - 1.1.4.1.6.7.1. Permitir que o sistema agrupe e gere consultas da avaliação de riscos em todos os níveis da base de dados, incluindo a estrutura organizacional, processos e riscos;
 - 1.1.4.1.6.7.2. Apresentar a listagem de problemas e planos de ação com possibilidade de desdobramentos;
 - 1.1.4.1.6.7.3. Permitir salvar relatórios no formato PDF;
 - 1.1.4.1.6.7.4. Permitir que os responsáveis pelos controles e auditores independentes possam acessar facilmente sua informação no sistema;
 - 1.1.4.1.6.7.5. Permitir que os responsáveis pelos processos possam acessar facilmente sua informação no sistema;

- 1.1.4.1.6.7.6. Apresentar listagens ou relatórios da avaliação de riscos, visando a fácil identificação de pontos críticos na organização;
- 1.1.4.1.6.7.7. Apresentar os objetivos estratégicos e da avaliação dos riscos de maneira gráfica e visual;
- 1.1.4.1.6.7.8. Apresentar a matriz de riscos para a fácil identificação dos riscos dentro dos quadrantes do método de avaliação;
- 1.1.4.1.6.7.9. Garantir o acompanhamento do plano de riscos permitindo uma fácil visualização do fluxograma do processo, riscos por etapa, controles e tratamentos, matriz de riscos x etapa e demais elementos;
- 1.1.4.1.6.7.10. Apresentar a matriz de riscos para a fácil identificação da relação entre riscos e atividades;
- 1.1.4.1.6.7.11. Apresentar o cálculo do risco médio gerado automaticamente e agrupado por Unidade Organizacional, Processo, Risco, Tipo de Risco com visões gráficas da matriz de risco em um portal interativo;
- 1.1.4.1.6.7.12. Permitir comparar os resultados entre as revisões do plano de risco e controle;
- 1.1.4.1.6.7.13. Permitir a definição de indicadores de desempenho associados aos processos e acompanhamento do cumprimento das metas estabelecidas;
- 1.1.4.1.6.7.14. Possibilitar a geração de diversos tipos de relatórios e gráficos contendo informações detalhadas ou resumidas sobre os processos e atividades;
- 1.1.4.1.6.7.15. Possuir semáforos que sinalizam visualmente o nível de cumprimento dos resultados;
- 1.1.4.1.6.7.16. Possuir indicador de tendência sobre possíveis problemas futuros;
- 1.1.4.1.6.7.17. Permitir a formatação dos resultados em planilhas e gráficos configuráveis pelo usuário;
- 1.1.4.1.6.7.18. Permitir a visualização dos recursos e custos requeridos para a execução dos processos.

1.2. Monitoração da marca

- 1.2.1. A CONTRATADA deverá prover solução tecnológica que permita o monitoramento contínuo de ambientes digitais públicos e restritos, com foco na identificação de ameaças à segurança da marca da CONTRATANTE, incluindo menções indevidas, vazamentos de dados e uso não autorizado de ativos digitais.
- 1.2.2. A solução deverá realizar varreduras diárias em fontes abertas e ambientes restritos da internet, como fóruns, redes sociais, blogs, sites de compartilhamento de texto e comunidades digitais, com capacidade de gerar alertas automatizados sobre riscos identificados.
- 1.2.3. A solução deverá possuir capacidade de acesso automatizado e contínuo a repositórios da Deep Web e Dark Web, como redes Tor, Zeronet, fóruns especializados e sites de compartilhamento de conteúdo, com geração de relatórios e alertas sobre ameaças relevantes.
- 1.2.4. A solução deverá permitir a realização de pesquisas históricas em ambientes da Deep/Dark Web, com foco em menções à marca, projetos e ativos da CONTRATANTE.
- 1.2.5. A solução deverá permitir buscas por dados e informações potencialmente vazadas,

utilizando como parâmetros de pesquisa:

- 1.2.5.1. Domínio institucional;
- 1.2.5.2. Intervalos de endereços IP;
- 1.2.5.3. Nomes de executivos e colaboradores estratégicos;
- 1.2.5.4. Dados de cartões corporativos;
- 1.2.5.5. Nomes de projetos e documentos técnicos.
- 1.2.6. A solução deverá permitir a identificação de menções a projetos estratégicos da CONTRATANTE em ambientes da Deep/Dark Web.
- 1.2.7. A solução deverá monitorar informações sensíveis relacionadas à CONTRATANTE, incluindo credenciais expostas, dados pessoais e corporativos, com alertas em tempo real.
- 1.2.8. A solução deverá realizar monitoramento de uso indevido de ativos da marca (nome, logotipo, identidade visual) em perfis e páginas de redes sociais.
- 1.2.9. A solução deverá permitir o monitoramento de dados sensíveis de até 10 executivos e pessoas-chave da organização, como CPF, RG, CNH, nome completo, cartões, e-mails, em ambientes da surface, deep e dark web.
- 1.2.10. A solução deverá realizar buscas automatizadas por endereços de e-mail vinculados aos domínios da CONTRATANTE que tenham sido alvo de exposições de credenciais.
- 1.2.11. A solução deverá classificar e priorizar os riscos cibernéticos identificados, com base em critérios técnicos e automatizados, para facilitar a tomada de decisão.
- 1.2.12. A solução deverá permitir a execução de até 60 ações de takedown por ano, com emissão de notificações extrajudiciais e acompanhamento técnico para tratamento dos incidentes.

2. SERVIÇOS PARA O ITEM 2

- 2.1.1. Indicação das atividades e criticidade, para aplicação dos níveis mínimos de serviço :

FASE	CRITICIDADE (Conforme item 7.4 do termo de referência - NMS)
Análise de Incidentes Globais	BAIXA
Monitoração de Incidentes	MÉDIA

2.2. Análise de Incidentes Globais

- 2.2.1. A CONTRATADA deve monitorar a ocorrência de incidentes globais, através de RSS Feeds, de modo a antever eventuais ataques a CONTRATANTE;
- 2.2.2. Ataques direcionados ao mesmo segmento de mercado do CONTRATANTE devem ser imediatamente sinalizados para que seja tomada uma decisão em relação à atuação dos serviços contratados.

2.3. Monitoramento de Incidentes

2.3.1. Monitoramento de aplicações web, servidores, virtualizadores e rede de forma proativa e reativa (com anuência do IBGE) no ambiente internet e intranet da instituição.

2.3.2. São papéis da CONTRATADA:

2.3.2.1. Monitorar o ambiente quanto à disponibilidade e desempenho dos equipamentos que compõe a solução a ser utilizada no gerenciamento, bem como todo o escopo contratado quanto aos incidentes relacionados à segurança da informação;

2.3.2.1.1. O ambiente a ser monitorado possui até 2.100 (dois mil e cem) ativos, incluindo servidores, roteadores, switches, entre outros.

2.3.2.2. Fazer a gestão dos incidentes (criação de alertas, detecção e abertura de chamados);

2.3.2.3. Acompanhar do início ao fim os incidentes;

2.3.2.4. Realizar o acionamento por matriz de escalação hierárquica e funcional, para os incidentes;

2.3.2.5. Correlacionar o processo de eventos (gerenciar eventos durante todo o seu ciclo de vida) e o processo de incidentes de forma automatizada entre a ferramenta de ITSM (IT Service Management, ou Gestão de Serviços de TI) e ferramenta de monitoramento;

2.3.2.6. Acompanhar os processos através de indicadores de desempenho;

2.3.2.7. Para tal, a CONTRATADA deverá entregar ferramenta com as seguintes características.

2.3.2.8. Características gerais da plataforma:

2.3.2.8.1. A solução deve ser composta pelos seguintes elementos:

2.3.2.8.2. Coletores de eventos e agentes especializados responsáveis pela coleta de eventos (logs);

2.3.2.8.3. Armazenador de eventos e registros processados;

2.3.2.8.4. Correlacionador de eventos;

2.3.2.8.5. A solução deve ser capaz de ler logs que atualmente são gerenciados pela ferramenta atual que está em funcionamento no IBGE, o Loghrythm;

2.3.2.8.6. A solução deverá ser entregue em servidor virtual para instalação on premise no ambiente do IBGE, conforme as seguintes configurações:

2.3.2.8.7. Sistema de Virtualização Microsoft Hyper-V Server 2016 ou versões superiores, a critério do IBGE;

2.3.2.8.8. O IBGE disponibilizará os equipamentos que atuarão como servidores físicos hospedeiros para a console e coletores que a solução fornecerá;

2.3.2.8.9. Possuir, ao menos, duzentos DataSources nativos na plataforma disponível para eventuais integrações

2.3.2.8.10. Os bancos de dados utilizados pela ferramenta devem ser oferecidos em conjunto com a ferramenta, sem que haja custos futuros de expansão, manutenção ou licença para o IBGE;

2.3.2.8.11. A solução deve ser de fabricante nacional ou fabricante estrangeiro com

representação no Brasil.

- 2.3.2.8.12. A comunicação entre os componentes da solução deve ser feita através de criptografia, com uso de algoritmos RSA 2048, AES (128 bits ou mais) e/ou 3DES(192 bits ou mais), garantindo a autenticidade, confidencialidade e integridade dos dados, utilizando o protocolo TCP/IP.
- 2.3.2.8.13. Juntamente com a subscrição de atualização dos componentes da solução pelo período do contrato, a contratada deverá prover acesso à biblioteca de casos de uso do fabricante, que contenha pacotes especializados de regras, dashboards e coletores desenvolvidos pelo fabricante que permitam a implementação de correlação e monitoração avançada, sem necessidade de redensenvolvimento.
- 2.3.2.8.14. Possuir, ao menos, trezentos DataSources nativos na plataforma disponível para eventuais integrações.
- 2.3.2.8.15. Toda comunicação entre os componentes deverá ser criptografada;
- 2.3.2.8.16. A solução deverá ser capaz de implementar Ipv6;
- 2.3.2.8.17. Todos os módulos da solução (coletores, solução de armazenamento de logs e correlacionador) devem ser do mesmo fabricante.
- 2.3.2.8.18. Não serão aceitas soluções a serem projetadas, em fase de projeto, ou em desenvolvimento. Caso o suporte ao produto seja descontinuado antes da data do término deste edital, a empresa deverá fornecer a atualização necessária para que o produto continue a ter sua manutenção provida pelo fabricante ou substituir o sistema pela solução da nova geração;
- 2.3.2.8.19. Não serão aceitas soluções que contenham soluções que envolvam exfiltração de dados, seja por meio de um programa, um equipamento ou a combinação de ambos, para redes externas às redes do IBGE, tais como redes da empresa vendedora, da empresa desenvolvedora ou qualquer tipo de “nuvem” de dados;
- 2.3.2.8.20. Não serão aceitas soluções que causem custos adicionais de licenciamento, mão-de-obra ou equipamentos.
- 2.3.2.8.21. A solução deverá prover todas as licenças de software, sistemas operacionais, bancos de dados, subscrições ou qualquer outro tipo de licenciamento necessário para seu completo funcionamento, de acordo com as características e prazos estipulados. A infraestrutura de virtualização será fornecida pela CONTRATANTE.
- 2.3.2.8.22. A solução ofertada poderá ser composta por um ou mais softwares, desde que sejam do mesmo fabricante, totalmente interoperáveis entre si, gerenciados através de uma interface única e em número de licenças suficientes para atender aos volumes de dados e/ou quantidades de eventos solicitados.
- 2.3.2.8.23. As licenças de software deverão ser registradas junto ao fabricante da solução em nome da contratante;
- 2.3.2.8.24. O tipo de licenciamento é licença do tipo subscrição para instalação on-premises, com possibilidade de atualização enquanto durar o contrato de suporte.
- 2.3.2.8.25. A solução de SIEM ofertada não poderá ser do tipo opensource;
- 2.3.2.8.26. Deverá ser ofertada a última versão estável de todos os softwares;
- 2.3.2.8.27. Poderão ser considerados servidores para armazenamento de logs, coletores e tratamento de eventos em separado.

2.3.2.9. DOS AGENTES E COLETORES DE EVENTOS

- 2.3.2.9.1. A solução deverá estar dimensionada e licenciada para coleta, processamento e retenção conforme descrito abaixo:
 - 2.3.2.9.1.1. EPS/MPS médio de 3.000;
 - 2.3.2.9.1.2. Aproximadamente 7.6 TB de logs processados.
- 2.3.2.9.2. Para fins de dimensionamento e licenciamento, um evento é definido como qualquer pacote de log ou fluxo de rede recebido pela solução.
- 2.3.2.9.3. A solução deverá suportar, em episódios de ataque ou sobrecarga de eventos, duas vezes seu volume licenciado durante 6 horas consecutivas, mantendo o funcionamento da solução, sem perda de eventos ou restrições de funcionalidades.
- 2.3.2.9.4. A solução deverá ser capaz de receber eventos de fluxos de rede Netflow.
- 2.3.2.9.5. Coletar e aplicar parsing nos dados dos dispositivos monitorados em tempo próximo ao real (near-real-time).
- 2.3.2.9.6. Ser capaz de normalizar e categorizar os eventos em um padrão único que será usado pela solução;
- 2.3.2.9.7. Rotular eventos por zonas diferentes mesmo que estejam em redes com mesmo endereçamento IP;
- 2.3.2.9.8. Ser possível realizar a coleta de eventos de dispositivos não suportados nativamente através de conectores customizados;
- 2.3.2.9.9. Ajustar o horário dos eventos, com base em limites de diferença de hora entre os eventos originais e a hora correta obtida pelo sistema através desincronização de NTP (Network Time Protocol) com os servidores locais;
- 2.3.2.9.10. Marcar (através de tag, label ou similar) os eventos com base em unidade organizacional: departamento, setor, divisão corporativa ou similar;
- 2.3.2.9.11. Filtrar e selecionar os eventos que serão inseridos na solução e permitir a criação e alteração de filtros;
- 2.3.2.9.12. Possuir suporte aos protocolos de gerenciamento SNMPv1, SNMPv2, SNMPv3 e outras mais avançadas porventura existentes à época do fornecimento.
- 2.3.2.9.13. Possuir a funcionalidade de ler e normalizar eventos de log armazenados em formato texto (w3c), SQL database, compactados ou não.
- 2.3.2.9.14. A solução deverá suportar a coleta dos logs de outros sistemas e ativos que venham a ser incorporados pelo órgão durante a vigência do contrato, mesmo que não conste inicialmente no Termo de Referência. Nesse caso, a contratada poderá implementar conectores customizados, caso a solução não tenha capacidade de recebimento do log nativamente.
- 2.3.2.9.15. Ser capaz de coletar, no mínimo, os logs dos sistemas e ativos listado abaixo:
 - 2.3.2.9.15.1. Firewalls: Cisco ASA 5585x SSP10 com Firepower, Checkpoint 4600, VMWare NSX, Palo Alto;
 - 2.3.2.9.15.2. Soluções de WAF: Big IP F5, Akamai, Cloudflare, Barracuda;
 - 2.3.2.9.15.3. Roteadores: Cisco Nexus, Cisco RV320, Huawei/H3C MSR;
 - 2.3.2.9.15.4. Switches: Cisco, Huawei, Enterasys e Extreme;
 - 2.3.2.9.15.5. Plataformas de Virtualização: VMware ESX, HyperV, Acropolis/KVM e Oracle

VM;

- 2.3.2.9.15.6. Sistemas Operacionais: Linux (Debian, RedHat, Ubuntu, CentOS, Oracle Linux, Red Hat Enterprise Linux (RHEL)), Windows Server (2008, 2012, 2016 ou acima) e FreeBSD;
- 2.3.2.9.15.7. Antivirus: Windows Defender e SEP;
- 2.3.2.9.15.8. Servidores de E-mail on premise ou em nuvem: Microsoft Exchange;
- 2.3.2.9.15.9. Servidores de Aplicação e Web: Apache2, Squid, HAProxy, Apache, Jboss e Microsoft IIS7 (ou superior);
- 2.3.2.9.15.10. VPN: OpenVPN, CiscoVPN, Global Protect (Palo Alto)
- 2.3.2.9.15.11. Soluções hospedadas em nuvens tipo: Azure, AWS, Google Cloud, IBM Cloud, Defender for Cloud;
- 2.3.2.9.16. A solução deve poder coletar dados de feeds externos;
- 2.3.2.9.17. Para a coleta de dados e feeds externos deve suportar, no mínimo, os seguintes formatos/protocolos/fontes:
 - 2.3.2.9.17.1. Para Feeds Externos:
 - 2.3.2.9.17.1.1. CIFS
 - 2.3.2.9.17.1.2. FTP
 - 2.3.2.9.17.1.3. Manual Upload
 - 2.3.2.9.17.1.4. McAfee ATD
 - 2.3.2.9.17.1.5. NFS
 - 2.3.2.9.17.1.6. SCP
 - 2.3.2.9.17.1.7. SFTP
 - 2.3.2.9.17.1.8. TAXII
 - 2.3.2.9.17.2. Para Coleta de Dados
 - 2.3.2.9.17.2.1. SYSLOG
 - 2.3.2.9.17.2.2. MEF
 - 2.3.2.9.17.2.3. SCP
 - 2.3.2.9.17.2.4. HTTP
 - 2.3.2.9.17.2.5. FTP
 - 2.3.2.9.17.2.6. SFTP
 - 2.3.2.9.17.2.7. NFS (Tail mode or Copy mode)
 - 2.3.2.9.17.2.8. CIFS (Tail mode or Copy mode)
- 2.3.2.9.18. Prover mecanismo de coleta de logs de dispositivos não suportados nativamente, através de personalização de coletores, ou solução similar.
- 2.3.2.9.19. A solução deve ser composta de agentes que têm como função básica fazer a interface com o dispositivo monitorado, recebendo ou buscando eventos relevantes que serão inseridos na solução.
- 2.3.2.9.20. Suportar a coleta de dados de no mínimo 250 (duzentos e cinquenta) geradores de

eventos (logs);

- 2.3.2.9.21. Controlar a utilização da banda utilizada diretamente do conector sem a necessidade de usar recursos do sistema operacional;
- 2.3.2.9.22. Separar eventos por meio de anotações em campos, originados por quaisquer campos disponíveis e normalizados (ex: Cliente 1 - VLAN ID 10, Cliente 2- VLAN ID 20) mesmo que o evento seja de um mesmo firewall;
- 2.3.2.9.23. A modalidade de licenciamento deverá permitir a distribuição livre de elementos de coleta, filtragem e agregação, gerados com o uso de SDK ou API(Application Programming Interface), independentemente do número e arquitetura;
- 2.3.2.9.24. A camada de coleta deverá permitir ser instalada em modo distribuído, possibilitando a implementação de seus elementos o mais próximo possível dos dispositivos e softwares monitorados;
- 2.3.2.9.25. Os elementos da solução deverão permitir nativamente sua instalação em máquinas virtuais, servidores físicos, appliances e, conjuntamente com a aplicação alvo, quando desejado pela Instituição. Por exemplo, a Instituição poderá determinar que o elemento de interface seja instalado no mesmo servidor de uma aplicação, para evitar que os logs dessa aplicação percorram a rede em modo claro e pode determinar que o elemento de interface seja instalado em um servidor stand-alone na rede de roteadores, para que eventos de múltiplos dispositivos de roteamento sejam recebidos pelo mesmo elemento de interface;
- 2.3.2.9.26. A solução deve ser capaz de normalizar os eventos em um padrão único;
- 2.3.2.9.27. O componente de coleta de eventos deve suportar a captura, a normalização e o tratamento de eventos em tempo próximo ao real (near real-time);
- 2.3.2.9.28. O coletor da solução deverá ser capaz de armazenar os dados localmente (cache) em caso de indisponibilidade do componente correlacionador.
- 2.3.2.9.29. O envio dos dados em cache deve ocorrer imediatamente a disponibilização do correlacionador.
- 2.3.2.9.30. A solução deve ser capaz de enviar o evento bruto (raw) para o armazenamento e consulta futura;
- 2.3.2.9.31. Deve permitir acrescentar o horário (timestamp) correto da recepção do evento/log na solução, preservando o horário original do evento. Esse horário deve ser obtido pelo sistema através de sincronização com servidores NTP previamente definidos, e sincronizado entre todos os componentes da solução;
- 2.3.2.9.32. Tanto os eventos de segurança quanto os de conformidade devem ser normalizados para um único padrão de eventos utilizado pela solução;
- 2.3.2.9.33. A solução deve permitir múltiplos perfis de configuração.
- 2.3.2.9.34. A solução deverá enviar os eventos coletados para o correlacionador e permitir enviar para mais de um destino ao mesmo tempo.
- 2.3.2.9.35. Deverá implementar coleta de informações de fluxo - Netflow ou SFlow;
- 2.3.2.9.36. Será considerada no Edital a seguinte definição para conector: software desenvolvido e suportado pelo fabricante da solução que tem como função básica fazer a interface com o dispositivo monitorado, recebendo ou buscando eventos relevantes que serão inseridos na solução, contendo obrigatoriamente documentação de todos coletores nativos com informações de configurações de cada ativo suportado;

- 2.3.2.9.37. Realizar a agregação de eventos semelhantes que ocorrem dentro de um limite de tempo e quantidade de eventos específicos, sendo que permite agregar tanto os eventos cuja única diferença seja o horário de ocorrência, quanto especificar quais campos do evento normalizado devem ser considerados para fins de agregação;
- 2.3.2.9.38. Possuir a funcionalidade de atualização, gerenciamento e configuração centralizados de todos os conectores distribuídos da solução;
- 2.3.2.9.39. Permitir a categorização manual de eventos (já normalizados) inéditos não categorizados por padrão. Esta categorização deverá ser aplicada nos eventos futuros de mesma característica;
- 2.3.2.9.40. De forma a evitar a perda de eventos por sobrecarga ou indisponibilidade de conectores, a contratada deverá fornecer função redundante de balanceamento de cargas de serviço Syslog;
- 2.3.2.9.41. O balanceamento deverá ser capaz de implementar Weighted Round Robin e Round Robin.
- 2.3.2.9.42. Ao receber um evento syslog, a solução deverá buscar um conector disponível, de forma a garantir que não haverá perda de eventos por sobrecarga de conectores.
- 2.3.2.9.43. Será aceito o fornecimento da funcionalidade de balanceamento nativa ou por adição de elementos externos de qualquer fabricante. A solução de balanceamento redundante deverá estar dimensionada para suportar o volume de tráfego cotado.

2.3.2.10. DO ARMAZENAMENTO

- 2.3.2.10.1. Componente da solução responsável pela retenção dos dados coletados.
- 2.3.2.10.2. A solução deverá estar dimensionada e licenciada para efetuar a retenção e pesquisa em 100% dos eventos coletados;
- 2.3.2.10.3. Armazenar os dados: eventos, alertas, incidentes, bases de conhecimento, workflow nativo e toda informação pertinente à solução, tais como configuração, usuários, trilhas de auditoria e informações de depuração.
- 2.3.2.10.4. Ter a capacidade de definir política de retenção dos dados on-line, ou seja, dados mantidos no banco de dados da solução, disponíveis para consulta imediata;
- 2.3.2.10.5. Ser capaz de armazenar logs por tempo determinado e personalizado, conforme necessidade do órgão;
- 2.3.2.10.6. Deverá ter a capacidade de guardar eventos brutos em forma comprimida;
- 2.3.2.10.7. Deverá ter a capacidade de recuperar, sob demanda, registros sem modificação para preservação de evidência com qualidade forense;
- 2.3.2.10.8. De forma a permitir seu uso em auditorias e processos forenses, não deverá ser possível, sob nenhuma hipótese, a seleção e exclusão de eventos individuais. Deve ser possível apenas a exclusão de eventos conforme a política de retenção, ou seja, todos os eventos mais antigos que extrapolem o tempo de retenção ou o tamanho do armazenamento definido para esse tipo de registros;
- 2.3.2.10.9. Permitir o expurgo dos dados de forma automática com a personalização do período de tempo do expurgo.
- 2.3.2.10.10. Deverá permitir a utilização de volumes de armazenamento locais e externos. Deverá permitir a segregação de tipos de eventos diferentes em grupos lógicos de armazenamento diferentes, com políticas de retenção diferentes, de forma a permitir

a otimização de performance;

- 2.3.2.10.11. Deverá permitir exportar eventos para formato pdf e csv em estruturas NFS, CIFS, SAN e localmente. Deverá permitir que o usuário defina quais campos do evento serão exportados;
- 2.3.2.10.12. Implementar: políticas de controle de acesso aos dados, auditoria e tráfego dos dados criptografados com algoritmos padrões de mercado reconhecidamente seguros.
- 2.3.2.10.13. A solução deve permitir que os relatórios sejam executados periodicamente (diário, semanal, quinzenal, mensal, etc...) ou de forma tempestiva.
- 2.3.2.10.14. Deverá implementar acesso integrado com autenticação padrão LDAP.
- 2.3.2.10.15. Deverá implementar dashboards com visualização de EPS de entrada, EPS de saída e utilização de CPU;
- 2.3.2.10.16. Deverá permitir a livre customização da interface, definindo página inicial por usuário e dashboards customizados;
- 2.3.2.10.17. Deverá ser fornecido com dashboards pré-configurados e permitir a criação de novos dashboards;
- 2.3.2.10.18. Deverá implementar dashboards de monitoramento de resultados históricos;
- 2.3.2.10.19. Deverá possuir dashboard pré-configurados pelo menos para Windows, firewall, código malicioso, entre outros;
- 2.3.2.10.20. Deverá permitir pesquisas (queries) no histórico de eventos, fornecendo capacidade de drilldown, ou seja, visualizar os detalhes dos eventos, inclusive o raw event (dado cru), quando aplicável, para análise forense e investigação de incidentes.
- 2.3.2.10.21. Deverá permitir a procura por texto, campos pré-definidos, palavras chaves, operações booleanas e expressões regulares;
- 2.3.2.10.22. Deverá permitir a utilização de procuras complexas através do encadeamento de comandos de consulta;
- 2.3.2.10.23. Deverá permitir a configuração da visualização do resultado em formato de tabela e gráfico;
- 2.3.2.10.24. Deverá permitir a configuração do escopo de procura como local e distribuída por alguns ou todos os elementos da solução;
- 2.3.2.10.25. Deverá permitir a gravação da query de procura em formato de filtro para utilização futura;
- 2.3.2.10.26. Deverá permitir a gravação dos resultados da pesquisa em arquivo;
- 2.3.2.10.27. Deverá implementar funcionalidade assistente para facilitar a criação das queries;
- 2.3.2.10.28. Deverá implementar assistente gráfico para criação de queries;
- 2.3.2.10.29. Deverá implementar funcionalidade de sugestão de termos de procura enquanto se digita os critérios de pesquisa (recurso auto completar);
- 2.3.2.10.30. Deverá implementar funcionalidade de listagem das últimas queries realizadas para facilitar o reuso em pesquisas;
- 2.3.2.10.31. Deverá implementar indexação baseada em campo e palavra-chave para acelerar buscas; Deverá implementar alertas por syslog, SNMP e e-mail;
- 2.3.2.10.32. Deverá permitir visualização em tempo real de eventos que atendam ao critério de

seleção definido pelo usuário;

- 2.3.2.10.33. Deverá possuir relatórios pré-configurados separados em categorias;
- 2.3.2.10.34. Deverá possuir ferramenta gráfica para desenho de modelos de relatórios personalizados;
- 2.3.2.10.35. Deverá implementar tecnologia de procura distribuída por múltiplos elementos;
- 2.3.2.10.36. Deverá armazenar os eventos de forma compactada;
- 2.3.2.10.37. Apresentar relatórios de eventos, alertas e incidentes em nível técnico e gerencial, os quais devem ter a possibilidade de serem gerados em pdf, html e csv;
- 2.3.2.10.38. Deverá permitir o agendamento de geração de relatórios periódicos, notificar ou enviar automaticamente os relatórios gerados para os destinatários;
- 2.3.2.10.39. Apresentar painéis gráficos (dashboards) com indicativos de situações diversas;
- 2.3.2.10.40. A partir de um dado evento ou conjunto de eventos, mostrar de forma gráfica seus relacionamentos e fazer drill-down do mesmo para efetiva investigação e identificação de causa raiz;
- 2.3.2.10.41. Permitir pesquisa nos eventos históricos, fornecendo capacidade de drill-down, ou seja, visualizar os detalhes dos eventos, inclusive dados raw, quando aplicável, para análise forense e investigação de incidentes;
- 2.3.2.10.42. Deverá ter capacidade de definir política de retenção dos dados;
- 2.3.2.10.43. Os logs devem ser mantidos pelo período mínimo de 365 dias, conforme Marco Civil da Internet (LEI nº 12.965, de 23 de Abril de 2014);
- 2.3.2.10.44. Deverá ter capacidade de armazenar os eventos em formato original (raw);
- 2.3.2.10.45. O algoritmo de integridade utilizado no armazenamento pode ser configurado entre os seguintes: MD5, SHA-1, SHA-256 ou SHA-512;
- 2.3.2.10.46. A solução deve possuir a capacidade de gerenciar o armazenamento de longo prazo de dados de inteligência de TI em um repositório central (mínimo de 5 anos);
- 2.3.2.10.47. Deve utilizar algoritmos para verificação de integridade e autenticidade dos eventos armazenados para fins de auditoria (Ex: SHA1) devidamente reconhecidos como seguros;
- 2.3.2.10.48. Armazenar os eventos e os alertas, inclusive os normalizados, de forma indexada.
- 2.3.2.10.49. Possuir a funcionalidade de apresentação de relatórios de eventos, alertas e incidentes em nível técnico e gerencial, os quais devem ter a possibilidade de customização e de serem gerados em PDF e HTML.

2.3.2.11. DO CORRELACIONADOR

- 2.3.2.11.1. Componente da solução responsável pelo correlacionamento dos eventos coletados.
- 2.3.2.11.2. O correlacionador deve ser capaz de receber eventos dos agentes, coletores e de outros correlacionadores;
- 2.3.2.11.3. O correlacionador deve efetuar a análise dos eventos em tempo próximo ao real (near realtime);
- 2.3.2.11.4. Deve permitir ao administrador a criação de novas regras e a edição das existentes.

- 2.3.2.11.5. O correlacionador deve identificar anomalias baseadas em eventos e análise de dados históricos conforme período a ser definido;
- 2.3.2.11.6. O correlacionador deve permitir o correlacionamento de eventos e alertas com dados existentes em listas (watchlist). Deve permitir também a criação de novas listas e a personalização das existentes;
- 2.3.2.11.7. O correlacionador deve permitir a execução das regras agendadas contra eventos passados para análise histórica de atividades suspeitas, que executam em frequência e horário específico;
- 2.3.2.11.8. O correlacionador deve ter a capacidade de fazer o correlacionamento entre eventos oriundos de:
 - 2.3.2.11.8.1. Agentes (ou solução similar) ou coletores de outros correlacionadores;
 - 2.3.2.11.8.2. Diferentes ativos do mesmo tipo (por exemplo, Firewall A e Firewall B);
 - 2.3.2.11.8.3. Ativos de diferentes tipos (por exemplo, Firewall A e IPS B e Proxy C);
 - 2.3.2.11.8.4. Ativos e Banco de Dados (por exemplo, catraca e consultas a banco de dados);
- 2.3.2.11.9. O correlacionador deve ser capaz de inserir os alertas gerados no próprio fluxo de correlacionamento ou no fluxo de eventos. Deve permitir o correlacionamento de tais alertas/eventos, derivados de alertas, com novos eventos e/ou regras, no intuito de detectar padrões mais complexos de ameaças ou violações de conformidade;
- 2.3.2.11.10. O correlacionador deve priorizar os eventos e alertas com base, pelo menos, nos seguintes critérios:
 - 2.3.2.11.10.1. Severidade do evento;
 - 2.3.2.11.10.2. Criticidade do ativo;
- 2.3.2.11.11. Como resultado da aplicação de regras, o correlacionador deve ser capaz de executar ações automáticas como: enviar e-mail, enviar mensagem para o usuário conectado ao console, executar comando e abrir caso na ferramenta de incidentes interna.
- 2.3.2.11.12. O correlacionador deve armazenar os eventos, alertas e incidentes na base de dados da solução.
- 2.3.2.11.13. Fornecer a informação sobre os eventos que compõem um alerta e/ou incidente de segurança, identificado pelas regras de correlação da solução, referenciando tais eventos básicos a partir do evento alerta/incidente.
- 2.3.2.11.14. Correlacionar os eventos coletados de forma a evidenciar incidentes que caracterizem um ataque.
- 2.3.2.11.15. A solução deve possuir um mecanismo de correlação avançada para processar e comparar informações de logs de diferentes fontes e fluxos de rede;
- 2.3.2.11.16. A solução deve permitir que os clientes escrevam suas próprias regras;
- 2.3.2.11.17. Deve fornecer a funcionalidade de geração de alertas (sonoros e/ou visuais) para incidentes de alta criticidade detectados no correlacionamento de eventos.
- 2.3.2.11.18. Deve fornecer a funcionalidade de verificação de conformidade com as políticas, controles e normas internas e externas.
- 2.3.2.11.19. Possuir a funcionalidade de geração de incidentes em módulos de tratamento interno.

- 2.3.2.11.20. Possuir a funcionalidade de definição de prioridade para os eventos, alerta e incidente.
- 2.3.2.11.21. O correlacionador deverá estar dimensionado e licenciado para processar 10% dos eventos coletados.
- 2.3.2.11.22. solução deve notificar e associar comportamentos anômalos baseados em múltiplos eventos que ocorrerem em um determinado período de tempo;
- 2.3.2.11.23. A correlação de eventos deve possuir uma linha de base (baseline) comportamental da rede, definido por suas regras de correlações, fornecendo alertas sempre que ocorrer algum evento fora do comportamento normal;
- 2.3.2.11.24. A solução deve possuir a capacidade de prover contextualização de dados de alertas de fontes diversas (ativos de rede e/ou segurança, servidores, aplicações, etc.) em um único console, otimizando com isso a capacidade e prazos de análise no processo de resposta a incidentes de segurança;
- 2.3.2.11.25. A solução deve possibilitar o envio de notificações ou alertas baseados no fator de importância e criticidade do ativo/dispositivo perante ao negócio;
- 2.3.2.11.26. Possuir mecanismo de controle de acesso baseado em autenticação de usuário integrada com serviço de diretório Microsoft AD;
- 2.3.2.11.27. Possuir acesso seguro e criptografado de forma a garantir a autenticidade, confidencialidade e integridade dos dados;
- 2.3.2.11.28. Manter seu próprio log de auditoria.
- 2.3.2.11.29. Fornecer visualização e ações diferenciadas por perfis de acesso;
- 2.3.2.11.30. Permitir que as visualizações e ações sejam personalizadas por grupos de usuários;
- 2.3.2.11.31. Ter a funcionalidade de utilização de ACL (Listas de Controle de Acesso) ou configuração via interface gráfica para limitar os recursos da solução aos grupos de usuários, conforme critério definido pelo órgão;
- 2.3.2.11.32. Possuir a capacidade de efetuar a segregação de funções dos usuários da solução;
- 2.3.2.11.33. Ter a funcionalidade de visualização de eventos e alertas de segurança em tempo real;
- 2.3.2.11.34. Ser capaz de criação de novas regras e alteração das existentes;
- 2.3.2.11.35. Exibir os eventos que compõem um alerta e/ou incidente de segurança identificado pelas regras de correlação da solução, referenciando estes eventos básicos a partir de evento de alerta/incidente;
- 2.3.2.11.36. Permitir a criação de novos painéis gráficos (dashboards) e alteração dos existentes;
- 2.3.2.11.37. Permitir a criação de novos relatórios e alteração dos existentes;
- 2.3.2.11.38. Permitir o agendamento de geração de relatórios periódicos e notificar/enviar automaticamente os relatórios gerados para os destinatários dos mesmos;
- 2.3.2.11.39. Permitir a criação de listas (watchlist) e alteração das existentes. Deve permitir a inserção e remoção dos dados de forma manual e automática através de regras;
- 2.3.2.11.40. Permitir a inserção manual de anotações em alertas;
- 2.3.2.11.41. A solução deve ser capaz de notificar o(s) administrador(es), ou usuários cadastrados, caso algum dispositivo monitorado pare de enviar eventos;
- 2.3.2.11.42. As funções de manutenção e operação da solução podem estar integradas no

mesmo console de administração. A solução deve:

- 2.3.2.11.42.1. Possuir acesso controlado e autenticado por usuário, baseado na autenticação integrada com serviço de diretório como Microsoft AD, Open-LDAP, ou similares, podendo ser o mesmo console de administração;
- 2.3.2.11.42.2. Possuir acesso seguro e criptografado de forma a garantir a autenticidade, confidencialidade e integridade dos dados.
- 2.3.2.11.42.3. Permitir a instalação de certificado digital para prover o acesso seguro, e configurar o repositório de certificados confiáveis.
- 2.3.2.11.42.4. Fornecer visualização e ações diferenciadas por perfis de acesso;
- 2.3.2.11.42.5. As visualizações e ações devem ser personalizadas por grupos de usuários, conforme critério do administrador;
- 2.3.2.11.42.6. Deve permitir a configuração via interface gráfica da lista de controle de acesso para limitar o acesso dos grupos de usuários aos recursos da solução, conforme critério do administrador;
- 2.3.2.11.42.7. Deve permitir a segregação de funções dos usuários da solução;
- 2.3.2.11.42.8. Deve permitir a visualização de eventos, alertas e incidentes;
- 2.3.2.11.42.9. Deve permitir a pesquisa nos eventos históricos, fornecendo capacidade de "drill-down", ou seja, visualizar os detalhes dos eventos, inclusive dado "raw", quando aplicável, para análise forense e investigação de incidentes;
- 2.3.2.11.43. Deve informar os eventos que compõem um alerta e/ou incidente de segurança de identificado pelas regras de correlação da solução, referenciando estes eventos básicos a partir do evento de alerta/incidente;
- 2.3.2.11.44. Deve permitir nativamente a visualização de painéis (dashboards), relatórios, listas (watchlists) e ter a funcionalidade de inserir e remover dados manualmente;
- 2.3.2.11.45. A solução deve possuir ferramenta de tratamento de incidentes interna ou ser fornecida com solução de tratamento de incidentes de segurança externa integrada, mesmo que de outro fabricante.
- 2.3.2.11.46. O tratamento de incidentes deve permitir a geração e escalção automatizada de casos.
- 2.3.2.11.47. Deverá possuir recurso de workflow automatizado, de forma que ações de criação, alteração e fechamento de casos possam ser realizadas automaticamente, como ações resultantes das regras de correlacionamento
- 2.3.2.11.48. Deve permitir o registro de ações tomadas e planejadas
- 2.3.2.11.49. Deve anexar os eventos relacionados ao caso, assim como relatórios e dashboards de forma a permitir a visualização de todo o histórico da investigação do chamado de segurança.
- 2.3.2.11.50. Deverá se integrar nativamente com a ferramenta de incidentes externos, permitindo que o SIEM abra casos na ferramenta externa diretamente e automaticamente.
- 2.3.2.11.51. Deverá possuir uma base de inteligência de ameaças global que aplica contexto e apoia na priorização de riscos nos eventos gerados. Essa base de inteligência deve ser alimentada em conjunto com uma equipe de pesquisadores que operam em 24/7 monitorando constantemente as ameaças ao redor do mundo.
- 2.3.2.11.52. A correlação de eventos deve ser feita por meio de regras de comportamento pré

programadas e implementadas pelo administrador. A correlação deve, minimamente, gerar informação, por meio da identificação de padrões de comportamento, obtidos dos registros enviados pelos ativos computacionais de rede adequados, a fim de:

- 2.3.2.11.52.1. correlacionar e alertar quanto ao uso impróprio de identidades em serviços de diretórios;
- 2.3.2.11.52.2. detectar comportamentos suspeitos de serem maliciosos;
- 2.3.2.11.52.3. categorizar comportamentos suspeitos quanto à criticidade do alerta;
- 2.3.2.11.52.4. alertar ameaças à proteção dos dados quanto aos requisitos de confidencialidade, integridade e disponibilidade;
- 2.3.2.11.52.5. analisar tráfego de rede para a identificação de ameaças e instruções de remediação;
- 2.3.2.11.52.6. alertar quanto à ocorrência de ataques a serviços web, minimamente, aqueles enumerados no "Open Web Application Security Project" (OWASP);
- 2.3.2.11.52.7. identificar comportamentos maliciosos de aplicações de estações de trabalho, tais como ActiveX, Adobe Flash Player, Java, Javascript;
- 2.3.2.11.52.8. identificar e alertar ataques de autenticação, tais como ataque de força bruta e de dicionário em serviços de rede (p.e. SSH, LDAP, NetBIOS, serviços de diretórios, etc.);
- 2.3.2.11.52.9. identificar atividades de negação de serviço;
- 2.3.2.11.52.10. detectar atuação de programas suspeitos (p.e. programas espiões, cavalos de tróia, rede zumbi – botnet – entre outras);
- 2.3.2.11.52.11. detectar e alertar ataques de rede (p.e. mascaramento de IP, tentativa de sequestro de sessão, etc.);
- 2.3.2.11.52.12. detectar e alertar comportamentos de violação de políticas de segurança (p.e. uso de proxy anônimo, redes P2P e BitTorrent, login em rede Tor, etc.);
- 2.3.2.11.52.13. detectar e alertar demais comportamentos suspeitos que visem a comprometer os requisitos fundamentais de segurança (confidencialidade, integridade e disponibilidade).
- 2.3.2.11.52.14. A solução deve estar adequada a procedimentos legais a fim de:
- 2.3.2.11.52.15. detectar e rastrear comportamentos suspeitos;
- 2.3.2.11.52.16. fornecer base de conhecimento e relatórios para justificação de decisões administrativas que venham a ser necessárias para o incremento de segurança;
- 2.3.2.11.52.17. apoiar procedimentos de análise e correlação das evidências para fins de perícia e apresentação do caso em juízo;
- 2.3.2.11.52.18. produzir as respostas em tempo suficiente para que ações de defesa possam ser postas em prática de maneira efetiva (resposta em tempo real ou quase-real).

2.3.2.12. PERFIS DE ACESSO

- 2.3.2.12.1. A solução deve permitir diferentes perfis de acesso ao sistema cujas permissões se dividem, minimamente, entre os seguintes perfis:
 - 2.3.2.12.1.1. administrador – para configurar parâmetros do equipamento;

- 2.3.2.12.1.2. operador – para operar o equipamento e executar ações padronizadas referente aos eventos registrados.
- 2.3.2.12.2. A solução deve permitir, minimamente, a utilização por 20 usuários entre administradores e operadores.
- 2.3.2.12.3. O perfil de administração deve conter, minimamente, as funções de:
 - 2.3.2.12.3.1. cadastro, edição e remoção de usuários administradores e operadores;
 - 2.3.2.12.3.2. cadastro, edição e remoção de regras de comportamento suspeito;
 - 2.3.2.12.3.3. criação, edição e remoção de conectores personalizados;
 - 2.3.2.12.3.4. criação, edição e remoção de regras de correlacionamento;
 - 2.3.2.12.3.5. funções do perfil operador.
- 2.3.2.12.4. O perfil de operador deve conter, minimamente, as funções de:
 - 2.3.2.12.4.1. visualização de estatísticas de ataques, indicando IP e portas de origem;
 - 2.3.2.12.4.2. número total de eventos suspeitos;
 - 2.3.2.12.4.3. grau de severidade geral dos eventos analisados;
 - 2.3.2.12.4.4. estações de trabalho suspeitas;
 - 2.3.2.12.4.5. categorização por tipo de produto gerador de evento suspeito correlacionado; e
 - 2.3.2.12.4.6. realização de pesquisas de eventos na base de dados, minimamente, por:
 - 2.3.2.12.4.6.1. IP de origem;
 - 2.3.2.12.4.6.2. assinatura de ataque;
 - 2.3.2.12.4.6.3. tipo de sensor;
 - 2.3.2.12.4.6.4. nome de vulnerabilidade;
 - 2.3.2.12.4.6.5. país de origem; e
 - 2.3.2.12.4.6.6. data e horário.
- 2.3.2.13. INSTALAÇÃO E ADMINISTRAÇÃO DA SOLUÇÃO DE SIEM
 - 2.3.2.13.1. A contratada deverá implementar e fazer a gestão de toda a solução de SIEM e de todos os seus componentes;
 - 2.3.2.13.2. A contratada será responsável pela migração das regras existentes na solução atual e criação de novas regras de correlação que reflitam as reais necessidades do ambiente do IBGE com o objetivo de identificar possível incidentes de segurança;
 - 2.3.2.13.3. A contratada será responsável pela criação de regras de correlação que reflitam as reais necessidades do ambiente do IBGE com o objetivo de identificar possível incidentes de segurança;
 - 2.3.2.13.4. Criar relatórios e modelos, criar filtros de pesquisa, fazer backups, criar dashboards, gerenciar usuários e utilizar os principais recursos da solução;
 - 2.3.2.13.5. Apresentar plano de instalação e configuração, que deverá contemplar todos os tipos de ativos em produção na rede da contratante.
 - 2.3.2.13.6. Atualizar os sistemas operacionais e demais softwares para a última versão disponível compatível com a solução ofertada.

- 2.3.2.13.7. Qualquer dano causado às instalações do IBGE ou aos equipamentos nele existentes deve ser reparado pela CONTRATADA conforme recomendação do fabricante ou Representante autorizado do equipamento danificado;
- 2.3.2.13.8. Os serviços de instalação de coletores nos ambiente do IBGE deverão ser realizados em horário previamente combinado com o IBGE, preferencialmente no horário de expediente normal do IBGE (2ª a 6ª feira, das 8h00min às 18h00min);
- 2.3.2.13.9. Qualquer atividade que possa colocar em risco o funcionamento normal das unidades do IBGE deverá, necessariamente, ser executada fora do horário do expediente, de 2ª a 6ª feira, entre 6h00min e 8h00min e entre 18h00min e 24h00min, e nos sábados e domingos, das 7h00min às 21h00min, sem custo adicional para o IBGE;
- 2.3.2.13.10. Fornecimento das licenças e execução da instalação ou atualização de todas as novas versões ou releases da solução, incluindo seus softwares e firmwares, disponibilizados pelo fabricante da solução, bem como a aplicação de correções (patches) dos softwares e firmwares da solução nas instalações do IBGE ou de forma remota.

3. SERVIÇOS PARA O ITEM 3

3.1.1. Indicação das atividades e criticidade, para aplicação dos níveis mínimos de serviço :

FASE	CRITICIDADE (Conforme item 7.4 do termo de referência - NMS)
Plano de Resposta aos Incidentes	MÉDIA
Suporte especializado	ALTA
Manutenção preventiva	MÉDIA
Resposta aos incidentes	ALTA
Análise de causa raiz (forense)	BAIXA

3.2. Prevenção e resposta aos incidentes

3.2.1. Plano de Resposta aos Incidentes

- 3.2.1.1. A CONTRATADA deve elaborar um Plano de Resposta aos Incidentes mais comuns. Tal plano deve conter, minimamente:
- 3.2.1.2. Tipo de incidente;
- 3.2.1.3. Ações a serem realizadas;
- 3.2.1.4. Responsáveis pela execução das ações, incluindo nome, telefone e e-mail.

3.2.2. Suporte especializado

- 3.2.2.1. Quanto ao suporte especializado a CONTRATADA deve:

- 3.2.2.2. Permitir a abertura, acompanhamento e validação de chamados através de e-mail, web site (portal do cliente), mensagem (MSTeams) e telefone (0800) no regime 24x7x365, com atendimento bilíngue (português e inglês);
- 3.2.2.3. Possuir processo de escalação funcional, mapeamento e documentado, com os seguintes níveis de atendimento: N1, N2 e N3, conforme melhores práticas descritas pelo ITIL;
- 3.2.2.4. Possuir canal com os fabricantes envolvidos na solução dos incidentes, bem como ser responsável pela abertura e acompanhamento dos chamados junto aos mesmos;
- 3.2.2.5. Possuir análise técnica documentada pelo N3 do SOC antes do envolvimento dos fabricantes, a fim de garantir o processo de escalação funcional.
- 3.2.2.6. Possuir os processos de gerenciamento de incidente, requisição, eventos, problemas, mudanças, incidentes críticos e atendimento aos usuários VIPs mapeados e documentados de acordo com as melhores práticas descritas pelo ITIL;
- 3.2.2.7. Os administradores de tecnologia do CONTRATANTE terão total acesso à plataforma para fins de auditoria, porém a responsabilidade pela operação diária da solução será da CONTRATADA.

3.2.3. Manutenção preventiva

- 3.2.3.1. Quanto à manutenção preventiva a CONTRATADA deve:
- 3.2.3.2. Atualizar os firmwares e/ou softwares das soluções que compõe a solução e das respectivas consoles de gerenciamento;
- 3.2.3.3. Realizar os ajustes e melhorias constantes, de acordo com as melhores práticas dos fabricantes, as mantendo documentadas e acessíveis no portal do cliente;
- 3.2.3.4. Propor melhorias no ambiente de forma proativa, periodicamente, as mantendo documentadas no portal do cliente e as submetendo para a aprovação da CONTRATANTE.

3.2.4. Resposta aos incidentes.

- 3.2.4.1. A implantação de controles e ajustes necessários durante um eventual incidente nas demais ferramentas de segurança no ambiente tecnológico da CONTRATANTE, fora do horário comercial, serão de responsabilidade da CONTRATADA.
- 3.2.4.2. A implantação dos demais controles e ajustes necessários durante um eventual incidente serão de responsabilidade da CONTRATANTE.

3.3. Análise de causa raiz (forense)

- 3.3.1. Para cada incidente identificado deverá ser elaborado e entregue um relatório detalhando minimamente:
 - 3.3.1.1. Os impactos observados;
 - 3.3.1.2. A(s) vulnerabilidade(s) explorada(s);
 - 3.3.1.3. O método de ataque;
 - 3.3.1.4. A origem do ataque.

ANEXO I-B - DESCRIÇÃO DO AMBIENTE COMPUTACIONAL DO IBGE

A Instituto Brasileiro de Geografia e Estatística (IBGE) possui em julho de 2021, segundo o SDA, 4.342 servidores públicos e 5.942 contratos temporários distribuídos por todos os Estados da Federação e no Distrito Federal. O ambiente computacional possui estações de trabalho, notebooks, impressoras, servidores, switches de rede, storage, firewall, wi-fi access points, sistemas de backup, smartphones, tablets e outros.

As tabelas abaixo ilustram o ambiente atual da IBGE (https://www.ibge.gov.br/np_download/novoportal/documentos_institucionais/PDTI_2023_2024.pdf) .

ANEXO I-C – TERMO DE COMPROMISSO DE MANUTENÇÃO DO SIGILO**INTRODUÇÃO**

O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da Contratante em decorrência de relação contratual, vigente ou não.

Referência: Art. 18, Inciso V, alínea “a” da IN SGD/ME Nº 94/2022.

Pelo presente instrumento o <NOME DO ÓRGÃO>, sediado em <ENDEREÇO>, CNPJ nº <CNPJ>, doravante denominado CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ nº <Nº do CNPJ>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º <nº do contrato> doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da CONTRATANTE;

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

1 – OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas disponibilizadas pela CONTRATANTE e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

2 – CONCEITOS E DEFINIÇÕES

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

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

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

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

3 – DA INFORMAÇÃO SIGILOSA

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

4 – DOS LIMITES DO SIGILO

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

- I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;
- II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;
- III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

5 – DIREITOS E OBRIGAÇÕES

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

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

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

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

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

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

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

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

- I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;
- II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;
- III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e
- IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

6 – VIGÊNCIA

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

7 – PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 156 da Lei 14.133/21.

8 – DISPOSIÇÕES GERAIS

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

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes

buscarão solucionar as divergências de acordo com os princípios de boafé, da equidade, da razoabilidade, da economicidade e da moralidade.

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

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

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

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo; IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

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

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

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

9 – FORO

A CONTRATANTE elege o foro da <CIDADE DA CONTRATANTE>, 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

10 – ASSINATURAS

COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

CONTRATADA	CONTRATANTE
<Nome> <Qualificação>	<Nome> Matrícula: xxxxxxxx
TESTEMUNHAS	
<Nome> <Qualificação>	<Nome> <Qualificação>

ANEXO I-D - TERMO DE CIÊNCIA

INTRODUÇÃO			
O Termo de Ciência visa obter o comprometimento formal dos empregados da Contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no órgão/entidade. No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados. Referência: Art. 18, Inciso V, alínea “b” da IN SGD/ME Nº 94/2022.			
1 – IDENTIFICAÇÃO			
CONTRATO Nº	xxxx/aaaa		
OBJETO	<objeto do contrato>		
CONTRATADA	<nome da contratada>	CNPJ	xxxxxxxxxxxxx
PREPOSTO	<Nome do Preposto da Contratada>		
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>	MATR.	xxxxxxxxxxxxx

2 – CIÊNCIA

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

Funcionários da Contratada		
Nome	Matrícula	Assinatura
<Nome do(a) Funcionário(a)>	<xxxxxxxxxx>	
<Nome do(a) Funcionário(a)>	<xxxxxxxxxx>	
☐		

ANEXO I-E - SISTEMAS DO IBGE AGRUPADOS POR TEMA

Grupo	Sistemas
Censo Demográfico	
	Aplicações GTD
	SAPC
	SIGC Censo Demográfico
	Questionário WEB
Pesquisa Agropecuárias	
	PCA Centralizado
	SIGC Censo Agro
	Projeto de sensoriamento remoto
Pesquisas Domiciliares e Sociais	
	SIGC
	SIGC CNEFE
	SIQ-GERINS
	SIGC Registro Civil
	SISCOD
	POF6 2018
	SIGC PENSE
	SIGC MUNIC
	SIGC PNSB
	SIGC CNEFE
	PNADC
	Amostra Mestra
	SIGC PNDS
	SIGC PeNSE
	ESTADIC
Pesquisas Econômicas	
	PMC - Módulo UE
	PMS - Módulo UE
	SIPEA
	SIGC SNIPC
	SIGC SINAPI
	Painel Pesquisas Conjunturais
	Painel Pesquisas Estruturais por Empresas
	PIMPPF Gerenciador
	CEMPRE
Pesquisas Geociências	
	FMESERVER
	Base Territorial

TERMO DE REFERÊNCIA - SERVIÇOS DE TIC - LICITAÇÃO

Sistemas Administrativos	
	BDO
	Central de Atendimento
	SDA
	Eleição Conselho Curados
	Eleição CGPCC
	Novos Servidores
	Acompanhamento servidores
	GED
	SAPC
	Loja Virtual IBGE
	ContacCenter
	BITIC
	BIDECOF
	Movimentados do BNDES
	Auditoria Interna
	Kbasetic
	Trabalho Remoto
	Escritório de Projetos
	Tarifador
	EDATA
	Lista telefônica
	Gestão de riscos
	Cadastro de editais
	Custo deslocamento
	Atendimento IBGE
	CEMPRE Web
Sistemas de Treinamento	
	PCA Centralizado
	IPP
	SIGC MUNIC
	SIGC PNADC
	SIGC Registro Civil
	SIGC SINAPI
	SIGC SNIPC
	SIPEA
	SISCOD
	SIGC VEG
	PCA CENTRALIZADO
	GESTAO DE RISCOS
	SISCOD2
Sites Intranet	
	Intranet IBGE

TERMO DE REFERÊNCIA - SERVIÇOS DE TIC - LICITAÇÃO

	Intranet CDDI
	Intranet DGC
	Intranet DE
	Intranet DI
	Intranet DPE
	Intranet Presidência
	Intranet AL
	Intranet AM
	Intranet BA
	Intranet CE
	Intranet DF
	Intranet ES
	Intranet GO
	Intranet MG
	Intranet MT
	Intranet PB
	Intranet PR
	Intranet RJ
	Intranet RO
	Intranet RS
	Intranet SC
	Intranet SP
	Intranet TO
Sites Internet	
	Escola Virtual
	ENCE
	IBGE
	Quarentena
	WEBMAIL IBGE
	SIDRA
	Metadado
	BME
Aplicação Desktop	
	Apps Extranet IBGE
	Ultimus
	SAS Enterprise Guide
	SUPORTE TIC

ANEXO I-F - Termo de Responsabilidade de Terceiros sobre Ativo de Tecnologia do IBGE

Termo de Responsabilidade de Terceiros sobre Ativo de Tecnologia do IBGE

Eu, _____ (nome), nascido no(a) _____ (país), _____ (estado civil), _____ (profissão), documento de identidade nº _____, expedido pela _____/_____(UF), CPF nº _____, residente e domiciliado em _____, doravante chamado _____ consultor, e eu, _____ (nome), nascido no(a) _____ (país), _____ (estado civil), _____ (profissão), documento de identidade nº _____, expedido pela _____/_____(UF), CPF nº _____, residente e domiciliado em _____, preposto da empresa _____, no contrato _____ perante a FUNDAÇÃO INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA – IBGE, fundação pública vinculada ao Ministério do Planejamento e Orçamento, instituída nos termos do Decreto-Lei n. 161, de 13 de fevereiro de 1967, com duração indeterminada, com sede na Avenida Franklin Roosevelt, n. 166, na cidade do Rio de Janeiro (RJ), CEP: 20.021-120, inscrita no CNPJ sob o n. 33.787.094/0001-40, regida pela Lei n. 5.878, de 11 de maio de 1973 na forma do Estatuto da Fundação, aprovado pelo Decreto n. 11.177, de 18 de agosto de 2022 e demais disposições que lhe sejam aplicáveis, em concordância com a Política de Segurança da Informação e Comunicações do IBGE, responsabilizo-me pelo(s) ativo(s) de tecnologia da informação tipo _____ modelo _____ número de série _____ ano _____ patrimônio _____, comprometendo-me a:

- a) zelar pela guarda, conservação e devolução do(s) mesmo(s);
- b) utilizá-lo (s) de forma eficiente e eficaz, obedecendo os aspectos éticos legais, para condução dos projetos ou atividades de interesse do IBGE;
- c) notificar imediatamente ao fiscal técnico do contrato as avarias ou danos que esse(s) venha(m) a sofrer, bem como em caso de perda(s) ou extravio(s) do ativo(s), estando ciente da minha responsabilidade sobre o ocorrido;
- d) assumir os custos de reparos de danos eventuais que não tenham origem no seu uso regular previsto (considerando avaliação técnica, se for o caso).
- e) notificar imediatamente ao fiscal técnico do contrato em caso de infecção por vírus e congêneres que prejudiquem a integridade dos sistemas do IBGE ou de seus arquivos;
- f) utilizar somente software que tenha como objetivo o desenvolvimento ou a execução dos projetos e atividades do IBGE, e sejam disponibilizados pelo IBGE ou objetos de efetivo e válido contrato de

TERMO DE REFERÊNCIA - SERVIÇOS DE TIC - LICITAÇÃO

cessão de direito de uso ou de avaliação, não instalando qualquer outro software não autorizado pelo IBGE;

- g) não emprestar, alugar ou vender o(s) ativo(s);
- g) devolver o(s) ativo(s) ao fiscal técnico do contrato após o encerramento das atividades ou projetos relacionados ao seu uso e/ou quando do término do contrato com o IBGE;
- h) registrar na autoridade policial da jurisdição a ocorrência de roubo ou furto do(s) ativo(s) e notificar este fato ao fiscal técnico do contrato, apresentando o respectivo Boletim de Ocorrência (B.O.). Verificado o dolo ou culpa no desaparecimento do Bem Móvel, o IBGE deverá ser ressarcido do valor do equipamento, sob pena de ajuizamento de ação por danos ao patrimônio público. Nos casos em que restar pagamentos a serem feitos à empresa, o IBGE fica autorizado a descontar o valor do equipamento roubado ou furtado dos pagamentos ainda restantes do contrato em vigor. Fica, ainda, o consultor ciente de que no caso de perda, roubo ou extravio do material, será providenciado o registro no Sistema Integrado de Administração Financeira do Governo Federal – SIAFI, na Conta Contábil correspondente a Crédito Administrativo Decorrente de Dano ao Patrimônio, no CPF do usuário, até a conclusão da apuração

O IBGE irá monitorar o conteúdo dos arquivos existentes em seu(s) ativo(s) de tecnologia da informação, buscando preservar a integridade das informações institucionais e manter o gerenciamento de seus sistemas.

A qualquer tempo e sem aviso prévio, o IBGE poderá exercer fiscalização com fins de auditoria e verificação do conteúdo dos arquivos e de uso não autorizado de software, inclusive para apuração de eventual uso indevido do ativo de tecnologia da informação, razão pela qual inexistirá qualquer espécie de direito à privacidade no uso do(s) referido(s) ativo(s) de tecnologia.

Todo e qualquer procedimento não previsto neste termo que possa danificar o(s) ativo(s) de tecnologia ou afetar de forma negativa o IBGE, seus funcionários, convênios, fornecedores ou parceiros, será de minha inteira e restrita responsabilidade.

A cessão desse equipamento se dá tempo definido para execução de minhas atividades para o IBGE, de acordo com o contrato _____ celebrado entre o IBGE e a empresa _____. Comprometo-me a devolver imediatamente ao IBGE o equipamento quando ocorrer o desligamento de minhas atividades no IBGE, seja pelo término do contrato entre as partes ou de minha relação jurídica com a empresa contratada.

A responsabilidade pelo equipamento é solidária entre a empresa contratada e o consultor contratado para prestação dos serviços.

O descumprimento de quaisquer dos compromissos do presente Termo é passível de sanções administrativas, cíveis e penais previstas no Estatuto do Servidor Público Federal (Lei n. 8.112, de 11 de dezembro de 1990), e pela avaliação da Comissão de Ética do IBGE, no Código Penal (Decreto-Lei n. 2.848, de 7 de dezembro de 1940, com as alterações da Lei n. 9.983, de 14 de julho de 2000) e no Código Civil (Lei n. 10.406, de 10 de janeiro de 2002), ou na legislação que regule ou venha a regular a matéria.

Elegem as partes o Foro da Justiça Federal da sede da Seção Judiciária do Rio de Janeiro como o competente para dirimir quaisquer questões oriundas do presente termo.

Declaro estar de acordo com o presente Termo.

TERMO DE REFERÊNCIA - SERVIÇOS DE TIC - LICITAÇÃO

consultor

_____, ____ de _____ de 20__.

preposto

_____, ____ de _____ de 20__.

ANEXO I-G - Modelo de Ordem de Serviço (OS) ou Ticket para abertura de chamados

ESTRUTURA DO MODELO

Número da OS ou Ticket

Data de emissão

Descrição detalhada do serviço

Quantidade de horas técnicas (mínimo 4h)

Local de execução (remoto/presencial)

Prazo para execução

Indicadores de qualidade (SLA)

Observações adicionais

Assinaturas ou Autorizações das partes (Contratada e Administração)



Documento assinado eletronicamente por FLAVIA MARINHO DE LIMA, Coordenador, em 10 de Março de 2026, às 21:57:54, horário de Brasília, com fundamento legal no § 3º do Art. 4º do Decreto Nº 10.543, de 13 de Novembro de 2020.



A autenticidade deste documento pode ser conferida no site <https://transparenciasda.ibge.gov.br/docs/validador.jsf> informando o código verificador 6591272168990920274 e o código CRC D3E73230.



Documento assinado eletronicamente por JUSSARA ROBERTA DE FREITAS SILVA, Gerente Nível II, em 11 de Março de 2026, às 10:04:17, horário de Brasília, com fundamento legal no § 3º do Art. 4º do Decreto Nº 10.543, de 13 de Novembro de 2020.



A autenticidade deste documento pode ser conferida no site <https://transparenciasda.ibge.gov.br/docs/validador.jsf> informando o código verificador 8640431090520997022 e o código CRC 353D3A99.



Documento assinado eletronicamente por ANTONIO AGRA LOPES NETO, Gerente Nível II, em 11 de Março de 2026, às 12:24:06, horário de Brasília, com fundamento legal no § 3º do Art. 4º do Decreto Nº 10.543, de 13 de Novembro de 2020.



A autenticidade deste documento pode ser conferida no site <https://transparenciasda.ibge.gov.br/docs/validador.jsf> informando o código verificador 5805077893650271203 e o código CRC 7060F779.



Documento assinado eletronicamente por MARCOS VINICIUS FERREIRA MAZONI, Diretor, em 11 de Março de 2026, às 16:56:01, horário de Brasília, com fundamento legal no § 3º do Art. 4º do Decreto Nº 10.543, de 13 de Novembro de 2020.



A autenticidade deste documento pode ser conferida no site <https://transparenciasda.ibge.gov.br/docs/validador.jsf> informando o código verificador 1955814608027824386 e o código CRC D3976495.

IBGE-FUN.INST.BRAS.GEOGRAFIA E ESTATISTICA

Estudo Técnico Preliminar 38/2025

1. Informações Básicas

Número do processo: 03603.000077/2025-45

2. Descrição da necessidade

2. Justificativa para Contratação de empresa especializada para execução de serviços técnicos contínuos referente ao Serviço Gerenciado de Segurança da Informação de forma REMOTA, pelo período de 24 (vinte e quatro) meses, conforme condições estabelecidas no presente Estudo Técnico Preliminar, podendo ser renovado até o limite da lei, conforme condições e exigências estabelecidas neste instrumento.

2.1. A crescente complexidade dos ambientes digitais e o aumento exponencial das ameaças cibernéticas exigem das instituições públicas uma postura proativa e estratégica na proteção de seus ativos de informação. Nesse contexto, torna-se imprescindível a contratação de um serviço especializado de Centro de Operações de Segurança (SOC), com capacidade técnica para realizar o monitoramento contínuo, a detecção e a resposta a incidentes de segurança da informação.

2.2. O SOC atua como uma unidade centralizada de defesa cibernética, composta por equipes especializadas (Blue Team e Red Team), responsáveis por:

2.2.1. Monitoramento e correlação de eventos de segurança, com análise de logs, tráfego de rede e comportamento de sistemas;

2.2.2. Gestão de incidentes de segurança, com resposta rápida e eficaz a ataques e falhas;

Execução de testes de invasão e avaliações de vulnerabilidades, visando identificar e corrigir brechas antes que sejam exploradas por agentes maliciosos;

2.2.3. Elaboração de relatórios técnicos e estratégicos, que subsidiam decisões gerenciais e fortalecem a governança de segurança da informação.

2.3. A contratação visa garantir a confidencialidade, integridade e disponibilidade dos dados institucionais, conforme diretrizes da Lei Geral de Proteção de Dados (LGPD) e da Nova Lei de Licitações e Contratos (Lei nº 14.133/2021). Além disso, contribui para o cumprimento de normativas internas e externas relacionadas à segurança da informação, como as resoluções do Comitê Gestor da Segurança da Informação e os requisitos de auditoria dos órgãos de controle.

2.4. Diante da inexistência de estrutura interna capaz de atender a essas demandas com a profundidade e a continuidade necessárias, a contratação de um SOC por meio de empresa especializada é a solução mais viável técnica e economicamente, conforme previsto no Termo de Referência e no Mapa de Gerenciamento de Riscos.

3. Área requisitante

Área Requisitante	Responsável
DTI/COTEC	Flávia Marinho de Lima

4. Necessidades de Negócio

- 4.1. Garantir a confidencialidade, integridade, autenticidade e disponibilidade das informações;
- 4.2. Manter a privacidade do informante e o sigilo das informações prestadas, conforme previsto na Lei n. 5534, de 14.11.68;
- 4.3. Permitir que as atividades desempenhadas na Instituição tratem as informações e estudos de natureza estatística, geográfica, cartográfica, demográfica e administrativa com a devida segurança para garantir a legalidade de suas ações;
Permitir maior transparência e autonomia na análise de eventuais vulnerabilidades encontradas na rede e nos Sistemas utilizados pelo IBGE, através da checagem do nível de segurança do IBGE;
- 4.4. Análise geral do ambiente do IBGE quanto a segurança da informação para identificar, mapear, documentar, controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica do IBGE;
- 4.5. Revisão e elaboração de um conjunto de documentos para a atualização constante da Política de Segurança da Informação do IBGE.
- 4.6. Formalizar os procedimentos e instruções para configuração de ativos de TI, de forma a padronizar e orientar os técnicos, bem como definir os responsáveis por sua atualização;
- 4.7. Ajustar a cultura de segurança da informação dentro da IBGE, abordando conceitos de boas práticas e a política e normas de segurança em vigor;
- 4.8. Contratação de empresa para prestação de serviços gerenciados de segurança;
- 4.9. Atuar na infraestrutura de serviços de informática do IBGE para otimização e atualização dos serviços;
- 4.10. Monitorar externa e internamente as aplicações web, servidores, virtualizadores e rede de forma proativa e reativa (com anuência do IBGE) no ambiente internet e intranet da instituição, bem como monitoramento constante de fóruns, grupos ativistas e de crackers, além de movimentações de ataques cibernéticos realizados por grupos articulados.

5. Necessidades Tecnológicas

- 5.1. Melhorar continuamente a prestação de serviços de TI.
- 5.2. Prover soluções tecnológicas para o atendimento das necessidades institucionais com o uso de tecnologias atualizadas.
- 5.3. Melhorar de forma efetiva a segurança da informação no ambiente da instituição.

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

- 6.1. Capacidade de operação contínua (24x7): A solução deve garantir monitoramento ininterrupto dos ativos de rede, sistemas e aplicações, com equipe técnica especializada disponível em tempo integral para resposta a incidentes, análise de alertas e mitigação de ameaças.
- 6.2. Infraestrutura tecnológica robusta e escalável: O fornecedor deve possuir infraestrutura própria ou contratada que permita a execução dos serviços de forma segura, com redundância, alta disponibilidade e escalabilidade conforme o crescimento da demanda institucional.
- 6.3. Conformidade com normas e boas práticas de segurança da informação: A solução deve estar alinhada com frameworks reconhecidos como ISO/IEC 27001, NIST Cybersecurity Framework, e atender aos requisitos da Política de Segurança da Informação da instituição.
- 6.4. Integração com ferramentas de SIEM e outras soluções de segurança: O SOC deve ser capaz de integrar-se com ferramentas de monitoramento, análise de logs, antivírus, firewalls, IDS/IPS, entre outras, para garantir uma visão holística do ambiente.
- 6.5. Equipe técnica qualificada e certificada: Os profissionais envolvidos devem possuir certificações reconhecidas na área de segurança da informação (ex.: CISSP, CEH, CompTIA Security+, etc.), além de experiência comprovada em ambientes similares ao da instituição:
 - 6.5.1. Os serviços deverão ser prestados por técnicos devidamente capacitados, de acordo com os critérios estabelecidos a seguir:

6.5.1.1. A fim de garantir a prestação do serviço em conformidade com o framework ITIL, a CONTRATADA deve possuir ao menos um profissional com a certificação ITIL Foundation;

6.5.1.2 A fim de garantir o conhecimento generalista em Segurança da Informação, a CONTRATADA deve possuir ao menos um profissional com a certificação CISSP ou CISM;

6.5.1.3 A fim de garantir o conhecimento técnico em Segurança da Informação, a CONTRATADA deve possuir ao menos um profissional com a certificação Security+;

6.5.1.4 A fim de garantir a existência de profissional com experiência de hacker ético, fundamental em momentos de crise de segurança, a CONTRATADA deve possuir ao menos um profissional com a certificação CEH, OSCP ou equivalente.

6.5.1.5 A empresa contratada deverá possuir certificação ISO/IEC 27001 durante toda a vigência do contrato, emitida em nome da CONTRATADA por organização independente acreditada por autoridade globalmente reconhecida.

6.5.1.6 A CONTRATADA deverá apresentar, em até 5 dias antes da assinatura do contrato, a comprovação da exigência de certificação listadas do itens 4.21.1 a 4.21.6 .

6.6. Relatórios gerenciais e técnicos periódicos: A contratada deverá fornecer relatórios mensais com indicadores de desempenho, eventos de segurança, ações corretivas e sugestões de melhoria, além de relatórios de incidentes em tempo real.

6.7. Plano de resposta a incidentes e continuidade de negócios: A solução deve incluir procedimentos formais para resposta a incidentes, contenção, erradicação e recuperação, bem como plano de continuidade de negócios em caso de falhas críticas.

6.8. Aderência à legislação vigente: A contratação deve observar os princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência, conforme previsto na Lei nº 14.133/2021, e atender às exigências da LGPD (Lei Geral de Proteção de Dados Pessoais).

6.9. Segurança física e lógica dos dados monitorados: A contratada deve garantir que os dados coletados e analisados estejam protegidos contra acessos não autorizados, vazamentos e alterações indevidas, com mecanismos de criptografia e controle de acesso.

6.10. Capacidade de atuação proativa e reativa: O SOC deve atuar preventivamente na identificação de vulnerabilidades e ameaças, bem como reativamente na contenção e mitigação de ataques, conforme definido em SLA (Acordo de Nível de Serviço).

7. Estimativa da demanda - quantidade de bens e serviços

7.1 Os serviços serão utilizados em diversas demandas relacionadas direta e indiretamente à proteção dos ativos de tecnologia da informação e comunicação (TIC) da instituição, conforme os assuntos abaixo:

7.1.1 O volume de trabalho estimado para esta contratação foi baseado nos registros históricos da Diretoria de Tecnologia da Informação do IBGE, coletados de sua Central de Atendimento, do PDTI vigente, dos dados apresentados no documento Relatório de Disponibilidade do Parque, que mostra o panorama do parque computacional e dos serviços de TIC do IBGE, e da análise de contratações similares de outros Órgãos da Administração Pública Federal (APF).

7.2 A demanda estimada contempla a prestação de serviços gerenciados de segurança da informação por meio de um Centro de Operações de Segurança (SOC) remoto, com funcionamento ininterrupto (24x7), abrangendo:

7.2.1. Monitoramento de segurança contínuo de aproximadamente 2100 mil ativos de rede, incluindo servidores físicos e virtuais, estações de trabalho, dispositivos de rede e aplicações críticas;

7.2.2. Análise de logs e eventos de segurança gerados por ferramentas como SIEM, IDS/IPS, antivírus, firewalls e sistemas operacionais;

7.2.3. Resposta a incidentes de segurança, com tempo de reação conforme níveis de criticidade definidos em SLA;

7.2.4. Emissão de relatórios técnicos e gerenciais mensais, além de relatórios de incidentes sob demanda;

7.2.5. Apoio na revisão e atualização da Política de Segurança da Informação e dos procedimentos operacionais relacionados à segurança;

7.2.6. Monitoramento de ameaças externas, incluindo grupos ativistas, fóruns e redes de compartilhamento de vulnerabilidades;

7.2.7. Apoio técnico na identificação e correção de vulnerabilidades em sistemas e infraestrutura de TIC.

7.3. A estimativa dos quantitativos apresentados neste processo foi construída com base em análise técnica fundamentada principalmente na demanda real observada no contrato anterior, cujo comportamento operacional se manteve estável ao longo do período analisado. Os volumes de consumo desse contrato, amplamente documentados em relatórios periódicos, dashboards de segurança, registros de incidentes e estatísticas operacionais elaborados pela Administração, constituem a melhor referência disponível para dimensionamento da necessidade atual.

7.3.1. A metodologia utilizada para a estimativa consistiu na consolidação dos dados históricos provenientes do ambiente de produção, especialmente aqueles relacionados ao número de alertas processados, incidentes tratados, chamados registrados nas plataformas internas da Central de Atendimento e via Correio Eletrônico quando a demanda é sigilosa, além da volumetria de eventos monitorados pelo SIEM. Esses dados foram obtidos diretamente dos documentos já existentes no IBGE, tais como relatórios mensais de operação, registros de desempenho e evidências extraídas das ferramentas corporativas, os quais refletem com precisão o comportamento da demanda típica do serviço dos itens a serem adquiridos conforme o ETP e TR.

7.3.2. Para fins de conformidade com o art. 15 da IN SGD/ME nº 94/2022, esclarece-se que a estimativa apresentada considerou séries históricas consolidadas do órgão, bem como evidências documentais que registram o consumo efetivo do serviço ao longo do contrato anterior. Embora os quantitativos tenham sido apresentados de forma sintética nos artefatos, toda a fundamentação utilizada está respaldada nos documentos oficiais já existentes no IBGE, que foram expressamente considerados pela equipe técnica na formação da estimativa. Assim, a metodologia adotada incorpora dados verificados, critérios objetivamente mensuráveis e amparo documental suficiente para atender às exigências normativas aplicáveis.

7.3.3. Dessa forma, entende-se que a justificativa de necessidade e a estimativa de consumo estão adequadamente fundamentadas, uma vez que se baseiam em informações confiáveis, historicamente aferidas e já disponíveis no IBGE, permitindo concluir pela pertinência dos quantitativos definidos para a contratação. A quantidade de serviços será dimensionada com base em:

7.3.3.1. Número de ativos monitorados;

7.3.3.2. Volume médio de eventos de segurança registrados mensalmente;

7.3.3.3. Complexidade do ambiente tecnológico do IBGE;

7.3.3.4. Necessidade de cobertura integral (24x7), incluindo finais de semana e feriados;

7.3.3.5. Escopo de atuação definido no Termo de Referência, que incluirá atividades proativas e reativas de segurança.

7.4. A contratação será realizada por meio de licitação, conforme previsto na Lei nº 14.133/2021, e observará os princípios da economicidade, eficiência e adequação ao interesse público, com base em estudo comparativo de preços praticados por outros órgãos da Administração Pública Federal.

8. Levantamento de soluções

8.1 A solução proposta consiste na **prestação de serviços gerenciados de segurança da informação**, por meio de um **Centro de Operações de Segurança (SOC) remoto com funcionamento contínuo (24x7)**, pelo período inicial de 2 anos, com possibilidade de prorrogação conforme previsto na Lei nº 14.133/2021, até o limite da lei, conforme condições e exigências estabelecidas neste instrumento.

8.2 O escopo da solução inclui:

- Monitoramento contínuo e remoto dos ativos de TIC da instituição, abrangendo servidores, aplicações, redes e dispositivos de segurança;
- Execução de testes de intrusão internos e externos, com periodicidade definida em contrato;
- Gestão de vulnerabilidades, com identificação, classificação, priorização e recomendação de correções;
- Monitoramento de ameaças cibernéticas em fontes abertas, deep web e dark web, incluindo menções à marca institucional;

- Resposta a incidentes de segurança, com atuação proativa e reativa conforme níveis de criticidade;
- Emissão de relatórios técnicos e gerenciais periódicos, com indicadores de desempenho, eventos de segurança e recomendações;

8.3 Alternativas de Solução Consideradas

Solução 1 – Interna com Ferramentas e Equipe Própria

Aquisição de ferramentas de segurança, capacitação de equipe interna e estruturação de processos para gestão de vulnerabilidades, monitoramento da marca, detecção e resposta a incidentes.

Desvantagens: Elevado custo inicial, necessidade de equipe especializada, tempo de implantação e risco de descontinuidade por rotatividade de pessoal.

Solução 2 – SOC Presencial nas Dependências da Instituição

Contratação de empresa especializada para montar e operar um SOC físico dentro das instalações da instituição, com equipe dedicada.

Desvantagens: Exige espaço físico, infraestrutura local, maior custo operacional e menor flexibilidade para escalabilidade.

Solução 3 – SOC Remoto 24x7 (Solução Recomendada)

Contratação de empresa especializada para operar um SOC remoto, com equipe técnica dedicada e infraestrutura própria, garantindo monitoramento contínuo, gestão de vulnerabilidades, resposta a incidentes e consultoria especializada.

Vantagens: Redução de custos com infraestrutura local, maior escalabilidade, acesso a equipe especializada, operação contínua e aderência às melhores práticas do mercado.

9. Análise comparativa de soluções

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			X

	Solução 3			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X

10. Registro de soluções consideradas inviáveis

10.1. Solução 1 – Estruturação interna com ferramentas e equipe própria

A implantação de um SOC interno, com aquisição de ferramentas especializadas, treinamento contínuo e alocação de equipe técnica dedicada em regime 24x7, foi considerada inviável. Essa alternativa exige investimentos elevados em infraestrutura, licenciamento de software, capacitação constante e manutenção de uma equipe altamente especializada. Além disso, a rápida evolução das ameaças cibernéticas demanda atualização contínua de conhecimento e tecnologia, o que representa um risco à sustentabilidade operacional e à efetividade da solução. Diante da inviabilidade técnica e operacional, não foi realizado levantamento de custos para esta alternativa.

10.2. Solução 2 – SOC presencial nas dependências da instituição

A contratação de empresa especializada para montar e operar um SOC físico dentro das instalações da instituição também foi considerada inviável. Essa alternativa implica em complexidade logística, necessidade de espaço físico adequado, infraestrutura local, e maior custo com deslocamento e manutenção de equipe dedicada. Além disso, limita a escalabilidade e a flexibilidade da operação, dificultando a adaptação a cenários emergenciais ou de expansão da demanda.

10.2. Solução 3 – SOC remoto 24x7 (Solução viável)

A contratação de empresa especializada para prestação de serviços gerenciados de segurança da informação por meio de SOC remoto, com operação contínua (24x7), foi considerada viável e recomendada. A solução contempla gestão de vulnerabilidades, monitoramento da marca institucional em ambientes externos, detecção e resposta a incidentes de segurança, e emissão de relatórios técnicos e gerenciais. A operação remota permite maior escalabilidade, redução de custos com infraestrutura local, e aderência às melhores práticas de segurança da informação. A solução é compatível com o uso de serviços em nuvem, considerando que os dados trafegados são de controle e monitoramento, sem envolvimento direto de documentos sigilosos ou informações críticas que comprometam as atividades institucionais.

11. Análise comparativa de custos (TCO)

11.1. Solução Viável 3

Foi feita a análise do custo total pelos 24 meses desta contratação, com aplicação da previsão futura de reajuste conforme índice IPCA.

GRUPO	Nº DO ITEM	DESCRIÇÃO	MÉDIA/MEDIANA DO VALOR TOTAL DO ITEM	ANO 1	ANO 2 + (REAJUSTE IPCA: ANO 1 + 4,9%)
1	1	Gestão de Riscos - Processo integrado envolvendo a Gestão de Vulnerabilidades, Gestão de Riscos, Compliance e Monitoração de Marca CATSER: 27014	R\$4.163.712,00	R\$4.163.712,00	R\$4.367.733,89
1	2	Gestão de Incidentes - Processo integrado envolvendo a Análise de Incidentes Globais e o Monitoramento de Incidentes CATSER: 27014	R\$1.713.551,52	R\$1.713.551,52	R\$1.797.515,54
1	3	Resposta aos Incidentes - Processo integrado envolvendo a prevenção, bloqueio e resposta aos incidentes, bem como a análise de sua causa raiz CATSER: 27014	R\$1.050.624,00	R\$1.050.624,00	R\$1.102.104,58
		Total	**R\$ 6.927.887,52**	R\$6.927.887,52	R\$7.267.354,01

11.2. Justificativa Técnica e Econômica

A solução remota apresenta **menor custo de propriedade** em comparação com alternativas presenciais ou internas, por eliminar despesas com infraestrutura física, equipe dedicada local e manutenção de ferramentas. Além disso, permite **escalabilidade**, **redução de riscos operacionais** e **acesso a expertise especializada**, o que contribui para a **eficiência e efetividade da segurança da informação institucional**.

12. Descrição da solução de TIC a ser contratada

Item Objeto		Descrição	Quantidade	Unidade
1	Gestão de Riscos CATSER - 27014	Processo integrado envolvendo a Gestão de Vulnerabilidades, Compliance e Monitoração de Marca	24	UM
2	Gestão de Incidentes CATSER - 27014	Processo integrado envolvendo a Análise de Incidentes Globais e o Monitoramento de Incidentes	24	UM
3	Resposta aos Incidentes CATSER - 27014	Processo integrado envolvendo a prevenção, bloqueio e resposta aos incidentes, bem como a análise de sua causa raiz	24	UM

12. Considerações gerais (descrição):

12.1. Modelo de atuação:

12.1.1. A fim de garantir a qualidade da entrega do objeto como um todo, os itens desta contratação devem possuir o seguinte modelo de atuação:

12.1.1.1. Tal serviço deve ser provido através de Centro de Operações de Segurança (Security Operation Center – SOC 24x7, de forma remota, atendendo ao descrito neste Termo de Referência.

12.1.1.2. Algumas atividades, após comum acordo com a CONTRATANTE, poderão ser realizadas mediante atendimento presencial ou virtual (exceto Pentest Físico) em uma das unidades localizadas no município do Rio de Janeiro ou São Paulo, em até 24 horas ao comunicado da CONTRATANTE:

12.1.1.2.1. Migração de versionamento dos equipamentos gerenciados;

- 12.1.1.2.2. Necessidade de modernização dos equipamentos gerenciados;
- 12.1.1.2.3. Incidentes massivos ou desastres;
- 12.1.1.2.4. Pentestes físicos (somente presencial);
- 12.1.1.2.5. Inacessibilidade dos equipamentos gerenciados.

12.1.1.3. Seguem os endereços das unidades RJ e SP:

Localidade	Endereço
Rio de Janeiro	Rua General Canabarro, 706, Maracanã, Rio de Janeiro - RJ. CEP 20271-205
São Paulo	Rua Urussuí, 93, ITAIM BIBI, São Paulo - SP. CEP 04542050

12.1.1.4. Além da operação e suporte das ferramentas entregues como objeto deste contrato, a CONTRATADA deverá atuar nas soluções de segurança da informação da CONTRATANTE fazendo recomendações das melhores práticas de segurança, provenientes de análises globais, e melhorias na proteção do ambiente. Visão do parque institucional do IBGE disponível em: https://www.ibge.gov.br/np_download/novoportal/documentos_institucionais/PDTI_2023_2024.pdf .

12.2. Bens e serviços que compõem a Solução:

- 12.2.1. Garantia de nível de serviço.
- 12.2.2. Transferência de conhecimento.
- 12.2.3. Disponibilidade dos serviços.
- 12.2.4. Demais itens apresentados no Anexo I-A Especificação Técnica

12.3. Requisitos de formação de equipe (capacitação dos profissionais):

- 12.3.1. A fim de garantir a prestação do serviço em conformidade com o framework ITIL, a CONTRATADA deve possuir ao menos um profissional com a certificação ITIL Foundation;
- 12.3.2. A fim de garantir o conhecimento generalista em Segurança da Informação, a CONTRATADA deve possuir ao menos um profissional com a certificação CISSP ou CISM;
- 12.3.3. A fim de garantir o conhecimento técnico em Segurança da Informação, a CONTRATADA deve possuir ao menos um profissional com a certificação Security+;
- 12.3.4. A fim de garantir a existência de profissional com experiência de hacker ético, fundamental em momentos de crise de segurança, a CONTRATADA deve possuir ao menos um profissional com a certificação CEH, OSCP ou equivalente.
- 12.3.5. A empresa contratada deverá possuir certificação ISO/IEC 27001 durante toda a vigência do contrato, emitida em nome da CONTRATADA por organização independente acreditada por autoridade globalmente reconhecida.
- 12.3.6. A CONTRATADA deverá apresentar, em até 5 dias antes da assinatura do contrato, a comprovação da exigência de certificação listadas do itens 12.3.1 a 12.3.5 .

12.4. INFORMAÇÕES IMPORTANTES PARA O DIMENSIONAMENTO DA PROPOSTA:

12.4.1. A demanda do órgão tem como base as seguintes características:

12.4.1.1. Modelo de atuação:

12.4.1.2. Tal serviço deve ser provido através de Centro de Operações de Segurança (Security Operation Center – SOC) remoto.

12.4.1.3. As seguintes atividades, em comum acordo com a CONTRATANTE, deverão ser realizadas mediante atendimento presencial ou virtual (exceto Pentest Físico), em uma das unidades do município do Rio de Janeiro ou São Paulo, em até 24 horas ao comunicado da CONTRATANTE:

12.4.1.3.1. Migração de versionamento dos equipamentos gerenciados;

12.4.1.3.2. Modernização dos equipamentos gerenciados;

12.4.1.3.3. Incidentes massivos ou desastres;

12.4.1.3.4. Execução do Pentest Físico (Presencial);

12.4.1.3.5. Inacessibilidade dos equipamentos gerenciados.

12.4.1.3.6. Os endereços das unidades do Rio de Janeiro e São Paulo podem ser verificadas no link <https://www.ibge.gov.br/acesso-informacao/institucional/quem-e-quem.html>

12.4.1.3.7. Além da operação e suporte das ferramentas entregues como objeto deste contrato, a CONTRATADA deverá atuar nas soluções de segurança da informação da CONTRATANTE fazendo recomendações das melhores práticas de segurança, provenientes de análises globais, e melhorias na proteção do ambiente. Visão do parque institucional do IBGE disponível em: https://www.ibge.gov.br/np_download/novoportal/documentos_institucionais/PDTI_2023_2024.pdf.

12.4.1.4. A contratada deverá levar em consideração:

12.4.1.4.1. Entrega das ferramentas conforme indicado no Anexo I-A deste Termo de Referência, bem como a gerência dos serviços, entrega de relatórios, canais de comunicação, a forma de prestação do serviço e demais especificações deste Termo de Referência e seus anexos.

12.4.1.5. Descrição do ambiente de TIC do IBGE

12.4.1.5.1. **Nos Anexos I-A , I-B e I-C deste Estudo Técnico Preliminar foram apresentados os itens que compõem o parque tecnológico do IBGE, alvos deste estudo.**

12.4.1.5.3. Sistemas Computacionais:

Os recursos de tecnologia da informação utilizados pelo IBGE abrangem uma ampla gama de equipamentos computacionais, com diferentes capacidades de processamento, armazenamento e finalidade. O parque tecnológico inclui desde estações de trabalho convencionais (desktops e notebooks) utilizadas em atividades administrativas e operacionais, até servidores dedicados e supercomputadores voltados ao processamento de dados científicos e estatísticos de alta complexidade.

12.4.1.5.4. – Heterogeneidade do Parque Computacional:

O parque computacional do IBGE é caracterizado por sua heterogeneidade, resultado de aquisições realizadas ao longo dos anos com diferentes padrões técnicos e fornecedores, o que exige estratégias específicas de gestão, manutenção e segurança.

12.4.1.5.5. – Distribuição Geográfica:

A infraestrutura computacional está distribuída geograficamente entre as diversas unidades do IBGE em todo o território nacional. O Data Center principal está localizado na cidade do Rio de Janeiro, enquanto o Data Center secundário encontra-se em São Paulo, garantindo redundância e continuidade operacional.

12.4.1.5.6 – Requisitos de Segurança da Informação:

A confidencialidade, integridade, autenticidade e disponibilidade dos dados processados e armazenados nos ambientes computacionais do IBGE são requisitos críticos para o cumprimento da missão institucional. Diante disso, torna-se imprescindível a implementação progressiva de mecanismos avançados de segurança da informação, incluindo monitoramento contínuo, gestão de vulnerabilidades, controle de acesso, criptografia e resposta a incidentes.

12.5. Em até 5(cinco) dias antes da assinatura do contrato, a empresa vencedora deverá comprovar que possui em seu quadro de funcionários, pelo menos, os seguintes títulos/certificações:

- 12.5.1. Certificação ITIL Foundation;
- 12.5.2. Certificação CISSP ou CISM;
- 12.5.3. Certificação Security+;
- 12.5.4. Certificação CEH, OSCP ou equivalente
- 12.5.6. Certificação ISO/IEC 27001

13. Estimativa de custo total da contratação

Valor (R\$): 6.927.887,52

13.1 A estimativa de custo total da contratação foi elaborada com base em pesquisas de mercado, contratações similares realizadas por órgãos da Administração Pública disponíveis no Portal Compras.gov.br, e na análise do escopo técnico previsto para o serviço de **SOC remoto 24x7**.

13.2 A contratação contempla os seguintes componentes:

GRUPO	ITEM				VALOR UNITÁRIO	
-------	------	--	--	--	-------------------	--

		ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QUANTIDADE DO ITEM (A)	ESTIMADO (B)	VALOR TOTAL ESTIMADO (C = A x B)
1	1	Gestão de Riscos - Processo integrado envolvendo a Gestão de Vulnerabilidades, Gestão de Riscos, Compliance e Monitoração de Marca CATSER: 27014	Mês	24	R\$173.488,00	R\$4.163.712,00
	2	Gestão de Incidentes - Processo integrado envolvendo a Análise de Incidentes Globais e o Monitoramento de Incidentes CATSER: 27014	Mês	24	R\$71.397,98	R\$1.713.551,52
	3	Resposta aos Incidentes - Processo integrado envolvendo a prevenção, bloqueio e resposta aos incidentes, bem como a análise de sua causa raiz CATSER: 27014	Mês	24	R\$43.776,00	R\$1.050.624,00
		TOTAL	Mês	24	-	R\$6.927.887,52

Total estimado para 2 anos: R\$ 6.927.887,52

Caso haja prorrogação contratual conforme previsto na Lei nº 14.133/2021, deverá ser considerando a manutenção dos mesmos valores e escopo.

13.3 Observações

- Os valores apresentados são estimativas baseadas em contratações similares e poderão ser ajustados conforme resultado da pesquisa de preços oficial.
- A contratação será realizada por meio de licitação, observando os princípios da economicidade, eficiência e adequação ao interesse público.
- O modelo de contratação por serviço gerenciado permite previsibilidade orçamentária e escalabilidade conforme a evolução das necessidades institucionais.

14. Justificativa técnica da escolha da solução

14.1. A contratação de serviços gerenciados de segurança da informação, por meio de um **Centro de Operações de Segurança (SOC) remoto com funcionamento contínuo (24x7)**, é uma medida estratégica e necessária para garantir a proteção dos ativos tecnológicos da instituição, a continuidade dos serviços públicos e a conformidade com normas legais e regulatórias.

14.2. Fundamentação Legal

Nos termos do **art. 18 da Lei nº 14.133/2021**, o Estudo Técnico Preliminar deve evidenciar o problema a ser resolvido e a melhor solução disponível, considerando a viabilidade técnica e econômica da contratação. A contratação de serviços especializados de segurança da informação está alinhada com os princípios da legalidade, eficiência, economicidade e interesse público, além de atender às diretrizes da **IN SGD/ME nº 01/2019**, que estabelece critérios para contratações de TIC no âmbito da Administração Pública Federal.

14.3. Justificativa Técnica

O ambiente tecnológico da instituição é composto por um parque computacional heterogêneo e distribuído geograficamente, com ativos críticos que suportam sistemas estatísticos, geográficos, administrativos e científicos. A crescente sofisticação das ameaças cibernéticas, aliada à escassez de profissionais especializados e à necessidade de monitoramento contínuo, torna inviável a manutenção de uma estrutura interna dedicada à segurança da informação.

14.4. A contratação de um SOC remoto 24x7 permitirá:

14.4.1. Monitoramento contínuo de ativos de rede, servidores, aplicações e dispositivos de segurança;

14.4.2. Detecção e resposta a incidentes em tempo real;

14.4.3. Gestão de vulnerabilidades e apoio à conformidade com a LGPD;

14.4.4. Emissão de relatórios técnicos e gerenciais para tomada de decisão;

14.4.5. Monitoramento de ameaças externas, incluindo menções à marca institucional em ambientes abertos e redes obscuras (deep/dark web).

14.5. Adoção por Outros Órgãos Públicos

14.5.1. A solução proposta é amplamente adotada por **órgãos da Administração Pública Federal, Estadual e Municipal**, incluindo instituições de natureza **estatística, judiciária, financeira, educacional, científica e de controle**, que operam ambientes críticos e sensíveis à segurança da informação. Essas instituições enfrentam desafios semelhantes, como:

14.5.1.1. Necessidade de conformidade com a **Lei Geral de Proteção de Dados Pessoais (LGPD)**;

14.5.1.2. Alta exposição a riscos cibernéticos devido à natureza dos dados tratados;

14.5.1.3. Limitações orçamentárias e de pessoal para manter estruturas internas de segurança;

14.5.1.4. Demandas por monitoramento contínuo e resposta rápida a incidentes.

14.5.1.5. A adoção de SOC remoto por essas entidades demonstra a **viabilidade técnica e operacional** da solução, além de reforçar sua **aderência às melhores práticas internacionais**, como ISO/IEC 27001, NIST Cybersecurity Framework e CIS Controls.

14.6. Viabilidade Econômica

14.6.1. A solução remota apresenta **menor custo de propriedade** em comparação com alternativas internas ou presenciais, por eliminar despesas com infraestrutura física, equipe dedicada local e manutenção de ferramentas. Além disso, permite **escalabilidade, redução de riscos operacionais e acesso a expertise especializada**, o que contribui para a **eficiência e efetividade da segurança da informação institucional**.

14.7. Alinhamento Estratégico

14.7.1. A contratação está alinhada ao Plano Diretor de Tecnologia da Informação (PDTI), à Política de Segurança da Informação da instituição e às diretrizes de governança digital estabelecidas pelo Governo Federal. Também atende às exigências da LGPD e aos padrões internacionais de segurança, promovendo a **resiliência organizacional** e a **continuidade dos serviços públicos essenciais**.

15. Justificativa econômica da escolha da solução

15. A contratação de serviços gerenciados de segurança da informação por meio de um **Centro de Operações de Segurança (SOC) remoto com funcionamento contínuo (24x7)** representa uma solução economicamente vantajosa para a Administração Pública, considerando os seguintes aspectos:

15.1. Redução de Custos com Infraestrutura e Recursos Humanos:

15.1.1. A implantação de um SOC interno exigiria investimentos significativos em infraestrutura física, aquisição de ferramentas especializadas (SIEM, IDS/IPS, antivírus corporativo, etc.), licenciamento de software, e contratação de equipe técnica altamente qualificada para operar em regime 24x7. Além disso, haveria custos recorrentes com capacitação, manutenção e atualização tecnológica.

15.1. 2. A solução remota, por outro lado, transfere esses encargos para o fornecedor, que já dispõe de estrutura consolidada, equipe certificada e ferramentas atualizadas, permitindo à Administração focar em sua atividade-fim com menor custo de propriedade (TCO).

15.2. Economia Escalonada e Previsibilidade Orçamentária

15.2. 1. A contratação por meio de serviços gerenciados permite a **previsibilidade de custos**, com valores mensais fixos e escaláveis conforme a demanda. Isso facilita o planejamento orçamentário e evita gastos imprevistos com aquisição emergencial de ferramentas ou contratação de serviços pontuais de resposta a incidentes.

15.2. 2. Além disso, a modalidade de prestação contínua permite diluir os custos ao longo do tempo, evitando desembolsos elevados em fases iniciais do projeto.

15.3. Comparativo com Contratações Similares

15.3.1. Diversos órgãos da Administração Pública Federal, Estadual e Municipal têm adotado soluções de SOC remoto 24x7 por meio de licitações regidas pela Lei nº 14.133/2021. A análise de editais publicados no Portal Compras.gov.br demonstra que:

15.3.2. A contratação de SOC remoto é recorrente em instituições que operam ambientes críticos, como órgãos de controle, justiça, estatística, saúde e educação;

15.3.3. Os valores praticados são compatíveis com o mercado e apresentam boa relação custo-benefício, especialmente quando comparados com soluções internas ou presenciais;

15.3.4. A terceirização da operação de segurança permite acesso a tecnologias de ponta e profissionais especializados, sem os custos de retenção e capacitação interna.

15.4. Mitigação de Riscos Financeiros e Operacionais

15.4.1. A contratação de SOC remoto contribui para a **redução de riscos financeiros**, ao evitar prejuízos decorrentes de incidentes de segurança, como vazamento de dados, indisponibilidade de sistemas, ataques de ransomware e sanções legais por descumprimento da LGPD.

15.4.2. Além disso, a atuação proativa e reativa do SOC permite identificar e mitigar vulnerabilidades antes que se tornem incidentes críticos, protegendo os ativos da instituição e garantindo a continuidade dos serviços públicos.

15.5. Alinhamento com Princípios da Nova Lei de Licitações

15.5.1. A solução atende aos princípios da **economicidade, eficiência, eficácia e sustentabilidade**, conforme previsto na Lei nº 14.133/2021. A contratação é justificada por meio de análise comparativa de soluções, estudo de viabilidade técnica e econômica, e alinhamento com o Plano Diretor de TIC e a Política de Segurança da Informação da instituição.

16. Benefícios a serem alcançados com a contratação

16.1. A contratação de serviços gerenciados de segurança da informação por meio de um **Centro de Operações de Segurança (SOC) remoto com funcionamento contínuo (24x7)** proporcionará uma série de benefícios estratégicos, operacionais, técnicos e legais à instituição, conforme descrito abaixo:

16.1.1. Fortalecimento da Postura de Segurança Institucional

16.1.1.1. Monitoramento contínuo e especializado dos ativos de TIC, com detecção proativa de ameaças e vulnerabilidades.

16.1.1.2. Resposta rápida e coordenada a incidentes de segurança, reduzindo o tempo de exposição e mitigando impactos operacionais.

16.1.1.2. Adoção de práticas alinhadas aos principais frameworks internacionais de segurança, como **ISO/IEC 27001, NIST CSF e CIS Controls**.

16.1.2. Conformidade Legal e Regulatória

16.1.2.1. Atendimento aos requisitos da **Lei Geral de Proteção de Dados Pessoais (LGPD)**, garantindo proteção adequada aos dados pessoais tratados pela instituição.

16.1.2.2. suporte à implementação e manutenção da **Política de Segurança da Informação (PSI)** institucional.

16.1.2.3. Conformidade com a **Lei nº 14.133/2021**, que exige planejamento, eficiência e mitigação de riscos nas contratações públicas.

16.1.3. Redução de Riscos e Prejuízos Potenciais

16.1.3.1. Prevenção de vazamentos de dados, ataques de ransomware, acessos indevidos e interrupções de serviços críticos.

16.1.3.2. Redução de riscos reputacionais e financeiros decorrentes de incidentes de segurança.

16.1.3.3. Monitoramento de ameaças externas, incluindo menções à marca institucional em ambientes abertos, fóruns e redes obscuras (deep/dark web).

16.1.4. Eficiência Operacional e Econômica

16.1.4.1. Eliminação da necessidade de estrutura física local e equipe dedicada interna, reduzindo custos com infraestrutura, capacitação e manutenção.

16.1.4.2. Previsibilidade orçamentária por meio de contratação com valores mensais fixos e escaláveis.

16.1.4.3. Acesso a equipe técnica especializada e ferramentas avançadas sem necessidade de aquisição direta.

16.1.5. Melhoria Contínua e Apoio à Governança de TIC

16.1.5.1. Geração de relatórios técnicos e gerenciais com indicadores de desempenho, eventos de segurança e recomendações de melhoria.

16.1.5.2. Apoio à tomada de decisão estratégica por meio de dados confiáveis e atualizados sobre o ambiente de segurança.

16.1.5.3. Integração com o Plano Diretor de TIC (PDTI) e com os objetivos institucionais de transformação digital e governança de dados.

16.1.6. Aderência a Práticas Consolidadas na Administração Pública

16.1.6.1. A solução é amplamente adotada por órgãos públicos que operam ambientes críticos, como instituições de controle, justiça, saúde, educação e estatística.

16.1.6.2. Editais publicados no Portal Compras.gov demonstram que a contratação de SOC remoto 24x7 é uma prática consolidada, com boa relação custo-benefício e alta efetividade na proteção de ativos institucionais.

17. Providências a serem Adotadas

17.1. Para viabilizar a contratação dos serviços gerenciados de segurança da informação por meio de um Centro de Operações de Segurança (SOC) remoto com funcionamento contínuo (24x7), serão adotadas as seguintes providências:

17.1.1. Elaboração do Termo de Referência (TR)

17.1.1.1 O TR será desenvolvido com base nas necessidades de negócio e tecnológicas identificadas neste ETP, contemplando escopo detalhado, requisitos técnicos, critérios de desempenho, indicadores de qualidade, níveis de serviço (SLA), e obrigações da contratada.

17.1.2. Consulta ao mercado e pesquisa de preços

17.1.2.1. Serão realizadas consultas a fornecedores especializados e análise de contratações similares disponíveis no Portal Compras.gov.br, com o objetivo de obter referências de preços praticados, modelos de prestação de serviços e parâmetros técnicos utilizados por outros órgãos da Administração Pública.

17.1.3. Definição da modalidade de licitação

17.1.3.1. A modalidade será definida conforme critérios da Lei nº 14.133/2021, considerando a natureza do objeto, o valor estimado da contratação e a viabilidade de adoção de critérios de julgamento por técnica e preço, ou menor preço, conforme aplicável.

17.1.4. Análise jurídica e conformidade normativa

17.1.4.1. O processo será submetido à análise da assessoria jurídica, visando garantir conformidade com a legislação vigente, especialmente no que se refere à proteção de dados, segurança da informação, e contratação de serviços especializados de TIC.

17.1.5. Planejamento orçamentário e reserva de recursos

17.1.5.1 Será realizada a previsão orçamentária para os exercícios correspondentes ao período contratual, com reserva de recursos financeiros compatíveis com o custo total de propriedade (TCO) estimado no presente ETP.

17.1.6. Definição de equipe de fiscalização e gestão contratual

17.1.6.1. Será designada equipe técnica responsável pela fiscalização da execução contratual, acompanhamento dos indicadores de desempenho, validação dos relatórios entregues e gestão dos riscos associados à prestação dos serviços.

17.1.7. Publicação e transparência do processo

17.1.7.1. Todas as etapas do processo serão registradas e publicadas no Portal Nacional de Contratações Públicas (PNCP), garantindo transparência, publicidade e controle social, conforme previsto na Lei nº 14.133/2021.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

Com base no estudo exposto acima, especialmente no que tange à solução de mercado escolhida, que inclui critérios e práticas de sustentabilidade, a Equipe de Planejamento considera que a contratação é viável, além de ser necessária para o atendimento das necessidades e interesses da Administração.

19. Responsáveis

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

JUSSARA ROBERTA DE FREITAS SILVA

Equipe de apoio

RODRIGO POUBEL DOS SANTOS

Equipe de apoio

ANTONIO AGRA LOPES NETO

Equipe de apoio

FLAVIA MARINHO DE LIMA

Equipe de apoio

Lista de Anexos

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

- Anexo I - ETP_Serviço Gerenc Segurança 24x7_Anexos_ComprasGov_V2.pdf (784.01 KB)

ANEXO I-A – ESPECIFICAÇÃO TÉCNICA**1. SERVIÇOS PARA O ITEM 1****1.1. Gestão de Vulnerabilidades**

- 1.1.1. A atividade de Gestão de Vulnerabilidades poderá ser realizada in loco ou remotamente, conforme determinação do IBGE, e terá como objetivo principal a análise geral do ambiente do IBGE quanto a segurança da informação para identificar, mapear, documentar, controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica do IBGE, bem como apresentar recomendações de melhorias e/ou correções das vulnerabilidades identificadas durante os testes.
- 1.1.2. Fazem parte do processo de gestão de vulnerabilidades as fases de Varredura de vulnerabilidades, Teste de Invasão, Alerta de Vulnerabilidades e Controle das vulnerabilidades. Estas fases devem atuar de forma integrada com o objetivo de proverem informações suficientes para uma proteção mais eficaz do ambiente da contratada.
- 1.1.3. A periodicidade da execução das fases supracitadas dentro da vigência contratual de 24 meses deverá seguir as exigências da tabela abaixo, bem como está definida a criticidade das atividades, para aplicação dos níveis mínimos de serviço :

FASE	PERIODICIDADE	TOTAL DE EXECUÇÕES NO CONTRATO	CRITICIDADE (Conforme item 7.4 do termo de referência - NMS)
Varredura de vulnerabilidades (Interno)	Mensal	24	BAIXA
Teste de invasão (Externo)	Trimestral	8	BAIXA
Alerta de vulnerabilidades	Semanal	106	MÉDIA
Controle de vulnerabilidades	Diária	730	BAIXA

1.1.4. Características gerais.

- 1.1.4.1. Deverá ser considerado um total de 2100 IPs para o monitoramento de vulnerabilidades e 99 URLs para aplicações.
- 1.1.4.2. A empresa contratada deverá entregar ao gestor do contrato, ou técnico indicado por ele, todo detalhamento dos testes, sejam manuais ou automatizados, a serem realizados, desde os ativos a serem testados, qual procedimento adotado,

ferramentas utilizadas, entre outras informações que possam ser solicitadas.

- 1.1.4.3. Os testes de infraestrutura só poderão acontecer mediante autorização do gestor técnico do contrato, ou técnico indicado por ele, com anuência da DTI – Diretoria de Tecnologia da Informação.
- 1.1.4.4. Os testes de sistemas só poderão acontecer mediante autorização do gestor técnico do contrato, ou técnico indicado por ele, com anuência da área técnica responsável pela sustentação em produção do sistema do escopo.
- 1.1.4.5. Todos os testes a serem realizados deverão ser precedidos de caderno de testes, contendo todo o detalhamento das ações a serem executadas, possíveis comprometimentos, possíveis ações de contorno, dentre outras informações que se julguem necessárias para garantia da segurança e do sigilo das informações do IBGE.
- 1.1.4.6. Todas as fases dos testes serão acompanhadas e supervisionadas a critério da CONTRATANTE.
- 1.1.4.7. Quaisquer atividades que possam comprometer ou prejudicar algum ambiente ou ativo deverão ser reportadas, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos.
- 1.1.4.8. O Responsável Técnico deverá estar presente, no mínimo, 1 (um) dia por semana nas dependências do CONTRATANTE ou virtualmente para efetuar o acompanhamento dos serviços e repassar as informações para o CONTRATANTE, durante a execução dos Testes de Invasão;

1.1.5. Varredura de vulnerabilidades

- 1.1.5.1. Deverá ser realizada mensalmente uma varredura interna de vulnerabilidades no escopo descrito abaixo;
- 1.1.5.2. A varredura de vulnerabilidades do ambiente de TI deve considerar até 2100 (dois mil e cem) endereços IPs e 99 (noventa e nove) Aplicações Web definidos pelo IBGE, devendo considerar as seguintes etapas:
 - 1.1.5.2.1.1. Levantamento de todos os ativos da infraestrutura de TIC que deverão ser alvo da varredura. Para cada ativo, deverão ser levantados além das informações básicas, as informações de criticidade do ativo no ambiente e as informações das janelas de manutenção e mudança caso seja necessário aplicar patch e/ou correções;
 - 1.1.5.2.1.2. Execução da varredura de vulnerabilidades;
 - 1.1.5.2.1.3. Análise dos resultados e priorização das vulnerabilidades;
 - 1.1.5.2.1.4. Elaboração e entrega de um Plano de Remediação considerando a criticidade da vulnerabilidade identificada e, também, os critérios definidos na fase de Levantamento de Ativos.
 - 1.1.5.2.1.5. Para toda vulnerabilidade encontrada, a CONTRATADA deverá descrever de forma detalhada as ações para correção. Caso precise ter acesso as configurações dos ativos de tecnologia ou o código fonte para propor as soluções de correção, a Contratada deverá justificar a necessidade, ficando a cargo do IBGE decidir pela liberação;
 - 1.1.5.2.1.6. Deve ser também apresentado a Matriz de Risco das vulnerabilidades detectadas e o grau de maturidade do IBGE em cada item analisado.

1.1.6. Para realização da varredura de vulnerabilidades deve ser entregue uma ferramenta com as seguintes características:

1.1.6.1. Necessidades gerais:

- 1.1.6.1.1. A solução de varredura de vulnerabilidades deverá ser fornecida como Software como Serviço (SaaS), hospedada em infraestrutura de nuvem que atenda aos requisitos legais de proteção de dados e segurança da informação, conforme a Lei Geral de Proteção de Dados (LGPD) e demais normativas aplicáveis. Preferencialmente, os dados devem ser armazenados em data centers localizados no Brasil, conforme diretrizes da Portaria SGD/MGI nº 5.950/2023.
- 1.1.6.1.2. Caso seja necessário serem instalados coletores na modalidade on-premises (uso interno), este deve ser compatível com sistemas de virtualização VMWare e Microsoft HyperV, devendo também ser fornecido todo o licenciamento referente a banco de dados, aplicações e softwares necessários para seu funcionamento.
- 1.1.6.1.3. Caso seja necessária a instalação de coletores na modalidade on-premises (uso interno), a solução deverá adotar as melhores práticas de segurança da informação para comunicação entre os componentes da ferramenta, incluindo, mas não se limitando a:
 - 1.1.6.1.3.1. Utilização de protocolos seguros e atualizados (como TLS 1.2 ou superior) para transmissão de dados;
 - 1.1.6.1.3.2. Autenticação mútua entre os coletores e os servidores centrais, preferencialmente com uso de certificados digitais;
 - 1.1.6.1.3.3. Criptografia de dados em trânsito e, quando aplicável, em repouso;
 - 1.1.6.1.3.4. Segmentação de rede e restrição de acesso por meio de listas de controle ou grupos de segurança;
 - 1.1.6.1.3.5. Monitoramento contínuo e registro de logs de comunicação para fins de auditoria e resposta a incidentes;
 - 1.1.6.1.3.6. Compatibilidade com ambientes híbridos e respeito às políticas de segurança da organização contratante.
- 1.1.6.1.4. A solução deve ser integrada e fornecida por um único fabricante, podendo incluir componentes de terceiros desde que devidamente homologados e certificados pelo fabricante principal, respeitando os princípios da interoperabilidade e segurança.
- 1.1.6.1.5. A solução deverá possuir no mínimo duas certificações reconhecidas internacionalmente relacionadas à segurança da informação e privacidade, tais como:
- 1.1.6.1.6. Cloud Security Alliance (CSA) STAR;
- 1.1.6.1.7. ISO/IEC 27001;
- 1.1.6.1.8. ISO/IEC 27017 ou 27018;
- 1.1.6.1.9. SOC 2 Type II;
- 1.1.6.1.10. Certificações equivalentes que comprovem conformidade com boas práticas de segurança e privacidade.
- 1.1.6.1.11. A plataforma SaaS deverá garantir alta disponibilidade, com operação contínua 24x7x365 e SLA mínimo de 99%, conforme padrões de mercado e requisitos de continuidade de serviço público.
- 1.1.6.1.12. O ofertante deve oferecer manutenção e atualização constante da plataforma durante todo o período de vigência do contrato de serviço.

- 1.1.6.1.13. As atualizações de serviço devem ser transparentes para o administrador da solução, sem afetar nenhum dos dados armazenados ou serviços fornecidos.
- 1.1.6.1.14. Todas as comunicações entre componentes, transferência de dados e sincronização da solução devem ser criptografadas de ponta a ponta, fazendo uso de no mínimo TLS 1.2, certificados assinados com RSA 2048 bits e algoritmo de assinatura SHA256.
- 1.1.6.1.15. Certificados utilizados devem ser emitidos por Autoridades Certificadoras confiáveis, conforme cadeia de confiança reconhecida internacionalmente.
- 1.1.6.1.16. A solução deve permitir criação de usuários distintos.
- 1.1.6.1.17. Deve permitir separação de funções e permissões na console.
- 1.1.6.1.18. A console deve ser acessível a partir de, pelo menos, um dos navegadores comerciais dentre Google Chrome, Microsoft Edge e Mozilla Firefox.
- 1.1.6.1.19. Realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance) e indícios e padrões de códigos maliciosos conhecidos (malware);
- 1.1.6.1.20. Possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;
- 1.1.6.1.21. Suportar varreduras de dispositivos de IoT;
- 1.1.6.1.22. Ter a capacidade de adicionar etiquetas (tags) aos ativos de maneira automática, manual e através de regras com parâmetros específicos;
- 1.1.6.1.23. Atribuir uma severidade a todas as vulnerabilidades identificadas com base na pontuação do CVSS (Common Vulnerability Scoring System), preferencialmente utilizando a versão mais atualizada;
- 1.1.6.1.24. Calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança, sistema e conformidade, bem como hierarquias e prioridades;
- 1.1.6.1.25. Possuir assinaturas intrusivas e a possibilidade de inseri-las ou não nas varreduras, buscando maior efetividade nos testes.
- 1.1.6.1.26. Fornecer criptografia de ponta a ponta dos dados de vulnerabilidade;
- 1.1.6.1.27. Possuir a capacidade de criar um inventário do ambiente coletando e alimentando continuamente os dados do sistema, conformidade e segurança dos ativos de TI;
- 1.1.6.1.28. Possuir um sistema de busca do inventário com no mínimos as seguintes características:
 - 1.1.6.1.28.1. Por sistema operacional;
 - 1.1.6.1.28.2. Por fabricante do hardware;
 - 1.1.6.1.28.3. Por um determinado software instalado;
 - 1.1.6.1.28.4. Por Ativos impactados por uma determinada vulnerabilidade;
- 1.1.6.1.29. Fornecer gerenciamento de fluxo de trabalho de correção com base em políticas com criação e atribuição automática de registro de problema.
- 1.1.6.1.30. Possuir um sistema de pontuação e priorização das vulnerabilidades;
- 1.1.6.1.31. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
 - 1.1.6.1.31.1. CVSSv3 Impact Score;

- 1.1.6.1.31.2. Idade da Vulnerabilidade;
- 1.1.6.1.31.3. Número de produtos afetados pela vulnerabilidade;
- 1.1.6.1.31.4. Intensidade baseada no Número e Frequência de ameaças que utilizaram a vulnerabilidade ao longo do tempo;
- 1.1.6.1.32. Fazer a correlação em tempo real de ameaças ativas contra suas vulnerabilidades, incluindo feeds de inteligência de ameaças ao vivo
- 1.1.6.1.33. Suportar análise de vulnerabilidades de ambientes ativos utilizados em ambiente de automação;
- 1.1.6.1.34. Possuir uma API abrangente para automação de processos e integração com aplicações terceiras, sendo disponibilizada a documentação técnica para uso;
- 1.1.6.1.35. Permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;
- 1.1.6.1.36. Produzir relatórios nos seguintes formatos: PDF, CSV e HTML;
- 1.1.6.1.37. Deve ser possível determinar em tempo real quais portas estão abertas em determinado ativo;
- 1.1.6.1.38. Realizar em tempo real a descoberta de novos ativos para no mínimo:
 - 1.1.6.1.38.1. Bancos de dados;
 - 1.1.6.1.38.2. Hypervisors;
 - 1.1.6.1.38.3. Dispositivos móveis;
 - 1.1.6.1.38.4. Dispositivos de rede;
 - 1.1.6.1.38.5. Servidores físicos e virtuais;
 - 1.1.6.1.38.6. Aplicações;
- 1.1.6.1.39. Realizar em tempo real a identificação de informações sensíveis no tráfego de rede do ambiente;
- 1.1.6.1.40. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede em tempo real sem a necessidade de um agente:
 - 1.1.6.1.40.1. Caso seja necessário serem instalados coletores na modalidade on-premises (uso interno), este deve ser compatível com sistemas de virtualização VMWare e Microsoft HyperV, devendo também ser fornecido todo o licenciamento referente a banco de dados, aplicações e softwares necessários para seu funcionamento.
- 1.1.6.1.41. A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.
- 1.1.6.2. Deve possuir configuração de segurança e acesso restrito à console, atendendo aos seguintes itens:
 - 1.1.6.2.1. Suportar autenticação de dois fatores para os usuários e login.
 - 1.1.6.2.2. Suportar a configuração de segurança de senha e personalizar a política de segurança para a configuração de gerenciamento de senha:
 - 1.1.6.2.2.1. Idade e validade da senha;
 - 1.1.6.2.2.2. Conta de usuário bloqueada após o número de login com falha;

- 1.1.6.2.2.3. Comprimento mínimo da senha;
- 1.1.6.2.2.4. Complexidade de senha, caracteres alfanuméricos e numéricos a serem usados;
- 1.1.6.2.2.5. Forçar alteração de senha no login inicial;
- 1.1.6.2.2.6. Notificação para senha expirada antes do número de dias.
- 1.1.6.2.3. Executar relatórios manuais e periódicos de acordo com a frequência estabelecida pelo administrador;
- 1.1.6.2.4. Permitir a criação de relatórios baseado nos seguintes alvos: Todos os ativos existentes e alvos específicos;
- 1.1.6.2.5. Suportar a criação de relatórios criptografados (protegidos por senha configurável);
- 1.1.6.2.6. Suportar o envio automático de relatórios para destinatários específicos;
- 1.1.6.2.7. Ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
- 1.1.6.2.8. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
- 1.1.6.2.9. Fornecer relatórios de correção: tendência de ticket por grupo de ativos, usuário e vulnerabilidade
- 1.1.6.2.10. Permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas
- 1.1.6.2.11. Permitir a coleta de informações detalhadas sobre o ativo gerenciado, deve detalhar pelo menos os seguintes dados para cada ativo:
 - 1.1.6.2.11.1. Serviços em execução
 - 1.1.6.2.11.2. Software instalado
 - 1.1.6.2.11.3. Usuários
 - 1.1.6.2.11.4. Portas abertas
 - 1.1.6.2.11.5. Nome do host
 - 1.1.6.2.11.6. FQDN
 - 1.1.6.2.11.7. IP v4 / v6
 - 1.1.6.2.11.8. Endereço MAC
 - 1.1.6.2.11.9. Processador
 - 1.1.6.2.11.10. Memória
 - 1.1.6.2.11.11. Volumes de disco
 - 1.1.6.2.11.12. BIOS
- 1.1.6.2.12. Classificar automaticamente os ativos por famílias de tecnologia, tipo de dispositivo, tipo de plataforma e fabricante.
- 1.1.6.2.13. Normalizar automaticamente os nomes dos fabricantes de HW e SW com seus dados relevantes, como o nome dos aplicativos e versões, para facilitar sua posterior busca na solução.

- 1.1.6.2.14. A solução deverá possuir funcionalidade de etiquetagem (tags) de ativos, com o objetivo de facilitar a organização, identificação e agrupamento dos ativos conforme critérios definidos pela organização contratante.
- 1.1.6.2.15. É desejável que a ferramenta permita a criação e aplicação de tags com base em múltiplos parâmetros, incluindo pelo menos 4 (quatro) das seguintes opções:
 - 1.1.6.2.15.1. Etiquetagem manual ou estática;
 - 1.1.6.2.15.2. Palavras-chave associadas aos ativos;
 - 1.1.6.2.15.3. Endereços IP e intervalos de IP;
 - 1.1.6.2.15.4. Segmentos de rede;
 - 1.1.6.2.15.5. Portas abertas detectadas;
 - 1.1.6.2.15.6. Identificadores de vulnerabilidades específicas;
 - 1.1.6.2.15.7. Expressões regulares (Regex);
 - 1.1.6.2.15.8. Scripts customizados, como scriptlets em linguagens compatíveis com a solução, não sendo exigido suporte exclusivo a uma linguagem específica.
- 1.1.6.2.16. A solução proposta deve possuir a capacidade de obter e exibir informações sobre os ciclos de vida de hardware / software (EOL / EOS).
- 1.1.6.2.17. A solução deve permitir identificar o tipo de licenças associadas ao software instalado, classificando-as como comercial, open source e outros tipos de licenciamento.
- 1.1.6.2.18. A solução deve permitir a detecção de software não autorizado e permitir sua desinstalação em plataformas Microsoft Windows.
- 1.1.6.2.19. A solução deve permitir detectar hardwares e softwares desatualizados, sem suporte do fabricante - em final de vida útil.
- 1.1.6.2.20. A solução deve permitir atribuir criticidade ao ativo para priorizá-lo durante o processo de gerenciamento.
- 1.1.6.2.21. Possuir relatórios pré configurados com as seguintes informações:
 - 1.1.6.2.21.1. Hosts verificados sem credenciais;
 - 1.1.6.2.21.2. Top 100 Vulnerabilidades mais críticas;
 - 1.1.6.2.21.3. Top 10 Hosts infectados por Malwares;
 - 1.1.6.2.21.4. Hosts exploráveis por Malwares;
 - 1.1.6.2.21.5. Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
 - 1.1.6.2.21.6. Vulnerabilidades críticas e exploráveis;
 - 1.1.6.2.21.7. Máquinas com vulnerabilidades que podem ser exploradas;
- 1.1.6.2.22. Possuir dashboards customizáveis onde o administrador pode deletar, editar ou criar painéis de acordo com a necessidade;
- 1.1.6.2.23. Inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.
- 1.1.6.2.24. Possuir integração nativa do mesmo fabricante ou com terceiros, a solução de gestão de patches;
- 1.1.6.3. Características específicas da funcionalidade de gestão de vulnerabilidade e

varreduras de ativos:

- 1.1.6.3.1. Realizar varreduras (scans) de vulnerabilidades, de acordo com os somatórios de endereços IP licenciados;
- 1.1.6.3.2. Permitir a instalação e distribuição de no mínimo 5 scanners no ambiente;
- 1.1.6.3.3. Permitir a configuração de vários painéis e widgets;
- 1.1.6.3.4. Medir e reportar ameaças;
- 1.1.6.3.5. Visualizar ameaças críticas no ambiente da rede corporativa;
- 1.1.6.3.6. Realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como appliances virtuais;
- 1.1.6.3.7. Suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;
- 1.1.6.3.8. Fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de configurações e vulnerabilidades;
- 1.1.6.3.9. Incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia;
- 1.1.6.3.10. No caso onde uma atividade de varredura seja interrompida por invadir o período não permitido, o mesmo deve ser reiniciado de onde parou;
- 1.1.6.3.11. Ser configurável para permitir a otimização das configurações de varredura;
- 1.1.6.3.12. Permitir a utilização de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux, para varreduras autenticadas;
- 1.1.6.3.13. Informar a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
- 1.1.6.3.14. Realizar pesquisas de dados confidenciais;
- 1.1.6.3.15. Conter a funcionalidade de gestão de vulnerabilidade de aplicativos Web.
- 1.1.6.3.16. Realizar varreduras de vulnerabilidades em aplicações Web, cobrindo no mínimo, mas não limitando-se a base de ameaças apontadas pelo OWASP Top 10;
- 1.1.6.3.17. Analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;
- 1.1.6.3.18. Executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);
- 1.1.6.3.19. Avaliar no mínimo os padrões de segurança OWASP Top 10, CWE e WASC;
- 1.1.6.3.20. Identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal;
- 1.1.6.3.21. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os elementos JSON e XML;
- 1.1.6.3.22. Permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;
- 1.1.6.3.23. Realizar testes/varreduras em aplicações separadas, simultaneamente
- 1.1.6.3.24. Suportar override de DNS para os testes de aplicações web

- 1.1.6.3.25. Oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada antes no aplicativo Web.
- 1.1.6.3.26. Excluir determinadas URLs da varredura através de expressões regulares;
- 1.1.6.3.27. Instituir no mínimo os seguintes limites:
 - 1.1.6.3.27.1. Número máximo de URLs para crawl e navegação;
 - 1.1.6.3.27.2. Número máximo de diretórios para varreduras;
 - 1.1.6.3.27.3. Tempo máximo para a varredura;
 - 1.1.6.3.27.4. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;
 - 1.1.6.3.27.5. Número máximo de requisições HTTP por segundo;
- 1.1.6.3.28. Agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
- 1.1.6.3.29. Suportar o envio de notificações por email;
- 1.1.6.3.30. Ser compatível com avaliação de web services REST e SOAP;
- 1.1.6.3.31. Suportar os seguintes esquemas de autenticação:
 - 1.1.6.3.31.1. Autenticação Básica (Digest);
 - 1.1.6.3.31.2. NTLM;
 - 1.1.6.3.31.3. Autenticação de Cookies;
 - 1.1.6.3.31.4. Autenticação através de Selenium;
- 1.1.6.3.32. Importar scripts de autenticação selenium previamente configurados pelo usuário;
- 1.1.6.3.33. Exibir os resultados das varreduras de forma temporal para acompanhamento de correções e introdução de novas vulnerabilidades;
- 1.1.6.3.34. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
- 1.1.6.3.35. Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências;
- 1.1.6.3.36. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;
- 1.1.6.3.37. Serviço de Detecção de Malware em aplicativos Web
- 1.1.6.3.38. Ter a capacidade de varrer e identificar infecções por malware nas propriedades da web
- 1.1.6.3.39. Suportar capacidade de detecção de malware de dia zero.
- 1.1.6.3.40. Fornecer uma visão abrangente da atividade de verificação, páginas infectadas e tendências de infecção por malware.
- 1.1.6.3.41. Fornecer um relatório interativo com análise poderosa e distribuição segura dos resultados da verificação.
- 1.1.6.3.42. Fornecer relatórios de resumo e resumo do site que podem ser exportados para o formato HTML e PDF.
- 1.1.6.3.43. Realizar varreduras nos seguintes componentes:
 - 1.1.6.3.43.1. AngularJS, Apache, Apache Tomcat, Apache Tomcat JK connector, Apache Spark e Apache Struts;

- 1.1.6.3.43.2. Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI
- 1.1.6.3.43.3. JBoss AS e WildFly
- 1.1.6.4. Características específicas da funcionalidade de gestão de vulnerabilidade com a políticas de conformidade
 - 1.1.6.4.1. Fornecer um console interativo e centralizado para especificar os padrões de linha de base necessários para diferentes conjuntos de hosts. Os grupos de ativos devem ser compartilhados em toda a plataforma, portanto, os hosts descobertos e categorizados pela função de negócios no Gerenciamento de vulnerabilidades podem ter automaticamente as políticas de proteção adequadas avaliadas no Conformidade de política ;
 - 1.1.6.4.2. Permitir ao usuário final utilizar biblioteca integrada de políticas amplamente utilizadas.
 - 1.1.6.4.3. Usar um host previamente escaneado como uma “imagem dourada”;
 - 1.1.6.4.4. Permitir criar políticas personalizadas através de um editor interativo baseado na web;
 - 1.1.6.4.5. Permitir interativamente escolher quais configurações devem ser monitoradas;
 - 1.1.6.4.6. Permitir que o usuário final teste os controles imediatamente sem redigitar ou relatar;
 - 1.1.6.4.7. Ter uma biblioteca rica de controles para sistemas operacionais, dispositivos de rede, bancos de dados e aplicativos;
 - 1.1.6.4.8. A solução deve incluir indicadores de ameaças em tempo real que ajudam a avaliar e priorizar as vulnerabilidades detectadas, categorizados da seguinte forma:
 - 1.1.6.4.8.1. Dia Zero: vulnerabilidades para as quais não há patch disponível e para as quais um ataque ativo foi observado.
 - 1.1.6.4.8.2. Exploração pública: Vulnerabilidades cujo mecanismo de exploração é conhecido, para o qual existe um código de exploração e está disponível publicamente.
 - 1.1.6.4.8.3. Ataques ativos: vulnerabilidades que estão sendo atacadas ativamente.
 - 1.1.6.4.8.4. Movimento lateral: vulnerabilidades que permitem ao invasor espalhar o ataque amplamente pela rede violada.
 - 1.1.6.4.8.5. Fácil exploração: vulnerabilidades que podem ser facilmente exploradas, exigindo poucas habilidades e pouco conhecimento
 - 1.1.6.4.8.6. Perda de dados: vulnerabilidades cuja exploração causará perda massiva de dados
 - 1.1.6.4.8.7. Negação de serviço: vulnerabilidades cuja carga útil pode sobrecarregar - impedir que sistemas comprometidos estejam permanentemente - temporariamente disponíveis.
 - 1.1.6.4.8.8. No Patch: Vulnerabilidades para as quais não há solução do provedor
 - 1.1.6.4.8.9. Malware: vulnerabilidades associadas a infecções por malware
 - 1.1.6.4.8.10. Kit de exploração: vulnerabilidades para as quais um kit de exploração está disponível

- 1.1.6.4.9. Monitorar a integridade dos arquivos e observar mudanças.
- 1.1.6.4.10. Permitir a configuração de controles personalizados sem escrever código ou scripts.
- 1.1.6.4.11. Ter o recurso “Scan Anywhere” em um único console.
- 1.1.6.4.12. Permitir a verificação sob demanda ou em um cronograma;
- 1.1.6.4.13. Avaliar detalhadamente através de varreduras autenticadas;
- 1.1.6.4.14. Gerenciar exceções por meio de um processo de aprovações documentadas;
- 1.1.6.4.15. A solução proposta deve fornecer um workflow de correção baseado em políticas de criação e atribuição, re-atribuindo tickets de acordo com as condições definidas pelo administrador da solução através de políticas ou manualmente.
- 1.1.6.4.16. A solução deve permitir a criação de tickets com status aberto, fechado, ignorado, com base nos seguintes critérios:
 - 1.1.6.4.16.1. Host(s) a quem a regra se aplica;
 - 1.1.6.4.16.2. Vulnerabilidade (s) a que a regra se aplica;
 - 1.1.6.4.16.3. Usuário atribuído;
 - 1.1.6.4.16.4. Data de criação – expiração;
 - 1.1.6.4.16.5. Mudança de estado.
- 1.1.6.4.17. A solução deve permitir a criação de tickets de correção automaticamente a partir do resultado de uma varredura de vulnerabilidade - com base nas informações de um host específico e também manualmente por um administrador de solução.
- 1.1.6.4.18. Permitir a personalização de relatórios abrangentes, como por exemplo, documentar o progresso de TI em relação à correção das vulnerabilidades, informar as prioridades a serem corrigidas ou fomentar gerentes e auditores com o histórico das análises realizadas.
- 1.1.6.4.19. Permitir a geração de relatórios a qualquer momento, em qualquer lugar - sem redigitalizar
- 1.1.6.4.20. Comparar taxas de conformidade entre políticas, tecnologias e ativos
- 1.1.6.4.21. Disponibilizar histórico das varreduras realizadas com as respectivas políticas, assim como o andamento das correções efetuadas
- 1.1.6.4.22. Criar relatórios diferentes para diferentes públicos
- 1.1.6.4.23. Permitir o gerenciamento de risco e conformidade orientado a dados
- 1.1.6.4.24. Compartilhar dados com sistemas de gestão de risco e outros aplicativos corporativos
- 1.1.6.4.25. Agentes:
 - 1.1.6.4.25.1. A solução proposta deve oferecer um agente de baixo impacto nos sistemas operacionais onde está instalado e no consumo de largura de banda que utilizará na rede.
 - 1.1.6.4.25.2. A solução deve ser instalada em servidores, estações de trabalho, e máquinas virtuais, suportando sua implantação em rede local, em rede doméstica e na nuvem.
 - 1.1.6.4.25.3. A solução deve oferecer suporte para sua implantação em pelo menos os seguintes sistemas operacionais:

- 1.1.6.4.25.3.1. Windows Server 2019 e posterior (x86, x64)
- 1.1.6.4.25.3.2. CentOS 7.x (x64), 8.x (x64)
- 1.1.6.4.25.4. Red Hat Enterprise Linux (RHEL)
- 1.1.6.4.25.5. O agente da solução deve se atualizar automaticamente e gerir as suas atualizações automaticamente.
- 1.1.6.4.25.6. A solução deve suportar plataformas de nuvem AWS, GCP, Azure.
- 1.1.6.4.25.7. A solução deve ser capaz de coletar informações sobre o inventário de ativos.
- 1.1.6.4.25.8. A solução deve prover nativamente um dispositivo capaz de concentrar requisições dos agentes para encaminhamento a console de gerenciamento de forma a evitar a conexão direta de agentes com a plataforma.
- 1.1.6.4.25.9. O agente de gerenciamento deve suportar o uso de proxy.
- 1.1.6.4.25.10. Deve ser possível definir o intervalo de comunicação entre o agente e a console de gerenciamento.
- 1.1.6.4.25.11. Deve ser possível limitar o consumo de CPU e memória do agente.
- 1.1.6.4.25.12. Deve permitir a definição de um período global de inatividade dos agentes
- 1.1.6.4.26. Scanners:
 - 1.1.6.4.26.1. A solução deve permitir o uso de scanners capazes de identificar vulnerabilidades através de varreduras em ranges de IP definidos pelo administrador.
 - 1.1.6.4.26.2. Não deverá haver restrições para instalação de scanners virtuais no ambiente.
 - 1.1.6.4.26.3. Deve ser permitido o uso de scanners externos, sem necessidade de instalação, em nuvem própria do fabricante para varreduras de ativos publicados na internet.
 - 1.1.6.4.26.4. Os scanners virtuais devem suportar pelo menos um dos hypervisors abaixo:
 - 1.1.6.4.26.4.1. Hyper-V
 - 1.1.6.4.26.4.2. VMWare
 - 1.1.6.4.26.5. Os Scanners devem suportar a varredura de ambientes em nuvem para pelo menos os seguintes provedores:
 - 1.1.6.4.26.5.1. Azure
 - 1.1.6.4.26.5.2. AWS
 - 1.1.6.4.26.5.3. Google Cloud Platform
 - 1.1.6.4.26.5.4. Oracle
 - 1.1.6.4.26.6. Os scanners devem reportar vulnerabilidades para a console, permitindo uma visão consolidada das vulnerabilidades.
 - 1.1.6.4.26.7. Deve ser permitido o agendamento de varreduras para máquinas que possuam uma determinada versão de banco de dados em execução.
 - 1.1.6.4.26.8. Deve ser permitido a varredura sob demanda para um ou mais ativos de rede.
 - 1.1.6.4.26.9. O mesmo scanner deve ser capaz de varrer por falhas de conformidade e também por vulnerabilidades.

- 1.1.6.4.26.10. O scanner deverá consolidar vulnerabilidades encontradas em um ativo que possua agente instalado.
- 1.1.6.4.26.11. A solução deve permitir a configuração do tipo de varredura a ser realizada, permitindo pelo menos definir as seguintes configurações ao defini-la:
- 1.1.6.4.26.12. Configuração de quantidades de portas TCP/UDP a serem validadas.
- 1.1.6.4.26.13. Consumo de largura de banda e recursos (alto, médio, baixo).
- 1.1.6.4.26.14. Digitalize para dispositivos que não suportam ping - traceroute.
- 1.1.6.4.26.15. Detecção de balanceadores de carga.
- 1.1.6.4.26.16. Configuração de força bruta para usar em senhas.
- 1.1.6.4.26.17. Uso de um cabeçalho HTTP personalizado.
- 1.1.6.4.26.18. Ignorar pacotes.
- 1.1.6.4.26.19. Instalação de agente temporário para validação de registro local.
- 1.1.6.4.27. Categorização e Gestão de Ativos Tecnológicos
 - 1.1.6.4.28. Para realização da Categorização e Gestão dos ativos tecnológicos deve ser entregue uma ferramenta com as seguintes características:
 - 1.1.6.4.29. A solução deve identificar e inventariar automaticamente todos os ativos conectados à rede, incluindo servidores, estações de trabalho, dispositivos de rede e ativos em nuvem.
 - 1.1.6.4.30. A solução deve identificar e inventariar automaticamente todos os ativos conectados à rede, incluindo servidores, estações de trabalho, dispositivos de rede e ativos em nuvem.
 - 1.1.6.4.31. A solução deve ser capaz de detectar ativos não gerenciados e fornecer mecanismos para sua categorização e monitoramento contínuo.
 - 1.1.6.4.32. A solução deve correlacionar ativos descobertos com informações de segurança, permitindo a análise de riscos e priorização de ações corretivas.
 - 1.1.6.4.33. A solução deve possuir integração via API para permitir a exportação e análise de dados em sistemas de terceiros, como SIEM, ITSM e CMDBs.
 - 1.1.6.4.34. A documentação da API da solução deverá ter acesso público através de website ou documentação do próprio fabricante.
 - 1.1.6.4.35. A console de administração deverá possuir controle de acesso, no mínimo permitindo usuários com capacidade de somente visualizar as informações e usuários com capacidade de administrar os ativos e configurar políticas.
 - 1.1.6.4.36. A solução deve permitir a descoberta de ativos em tempo real, utilizando múltiplos métodos, incluindo varreduras ativas, passivas e agentes instalados nos dispositivos.
 - 1.1.6.4.37. A solução deve ser capaz de identificar softwares instalados em cada ativo e correlacioná-los com vulnerabilidades conhecidas, permitindo a gestão de riscos com base em ameaças reais.

- 1.1.6.4.38. A solução deve possibilitar a criação de relatórios personalizados sobre o inventário de ativos, incluindo estado de conformidade e nível de risco associado.
- 1.1.6.4.39. A solução deve permitir a categorização dos ativos por tipo, localização, sistema operacional, uso e outras características personalizáveis.
- 1.1.6.4.40. A solução deve ser capaz de identificar mudanças nos ativos, alertando sobre novos dispositivos conectados à rede, remoção de dispositivos e alterações na configuração de hardware ou software.
- 1.1.6.4.41. A solução deve integrar-se com outras ferramentas para ampliar as capacidades de análise e correção de vulnerabilidades nos ativos gerenciados.
- 1.1.6.4.42. A solução deve permitir a visualização dos ativos por meio de dashboards interativos, facilitando a análise e a tomada de decisão.
- 1.1.6.4.43. A solução deve suportar a aplicação de políticas de segurança e conformidade para avaliar continuamente os ativos contra padrões predefinidos.
- 1.1.6.4.44. A solução deve permitir a configuração de alertas automatizados para notificações sobre novos ativos, ativos fora de conformidade ou mudanças na infraestrutura.
- 1.1.6.4.45. A solução deve possibilitar a segmentação dos ativos em grupos para melhor gerenciamento e aplicação de políticas específicas.
- 1.1.6.4.46. A solução deve permitir auditoria detalhada das ações realizadas dentro da ferramenta, garantindo rastreabilidade e conformidade com normativas.
- 1.1.6.4.47. A solução deve permitir a customização dos critérios de risco dos ativos, permitindo que a organização adapte a análise de segurança conforme suas necessidades.
- 1.1.6.4.48. A solução deve suportar a criação de inventários automatizados e relatórios programados para distribuição periódica aos responsáveis pela segurança.
- 1.1.6.4.49. A solução deve permitir integração com serviços de nuvem pública, como AWS, Azure e Google Cloud, para descoberta e gerenciamento de ativos em ambientes híbridos.
- 1.1.6.4.50. A solução proposta deve possuir a capacidade de obter e exibir informações sobre os ciclos de vida de hardware / software (EOL / EOS)
- 1.1.6.4.51. A solução deve permitir identificar o tipo de licenças associadas ao software instalado, classificando-as como comercial, open source e outros tipos de licenciamento.
- 1.1.6.4.52. A solução deve permitir a detecção de software não autorizado e permitir sua desinstalação em plataformas Microsoft Windows.
- 1.1.6.4.53. A solução deve permitir detectar hardwares e softwares desatualizados, sem suporte do fabricante - em final de vida útil.

- 1.1.6.4.54. A solução deve permitir atribuir criticidade ao ativo para priorizá-lo durante o processo de gerenciamento.
- 1.1.6.4.55. A solução proposta permitirá a coleta de informações detalhadas sobre o ativo gerenciado, devendo detalhar pelo menos os seguintes dados para cada ativo:
 - 1.1.6.4.55.1. Serviços em execução
 - 1.1.6.4.55.2. Software instalado
 - 1.1.6.4.55.3. Usuários
 - 1.1.6.4.55.4. Portas abertas
 - 1.1.6.4.55.5. Nome do host
 - 1.1.6.4.55.6. FQDN
 - 1.1.6.4.55.7. IP v4 / v6
 - 1.1.6.4.55.8. Endereço MAC
 - 1.1.6.4.55.9. Processador
 - 1.1.6.4.55.10. Memória
 - 1.1.6.4.55.11. Volumes de disco
 - 1.1.6.4.55.12. BIOS
- 1.1.6.4.56. A solução deve classificar automaticamente os ativos por famílias de tecnologia, tipo de dispositivo, tipo de plataforma e fabricante.
- 1.1.6.4.57. A solução deve normalizar automaticamente os nomes dos fabricantes de hardware e software com seus dados relevantes, como o nome dos aplicativos e versões, para facilitar sua posterior busca na solução.
- 1.1.6.4.58. A solução deve possuir a habilidade de etiquetagem (tags) de ativos para facilitar a identificação, deve permitir a geração de tags, pelo menos, usando os seguintes parâmetros:
 - 1.1.6.4.58.1. Palavras-chave
 - 1.1.6.4.58.2. Endereço IP e intervalos de IP
 - 1.1.6.4.58.3. Segmento de rede
 - 1.1.6.4.58.4. Portas abertas
- 1.1.6.5. Informações de inventário considerando, no mínimo:
 - 1.1.6.5.1.1. Sistema operacional,
 - 1.1.6.5.1.2. Presença ou ausência de determinado software instalado ou serviço em execução.
 - 1.1.6.5.1.3. Última localização geográfica detectada incluindo cidade e país
 - 1.1.6.5.1.4. Regex
- 1.1.6.5.2. A solução deve permitir agrupamento manual a critério do administrador da solução.

- 1.1.6.5.3. A solução deve permitir atribuir criticidade ao ativo para priorizá-lo durante o processo de gerenciamento.
- 1.1.6.5.4. Deve permitir criação de dashboards personalizados que sejam capazes de trazer as seguintes informações sobre os ativos:
 - 1.1.6.5.4.1. Categorias de softwares instalados nos ativos
 - 1.1.6.5.4.2. Hosts que executam máquinas virtuais
 - 1.1.6.5.4.3. Sistemas operacionais utilizados
 - 1.1.6.5.4.4. Serviços e portas TCP ou UDP abertas
 - 1.1.6.5.4.5. Softwares de segurança instalados
 - 1.1.6.5.4.6. Memória total utilizada
 - 1.1.6.5.4.7. Quantidade de processadores
 - 1.1.6.5.4.8. Quantidade de armazenamento disponível
- 1.1.6.5.5. A solução deve permitir uma interface de busca de ativos que utilize sintaxe lógica baseada, no mínimo, nos critérios abaixo:
 - 1.1.6.5.5.1. Fabricante de hardware
 - 1.1.6.5.5.2. Último usuário logado
 - 1.1.6.5.5.3. Categoria de software instalado
- 1.1.6.5.6. A solução deve permitir a visualização de quantidade de máquinas com um determinado software instalado.
- 1.1.6.5.7. Deve permitir visibilidade a respeito de hosts que executam containers e containers em execução.
- 1.1.6.5.8. Além de workstations e servidores, a solução deve permitir visibilidade a respeito de ativos tais como switches, roteadores, firewalls, impressoras, etc.
- 1.1.6.6. Gestão de Vulnerabilidade, Detecção e Resposta
 - 1.1.6.6.1. A solução deve permitir descobrir, avaliar, priorizar e auxiliar na correção de vulnerabilidades e configurações em toda a infraestrutura de rede, incluindo estações de trabalho, servidores, dispositivos de rede, dispositivos de telecomunicações e dispositivos de segurança, hypervisors, máquinas virtuais, proporcionando através de única interface para o administrador via um portal web para gerenciamento de todos os ativos, permitindo o gerenciamento centralizado de todos os componentes da solução a partir de um único ponto, sem a necessidade de incorrer em consoles ou componentes adicionais fora dele para a administração dos serviços oferecidos.
 - 1.1.6.6.2. A solução deve ser licenciada por Asset (IP - HOST) para ativos de infraestrutura.
 - 1.1.6.6.3. A solução deve ser licenciada por URLs para varreduras de aplicação web.
 - 1.1.6.6.4. A solução deve permitir varreduras de vulnerabilidade com base em:
 - 1.1.6.6.4.1. Sistemas Operacionais
 - 1.1.6.6.4.2. Serviços WEB
 - 1.1.6.6.4.3. Portas TCP e UDP

- 1.1.6.6.4.4. Serviços
- 1.1.6.6.4.5. Aplicações
- 1.1.6.6.4.6. Bancos de dados
- 1.1.6.6.4.7. Dispositivos de rede como switches, roteadores e balanceadores de carga
- 1.1.6.6.5. No mínimo, a ferramenta deve abranger os seguintes sistemas operacionais, bancos de dados e aplicativos:
 - 1.1.6.6.5.1. Microsoft Windows
 - 1.1.6.6.5.2. LINUX
 - 1.1.6.6.5.3. Mac OS X
 - 1.1.6.6.5.4. VMware
- 1.1.6.6.6. Detectar e analisar vulnerabilidades nas principais versões de Bancos de Dados, pelo menos:
 - 1.1.6.6.6.1. Microsoft SQL Server
 - 1.1.6.6.6.2. MySQL
 - 1.1.6.6.6.3. Oracle
 - 1.1.6.6.6.4. PostgreSQL
 - 1.1.6.6.6.5. Detectar e analisar vulnerabilidades em plataformas WEB, pelo menos:
 - 1.1.6.6.6.6. IIS
 - 1.1.6.6.6.7. Apache Tomcat
- 1.1.6.6.7. Detectar e analisar vulnerabilidades em portas e serviços TCP e UDP
- 1.1.6.6.8. Detectar vulnerabilidades em pelo menos os seguintes aplicativos ou plataformas:
 - 1.1.6.6.8.1. Adobe
 - 1.1.6.6.8.2. Apple
 - 1.1.6.6.8.3. HP
 - 1.1.6.6.8.4. McAfee
 - 1.1.6.6.8.5. Microsoft
 - 1.1.6.6.8.6. Oracle
 - 1.1.6.6.8.7. Oracle Java
 - 1.1.6.6.8.8. VMware
 - 1.1.6.6.8.9. Linux
- 1.1.6.6.9. Permitir a descoberta de vulnerabilidades na rede, oferecendo as seguintes alternativas de varredura:
 - 1.1.6.6.10. Varredura ativa de rede não autenticada
 - 1.1.6.6.11. Varredura ativa de rede autenticada
- 1.1.6.7. Varreduras externas
 - 1.1.6.7.1.1. O mecanismo de varredura deve ter uma taxa de precisão de detecção de vulnerabilidade de 99,99966% durante os últimos 10 anos.

- 1.1.6.7.1.2. A base de conhecimento de vulnerabilidade deve ser atualizada no mínimo semanalmente, garantindo a incorporação de pelo menos 20 CVEs a ela e deve ter pelo menos uma base de conhecimento de 35.000 CVEs relacionados incluindo tecnologias legadas e atuais.
- 1.1.6.7.1.3. A solução deve oferecer suporte ao padrão da indústria para pontuação de vulnerabilidade do Common Vulnerability Scoring System (CVSS)
- 1.1.6.7.1.4. A solução deve oferecer suporte ao padrão da indústria para adicionar detecções personalizadas usando Open Vulnerability Assessment Language (OVAL).
- 1.1.6.7.1.5. A solução deve permitir vincular as vulnerabilidades detectadas e indicar sua relação com ameaças como Vírus, Trojan e Malware.
- 1.1.6.7.1.6. A solução deve ser capaz de indicar explorações disponíveis e códigos disponíveis para uma vulnerabilidade, quando aplicável
- 1.1.6.7.1.7. O banco de dados deve relacionar a maioria das vulnerabilidades ao CVE e Bugtraq.
- 1.1.6.7.1.8. A solução deve oferecer suporte à integração para autenticação por ferramentas de cofres de senha com ao menos uma das seguintes fabricantes, Delinea, CyberArk, BeyondTrust
- 1.1.6.7.1.9. A solução deve permitir buscas interativas de vulnerabilidade utilizando filtros como severidade, categoria, sistema operacional, status, classificação do CVSS, CVE ou KB.
- 1.1.6.7.1.10. A solução deve permitir a utilização de operadores lógicos na busca de vulnerabilidades para que seja possível encontrar, no mínimo, as seguintes informações:
 - 1.1.6.7.1.10.1. Vulnerabilidades associadas a ransomware e que possuem patches disponíveis
 - 1.1.6.7.1.10.2. Vulnerabilidades detectadas em um segmento de rede
 - 1.1.6.7.1.10.3. Vulnerabilidades detectadas em serviços específicos
 - 1.1.6.7.1.10.4. Vulnerabilidades detectadas por um usuário específico
 - 1.1.6.7.1.10.5. Vulnerabilidades detectadas em hardware específico
 - 1.1.6.7.1.10.6. A busca de vulnerabilidades deve permitir agrupamento para mostrar, no mínimo, as seguintes visualizações:
 - 1.1.6.7.1.10.7. Quantidade de ocorrências de uma mesma vulnerabilidade
 - 1.1.6.7.1.10.8. Quantidade de vulnerabilidades por sistema operacional
 - 1.1.6.7.1.10.9. Quantidade de vulnerabilidades por host
 - 1.1.6.7.1.10.10. Quantidade de vulnerabilidades por Exploit disponível
 - 1.1.6.7.1.10.11. Quantidade de vulnerabilidades por produto/software vulnerável
- 1.1.6.7.1.11. A solução deve permitir exportar buscas e filtros criados para um dashboard
- 1.1.6.7.1.12. A solução deve permitir salvar filtros criados em buscas para reutilização

- 1.1.6.7.1.13. Deve mostrar dashboards que apresentem variação histórica de vulnerabilidades novas, corrigidas, reabertas
- 1.1.6.7.1.14. Deve permitir mostrar dashboards que contenham quantidades de vulnerabilidades associadas a ransomware, que contém exploits públicos e que permitem exploração sem autenticação
- 1.1.6.7.1.15. Deve mostrar dashboards que mostrem o racional de vulnerabilidades que podem ser corrigidas através de patches
- 1.1.6.7.1.16. Deve mostrar patches faltantes em sistemas operacionais independente da relação com uma vulnerabilidade existente
- 1.1.6.8. Gestão de Configuração
 - 1.1.6.8.1. A solução deve permitir a avaliação e o relatório de problemas de configuração, com base nas referências do padrão da indústria do Centro de Segurança da Internet (CIS).
 - 1.1.6.8.2. O fabricante deve ser oficialmente certificado pelo CIS para fornecer este nível de controles.
 - 1.1.6.8.3. A solução deve oferecer avaliação de configuração com base no benchmark CIS padrão da indústria, cobrindo esta funcionalidade nas seguintes categorias:
 - 1.1.6.8.3.1. Sistemas operacionais
 - 1.1.6.8.3.2. Software de servidor
 - 1.1.6.8.3.3. Provedores de nuvem
 - 1.1.6.8.3.4. Dispositivos de rede
 - 1.1.6.8.3.5. Software de desktop
 - 1.1.6.8.4. A solução deve suportar detecção de falhas de conformidades através de varreduras autenticadas ou através de agente instalado diretamente no ativo monitorado.
 - 1.1.6.8.5. A solução deve permitir que os administradores recebam informação de conformidade de sistemas operacionais Windows e Linux, mesmo que não estejam conectados à rede corporativa.
 - 1.1.6.8.6. A solução deve permitir a avaliação de certificados digitais (internos e externos) e configurações de TLS em busca de problemas e vulnerabilidades, resultando em diferentes graus de conformidade de acordo com os resultados da avaliação de seu emissor, prazo de validade, tipo de certificado, robustez do algoritmo e o conjunto de criptografia usados.
- 1.1.6.9. Detecção e priorização de ameaças
 - 1.1.6.9.1. A solução proposta deve permitir enviar alertas em tempo real sobre irregularidades na rede, identificar ameaças e monitorar mudanças inesperadas que ocorram.
 - 1.1.6.9.2. A solução deve permitir enviar notificações para usuários específicos e grupos de usuários para o perfil de monitoramento ou perfis de monitoramento múltiplos.
 - 1.1.6.9.3. A solução deve permitir a personalização do perfil de monitoramento associado a uma lista específica de critérios.
 - 1.1.6.9.4. A solução deve permitir que os alertas sejam personalizados para uma ampla variedade de condições que afetam sistemas, certificados, vulnerabilidades, portas, serviços e software. Cada regra deve permitir que seja configurada para detectar mudanças gerais comuns - para se ajustar a circunstâncias muito específicas.

- 1.1.6.9.5. A solução deve permitir a atribuição de destinatários diferentes para cada alerta.
- 1.1.6.9.6. A solução deve enviar alertas de monitoramento sobre vulnerabilidades, configurações incorretas e outros parâmetros definidos pelo administrador da solução, incluindo:
 - 1.1.6.9.6.1. Ativos com sistemas operacionais não aprovados
 - 1.1.6.9.6.2. Certificados expirados ou expirando
 - 1.1.6.9.6.3. Portas abertas
 - 1.1.6.9.6.4. Vulnerabilidades graves
 - 1.1.6.9.6.5. Tickets de correção abertos, resolvidos e fechados
 - 1.1.6.9.6.6. Software não aprovado
- 1.1.6.9.7. A solução proposta deve fornecer fontes de inteligência de ameaças em tempo real e técnicas de aprendizado de máquina para fornecer controle de administrador sobre a evolução das ameaças relacionadas a vulnerabilidades encontradas nos ativos da organização e identificar quais corrigir primeiro.
- 1.1.6.9.8. A solução deve permitir consultas ad-hoc com múltiplas variáveis e critérios, como classe de ativo, tipo de vulnerabilidade, indicadores de ameaça em tempo real, etiqueta de ativo e sistema operacional, de modo que, por exemplo, seja possível pesquisar todas as vulnerabilidades que tenham um alta classificação de gravidade, são fáceis de explorar e foram lançados na semana passada.
- 1.1.6.9.9. A solução deve permitir que se faça uma correlação em tempo real das ameaças ativas contra as vulnerabilidades detectadas nos ativos corporativos.
- 1.1.6.9.10. A solução deve incluir indicadores de ameaças em tempo real que ajudem a avaliar e priorizar as vulnerabilidades detectadas, categorizados da seguinte forma:
 - 1.1.6.9.10.1. Vulnerabilidades para as quais não há patch disponível e para as quais um ataque ativo foi observado.
 - 1.1.6.9.10.2. Vulnerabilidades cujo mecanismo de exploração é conhecido, para o qual existe um código de exploração e está disponível publicamente.
 - 1.1.6.9.10.3. Vulnerabilidades que estão sendo ativamente utilizadas como fonte de ataques.
 - 1.1.6.9.10.4. Vulnerabilidades que permitem ao invasor espalhar o ataque amplamente pela rede violada.
 - 1.1.6.9.10.5. Vulnerabilidades que podem ser facilmente exploradas, exigindo poucas habilidades e pouco conhecimento.
 - 1.1.6.9.10.6. Vulnerabilidades cuja exploração causará perda massiva de dados.
 - 1.1.6.9.10.7. Vulnerabilidades cuja carga útil pode sobrecarregar ou impedir que sistemas comprometidos estejam permanentemente ou temporariamente disponíveis.
 - 1.1.6.9.10.8. Vulnerabilidades para as quais não há correção do provedor.
 - 1.1.6.9.10.9. Vulnerabilidades associadas a infecções por malware.
- 1.1.6.9.11. A solução deve atribuir uma pontuação a cada vulnerabilidade de forma contextual de forma a quantificar o risco associado a esta vulnerabilidade.
- 1.1.6.9.12. Os fatores de risco devem considerar pelo menos os fatores abaixo:
 - 1.1.6.9.12.1. Malwares associados

- 1.1.6.9.12.2. Atores maliciosos associados
- 1.1.6.9.12.3. Possibilidade de remediação
- 1.1.6.9.13. A solução proposta deve fornecer um workflow de correção baseado em políticas de criação e atribuição, atribuindo tickets de acordo com as condições definidas pelo administrador da solução através de políticas ou manualmente.
- 1.1.6.9.14. A solução deve permitir a criação de tickets com status aberto, fechado, ignorado, com base nos seguintes critérios:
 - 1.1.6.9.14.1. Host(s) a quem a regra se aplica
 - 1.1.6.9.14.2. Vulnerabilidade(s) a que a regra se aplica
 - 1.1.6.9.14.3. Usuário atribuído
 - 1.1.6.9.14.4. Data de criação ou expiração
 - 1.1.6.9.14.5. Mudança de estado
- 1.1.6.9.15. A solução deve permitir a criação de tickets de correção automaticamente a partir do resultado de uma varredura de vulnerabilidade, com base nas informações de um host específico e também manualmente por um administrador de solução.
- 1.1.7. Gestão de Patches
 - 1.1.8. A solução proposta deve correlacionar vulnerabilidades e patches automaticamente para os hosts do IBGE contabilizando até 2100 servidores (dois mil e duzentos e dez servidores).
 - 1.1.9. A solução deve mapear automaticamente os patches com CVEs associados às vulnerabilidades detectadas.
 - 1.1.10. Deve mostrar patches faltantes mesmo que não exista correlação com uma vulnerabilidade existente
 - 1.1.11. A solução de Gestão de Patches deve ser do mesmo fabricante da solução de Gestão de Vulnerabilidades compartilhando a mesma console de gestão das soluções.
 - 1.1.12. Deve mostrar patches faltantes para no mínimo as seguintes categorias:
 - 1.1.12.1. Navegadores
 - 1.1.12.2. Ferramentas de compressão de arquivos
 - 1.1.12.3. Visualizadores de PDF
 - 1.1.12.4. Sistemas operacionais
 - 1.1.13. A solução deve permitir aplicação de patches de segurança para, no mínimo, as plataformas abaixo:
 - 1.1.13.1. Windows Server 2019 e posterior
 - 1.1.13.2. CentOS 7.x e 8.x
 - 1.1.13.3. Red Hat Enterprise Linux (RHEL)
 - 1.1.14. A solução deve possuir um catálogo com no mínimo 35.000 patches e permitir aplicação de patches para, no mínimo, os produtos abaixo:
 - 1.1.15. 7-Zip
 - 1.1.16. Acro Software CutePDF Writer

- 1.1.17. AdoptOpenJDK JDK
- 1.1.18. AdoptOpenJDK JRE
- 1.1.19. Adobe Acrobat
- 1.1.20. Adobe Flash
- 1.1.21. Adobe Reader
- 1.1.22. Adobe Shockwave
- 1.1.23. AIMP DevTeam AIMP
- 1.1.24. Amazon Correo
- 1.1.25. Apache Software Foundaon Tomcat
- 1.1.26. Apple iCloud
- 1.1.27. Apple iTunes
- 1.1.28. Apple Mobile Device Support
- 1.1.29. Apple Software Update
- 1.1.30. Atlassian HipChat
- 1.1.31. Sourcetree
- 1.1.32. Audacity
- 1.1.33. Azul Zulu JDK
- 1.1.34. Azul Zulu JRE
- 1.1.35. Bandicam Company Bandicut
- 1.1.36. Blue Jeans
- 1.1.37. Blue Jeans Outlook Addin
- 1.1.38. Barco ClickShare
- 1.1.39. Botkind Allway Sync
- 1.1.40. Box Drive
- 1.1.41. Box Edit
- 1.1.42. Box Sync
- 1.1.43. CDBurnerXP
- 1.1.44. Cisco Jabber
- 1.1.45. Cisco WebEx Teams
- 1.1.46. Citrix GoToMeeng
- 1.1.47. Citrix Receiver
- 1.1.48. Citrix Workspace App
- 1.1.49. Code4ward.net Royal Applications
- 1.1.50. CoreFTP
- 1.1.51. Corel WinDVD Pro

- 1.1.52. dotPDN LLC Paint.NET
- 1.1.53. Dropbox
- 1.1.54. Evernote
- 1.1.55. FileZilla
- 1.1.56. Foxit PhantomPDF
- 1.1.57. Foxit Reader
- 1.1.58. Gimp
- 1.1.59. GIT
- 1.1.60. GlavSo TightVNC
- 1.1.61. Chrome
- 1.1.62. Google Drive
- 1.1.63. Google Desktop
- 1.1.64. Google Drive File Stream
- 1.1.65. Google Earth Pro
- 1.1.66. Gretech GOM Player
- 1.1.67. Inkscape
- 1.1.68. IrfanView
- 1.1.69. Jabra Direct
- 1.1.70. JAM Software TreeSizeFree
- 1.1.71. Juraj Simlovic TED Notepad
- 1.1.72. KeePass
- 1.1.73. LibreOffice
- 1.1.74. Lightning ImgBurn
- 1.1.75. LogMeIn
- 1.1.76. Malwarebytes An-Malware Home
- 1.1.77. Microsoft .Net
- 1.1.78. Microsoft .Net Core
- 1.1.79. AnXSS
- 1.1.80. Azure Site Recovery Provider
- 1.1.81. Azure Informaon Protecon Client
- 1.1.82. BizTalk Server
- 1.1.83. Business Contact Manager
- 1.1.84. CAPICOM
- 1.1.85. Microsoft Commerce Server
- 1.1.86. Microsoft Content Management Server

- 1.1.87. Windows Defender
- 1.1.88. Microsoft Digital Image
- 1.1.89. DirectX
- 1.1.90. Microsoft Dynamics
- 1.1.91. Microsoft Edge
- 1.1.92. Microsoft Enhanced Migaon Experience Toolkit
- 1.1.93. Exchange Server
- 1.1.94. Exchange System Manager
- 1.1.95. Microsoft Expression
- 1.1.96. Forefront Server
- 1.1.97. Front Page Server
- 1.1.98. Host Integraon Server
- 1.1.99. Microsoft Identy Manager
- 1.1.100. Internet Explorer
- 1.1.101. Internet Informaon Server
- 1.1.102. ISA Server
- 1.1.103. Microsoft Journal Viewer
- 1.1.104. Live Meeng
- 1.1.105. Live Messenger
- 1.1.106. Skype for Business Server
- 1.1.107. MDAC
- 1.1.108. Microsoft Mouse and Keyboard Center
- 1.1.109. Microsoft Step By Step Interacve Training
- 1.1.110. Mscomctl
- 1.1.111. MSN Messenger
- 1.1.112. MSXML
- 1.1.113. Office Communicator 2005
- 1.1.114. Office Web Components XP
- 1.1.115. Producer for PowerPoint 1.1
- 1.1.116. Small Business Accounng 2006
- 1.1.117. Works 6-9 Converter
- 1.1.118. Office Communicator 2007
- 1.1.119. Office Communicaons Server 2007 R2
- 1.1.120. Office Communicator 2007 R2
- 1.1.121. Producer for PowerPoint 2003

- 1.1.122. Suíte Office nas versões 2000, 2002, 2003, 2007, 2010, 2013, 2016
- 4.3.8.6.112. System Center Operations Manager
- 1.1.123. Microsoft SQL Server nas versões 2005, 2008, 2008 R2, 2012, 2014, 2016, 2017, 2019
- 4.3.8.6.114. SQL Management Studio
- 1.1.124. Microsoft Visual Studio
- 1.1.125. Windows Server 2012, 2016, 2019
- 1.1.126. A solução deve permitir a criação de dashboards para acompanhamento de aplicação de patches.
- 1.1.127. Os Dashboards devem permitir inclusão de filtros personalizados para incluir, no mínimo, os requisitos abaixo:
 - 1.1.127.1. Ativos que não possuem patches de segurança instalados ;
 - 1.1.127.2. Ativos pendentes de boot para aplicação de patches ;
 - 1.1.127.3. Patches faltantes por fabricante ;
 - 1.1.127.4. Status de aplicação de patches ;
 - 1.1.127.5. Patches faltantes por severidade ;
- 1.1.128. A solução deve permitir mostrar em um mesmo dashboard a quantidade de Ativos que possuem um software instalado e quantidade de patches relevantes a esse mesmo software
- 1.1.129. A solução deve conter uma lista de produtos e softwares priorizados, permitindo visualizar patches relevantes a esses produtos
- 1.1.130. A solução deve permitir a criação de tarefas de instalação a partir de produtos e softwares priorizados
- 1.1.131. A solução deve oferecer uma interface que permita buscas com uma sintaxe lógica para visualizar detalhes de um patch específico
- 1.1.132. As buscas devem considerar, no mínimo, os filtros abaixo:
 - 1.1.132.1. Fabricante da aplicação ou software
 - 1.1.132.2. Patches que corrigem falhas de segurança
 - 1.1.132.3. Patches de sistema operacional ou aplicações
 - 1.1.132.4. Severidade do fabricante
 - 1.1.132.5. Número do KB ou boletim
 - 1.1.132.6. CVE associado
- 1.1.133. A solução deve ser capaz de apresentar informações de patches que já consideram e resolvem correções anteriores
- 1.1.134. A solução deve apontar vulnerabilidades resolvidas por um determinado patch
- 1.1.135. A solução deve apontar todas as versões da aplicação que são afetadas e precisam de correção
- 1.1.136. A solução deve conter referências do fabricante do software ou sistema operacional contendo descrição dos patches disponíveis
- 1.1.137. Deve ser possível visualizar agentes, último status de comunicação, a quantidade de patches aplicados e faltantes

- 1.1.138. Deve ser possível definir o intervalo em horas para verificação de patches e reporte à console
- 1.1.139. A solução deve suportar tarefas de instalação e remoção dos patches
- 1.1.140. A solução deve permitir a execução de scripts personalizados durante a tarefa de instalação de patches
- 1.1.141. Deve ser possível executar scripts Powershell antes e depois da instalação de correções
- 1.1.142. A solução deve permitir instalação de softwares através de scripts
- 1.1.143. A tarefa de aplicação de patches deve permitir alteração de chaves de registro
- 1.1.144. A tarefa de aplicação de correções deve permitir selecionar manualmente os patches a serem aplicados ou através de um filtro de seleção que considere, no mínimo, severidade do patch, fabricante, associação a uma vulnerabilidade, associação a riscos de segurança
- 1.1.145. Deve ser possível restringir a aplicação de patches a um grupo de máquinas baseados em ranges de IP, software instalado, portas abertas, serviços em execução
- 1.1.146. Deve ser possível o agendamento de execução de tarefas de patch de forma imediata
- 1.1.147. Deve ser possível agendar a execução de tarefas de patch em um horário específico com recorrência diária, semanal ou mensal
- 1.1.148. Deve ser possível agendar a execução de tarefas de patch com agendamento a partir do Patch Tuesday, da Microsoft, de forma automática
- 1.1.149. Deve ser possível configurar uma janela de tempo máximo para execução de patches em intervalo de horas ou minutos
- 1.1.150. A solução deve permitir customização de mensagens para o usuário antes, durante e após a aplicação de patches
- 1.1.151. Deve permitir o download de patches antes do início da tarefa, de forma a otimizar o processo de instalação
- 1.1.152. A solução deve permitir a supressão do reinício do sistema operacional, forçá-la ou permitir que o usuário reinicie o sistema, caso o patch aplicado exija o reinício.
- 1.1.153. A solução deve permitir colocar em quarentena ativos em risco para evitar exploração.
- 1.1.154. A solução deverá isolar dispositivos da rede e ainda permitir o controle e a aplicação de patches remotos via a própria solução e outros recursos autorizados usando tecnologia de agente em nuvem.
- 1.1.155. A solução deverá disponibilizar ações de correção de vulnerabilidades não corrigidas e fornecer mitigações alternativas onde a correção pode causar interrupções.
- 1.1.156. Deve ser possível restringir o licenciamento a um determinado grupo de máquinas baseado em critérios como sistema operacional, presença de softwares instalados e ranges de IPs
- 1.1.157. A solução deve conter a inteligência de filtrar automaticamente, sem intervenção, quais Ativos receberão os patches selecionados na tarefa de patch considerando a arquitetura do sistema operacional e também a pré-existência de determinada aplicação, evitando assim instalações indesejadas;

- 1.1.158. Deve ser possível gerar relatórios a partir do catálogo de patches a serem aplicados considerando filtros dos patches e dos Ativos;
- 1.1.159. O catálogo de patches a serem aplicados deve filtrar de forma simples quais são os patches que precisam ser instalados e exibir somente as últimas versões disponíveis de cada um deles, considerando a obsolescência de versões antigas;
- 1.1.160. Deve ser possível visualizar, pela interface, o status de instalação de cada uma das tarefas de patch criadas;
- 1.1.161. O status individual de cada tarefa de patch deve mostrar quais patches foram instalados com sucesso, as quais falharam e quais não foram instalados por não serem necessários;
- 1.1.162. A solução deve exibir, para os patches que não foram instalados com sucesso, qual o motivo do erro;
- 1.1.163. Deve ser possível gerar um relatório CSV para uma tarefa de patch específica, com a finalidade de validar seu progresso e situação final de execução;
- 1.1.164. A solução deve possuir controle de acesso no modelo Role Based Access Control, para que sejam definidos no mínimo dois perfis de usuários caso seja necessário, sendo um deles, necessariamente, incapaz de iniciar uma tarefa de execução de patch;
- 1.1.165. A solução deve possuir uma interface de API para permitir automatização com no mínimo as seguintes funções:
 - 1.1.165.1. Criação de tarefa de patch;
 - 1.1.165.2. Listagem de Ativos;
 - 1.1.165.3. Listagem de patches;
 - 1.1.165.4. Listagem de tarefas de patch;
 - 1.1.165.5. Criação e geração de relatórios.
- 1.1.166. Varreduras dinâmicas de aplicações WEB e API's :
 - 1.1.166.1. A ferramenta deverá ser dimensionada para atender até 99 aplicações web;
 - 1.1.166.2. A ferramenta de varreduras dinâmicas de vulnerabilidades em aplicações web e API's deve ser do mesmo fabricante da solução de Gestão de Vulnerabilidades compartilhando a mesma console de gestão das soluções.
 - 1.1.166.3. A solução proposta deve habilitar varreduras profundas dinâmicas para descobrir e catalogar todos os aplicativos da web e APIs na rede corporativa externa, redes corporativas internas e instâncias de nuvem.
 - 1.1.166.4. A solução deve permitir varreduras autenticadas, complexas e progressivas.
 - 1.1.166.5. A solução deve suportar varreduras programadas de serviços SOAP e REST API.
 - 1.1.166.6. A solução deve contar com API e integração com Jenkins para automação em ambiente de CI / CD.
 - 1.1.166.7. A solução deve detectar, identificar, avaliar, rastrear os 10 principais riscos OWASP (Top 10), como injeção de SQL, Cross-site script (XSS), XML External Entity (XXE), autenticação interrompida e configurações incorretas, também ameaças de WASC, vulnerabilidades CWE e CVEs associados em aplicações da web.

- 1.1.166.8. A solução deve suportar a capacidade de re-testar uma vulnerabilidade específica que foi detectada anteriormente na aplicação web.
- 1.1.166.9. A solução deve ter capacidade de encontrar aplicações web aprovadas e não aprovadas em sua rede, gerando um processo contínuo de catalogação e descoberta de aplicações web.
- 1.1.166.10. A solução deve gerar tags para facilitar a localização e o uso de ativos de aplicações web encontrados.
- 1.1.166.11. A solução deve permitir que se faça a varredura de grandes aplicações da web usando um mecanismo de varredura progressiva, que deve permitir a varredura em estágios incrementais e evitar quaisquer restrições que possam surgir ao tentar fazer a varredura de um aplicativo de uma vez.
- 1.1.166.12. A solução deve definir a hora exata de início e duração das verificações.
- 1.1.166.13. A solução deve permitir gerenciar várias varreduras de aplicações web, combinando vários scanners para acelerar o processo e obter resultados mais rapidamente.
- 1.1.166.14. A solução deve permitir integração nativa ou por meio de conectores, APIs ou outros mecanismos compatíveis com pelo menos uma ferramenta de Web Application Firewall (WAF) amplamente utilizada no mercado, tais como F5, Fortinet, Imperva, Citrix NetScaler ou equivalente, desde que compatível com a infraestrutura tecnológica da contratante;
- 1.1.166.15. A solução deve permitir a consolidação de dados de varredura automatizada com dados provenientes de ferramentas de avaliação manual de vulnerabilidades, como Burp Suite, Bugcrowd ou equivalentes, de forma a proporcionar uma visão unificada das vulnerabilidades identificadas em aplicações web;
- 1.1.166.16. A solução deve fornecer relatórios resumidos e de varredura do site que podem ser exportados para os formatos HTML e PDF.
- 1.1.166.17. A solução deve oferecer suporte à criação de escopos e funções definidos pelo usuário e permitir que as permissões apropriadas sejam atribuídas a cada função.
- 1.1.167. Relatórios e dashboards:
 - 1.1.167.1. A solução proposta deve permitir administração centralizada via interface gráfica WEB usando HTTPS.
 - 1.1.167.2. A solução deve possibilitar o acesso a console de todos os componentes do serviço a partir de um único ponto.
 - 1.1.167.3. A solução deve permitir a definição de diferentes perfis de usuários e funções para administração.
 - 1.1.167.4. A solução deve fornecer controles de acesso de usuário hierárquicos e baseados em funções que permitam a delegação de responsabilidades para refletir a estrutura organizacional.
 - 1.1.167.5. A solução deve permitir o acesso de um usuário autorizado de qualquer local.
 - 1.1.167.6. A solução deve suportar integração com uma biblioteca API XML extensível.
 - 1.1.167.7. A solução deve suportar autenticação de dois fatores para login de usuários.
 - 1.1.167.8. A solução deve suportar configurações de segurança de senha.
 - 1.1.167.9. A solução deve suportar personalizar a política de segurança para configurações de gerenciamento de senha, por:

- 1.1.167.10. Idade e expiração da senha.
- 1.1.167.11. Conta do usuário bloqueada após uma série de logins com falha.
- 1.1.167.12. Comprimento mínimo da senha.
- 1.1.167.13. Complexidade da senha, caracteres alfanuméricos e numéricos a serem usados.
- 1.1.167.14. Forçar mudança de senha no login inicial
- 1.1.167.15. A solução deve permitir a configuração de notificações de expiração de senha com antecedência mínima parametrizável, de forma a alertar os usuários com vários dias de antecedência, conforme política de segurança da contratante.
- 1.1.167.16. A solução deve suportar a capacidade de restringir o acesso apenas a partir da rede interna da empresa.
- 1.1.167.17. A solução deve suportar a capacidade de rastrear a atividade do usuário por nome da conta do usuário, data, ação e informações sobre a ação.
- 1.1.167.18. A solução deve suportar a capacidade de distribuir relatórios em PDF com segurança por meio de uma senha e um número restrito de download de relatórios por meio do link.
- 1.1.167.19. A solução deve suportar acesso por SSO (Single Sign-on) usando SAML 2.0.
- 1.1.167.20. A solução deve permitir o controle de alterações com trilhas de auditoria à prova de violação.
- 1.1.167.21. A solução proposta deve gerar relatórios por IPs, Grupo e Tags
- 1.1.167.22. A solução deve permitir a geração de relatórios de qualquer IP - Host previamente verificado.
- 1.1.167.23. A solução deve permitir agendar relatórios diários, semanais, mensais e sob demanda.
- 1.1.167.24. A solução deve permitir o envio de notificações por e-mail sempre que um relatório estiver disponível para o administrador da solução, usuários específicos e perfis diferentes criados na ferramenta.
- 1.1.167.25. A solução deve permitir pelo menos os seguintes tipos de relatórios:
 - 1.1.167.25.1. Relatório de correção
 - 1.1.167.25.2. Relatório de vulnerabilidades altamente críticas
 - 1.1.167.25.3. Relatório Executivo
 - 1.1.167.25.4. Relatório de autenticação
 - 1.1.167.25.5. Relatório de conformidade normativa e regulatória
 - 1.1.167.25.6. Relatório de remediação
- 1.1.167.26. A solução deve fornecer relatórios de correção por grupo de ativos, usuário e vulnerabilidade.
- 1.1.167.27. A solução deve permitir a criação de relatórios baseados em IPv4, endereços IPv6, nome do host, grupo de ativos e rótulos personalizados pelo administrador.
- 1.1.167.28. A solução deve permitir relatórios com cálculo de risco de segurança, permitindo um cálculo de risco global para todos os ativos incluídos no relatório.

- 1.1.167.29. A solução deve permitir relatórios que possibilitem o cálculo do risco do negócio, utilizando como base para o cálculo do risco de impacto ao negócio e do risco de segurança dos ativos incluídos no relatório.
- 1.1.167.30. A solução deve permitir relatar as descobertas com base no status das vulnerabilidades detectadas e seu status, conforme lista abaixo:
 - 1.1.167.30.1. Novo
 - 1.1.167.30.2. Resolvido
 - 1.1.167.30.3. Reaberto
 - 1.1.167.30.4. Ativo
- 1.1.167.31. A solução deve permitir relatórios que incluam vulnerabilidades com base na data de publicação.
- 1.1.167.32. A solução deve permitir incluir e excluir kernels Linux detectados na varredura de vulnerabilidade e que não estejam em execução.
- 1.1.167.33. A solução deve permitir a exclusão de vulnerabilidades encontradas em uma porta ou serviço que não esteja em execução.
- 1.1.167.34. A solução deve permitir excluir vulnerabilidades que não sejam exploráveis devido à configuração do sistema ou plataforma onde foi detectada.
- 1.1.167.35. A solução deve permitir a exclusão de patches da Microsoft que foram substituídos por um novo patch ou um patch cumulativo do mesmo fabricante.
- 1.1.167.36. A solução deve fornecer relatórios automatizados de tendências e diferenciais.
- 1.1.167.37. A solução deve fornecer várias opções de distribuição de relatórios, incluindo PDF criptografado.
- 1.1.167.38. A solução deve dar suporte à personalização do modelo de relatório conforme necessário.
- 1.1.167.39. A solução deve permitir a exportação de relatórios para os formatos HTML, MHT, PDF, DOC, CSV e XML
- 1.1.167.40. A solução deve permitir que relatórios sejam apresentados em tabelas e gráficos com as ocorrências ocorridas, permitindo a customização detalhada de cada relatório.
- 1.1.167.41. A solução deve permitir em seus relatórios comparar o nível de conformidade entre políticas, tecnologias e ativos.
- 1.1.167.42. A solução deve possuir um painel que, por padrão, permite que você veja as tendências de vulnerabilidades por gravidade, plataforma, idade e status de remediação.
- 1.1.167.43. A solução deve permitir a customização dos painéis fazendo uso de qualquer um dos dados disponíveis associados aos ativos varridos para selecionar diferentes tipos de gráficos, tabelas e visualizações sobre a priorização de vulnerabilidades.
- 1.1.167.44. A solução deve fornecer painéis executivos personalizáveis com uma visão unificada de todos os componentes da solução.
- 1.1.167.45. Deve ser possível criar dashboards que mostrem a pontuação de risco global de ativos e sua variação ao longo do tempo.

1.1. Teste de Invasão

1.1.1. Escopo

- 1.1.1.1. Os Testes de Invasão deverão contemplar tanto a infraestrutura quanto as aplicações, devendo ser realizados a partir do ambiente interno e externo a cada três meses.
- 1.1.1.2. O teste de Infraestrutura avaliará a possibilidade de exploração e comprometimento para até 254 (duzentos e cinquenta e quatro) endereços IPs, definidos pelo IBGE.
- 1.1.1.3. O teste de aplicações web avaliará a possibilidade de exploração e comprometimento de até 50 (cinquenta) aplicações web definidas pelo IBGE, podendo ocorrer retestes caso necessário;
- 1.1.1.3.1. O teste de aplicações web avaliará a possibilidade de exploração considerando as prerrogativas abaixo, onde deverão ser realizados minimamente, as seguintes verificações:
 - 1.1.1.3.1.1. “Cross Site Scripting (XSS)”;
 - 1.1.1.3.1.2. “Injeção de Código”;
 - 1.1.1.3.1.3. “Inclusão Remota de Arquivos (RFI)”;
 - 1.1.1.3.1.4. Deverão ser realizados mapeamentos e sondagens, com o objetivo de identificar possíveis vetores de entradas de ataques;
 - 1.1.1.3.1.5. “Referência Direta a Objetos”.
 - 1.1.1.3.1.6. “Vazamento de informações”, onde deve ser verificada a exposição inadvertida de informações sobre a aplicação e o servidor que a hospeda.
 - 1.1.1.3.1.7. “Gerenciamento de Sessões”.
 - 1.1.1.3.1.8. Pelo menos, as vulnerabilidades dos últimos dois relatórios OWASP Top 10.
- 1.1.1.3.2. Caso necessário, devem ser criados ataques customizados baseados na arquitetura das aplicações.
- 1.1.1.4. Serviço de Auditoria de Segurança em Códigos Fonte de Aplicações
 - 1.1.1.4.1. Para a realização das auditorias o IBGE disponibilizará, quando permitido, o código-fonte da aplicação a ser auditada, que deverá ser mantida sob sigilo pela CONTRATADA.
 - 1.1.1.4.2. A auditoria de códigos-fonte visa avaliar, dentre outros itens, os seguintes conceitos:
 - 1.1.1.4.2.1. Avaliação do fluxo de informações indo desde a arquitetura física (ex: fluxo de informações entre camadas web, camadas de aplicação e bancos de dados) até o fluxo de informações entre os módulos - variáveis e parâmetros.
 - 1.1.1.4.2.2. Avaliação das lógicas de negócio requisitadas e implementadas. Detecção de possíveis fraudes internas ou vulnerabilidades na implementação das lógicas de negócio.
 - 1.1.1.4.2.3. Avaliação da utilização das APIs e construtos da linguagem de programação apontamento dos locais no código onde é feito uso inseguro das bibliotecas do sistema, dos elementos da linguagem de programação e recomendações de correção classificadas por risco e custo.

- 1.1.1.4.2.4. Avaliação da exposição do código-fonte e das regras de negócio para entidades externas apontando os aspectos do código que estariam mais sujeitos a permitir o vazamento de segredos.
- 1.1.1.5. Uma vez que o objetivo destes testes é garantir a segurança do ambiente, e não comprovar a existência de brechas, deverá ser utilizada a “Técnica da caixa branca”, onde o avaliador terá acesso irrestrito a qualquer informação que possa ser relevante ao teste;
- 1.1.1.6. As atividades utilizadas para a execução dos testes não se resumirão apenas ao uso de ferramentas, devendo incluir também procedimentos e técnicas com interação humana e não oferecidos por ferramentas conhecidas
- 1.1.1.7. Os Testes de Invasão envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos e informações do IBGE, e devem observar orientações e técnicas emanadas por padrões internacionais ou equivalente apresentados pela empresa CONTRATADA, caso possua, em seu portfólio, normativos que complementem os demonstrados abaixo:
 - 1.1.1.7.1. OSSTMM 3 (The Open Source Security Testing Methodology Manual: at least those three channels PHYSSEC, SPECSEC, COMSEC or/and any new one which will be defined);
 - 1.1.1.7.2. ISSAF/PTF (Information Systems Security Assessment Framework);
 - 1.1.1.7.3. NIST Special Publication 800-115 (Technical Guide to Information Security Testing and assessment);
 - 1.1.1.7.4. NIST Special Publication 800-42 (Guideline on Network Security Testing)
 - 1.1.1.7.4.1. OWASP TESTING GUIDE 3.0 – The Open Web Application Security Project.
 - 1.1.1.7.4.2. PCI DSS (Payment Card Industry Data Security Standard)
 - 1.1.1.7.4.3. PCI SSC Information Supplement
 - 1.1.1.7.4.4. PTES (Penetration Testinf Execution Standard)
- 1.1.1.8. **Considerações gerais**
 - 1.1.1.8.1. Os alvos dos testes a serem efetuados, assim como suas condições serão definidos em reunião prévia entre a CONTRATADA e o IBGE;
 - 1.1.1.8.2. Todas as fases (ciclos) dos “Testes de Invasão” poderão ser acompanhadas e supervisionadas a qualquer momento pelo IBGE;
 - 1.1.1.8.3. A CONTRATADA não deverá alterar a integridade das informações, ou seja, não deve alterar informações dos servidores e sistemas que possam comprometer os serviços do IBGE;
 - 1.1.1.8.4. Cada fase deve ser feita durante o período que não comprometa processamento da CONTRATANTE e que as agências estejam fechadas sendo feita em no máximo 2 dias corridos no total;
 - 1.1.1.8.5. Os testes e avaliações poderão ser interrompidos por solicitação expressa do IBGE a qualquer momento;
 - 1.1.1.8.6. Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo deverá ser imediatamente reportada ao IBGE, haja vista a necessidade do IBGE de manter a disponibilidade dos seus ambientes, ativos e serviços;

- 1.1.1.8.7. Deve ser comunicado ao IBGE, e devidamente documentado, o andamento da análise/teste, especialmente se identificada uma situação crítica.
- 1.1.1.8.8. Cada teste de invasão deverá obedecer às seguintes fases:
 - 1.1.1.8.8.1. Planejamento;
 - 1.1.1.8.8.2. Descoberta;
 - 1.1.1.8.8.3. Ataque;
 - 1.1.1.8.8.4. Relatório de Teste de Invasão;
 - 1.1.1.8.8.5. Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste;
 - 1.1.1.8.8.6. Reavaliação, novo teste pós remediação (RETESTE);
 - 1.1.1.8.8.7. Relatório final do Teste de Invasão;
 - 1.1.1.8.8.8. Maturidade do IBGE e Matriz de risco.
- 1.1.1.9. **Planejamento:**
 - 1.1.1.9.1. Todas as premissas, processos, atividades descritas, inclusive os cronogramas serão detalhados e apresentados na fase de planejamento para os tipos de teste de penetração a seguir:
 - 1.1.1.9.1.1. PENTEST DE REDE: Este teste é focado em recursos de rede, onde o escopo é definido em termos de endereços IP e intervalos de rede. Os testes de rede externa também podem ter o escopo definido em termos de nomes de domínio (o avaliador precisa descobrir os endereços de rede associados a esses domínios como parte do teste).
 - 1.1.1.9.1.2. PENTEST DE APLICAÇÃO: Este teste é focado em aplicação, geralmente aplicação web, mobile e cliente/servidor. Os avaliadores se concentrarão em encontrar e explorar vulnerabilidades somente nessa aplicação.
 - 1.1.1.9.1.3. PENTEST DE REDE SEM FIO: Este teste é semelhante a um pentest de rede, mas o escopo é definido por redes sem fio, tanto faz se especificadas diretamente pelos identificadores de conjunto de serviços (SSIDs) e localização física ou apenas por localização (por exemplo, "qualquer rede sem fio em nosso Prédio de escritórios principais").
 - 1.1.1.9.1.4. PENTEST DE ACESSO REMOTO: este teste é semelhante a um pentest de rede, mas o escopo é definido em pontos específicos de acesso à rede corporativa (como VPN de acesso remoto de funcionários ou VPN B2B)
 - 1.1.1.9.1.5. PENTEST DE ENGENHARIA SOCIAL: quando os testes incluem a tentativa de enganar as pessoas para fornecer dados confidenciais ou privilégios de acesso ao avaliador, os tipos de truques a serem executados (como golpes de telefone, tentativas de phishing ou acesso físico) e alvos autorizados (como pessoas que podem ser alvo do teste, incluindo executivos, agentes do call center ou qualquer pessoa no escritório principal) são parte da definição do escopo.
 - 1.1.1.9.1.6. TESTE FÍSICO OU DE INSTALAÇÕES: estes testes abrangem controles de segurança física, como controle de acesso a instalações e recursos de TI. Um teste típico de segurança física pode incluir acesso a um centro de dados e acesso direto aos racks dos servidores. Também pode ser focado em ambientes de escritório, verificando a disponibilidade de informações confidenciais em

papel ou acesso a desktops e laptops dos usuários.

1.1.1.9.2. Deverá ser elaborado o “PLANO DE TESTE DE PENETRAÇÃO”, para cada teste ou reavaliação, contemplando as informações de PLANEJAMENTO do teste, tais como:

1.1.1.9.2.1. Objetivos, premissas e escopo do teste, datas e horas dos testes, realizações, metodologias, vulnerabilidades encontradas, categorização e severidade das vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades, apresentação das evidências apuradas, fontes de pesquisa, referências e ferramentas utilizadas.

1.1.1.9.3. Também na fase de planejamento, deverão ser atendidas e apresentadas, no mínimo, as seguintes informações:

1.1.1.9.3.1. Detalhes da infraestrutura alvo dos testes de invasão;

1.1.1.9.3.2. Equipamentos e recursos demandados para este teste;

1.1.1.9.3.3. Tipos de ataque que serão realizados;

1.1.1.9.3.4. Prazos (janela de tempo para execução dos testes);

1.1.1.9.3.5. Contato da CONTRATADA (responsáveis para tratamento de questões não abordadas nos testes);

1.1.1.9.4. A CONTRATADA deverá elaborar o “Plano de Teste de Invasão”, para cada teste que será realizado, contemplando as informações de planejamento do teste, tais como: objetivos, premissas e escopo do teste, metodologia de análise de vulnerabilidades, equipe envolvida, prazos do teste, de acordo com as informações abaixo:

1.1.1.9.4.1. O planejamento abrange a definição dos elementos a serem avaliados/testados, bem como a definição dos testes em si e o cronograma de execução. Deve ser realizado previamente, e em conjunto com o IBGE, sendo obrigatória, a autorização formal do IBGE antes da execução.

1.1.1.9.4.2. Deve apresentar todo o detalhamento das análises e testes a serem realizados, desde os ativos que serão testados, procedimentos adotados, técnicas e ferramentas utilizadas, entre outras informações que possam ser relevantes ou solicitadas.

1.1.1.9.4.3. Deve ser demonstrado e explanado a finalidade de cada ferramenta a ser utilizada, para avaliação e autorização prévia do IBGE.

1.1.1.9.4.4. Os testes e avaliações não poderão impactar o pleno funcionamento dos recursos testados, o que deve ser considerado na definição do cronograma. Caso o IBGE entenda que haja algum risco neste sentido, solicitará modificação da metodologia e/ou do cronograma, inclusive podendo requerer a execução em finais de semana, feriados ou fora do horário comercial.

1.1.1.9.4.5. Deverão ocorrer no mínimo 04 (quatro) reuniões de planejamento no IBGE a cada ano, sendo possível por parte do IBGE, solicitar demais reuniões presenciais ou remotas para alinhamento de informações adicionais relativas a esta etapa de planejamento.

1.1.1.9.4.6. Todas as ferramentas e recursos utilizados para a prestação dos serviços são de responsabilidade da CONTRATADA.

1.1.1.10. Descoberta:

- 1.1.1.10.1. O serviço deve contemplar a realização de análise de vulnerabilidade, visando identificar pontos de falha em suas configurações e versões que possam implicar em não atendimento as melhores práticas de segurança estabelecidas pelo mercado, além de identificar possíveis vulnerabilidades presentes em ativos, servidores, aplicações, sistemas, serviços, versões e configurações em produtos atualmente em uso pelo IBGE;
- 1.1.1.10.2. Os endereços IPs externos a serem testados serão definidos pelo IBGE durante a etapa de planejamento. Estes endereços IPs podem não ser todos pertencentes diretamente ao IBGE e, não necessariamente farão parte do mesmo bloco de endereços;
- 1.1.1.10.3. Neste processo é aceito o uso de ferramentas automatizadas de escaneamento próprias e padrões de mercado.
- 1.1.1.10.4. A análise de vulnerabilidade deve considerar as principais vulnerabilidades informadas pelos principais meios de informações até a data de execução da análise, tais como fabricante de softwares, canais de divulgações de vulnerabilidades, além de recomendações aceitas como boas práticas pelo mercado.
- 1.1.1.10.5. O método de análise de vulnerabilidades deve contemplar, no mínimo, não restringindo-se somente a estes, os seguintes itens:
 - 1.1.1.10.5.1. Identificação de pontos de entrada;
 - 1.1.1.10.5.2. Mapeamento todas as portas abertas e serviços;
 - 1.1.1.10.5.3. Descoberta de ativos, servidores, aplicações, sistemas, serviços e configurações;
 - 1.1.1.10.5.4. Identificação versões utilizadas e informar se esta é a versão atualizada;
 - 1.1.1.10.5.5. Testes de configuração;
 - 1.1.1.10.5.6. Testes de vulnerabilidades;
 - 1.1.1.10.5.7. Vetores de acesso;
 - 1.1.1.10.5.8. Vetores de criação;
 - 1.1.1.10.5.9. Vetores de alteração;
 - 1.1.1.10.5.10. Vetores de exclusão;
 - 1.1.1.10.5.11. Vetores de negação de serviço (comprometimento geral/parcial);
 - 1.1.1.10.5.12. Análise de mensagens de erro;
 - 1.1.1.10.5.13. Identificação da vulnerabilidade (de acordo com CVE- <http://cve.mitre.org/>), problema, bug, erro ou item em não conformidade com boas práticas de segurança.
- 1.1.1.10.6. O mapeamento deve ser proativo, identificando as ameaças confirmadas e ameaças potenciais, mapeando o grau do risco e classificando conforme padrões de mercado.
- 1.1.1.10.7. Todos os endereços IPs, ativos, servidores, aplicações, sistemas, serviços, versões e configurações foco da análise, devem ser previamente aprovados pelo IBGE, que pode eventualmente impedir alguns tipos de análises, bem como solicitar análises específicas, com foco de verificar a segurança de determinado ativo.
- 1.1.1.10.8. O resultado da análise deve seguir as seguintes etapas e conter os seguintes itens para análise de vulnerabilidades de infraestrutura:

- 1.1.1.10.8.1. Identificação e explicação do endereço IPs, ativos, servidores, aplicações, sistemas, serviços, versões e configurações encontrados;
- 1.1.1.10.8.2. Identificação de vulnerabilidades;
- 1.1.1.10.8.3. Metodologia utilizada passo-a-passo (descrição do teste);
- 1.1.1.10.8.4. Resultados obtidos (descrição do resultado);
- 1.1.1.10.8.5. Evidência do teste;
- 1.1.1.10.8.6. Classificação e priorização das vulnerabilidades por risco (seguindo o padrão CVSS);
- 1.1.1.10.8.7. Controles mitigatórios aplicáveis;
- 1.1.1.10.8.8. Definição da recomendação técnica para solução.

1.1.1.11. Ataque

- 1.1.1.11.1. Os testes devem incluir pelo menos as seguintes atividades, não se restringindo somente a estas:
 - 1.1.1.11.1.1. Leitura/Alteração/exclusão de configurações;
 - 1.1.1.11.1.2. Fingerprint;
 - 1.1.1.11.1.3. Descoberta da senha de acesso do ativo;
 - 1.1.1.11.1.4. Escalonamento(salto) de acessos, até o ponto máximo possível.
- 1.1.1.11.2. Os testes devem ser feitos nas seguintes camadas:
 - 1.1.1.11.2.1. Aplicação;
 - 1.1.1.11.2.2. Apresentação;
 - 1.1.1.11.2.3. Sessão;
 - 1.1.1.11.2.4. Transporte;
 - 1.1.1.11.2.5. Rede.
- 1.1.1.11.3. Os testes de infraestrutura devem avaliar a possibilidade de exploração, comprometimento e/ou vulnerabilidades de:
 - 1.1.1.11.3.1. Servidores (diversas plataformas);
 - 1.1.1.11.3.2. Serviços (web, ftp, telnet, e-mail, dns, outros);
 - 1.1.1.11.3.3. Ativos de rede (Firewall, Firewall de aplicação, IPS, Switches, Roteadores, Soluções de Balanceamentos, outros).
- 1.1.1.11.4. Nos testes deve ser utilizado a última metodologia disponível OSSTMM, item “Testes de Segurança em Rede de Dados (Capítulo 11 - Data Networks Security Testing)”.
- 1.1.1.11.5. Deve ser imediatamente comunicado ao IBGE cada salto (escalonamento de acesso) de endereços IPs, ativos, servidores, aplicações, sistemas, serviços ou domínios efetuados com sucesso, durante a realização de todos os testes manuais.
- 1.1.1.11.6. Os testes de aplicações web devem englobar baseados na publicação OWASP TESTING GUIDE 3.0 (The Open Web Application Security Project):
 - 1.1.1.11.6.1. Aplicações acessadas via internet ou Intranet;
 - 1.1.1.11.6.2. Portais web disponíveis;

- 1.1.1.11.6.3. Serviços web diversos detectados;
- 1.1.1.11.6.4. Webservices;
- 1.1.1.11.6.5. Sockets.
- 1.1.1.11.7. A critério do IBGE, será definido qual escopo de usuários utilizado em cada teste, podendo ser definidos um ou mais destes critérios para uma mesma aplicação:
 - 1.1.1.11.7.1. Sem credenciais;
 - 1.1.1.11.7.2. Credenciais comuns;
 - 1.1.1.11.7.3. Credenciais de administrador.
- 1.1.1.11.8. Os testes devem contemplar todas as páginas, telas e transações disponíveis na aplicação, incluindo páginas/telas disponíveis para usuários sem credencias, com credencias, páginas/telas de administração, bem como demais existentes.
- 1.1.1.11.9. Os testes em aplicações devem contemplar as seguintes fases e itens em seu planejamento e execução, não se limitando somente a estes:
 - 1.1.1.11.9.1. Coleta de Informações;
 - 1.1.1.11.9.2. Teste de lógica de negócios;
 - 1.1.1.11.9.3. Teste de autenticação;
 - 1.1.1.11.9.4. Gerenciamento de Sessões;
 - 1.1.1.11.9.5. Testes de validação de Dados;
 - 1.1.1.11.9.6. Teste de Web Services;
 - 1.1.1.11.9.7. Negação de Serviço.
- 1.1.1.11.10. Deve incluir os testes listados e descritos nas duas últimas versões do TOPTEN disponibilizadas pela OWASP;
- 1.1.1.11.11. Pentest deve incluir a avaliação funcional de segurança, inspeção de segurança de código fonte e a avaliação de vulnerabilidade, sobre uma aplicação genérica de porte médio em uma ou mais das linguagens abaixo definidas:
 - 1.1.1.11.11.1. Java
 - 1.1.1.11.11.2. C#
 - 1.1.1.11.11.3. C, C++, Objective-C
 - 1.1.1.11.11.4. Python
 - 1.1.1.11.11.5. Power Builder
 - 1.1.1.11.11.6. Perl
 - 1.1.1.11.11.7. Basic, VB, VB.NET, VBScript
 - 1.1.1.11.11.8. HTML5, JavaScript
 - 1.1.1.11.11.9. .NET, ASP
 - 1.1.1.11.11.10. E demais a ser informada na reunião prévia entre a CONTRATADA e o IBGE.
- 1.1.1.11.12. Avaliação funcional de segurança com análise de código e segurança em software que consiste em avaliação automatizada seguida por inspeção manual por amostragem;

1.1.1.11.13. Numa primeira verificação, o analista irá executar um sistema de inspeção automatizada de código fonte. O sistema de Avaliação funcional de segurança com análise de código e segurança em software irá destacar trechos do código que considerar sensíveis. A atividade de inspeção de código tem por objetivo:

- 1.1.1.11.13.1. Indicar código malicioso inserido pelo desenvolvedor;
- 1.1.1.11.13.2. Apontar código inseguro e sugerir melhorias;
- 1.1.1.11.13.3. Identificar vulnerabilidades latentes;
- 1.1.1.11.13.4. Apontar uso de funções do sistema operacional com problemas conhecidos de segurança;
- 1.1.1.11.13.5. Indicar implementações de controles de segurança fora dos padrões e normas.

1.1.1.11.14. Cada ponto fraco identificado é apontado com o código correspondente, descrição do problema e forma de solução.

1.1.1.11.15. Deve ser feita uma análise detalhada e manual do código-fonte do aplicativo. Muitas das vulnerabilidades detectadas em uma análise de código-fonte são semelhantes às vulnerabilidades detectadas durante um Teste de penetração de aplicativo.

1.1.1.11.16. Deve-se personalizar o plano de teste para adequar a tecnologia usada pelo aplicativo.

1.1.1.12. Relatório de Teste de Invasão, maturidade do IBGE e matriz de risco:

1.1.1.12.1. A CONTRATADA deverá elaborar “Relatório de Teste de Invasão/ Maturidade do IBGE e Matriz de risco” para cada teste realizado apresentando todas as informações sobre o mesmo, contemplando no mínimo:

- 1.1.1.12.1.1. Objetivos, premissas e escopo do teste;
- 1.1.1.12.1.2. Metodologia de análise de vulnerabilidades;
- 1.1.1.12.1.3. Descrição das ações realizadas;
- 1.1.1.12.1.4. Vulnerabilidades encontradas;
- 1.1.1.12.1.5. Categorização e severidades vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades;
- 1.1.1.12.1.6. Apresentação das evidências apuradas;
- 1.1.1.12.1.7. Fontes de pesquisa, pontos positivos encontrados, referências e ferramentas utilizadas.

1.1.1.12.2. Deverão ser entregues os relatórios:

- 1.1.1.12.2.1. Relatório Executivo, com considerações e recomendações: Relatório a ser entregue ao final do ciclo, que deverá conter um histórico com a evolução da situação real do ambiente diante das análises e testes aplicados, bem como processo de mitigação e verificações feitas que elenquem as conclusões do trabalho, recomendações referentes às vulnerabilidades identificadas e exploradas resolvidas e não resolvidas, conforme requisitos deste documento.
- 1.1.1.12.2.2. Relatório Detalhado: O relatório deve ser entregue ao final de cada ciclo contendo todos os procedimentos efetuados e seus resultados, com a identificação do problema de segurança, explicação do procedimento detalhado, evidência do teste (incluindo filmagens dos ataques bem sucedidos),

recomendações concretas e detalhadas para aprimoramento e correção das falhas e vulnerabilidades exploradas. Este deve descrever o passo-a-passo de como a vulnerabilidade/falha pode ser explorada, para efeito de validação da solução aplicada por parte do IBGE, e atender itens conforme requisitos deste documento.

- 1.1.1.12.3. Os relatórios deverão ser validados junto ao IBGE, onde poderão ser solicitadas tantas alterações e correções quantas forem necessárias, até que se chegue a uma versão final aceita por ambas as partes.
- 1.1.1.12.4. Não serão aceitos relatórios obtidos diretamente por ferramentas automatizadas utilizadas para a realização dos testes, sem a devida transcrição e contextualização adequada, bem como atendimento de todos os requisitos do edital.
- 1.1.1.12.5. Os relatórios devem ser entregues na língua portuguesa com atendimento aos requisitos do edital.
- 1.1.1.12.6. As entregas devem ser realizadas por meio físico e/ou digital a ser definido pelo IBGE. Se digital disponibilizar: 1 arquivo .doc não protegido contra gravação e 1 arquivo .pdf assinado digitalmente com certificado digital ICP Brasil; e protegido por criptografia que deverá conter no mínimo código hash de cada documento, a fim de garantir integridade destas entregas. A versão digital dos documentos deverá ser assinada digitalmente com certificado digital ICP Brasil.
- 1.1.1.12.7. Para auxiliar na solução para correção das vulnerabilidades identificadas, o relatório deve indicar ao IBGE mais de uma opção de correção para cada item de vulnerabilidade identificado. Estas opções devem ser validadas com IBGE durante a redação dos relatórios, de forma que considerem as peculiaridades do ambiente IBGE, até o aceite final do mesmo.
- 1.1.1.12.8. A CONTRATADA deve fornecer ao IBGE todas as informações necessárias para correção da vulnerabilidade, clarificando eventuais dúvidas durante a vigência de todo o contrato.
- 1.1.1.13. Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste:
 - 1.1.1.13.1. Ao final de ciclo, deve ser realizada uma apresentação detalhada, nas dependências do IBGE no Rio de Janeiro ou remotamente, conforme solicitação do IBGE, com local a ser definido posteriormente, das documentações e conclusões.
- 1.1.1.14. Reavaliação, novo teste após remediação
 - 1.1.1.14.1. A contratada fará novos testes do mesmo tipo, no próximo ciclo, após a correção das vulnerabilidades apontadas no respectivo relatório por parte do IBGE.
- 1.1.1.15. Restrições e Limites
 - 1.1.1.15.1. As janelas de tempo para a execução dos testes serão acordadas entre CONTRATADA e IBGE, priorizando sempre os períodos/horários de menor pico de forma a não impactar no negócio.

Restrição	Exemplo	Razão da Restrição
Tempo de restrição	Teste de intrusão só poderá ser feito durante final de semana ou dia não útil	Reduzir risco de causar impacto durante horas de trabalho normal para assegurar que as atividades do teste sejam

		controladas e monitoradas devidamente.
Tipo de teste	Não executar teste de engenharia social	Focar na análise dos resultados técnicos somente
	Não executar ataque de força bruta em sistema com autenticação	Evitar problemas de bloqueio de credenciais advindo do ataque de força bruta.
IPs e aplicações	Não executar teste em IPs não especificados no escopo	Evitar ambiente compartilhado
	Teste não deve envolver determinado componente de sistema X	Evitar impacto no negócio com corrupção/interrupção de determinado sistema

1.1.1.15.2. Em caso de problemas durante a execução dos testes de invasão o IBGE acionará a CONTRATADA para manutenções corretivas. Ao acionar a CONTRATADA o IBGE classificará o problema em um dos níveis de criticidade da tabela a seguir. Cada nível de severidade possui diferentes níveis mínimos de serviço, conforme descrito também nas tabelas a seguir:

CLASSIFICAÇÃO DE EVENTOS	
(A) EMERGENCIAL	São consideradas como “Emergência” todas as falhas cujas consequências tenham impactos sobre o serviço, rede , tráfego de dados e sincronismo e/ou recursos de manutenção que exigem ação corretiva imediata (independente da hora do dia ou do dia da semana).
(B) ALTA PRIORIDADE	Situações que podem configurar uma severidade emergencial. São situações potenciais e exigem atenção imediata. São situações potenciais que precedem, em sua maioria, uma situação que pode ser classificada num segundo momento como severidade emergencial.
(C) MÉDIA PRIORIDADE	Problemas que não prejudicam significativamente o funcionamento dos sistemas / serviços. São problemas graves ou perturbações que afetam uma área específica de determinada funcionalidade. Exemplos: degradação de desempenho, perda de funcionalidades.
(D) BAIXA PRIORIDADE E CONSULTA	Consulta geral e problemas secundários que têm um efeito pequeno na funcionalidade do produto. Ex.: Falhas de documentação, falhas no projeto e questionamentos operacionais.

1.1.2. Alerta de vulnerabilidades

1.1.2.1. Deve ser entregue, pelo menos, um relatório semanal descrevendo as novas

vulnerabilidades publicadas por seus respectivos fabricantes, em português. Tal relatório deve conter, ao menos:

- 1.1.2.1.1. Fabricante que publicou a vulnerabilidade;
- 1.1.2.1.2. Produtos envolvidos;
- 1.1.2.1.3. Descrição da vulnerabilidade;
- 1.1.2.1.4. Solução proposta para mitigação ou eliminação da vulnerabilidade.
- 1.1.2.2. Devem estar inclusas as vulnerabilidades de todos os softwares de prateleira existentes no parque da CONTRATANTE (Sistemas Operacionais, Bancos de Dados, Aplicativos de escritório, entre outros).
 - 1.1.2.2.1. A definição de tais softwares deve ser realizada no momento da adoção do serviço.
- 1.1.3. Controle das vulnerabilidades
 - 1.1.3.1. De modo a garantir a redução constante do risco, deverão ser implantadas as seguintes ações:
 - 1.1.3.2. Abertura de chamado no sistema da CONTRATANTE para tratamento de cada vulnerabilidade ou conjunto de vulnerabilidades identificadas e que não estejam no escopo de atuação da CONTRATADA;
 - 1.1.3.3. Acompanhamento da implementação do Plano de Remediação e da correção efetiva da vulnerabilidade identificada;
 - 1.1.3.4. Validação das correções aplicadas e sugeridas pelo Plano de Remediação, incluindo reteste do ativo para validar a efetividade da ação realizada;
 - 1.1.3.5. Atualização diária da lista de vulnerabilidades existentes no parque, considerando as correções aplicadas e as novas vulnerabilidades divulgadas no relatório de alerta de vulnerabilidades.
 - 1.1.3.6. A contratada deverá disponibilizar profissionais para sanar quaisquer dúvidas relativas as vulnerabilidades identificadas, bem como testar novamente as vulnerabilidades corrigidas.
- 1.1.4. GERENCIAMENTO DE RISCOS
 - 1.1.4.1. Quanto ao gerenciamento de riscos a CONTRATADA deverá:
 - 1.1.4.1.1. Estabelecer uma matriz de riscos juntamente com a Administração do IBGE e propor ações de tratamento desses riscos (mitigação, eliminação, transferências, etc);
 - 1.1.4.1.2. Realizar ações de análise de riscos, visando a criação de uma matriz em conformidade com as diretrizes da administração da Contratada;
 - 1.1.4.1.3. Elaborar um documento para que seja avaliado e homologado pela Contratada, contendo minimamente a matriz de riscos, os processos de mitigação e tratamento dos riscos reportados;
 - 1.1.4.1.4. Acompanhar e realizar ações de cobrança junto aos responsáveis para cada ação definida nos processos de mitigação e tratamento;
 - 1.1.4.1.5. Para que seja possível o adequado gerenciamento de riscos deve ser entregue uma ferramenta com as seguintes características:
 - 1.1.4.1.5.1. Administração:
 - 1.1.4.1.5.1.1. Possuir módulo único e central de administração do ambiente, com

possibilidade de definição de perfis de acesso e permissões para usuários e grupos de usuários;

- 1.1.4.1.5.1.2. Registrar atividades em trilhas de auditoria;
- 1.1.4.1.5.1.3. Permitir que o administrador parametrize quais funções do sistema cada usuário terá acesso através de perfis de acesso. Entende-se funções do sistema todos os menus contidos no sistema;
- 1.1.4.1.5.1.4. Suportar autenticação Single Sign-On (SSO) através do protocolo SAML. O recurso deve ser nativo e ter interface de configuração na própria solução para que o administrador realize as configurações;
- 1.1.4.1.5.1.5. Permitir a sincronização de usuários com o Active Directory da Microsoft de forma nativa e configurável dentro da própria solução em um ambiente on premise do cliente onde a solução está hospedada em outro servidor, sem necessidade de abertura de portas de firewall entre servidor de aplicação e AD do cliente, garantindo segurança do ambiente do cliente;
- 1.1.4.1.5.1.6. Permitir realizar testes de sincronização e envio de relatório de sincronização de usuários a cada execução;
- 1.1.4.1.5.1.7. Possuir interface para gestão e monitoramento da fila de serviços de execução;
- 1.1.4.1.5.1.8. Possuir interface para monitoramento de notificações enviadas por e-mail;
- 1.1.4.1.5.2. Usabilidade:
 - 1.1.4.1.5.2.1. Permitir utilizar soluções de código aberto como requisitos do sistema, incluindo: servidor web, servidor de aplicação Java, sistema operacional e banco de dados;
 - 1.1.4.1.5.2.2. Ser compatível com os navegadores internet: Google Chrome, Microsoft Internet Explorer;
 - 1.1.4.1.5.2.3. Permitir rodar em ambiente virtualizado;
 - 1.1.4.1.5.2.4. Permitir a configuração do armazenamento de conteúdo (documentos e anexos) de forma visual pelo administrador do sistema, com as opções de armazenamento em banco de dados (campo Blob) ou diretório em rede;
 - 1.1.4.1.5.2.5. Permitir a conversão de conteúdo para o formato PDF;
 - 1.1.4.1.5.2.6. Suportar idiomas padrão UTF8;
 - 1.1.4.1.5.2.7. Suportar o uso de Load balancing tanto na camada de banco de dados, quanto de aplicação, permitindo que a carga do sistema seja distribuída entre dois ou mais nós da solução;
 - 1.1.4.1.5.2.8. Possuir visualizador nativo HTML 5 para PDF sem a necessidade de instalação de softwares adicionais para visualização nas estações clientes.
- 1.1.4.1.5.3. Requisitos do sistema:
 - 1.1.4.1.5.3.1. Permitir utilizar soluções de código aberto como requisitos do sistema, incluindo: servidor web, servidor de aplicação Java, sistema operacional e banco de dados;
 - 1.1.4.1.5.3.2. Ser compatível com os navegadores internet: Google Chrome, Microsoft Internet Explorer;
 - 1.1.4.1.5.3.3. Permitir rodar em ambiente virtualizado;

- 1.1.4.1.5.3.4. Permitir a configuração do armazenamento de conteúdo (documentos e anexos) de forma visual pelo administrador do sistema, com as opções de armazenamento em banco de dados (campo Blob) ou diretório em rede;
- 1.1.4.1.5.3.5. Permitir a conversão de conteúdo para o formato PDF;
- 1.1.4.1.5.3.6. Suportar idiomas padrão UTF8;
- 1.1.4.1.5.3.7. Suportar o uso de Load balancing tanto na camada de banco de dados, quanto de aplicação, permitindo que a carga do sistema seja distribuída entre dois ou mais nós da solução;
- 1.1.4.1.5.3.8. Possuir visualizador nativo HTML 5 para PDF sem a necessidade de instalação de softwares adicionais para visualização nas estações clientes.
- 1.1.4.1.5.4. Segurança:
 - 1.1.4.1.5.4.1. Realizar comunicação segura entre os diferentes componentes da solução e com a estação de trabalho usando padrões de criptografia e protocolos, ambos não proprietários (ex: SSL);
 - 1.1.4.1.5.4.2. Deve possuir controle de acesso por identificação e senha, com cadastro de usuários, grupos e transações, onde as permissões para cada uma das transações possam ser dadas diretamente ao usuário ou implicitamente através de um grupo do qual ele faça parte;
 - 1.1.4.1.5.4.3. Registrar os acessos efetuados por todos os usuários em um arquivo de log, para fins de auditoria e elaboração de relatórios gerenciais. Esses dados serão acessíveis apenas por um grupo determinado de usuários autorizados, contendo no mínimo os seguintes dados: usuário, data, hora, transação realizada;
 - 1.1.4.1.5.4.4. A ferramenta deve prover mecanismos de segregação de usuários através de nível de atuação (usuários, gerentes de projeto, consultor do escritório de projetos, suporte, administração);
 - 1.1.4.1.5.4.5. A ferramenta deve possuir mecanismos para restringir as operações no sistema conforme o perfil dos usuários;
 - 1.1.4.1.5.4.6. A ferramenta deve possibilitar o controle de restrições de acesso por usuário e por grupo de usuários;
 - 1.1.4.1.5.4.7. A ferramenta deve manter registro das alterações feitas nos dados e documentos com data, hora e usuário;
 - 1.1.4.1.5.4.8. A ferramenta deve possibilitar registro e consulta a dados estatísticos sobre acesso de usuários como acesso simultâneo, tempo de logon, origem do acesso;
 - 1.1.4.1.5.4.9. Todas as senhas de usuários devem ser armazenadas utilizando algoritmos de criptografia salted hash;
 - 1.1.4.1.5.4.10. A solução deve permitir a configuração e autenticação em mais de um domínio para a mesma instância, de forma que em um mesmo ambiente, seja possível se autenticar através de Single Sign-On (SSO) em diferentes domínios, não necessitando que os mesmos estejam integrados entre si, sem qualquer necessidade de parametrização via arquivo de configuração ou customização do produto.
- 1.1.4.1.5.5. Gestão de riscos:
 - 1.1.4.1.5.5.1. Permitir a definição da metodologia de avaliação de pontuação do risco em

qualquer nível da organização;

- 1.1.4.1.5.5.2. Permitir diversos métodos para a avaliação de risco, tais como: matriz; critérios quantitativos; mais de um critério quantitativos para gerar os eixos da matriz, e; critérios qualitativos;
- 1.1.4.1.5.5.3. Classificar os riscos de acordo com a severidade para a organização e com a probabilidade da ocorrência no processo;
- 1.1.4.1.5.5.4. Permitir a avaliação periódica do risco, monitorando a sua evolução analiticamente e graficamente;
- 1.1.4.1.5.5.5. Permitir a criação de modelos (template) de plano de riscos, para facilitar a replicação de estruturas similares nas organizações;
- 1.1.4.1.5.5.6. Permitir uma abordagem estratégica na identificação dos principais objetivos da organização e dos riscos existentes para o alcance desses objetivos;
- 1.1.4.1.5.5.7. Permitir que os riscos possam ser facilmente identificados e associados a um processo;
- 1.1.4.1.5.5.8. Permitir a criação de bibliotecas de riscos, ou seja, que os nomes dos riscos e tipos de riscos sejam armazenados em um repositório único, garantindo um conjunto de riscos padronizados para a organização;
- 1.1.4.1.5.5.9. Permitir a definição de equipes responsáveis pela avaliação;
- 1.1.4.1.5.5.10. Manter o cadastro e acompanhamento das alterações (revisão) dos objetos e dos planos de risco;
- 1.1.4.1.5.5.11. Permitir a definição do custo dos controles e o valor do impacto ou ganho do risco possibilitando a realização de análises quantitativas do risco;
- 1.1.4.1.5.5.12. Permitir a abertura de eventos (incidentes, problemas, workflows) caso as consequências do risco superem o esperado, possibilitando a identificação das causas, análise da causa, criação de planos de ação e verificação da eficácia. Estes registros devem ser mantidos para histórico e entrada da nova avaliação do risco futuramente;
- 1.1.4.1.5.5.13. Possibilitar a abertura de um workflow específico caso a avaliação do risco esteja acima do esperado;
- 1.1.4.1.5.5.14. Possibilitar a aprovação do plano de riscos ao final do planejamento e a revalidação dentro de frequência pré-estabelecida;
- 1.1.4.1.5.5.15. Permitir que os riscos possam ser associados a mais de um processo, porém, que sejam analisados e documentados individualmente para cada processo;
- 1.1.4.1.5.5.16. Permitir a avaliação considerando o risco potencial, o risco inerente e o risco residual;
- 1.1.4.1.5.5.17. Permitir o cálculo automático do risco residual;
- 1.1.4.1.5.5.18. Permitir a associação de anexos e documentos controlados ao Risco;
- 1.1.4.1.5.5.19. Executar as avaliações de maneira on-line;
- 1.1.4.1.5.5.20. Permitir a análise de risco dos processos mapeados;
- 1.1.4.1.5.5.21. Apresentar graficamente as atividades que possuem riscos associados;
- 1.1.4.1.5.5.22. Mapear os processos e modelar todas as atividades relacionadas;
- 1.1.4.1.5.5.23. Permitir a análise de risco dos ativos;

- 1.1.4.1.5.5.24. Permitir a gestão dos riscos relacionados ao planejamento (Scorecard);
- 1.1.4.1.5.5.25. Permitir a criação de Indicadores e cards com as informações inseridas dentro da plataforma (perspectivas, objetivos e indicadores);
- 1.1.4.1.5.5.26. Permitir a habilidade de desenvolver ou adotar um framework para a gestão de riscos (COSO ERM, ISSO 31000, OCEG ou outros frameworks similares);
- 1.1.4.1.5.5.27. Mapear os riscos operacionais de acordo com framework COSO;
- 1.1.4.1.5.5.28. Permitir a associação de tratamentos e planos de ação no momento da criação da análise de risco;
- 1.1.4.1.5.5.29. Permitir a associação de controles aos riscos durante o cadastro, facilitando a utilização posterior;
- 1.1.4.1.5.5.30. Apresentar o histórico das avaliações do risco atualizado conforme última versão do método de avaliação;
- 1.1.4.1.5.5.31. Oferecer método de avaliação para a definição do nível do risco. Critérios quantitativos podem ser informados para a obtenção do resultado;
- 1.1.4.1.5.5.32. Personalizar as colunas para serem visualizadas na estrutura do plano de risco e controle;
- 1.1.4.1.5.5.33. Permitir a visualização da Matriz de Risco de todos os riscos de um plano de risco;
- 1.1.4.1.5.5.34. Permitir a visualização da Matriz de Risco agrupando quantitativamente as avaliações dos riscos;
- 1.1.4.1.5.5.35. Permitir a associações do risco no momento que está cadastrando um evento, ou seja, um incidente, problema ou workflow;
- 1.1.4.1.5.5.36. Permitir registrar uma justificativa, anexo ou documento para cada resultado da avaliação do risco;
- 1.1.4.1.5.5.37. Permitir associar causas, consequências, fontes de risco e melhores práticas ao risco;
- 1.1.4.1.5.5.38. Permitir criar e gerenciar KRI (Indicadores chave de risco), com geração de eventos casos do KRI estejam fora dos valores aceitáveis;
- 1.1.4.1.5.5.39. Permitir enviar e-mail para aprovação da inclusão do risco previamente a sua respectiva avaliação;
- 1.1.4.1.5.5.40. Permitir solicitar a avaliação de risco para o responsável no momento da Auditoria.
- 1.1.4.1.5.6. Problemas e tratamento:
 - 1.1.4.1.5.6.1. Permitir identificar problemas nas atividades de controle;
 - 1.1.4.1.5.6.2. Permitir identificar problemas na avaliação do risco;
 - 1.1.4.1.5.6.3. Permitir associar prioridade aos problemas;
 - 1.1.4.1.5.6.4. Permitir definir responsáveis aos problemas;
 - 1.1.4.1.5.6.5. Permitir monitorar prazos de planejamento e de execução;
 - 1.1.4.1.5.6.6. Permitir enviar e-mail automaticamente para o responsável assim que uma ocorrência for registrada;
 - 1.1.4.1.5.6.7. Permitir criar e monitorar múltiplos planos de ação para cada problema;

- 1.1.4.1.5.6.8. Permitir que os responsáveis pelos planos de ação possam ser diferentes dos responsáveis pelo problema;
- 1.1.4.1.5.6.9. Permitir que os planos de ação sejam revisados e aprovados por um usuário específico ou pelo responsável pelo problema;
- 1.1.4.1.5.6.10. Permitir que a situação de execução dos planos de ação seja monitorada;
- 1.1.4.1.5.6.11. Permitir que as notificações por e-mail possam ser definidas pelos usuários;
- 1.1.4.1.5.6.12. Permitir que o gestor tenha fácil acesso a todos os problemas e planos de ação de sua área de responsabilidade;
- 1.1.4.1.5.6.13. Permitir que trilhas de auditoria para qualquer alteração nas atividades e prazos relacionados aos problemas e planos de ação façam parte do sistema;
- 1.1.4.1.5.6.14. Permitir a análise de causa e de tendência;
- 1.1.4.1.5.6.15. Permitir a personalização da resposta ao risco;
- 1.1.4.1.5.6.16. Permitir a criação ou a associação de um ou mais planos de ação para cada tratamento do risco;
- 1.1.4.1.5.6.17. A solução deverá permitir a gestão estruturada de iniciativas relacionadas à segurança da informação, como planejamentos de correção de vulnerabilidades, auditorias e projetos de conformidade, com base nas boas práticas de gerenciamento de projetos descritas no PMBOK Guide, Se integrando e oferecendo funcionalidades compatíveis com práticas de gestão de projetos, como:
 - 1.1.4.1.5.6.17.1. Definição de escopo e objetivos;
 - 1.1.4.1.5.6.17.2. Planejamento de recursos e prazos;
 - 1.1.4.1.5.6.17.3. Monitoramento de progresso e riscos;
 - 1.1.4.1.5.6.17.4. Geração de relatórios gerenciais.
- 1.1.4.1.5.6.18. Permitir definir um tratamento para uma avaliação de risco e associar um plano de ação para este tratamento.
- 1.1.4.1.5.7. Consultas e relatórios:
 - 1.1.4.1.5.7.1. Permitir que o sistema agrupe e gere consultas da avaliação de riscos em todos os níveis da base de dados, incluindo a estrutura organizacional, processos e riscos;
 - 1.1.4.1.5.7.2. Apresentar a listagem de problemas e planos de ação com possibilidade de desdobramentos;
 - 1.1.4.1.5.7.3. Permitir salvar relatórios no formato PDF;
 - 1.1.4.1.5.7.4. Permitir que os responsáveis pelos controles e auditores independentes possam acessar facilmente sua informação no sistema;
 - 1.1.4.1.5.7.5. Permitir que os responsáveis pelos processos possam acessar facilmente sua informação no sistema;
 - 1.1.4.1.5.7.6. Apresentar listagens ou relatórios da avaliação de riscos, visando a fácil identificação de pontos críticos na organização;
 - 1.1.4.1.5.7.7. Apresentar os objetivos estratégicos e da avaliação dos riscos de maneira gráfica e visual;

- 1.1.4.1.5.7.8. Apresentar a matriz de riscos para a fácil identificação dos riscos dentro dos quadrantes do método de avaliação;
- 1.1.4.1.5.7.9. Garantir o acompanhamento do plano de riscos permitindo uma fácil visualização do fluxograma do processo, riscos por etapa, controles e tratamentos, matriz de riscos x etapa e demais elementos;
- 1.1.4.1.5.7.10. Apresentar a matriz de riscos para a fácil identificação da relação entre riscos e atividades;
- 1.1.4.1.5.7.11. Apresentar o cálculo do risco médio gerado automaticamente e agrupado por Unidade Organizacional, Processo, Risco, Tipo de Risco com visões gráficas da matriz de risco em um portal interativo;
- 1.1.4.1.5.7.12. Permitir comparar os resultados entre as revisões do plano de risco e controle;
- 1.1.4.1.5.7.13. Permitir a definição de indicadores de desempenho associados aos processos e acompanhamento do cumprimento das metas estabelecidas;
- 1.1.4.1.5.7.14. Possibilitar a geração de diversos tipos de relatórios e gráficos contendo informações detalhadas ou resumidas sobre os processos e atividades;
- 1.1.4.1.5.7.15. Possuir semáforos que sinalizam visualmente o nível de cumprimento dos resultados;
- 1.1.4.1.5.7.16. Possuir indicador de tendência sobre possíveis problemas futuros;
- 1.1.4.1.5.7.17. Permitir a formatação dos resultados em planilhas e gráficos configuráveis pelo usuário;
- 1.1.4.1.5.7.18. Permitir a visualização dos recursos e custos requeridos para a execução dos processos.

1.2. Monitoração da marca

- 1.2.1. A CONTRATADA deverá prover solução tecnológica que permita o monitoramento contínuo de ambientes digitais públicos e restritos, com foco na identificação de ameaças à segurança da marca da CONTRATANTE, incluindo menções indevidas, vazamentos de dados e uso não autorizado de ativos digitais.
- 1.2.2. A solução deverá realizar varreduras diárias em fontes abertas e ambientes restritos da internet, como fóruns, redes sociais, blogs, sites de compartilhamento de texto e comunidades digitais, com capacidade de gerar alertas automatizados sobre riscos identificados.
- 1.2.3. A solução deverá possuir capacidade de acesso automatizado e contínuo a repositórios da Deep Web e Dark Web, como redes Tor, Zeronet, fóruns especializados e sites de compartilhamento de conteúdo, com geração de relatórios e alertas sobre ameaças relevantes.
- 1.2.4. A solução deverá permitir a realização de pesquisas históricas em ambientes da Deep/Dark Web, com foco em menções à marca, projetos e ativos da CONTRATANTE.
- 1.2.5. A solução deverá permitir buscas por dados e informações potencialmente vazadas, utilizando como parâmetros de pesquisa:
 - 1.2.5.1. Domínio institucional;
 - 1.2.5.2. Intervalos de endereços IP;

- 1.2.5.3. Nomes de executivos e colaboradores estratégicos;
- 1.2.5.4. Dados de cartões corporativos;
- 1.2.5.5. Nomes de projetos e documentos técnicos.
- 1.2.6. A solução deverá permitir a identificação de menções a projetos estratégicos da CONTRATANTE em ambientes da Deep/Dark Web.
- 1.2.7. A solução deverá monitorar informações sensíveis relacionadas à CONTRATANTE, incluindo credenciais expostas, dados pessoais e corporativos, com alertas em tempo real.
- 1.2.8. A solução deverá realizar monitoramento de uso indevido de ativos da marca (nome, logotipo, identidade visual) em perfis e páginas de redes sociais.
- 1.2.9. A solução deverá permitir o monitoramento de dados sensíveis de até 10 executivos e pessoas-chave da organização, como CPF, RG, CNH, nome completo, cartões, e-mails, em ambientes da surface, deep e dark web.
- 1.2.10. A solução deverá realizar buscas automatizadas por endereços de e-mail vinculados aos domínios da CONTRATANTE que tenham sido alvo de exposições de credenciais.
- 1.2.11. A solução deverá classificar e priorizar os riscos cibernéticos identificados, com base em critérios técnicos e automatizados, para facilitar a tomada de decisão.
- 1.2.12. A solução deverá permitir a execução de até 60 ações de takedown por ano, com emissão de notificações extrajudiciais e acompanhamento técnico para tratamento dos incidentes.

2. SERVIÇOS PARA O ITEM 2

- 2.1.1. Indicação das atividades e criticidade, para aplicação dos níveis mínimos de serviço :

FASE	CRITICIDADE (Conforme item 7.4 do termo de referência - NMS)
Análise de Incidentes Globais	BAIXA
Monitoração de Incidentes	MÉDIA

2.2. Análise de Incidentes Globais

- 2.2.1. A CONTRATADA deve monitorar a ocorrência de incidentes globais, através de RSS Feeds, de modo a antever eventuais ataques a CONTRATANTE;
- 2.2.2. Ataques direcionados ao mesmo segmento de mercado do CONTRATANTE devem ser imediatamente sinalizados para que seja tomada uma decisão em relação à atuação dos serviços contratados.

2.3. Monitoramento de Incidentes

- 2.3.1. Monitoramento de aplicações web, servidores, virtualizadores e rede de forma proativa e

reativa (com anuência do IBGE) no ambiente internet e intranet da instituição.

2.3.2. São papéis da CONTRATADA:

- 2.3.2.1. Monitorar o ambiente quanto à disponibilidade e desempenho dos equipamentos que compõe a solução a ser utilizada no gerenciamento, bem como todo o escopo contratado quanto aos incidentes relacionados à segurança da informação;
- 2.3.2.1.1. O ambiente a ser monitorado possui até 2.100 (dois mil e cem) ativos, incluindo servidores, roteadores, switches, entre outros.
- 2.3.2.2. Fazer a gestão dos incidentes (criação de alertas, detecção e abertura de chamados);
- 2.3.2.3. Acompanhar do início ao fim os incidentes;
- 2.3.2.4. Realizar o acionamento por matriz de escalação hierárquica e funcional, para os incidentes;
- 2.3.2.5. Correlacionar o processo de eventos (gerenciar eventos durante todo o seu ciclo de vida) e o processo de incidentes de forma automatizada entre a ferramenta de ITSM (IT Service Management, ou Gestão de Serviços de TI) e ferramenta de monitoramento;
- 2.3.2.6. Acompanhar os processos através de indicadores de desempenho;
- 2.3.2.7. Para tal, a CONTRATADA deverá entregar ferramenta com as seguintes características.
- 2.3.2.8. Características gerais da plataforma:**
 - 2.3.2.8.1. A solução deve ser composta pelos seguintes elementos:
 - 2.3.2.8.2. Coletores de eventos e agentes especializados responsáveis pela coleta de eventos (logs);
 - 2.3.2.8.3. Armazenador de eventos e registros processados;
 - 2.3.2.8.4. Correlacionador de eventos;
 - 2.3.2.8.5. A solução deve ser capaz de ler logs que atualmente são gerenciados pela ferramenta atual que está em funcionamento no IBGE, o Loghrythm;
 - 2.3.2.8.6. A solução deverá ser entregue em servidor virtual para instalação on premise no ambiente do IBGE, conforme as seguintes configurações:
 - 2.3.2.8.7. Sistema de Virtualização Microsoft Hyper-V Server 2016 ou versões superiores, a critério do IBGE;
 - 2.3.2.8.8. O IBGE disponibilizará os equipamentos que atuarão como servidores físicos hospedeiros para a console e coletores que a solução fornecerá;
 - 2.3.2.8.9. Possuir, ao menos, duzentos DataSources nativos na plataforma disponível para eventuais integrações
 - 2.3.2.8.10. Os bancos de dados utilizados pela ferramenta devem ser oferecidos em conjunto com a ferramenta, sem que haja custos futuros de expansão, manutenção ou licença para o IBGE;
 - 2.3.2.8.11. A solução deve ser de fabricante nacional ou fabricante estrangeiro com representação no Brasil.
 - 2.3.2.8.12. A comunicação entre os componentes da solução deve ser feita através de criptografia, com uso de algoritmos RSA 2048, AES (128 bits ou mais) e/ou 3DES(192 bits ou mais), garantindo a autenticidade, confidencialidade e

integridade dos dados, utilizando o protocolo TCP/IP.

- 2.3.2.8.13. Juntamente com a subscrição de atualização dos componentes da solução pelo período do contrato, a contratada deverá prover acesso à biblioteca de casos de uso do fabricante, que contenha pacotes especializados de regras, dashboards e coletores desenvolvidos pelo fabricante que permitam a implementação de correlação e monitoração avançada, sem necessidade de redesenvolvimento.
- 2.3.2.8.14. Possuir, ao menos, trezentos DataSources nativos na plataforma disponível para eventuais integrações.
- 2.3.2.8.15. Toda comunicação entre os componentes deverá ser criptografada;
- 2.3.2.8.16. A solução deverá ser capaz de implementar Ipv6;
- 2.3.2.8.17. Todos os módulos da solução (coletores, solução de armazenamento de logs e correlacionador) devem ser do mesmo fabricante.
- 2.3.2.8.18. Não serão aceitas soluções a serem projetadas, em fase de projeto, ou em desenvolvimento. Caso o suporte ao produto seja descontinuado antes da data do término deste edital, a empresa deverá fornecer a atualização necessária para que o produto continue a ter sua manutenção provida pelo fabricante ou substituir o sistema pela solução da nova geração;
- 2.3.2.8.19. Não serão aceitas soluções que contenham soluções que envolvam exfiltração de dados, seja por meio de um programa, um equipamento ou a combinação de ambos, para redes externas às redes do IBGE, tais como redes da empresa vendedora, da empresa desenvolvedora ou qualquer tipo de “nuvem” de dados;
- 2.3.2.8.20. Não serão aceitas soluções que causem custos adicionais de licenciamento, mão-de-obra ou equipamentos.
- 2.3.2.8.21. A solução deverá prover todas as licenças de software, sistemas operacionais, bancos de dados, subscrições ou qualquer outro tipo de licenciamento necessário para seu completo funcionamento, de acordo com as características e prazos estipulados. A infraestrutura de virtualização será fornecida pela CONTRATANTE.
- 2.3.2.8.22. A solução ofertada poderá ser composta por um ou mais softwares, desde que sejam do mesmo fabricante, totalmente interoperáveis entre si, gerenciados através de uma interface única e em número de licenças suficientes para atender aos volumes de dados e/ou quantidades de eventos solicitados.
- 2.3.2.8.23. As licenças de software deverão ser registradas junto ao fabricante da solução em nome da contratante;
- 2.3.2.8.24. O tipo de licenciamento é licença do tipo subscrição para instalação on-premises, com possibilidade de atualização enquanto durar o contrato de suporte.
- 2.3.2.8.25. A solução de SIEM ofertada não poderá ser do tipo opensource;
- 2.3.2.8.26. Deverá ser ofertada a última versão estável de todos os softwares;
- 2.3.2.8.27. Poderão ser considerados servidores para armazenamento de logs, coletores e tratamento de eventos em separado.
- 2.3.2.9. **DOS AGENTES E COLETORES DE EVENTOS**
 - 2.3.2.9.1. A solução deverá estar dimensionada e licenciada para coleta, processamento e retenção conforme descrito abaixo:
 - 2.3.2.9.1.1. EPS/MPS médio de 3.000;

- 2.3.2.9.1.2. Aproximadamente 7.6 TB de logs processados.
- 2.3.2.9.2. Para fins de dimensionamento e licenciamento, um evento é definido como qualquer pacote de log ou fluxo de rede recebido pela solução.
- 2.3.2.9.3. A solução deverá suportar, em episódios de ataque ou sobrecarga de eventos, duas vezes seu volume licenciado durante 6 horas consecutivas, mantendo o funcionamento da solução, sem perda de eventos ou restrições de funcionalidades.
- 2.3.2.9.4. A solução deverá ser capaz de receber eventos de fluxos de rede Netflow.
- 2.3.2.9.5. Coletar e aplicar parsing nos dados dos dispositivos monitorados em tempo próximo ao real (near-real-time).
- 2.3.2.9.6. Ser capaz de normalizar e categorizar os eventos em um padrão único que será usado pela solução;
- 2.3.2.9.7. Rotular eventos por zonas diferentes mesmo que estejam em redes com mesmo endereçamento IP;
- 2.3.2.9.8. Ser possível realizar a coleta de eventos de dispositivos não suportados nativamente através de conectores customizados;
- 2.3.2.9.9. Ajustar o horário dos eventos, com base em limites de diferença de hora entre os eventos originais e a hora correta obtida pelo sistema através desincronização de NTP (Network Time Protocol) com os servidores locais;
- 2.3.2.9.10. Marcar (através de tag, label ou similar) os eventos com base em unidade organizacional: departamento, setor, divisão corporativa ou similar;
- 2.3.2.9.11. Filtrar e selecionar os eventos que serão inseridos na solução e permitir a criação e alteração de filtros;
- 2.3.2.9.12. Possuir suporte aos protocolos de gerenciamento SNMPv1, SNMPv2, SNMPv3 e outras mais avançadas porventura existentes à época do fornecimento.
- 2.3.2.9.13. Possuir a funcionalidade de ler e normalizar eventos de log armazenados em formato texto (w3c), SQL database, compactados ou não.
- 2.3.2.9.14. A solução deverá suportar a coleta dos logs de outros sistemas e ativos que venham a ser incorporados pelo órgão durante a vigência do contrato, mesmo que não conste inicialmente no Termo de Referência. Nesse caso, a contratada poderá implementar conectores customizados, caso a solução não tenha capacidade de recebimento do log nativamente.
- 2.3.2.9.15. Ser capaz de coletar, no mínimo, os logs dos sistemas e ativos listado abaixo:
 - 2.3.2.9.15.1. Firewalls: Cisco ASA 5585x SSP10 com Firepower, Checkpoint 4600, VMWare NSX, Palo Alto;
 - 2.3.2.9.15.2. Soluções de WAF: Big IP F5, Akamai, Cloudflare, Barracuda;
 - 2.3.2.9.15.3. Roteadores: Cisco Nexus, Cisco RV320, Huawei/H3C MSR;
 - 2.3.2.9.15.4. Switches: Cisco, Huawei, Enterasys e Extreme;
 - 2.3.2.9.15.5. Plataformas de Virtualização: VMware ESX, HyperV, Acropolis/KVM e Oracle VM;
 - 2.3.2.9.15.6. Sistemas Operacionais: Linux (Debian, RedHat, Ubuntu, CentOS, Oracle Linux, Red Hat Enterprise Linux (RHEL)), Windows Server (2008, 2012, 2016 ou acima) e FreeBSD;

- 2.3.2.9.15.7. Antivirus: Windows Defender e SEP;
- 2.3.2.9.15.8. Servidores de E-mail on premise ou em nuvem: Microsoft Exchange;
- 2.3.2.9.15.9. Servidores de Aplicação e Web: Apache2, Squid, HAProxy, Apache, Jboss e MicroSoft IIS7 (ou superior);
- 2.3.2.9.15.10. VPN: OpenVPN, CiscoVPN, Global Protect (Palo Alto)
- 2.3.2.9.15.11. Soluções hospedadas em nuvens tipo: Azure, AWS, Google Cloud, IBM Cloud, Defender for Cloud;
- 2.3.2.9.16. A solução deve poder coletar dados de feeds externos;
- 2.3.2.9.17. Para a coleta de dados e feeds externos deve suportar, no mínimo, os seguintes formatos/protocolos/fontes:
 - 2.3.2.9.17.1. Para Feeds Externos:
 - 2.3.2.9.17.1.1. CIFS
 - 2.3.2.9.17.1.2. FTP
 - 2.3.2.9.17.1.3. Manual Upload
 - 2.3.2.9.17.1.4. McAfee ATD
 - 2.3.2.9.17.1.5. NFS
 - 2.3.2.9.17.1.6. SCP
 - 2.3.2.9.17.1.7. SFTP
 - 2.3.2.9.17.1.8. TAXII
 - 2.3.2.9.17.2. Para Coleta de Dados
 - 2.3.2.9.17.2.1. SYSLOG
 - 2.3.2.9.17.2.2. MEF
 - 2.3.2.9.17.2.3. SCP
 - 2.3.2.9.17.2.4. HTTP
 - 2.3.2.9.17.2.5. FTP
 - 2.3.2.9.17.2.6. SFTP
 - 2.3.2.9.17.2.7. NFS (Tail mode or Copy mode)
 - 2.3.2.9.17.2.8. CIFS (Tail mode or Copy mode)
- 2.3.2.9.18. Prover mecanismo de coleta de logs de dispositivos não suportados nativamente, através de personalização de coletores, ou solução similar.
- 2.3.2.9.19. A solução deve ser composta de agentes que têm como função básica fazer a interface com o dispositivo monitorado, recebendo ou buscando eventos relevantes que serão inseridos na solução.
- 2.3.2.9.20. Suportar a coleta de dados de no mínimo 250 (duzentos e cinquenta) geradores de eventos (logs);
- 2.3.2.9.21. Controlar a utilização da banda utilizada diretamente do conector sem a necessidade de usar recursos do sistema operacional;
- 2.3.2.9.22. Separar eventos por meio de anotações em campos, originados por quaisquer

campos disponíveis e normalizados (ex: Cliente 1 - VLAN ID 10, Cliente 2- VLAN ID 20) mesmo que o evento seja de um mesmo firewall;

- 2.3.2.9.23. A modalidade de licenciamento deverá permitir a distribuição livre de elementos de coleta, filtragem e agregação, gerados com o uso de SDK ou API(Application Programming Interface), independentemente do número e arquitetura;
- 2.3.2.9.24. A camada de coleta deverá permitir ser instalada em modo distribuído, possibilitando a implementação de seus elementos o mais próximo possível dos dispositivos e softwares monitorados;
- 2.3.2.9.25. Os elementos da solução deverão permitir nativamente sua instalação em máquinas virtuais, servidores físicos, appliances e, conjuntamente com a aplicação alvo, quando desejado pela Instituição. Por exemplo, a Instituição poderá determinar que o elemento de interface seja instalado no mesmo servidor de uma aplicação, para evitar que os logs dessa aplicação percorram a rede em modo claro e pode determinar que o elemento de interface seja instalado em um servidor stand-alone na rede de roteadores, para que eventos de múltiplos dispositivos de roteamento sejam recebidos pelo mesmo elemento de interface;
- 2.3.2.9.26. A solução deve ser capaz de normalizar os eventos em um padrão único;
- 2.3.2.9.27. O componente de coleta de eventos deve suportar a captura, a normalização e o tratamento de eventos em tempo próximo ao real (near real-time);
- 2.3.2.9.28. O coletor da solução deverá ser capaz de armazenar os dados localmente (cache) em caso de indisponibilidade do componente correlacionador.
- 2.3.2.9.29. O envio dos dados em cache deve ocorrer imediatamente a disponibilização do correlacionador.
- 2.3.2.9.30. A solução deve ser capaz de enviar o evento bruto (raw) para o armazenamento e consulta futura;
- 2.3.2.9.31. Deve permitir acrescentar o horário (timestamp) correto da recepção do evento/log na solução, preservando o horário original do evento. Esse horário deve ser obtido pelo sistema através de sincronização com servidores NTP previamente definidos, e sincronizado entre todos os componentes da solução;
- 2.3.2.9.32. Tanto os eventos de segurança quanto os de conformidade devem ser normalizados para um único padrão de eventos utilizado pela solução;
- 2.3.2.9.33. A solução deve permitir múltiplos perfis de configuração.
- 2.3.2.9.34. A solução deverá enviar os eventos coletados para o correlacionador e permitir enviar para mais de um destino ao mesmo tempo.
- 2.3.2.9.35. Deverá implementar coleta de informações de fluxo - Netflow ou SFlow;
- 2.3.2.9.36. Será considerada no Edital a seguinte definição para conector: software desenvolvido e suportado pelo fabricante da solução que tem como função básica fazer a interface com o dispositivo monitorado, recebendo ou buscando eventos relevantes que serão inseridos na solução, contendo obrigatoriamente documentação de todos coletores nativos com informações de configurações de cada ativo suportado;
- 2.3.2.9.37. Realizar a agregação de eventos semelhantes que ocorrem dentro de um limite de tempo e quantidade de eventos específicos, sendo que permite agregar tanto os eventos cuja única diferença seja o horário de ocorrência, quanto especificar quais campos do evento normalizado devem ser considerados para fins de agregação;

- 2.3.2.9.38. Possuir a funcionalidade de atualização, gerenciamento e configuração centralizados de todos os conectores distribuídos da solução;
- 2.3.2.9.39. Permitir a categorização manual de eventos (já normalizados) inéditos não categorizados por padrão. Esta categorização deverá ser aplicada nos eventos futuros de mesma característica;
- 2.3.2.9.40. De forma a evitar a perda de eventos por sobrecarga ou indisponibilidade de conectores, a contratada deverá fornecer função redundante de balanceamento de cargas de serviço Syslog;
- 2.3.2.9.41. O balanceamento deverá ser capaz de implementar Weighted Round Robin e Round Robin.
- 2.3.2.9.42. Ao receber um evento syslog, a solução deverá buscar um conector disponível, de forma a garantir que não haverá perda de eventos por sobrecarga de conectores.
- 2.3.2.9.43. Será aceito o fornecimento da funcionalidade de balanceamento nativa ou por adição de elementos externos de qualquer fabricante. A solução de balanceamento redundante deverá estar dimensionada para suportar o volume de tráfego cotado.
- 2.3.2.10. DO ARMAZENAMENTO
 - 2.3.2.10.1. Componente da solução responsável pela retenção dos dados coletados.
 - 2.3.2.10.2. A solução deverá estar dimensionada e licenciada para efetuar a retenção e pesquisa em 100% dos eventos coletados;
 - 2.3.2.10.3. Armazenar os dados: eventos, alertas, incidentes, bases de conhecimento, workflow nativo e toda informação pertinente à solução, tais como configuração, usuários, trilhas de auditoria e informações de depuração.
 - 2.3.2.10.4. Ter a capacidade de definir política de retenção dos dados on-line, ou seja, dados mantidos no banco de dados da solução, disponíveis para consulta imediata;
 - 2.3.2.10.5. Ser capaz de armazenar logs por tempo determinado e personalizado, conforme necessidade do órgão;
 - 2.3.2.10.6. Deverá ter a capacidade de guardar eventos brutos em forma comprimida;
 - 2.3.2.10.7. Deverá ter a capacidade de recuperar, sob demanda, registros sem modificação para preservação de evidência com qualidade forense;
 - 2.3.2.10.8. De forma a permitir seu uso em auditorias e processos forenses, não deverá ser possível, sob nenhuma hipótese, a seleção e exclusão de eventos individuais. Deve ser possível apenas a exclusão de eventos conforme a política de retenção, ou seja, todos os eventos mais antigos que extrapolem o tempo de retenção ou o tamanho do armazenamento definido para esse tipo de registros;
 - 2.3.2.10.9. Permitir o expurgo dos dados de forma automática com a personalização do período de tempo do expurgo.
 - 2.3.2.10.10. Deverá permitir a utilização de volumes de armazenamento locais e externos. Deverá permitir a segregação de tipos de eventos diferentes em grupos lógicos de armazenamento diferentes, com políticas de retenção diferentes, de forma a permitir a otimização de performance;
 - 2.3.2.10.11. Deverá permitir exportar eventos para formato pdf e csv em estruturas NFS, CIFS, SAN e localmente. Deverá permitir que o usuário defina quais campos do evento serão exportados;

- 2.3.2.10.12. Implementar: políticas de controle de acesso aos dados, auditoria e tráfego dos dados criptografados com algoritmos padrões de mercado reconhecidamente seguros.
- 2.3.2.10.13. A solução deve permitir que os relatórios sejam executados periodicamente (diário, semanal, quinzenal, mensal, etc...) ou de forma tempestiva.
- 2.3.2.10.14. Deverá implementar acesso integrado com autenticação padrão LDAP.
- 2.3.2.10.15. Deverá implementar dashboards com visualização de EPS de entrada, EPS de saída e utilização de CPU;
- 2.3.2.10.16. Deverá permitir a livre customização da interface, definindo página inicial por usuário e dashboards customizados;
- 2.3.2.10.17. Deverá ser fornecido com dashboards pré-configurados e permitir a criação de novos dashboards;
- 2.3.2.10.18. Deverá implementar dashboards de monitoramento de resultados históricos;
- 2.3.2.10.19. Deverá possuir dashboard pré-configurados pelo menos para Windows, firewall, código malicioso, entre outros;
- 2.3.2.10.20. Deverá permitir pesquisas (queries) no histórico de eventos, fornecendo capacidade de drilldown, ou seja, visualizar os detalhes dos eventos, inclusive o raw event (dado cru), quando aplicável, para análise forense e investigação de incidentes.
- 2.3.2.10.21. Deverá permitir a procura por texto, campos pré-definidos, palavras chaves, operações booleanas e expressões regulares;
- 2.3.2.10.22. Deverá permitir a utilização de procuras complexas através do encadeamento de comandos de consulta;
- 2.3.2.10.23. Deverá permitir a configuração da visualização do resultado em formato de tabela e gráfico;
- 2.3.2.10.24. Deverá permitir a configuração do escopo de procura como local e distribuída por alguns ou todos os elementos da solução;
- 2.3.2.10.25. Deverá permitir a gravação da query de procura em formato de filtro para utilização futura;
- 2.3.2.10.26. Deverá permitir a gravação dos resultados da pesquisa em arquivo;
- 2.3.2.10.27. Deverá implementar funcionalidade assistente para facilitar a criação das queries;
- 2.3.2.10.28. Deverá implementar assistente gráfico para criação de queries;
- 2.3.2.10.29. Deverá implementar funcionalidade de sugestão de termos de procura enquanto se digita os critérios de pesquisa (recurso auto completar);
- 2.3.2.10.30. Deverá implementar funcionalidade de listagem das últimas queries realizadas para facilitar o reuso em pesquisas;
- 2.3.2.10.31. Deverá implementar indexação baseada em campo e palavra-chave para acelerar buscas; Deverá implementar alertas por syslog, SNMP e e-mail;
- 2.3.2.10.32. Deverá permitir visualização em tempo real de eventos que atendam ao critério de seleção definido pelo usuário;
- 2.3.2.10.33. Deverá possuir relatórios pré-configurados separados em categorias;
- 2.3.2.10.34. Deverá possuir ferramenta gráfica para desenho de modelos de relatórios personalizados;

- 2.3.2.10.35. Deverá implementar tecnologia de procura distribuída por múltiplos elementos;
- 2.3.2.10.36. Deverá armazenar os eventos de forma compactada;
- 2.3.2.10.37. Apresentar relatórios de eventos, alertas e incidentes em nível técnico e gerencial, os quais devem ter a possibilidade de serem gerados em pdf, html e csv;
- 2.3.2.10.38. Deverá permitir o agendamento de geração de relatórios periódicos, notificar ou enviar automaticamente os relatórios gerados para os destinatários;
- 2.3.2.10.39. Apresentar painéis gráficos (dashboards) com indicativos de situações diversas;
- 2.3.2.10.40. A partir de um dado evento ou conjunto de eventos, mostrar de forma gráfica seus relacionamentos e fazer drill-down do mesmo para efetiva investigação e identificação de causa raiz;
- 2.3.2.10.41. Permitir pesquisa nos eventos históricos, fornecendo capacidade de drill-down, ou seja, visualizar os detalhes dos eventos, inclusive dados raw, quando aplicável, para análise forense e investigação de incidentes;
- 2.3.2.10.42. Deverá ter capacidade de definir política de retenção dos dados;
- 2.3.2.10.43. Os logs devem ser mantidos pelo período mínimo de 365 dias, conforme Marco Civil da Internet (LEI nº 12.965, de 23 de Abril de 2014);
- 2.3.2.10.44. Deverá ter capacidade de armazenar os eventos em formato original (raw);
- 2.3.2.10.45. O algoritmo de integridade utilizado no armazenamento pode ser configurado entre os seguintes: MD5, SHA-1, SHA-256 ou SHA-512;
- 2.3.2.10.46. A solução deve possuir a capacidade de gerenciar o armazenamento de longo prazo de dados de inteligência de TI em um repositório central (mínimo de 5 anos);
- 2.3.2.10.47. Deve utilizar algoritmos para verificação de integridade e autenticidade dos eventos armazenados para fins de auditoria (Ex: SHA1) devidamente reconhecidos como seguros;
- 2.3.2.10.48. Armazenar os eventos e os alertas, inclusive os normalizados, de forma indexada.
- 2.3.2.10.49. Possuir a funcionalidade de apresentação de relatórios de eventos, alertas e incidentes em nível técnico e gerencial, os quais devem ter a possibilidade de customização e de serem gerados em PDF e HTML.

2.3.2.11. DO CORRELACIONADOR

- 2.3.2.11.1. Componente da solução responsável pelo correlacionamento dos eventos coletados.
- 2.3.2.11.2. O correlacionador deve ser capaz de receber eventos dos agentes, coletores e de outros correlacionadores;
- 2.3.2.11.3. O correlacionador deve efetuar a análise dos eventos em tempo próximo ao real (near realtime);
- 2.3.2.11.4. Deve permitir ao administrador a criação de novas regras e a edição das existentes.
- 2.3.2.11.5. O correlacionador deve identificar anomalias baseadas em eventos e análise de dados históricos conforme período a ser definido;
- 2.3.2.11.6. O correlacionador deve permitir o correlacionamento de eventos e alertas com dados existentes em listas (watchlist). Deve permitir também a criação de novas listas e a

personalização das existentes;

- 2.3.2.11.7. O correlacionador deve permitir a execução das regras agendadas contra eventos passados para análise histórica de atividades suspeitas, que executam em frequência e horário específico;
- 2.3.2.11.8. O correlacionador deve ter a capacidade de fazer o correlacionamento entre eventos oriundos de:
 - 2.3.2.11.8.1. Agentes (ou solução similar) ou coletores de outros correlacionadores;
 - 2.3.2.11.8.2. Diferentes ativos do mesmo tipo (por exemplo, Firewall A e Firewall B);
 - 2.3.2.11.8.3. Ativos de diferentes tipos (por exemplo, Firewall A e IPS B e Proxy C);
 - 2.3.2.11.8.4. Ativos e Banco de Dados (por exemplo, catraca e consultas a banco de dados);
- 2.3.2.11.9. O correlacionador deve ser capaz de inserir os alertas gerados no próprio fluxo de correlacionamento ou no fluxo de eventos. Deve permitir o correlacionamento de tais alertas/eventos, derivados de alertas, com novos eventos e/ou regras, no intuito de detectar padrões mais complexos de ameaças ou violações de conformidade;
- 2.3.2.11.10. O correlacionador deve priorizar os eventos e alertas com base, pelo menos, nos seguintes critérios:
 - 2.3.2.11.10.1. Severidade do evento;
 - 2.3.2.11.10.2. Criticidade do ativo;
- 2.3.2.11.11. Como resultado da aplicação de regras, o correlacionador deve ser capaz de executar ações automáticas como: enviar e-mail, enviar mensagem para o usuário conectado ao console, executar comando e abrir caso na ferramenta de incidentes interna.
- 2.3.2.11.12. O correlacionador deve armazenar os eventos, alertas e incidentes na base de dados da solução.
- 2.3.2.11.13. Fornecer a informação sobre os eventos que compõem um alerta e/ou incidente de segurança, identificado pelas regras de correlação da solução, referenciando tais eventos básicos a partir do evento alerta/incidente.
- 2.3.2.11.14. Correlacionar os eventos coletados de forma a evidenciar incidentes que caracterizem um ataque.
- 2.3.2.11.15. A solução deve possuir um mecanismo de correlação avançada para processar e comparar informações de logs de diferentes fontes e fluxos de rede;
- 2.3.2.11.16. A solução deve permitir que os clientes escrevam suas próprias regras;
- 2.3.2.11.17. Deve fornecer a funcionalidade de geração de alertas (sonoros e/ou visuais) para incidentes de alta criticidade detectados no correlacionamento de eventos.
- 2.3.2.11.18. Deve fornecer a funcionalidade de verificação de conformidade com as políticas, controles e normas internas e externas.
- 2.3.2.11.19. Possuir a funcionalidade de geração de incidentes em módulos de tratamento interno.
- 2.3.2.11.20. Possuir a funcionalidade de definição de prioridade para os eventos, alerta e incidente.
- 2.3.2.11.21. O correlacionador deverá estar dimensionado e licenciado para processar 10% dos eventos coletados.

- 2.3.2.11.22. solução deve notificar e associar comportamentos anômalos baseados em múltiplos eventos que ocorrerem em um determinado período de tempo;
- 2.3.2.11.23. A correlação de eventos deve possuir uma linha de base (baseline) comportamental da rede, definido por suas regras de correlações, fornecendo alertas sempre que ocorrer algum evento fora do comportamento normal;
- 2.3.2.11.24. A solução deve possuir a capacidade de prover contextualização de dados de alertas de fontes diversas (ativos de rede e/ou segurança, servidores, aplicações, etc.) em um único console, otimizando com isso a capacidade e prazos de análise no processo de resposta a incidentes de segurança;
- 2.3.2.11.25. A solução deve possibilitar o envio de notificações ou alertas baseados no fator de importância e criticidade do ativo/dispositivo perante ao negócio;
- 2.3.2.11.26. Possuir mecanismo de controle de acesso baseado em autenticação de usuário integrada com serviço de diretório Microsoft AD;
- 2.3.2.11.27. Possuir acesso seguro e criptografado de forma a garantir a autenticidade, confidencialidade e integridade dos dados;
- 2.3.2.11.28. Manter seu próprio log de auditoria.
- 2.3.2.11.29. Fornecer visualização e ações diferenciadas por perfis de acesso;
- 2.3.2.11.30. Permitir que as visualizações e ações sejam personalizadas por grupos de usuários;
- 2.3.2.11.31. Ter a funcionalidade de utilização de ACL (Listas de Controle de Acesso) ou configuração via interface gráfica para limitar os recursos da solução aos grupos de usuários, conforme critério definido pelo órgão;
- 2.3.2.11.32. Possuir a capacidade de efetuar a segregação de funções dos usuários da solução;
- 2.3.2.11.33. Ter a funcionalidade de visualização de eventos e alertas de segurança em tempo real;
- 2.3.2.11.34. Ser capaz de criação de novas regras e alteração das existentes;
- 2.3.2.11.35. Exibir os eventos que compõem um alerta e/ou incidente de segurança identificado pelas regras de correlação da solução, referenciando estes eventos básicos a partir de evento de alerta/incidente;
- 2.3.2.11.36. Permitir a criação de novos painéis gráficos (dashboards) e alteração dos existentes;
- 2.3.2.11.37. Permitir a criação de novos relatórios e alteração dos existentes;
- 2.3.2.11.38. Permitir o agendamento de geração de relatórios periódicos e notificar/enviar automaticamente os relatórios gerados para os destinatários dos mesmos;
- 2.3.2.11.39. Permitir a criação de listas (watchlist) e alteração das existentes. Deve permitir a inserção e remoção dos dados de forma manual e automática através de regras;
- 2.3.2.11.40. Permitir a inserção manual de anotações em alertas;
- 2.3.2.11.41. A solução deve ser capaz de notificar o(s) administrador(es), ou usuários cadastrados, caso algum dispositivo monitorado pare de enviar eventos;
- 2.3.2.11.42. As funções de manutenção e operação da solução podem estar integradas no mesmo console de administração. A solução deve:
 - 2.3.2.11.42.1. Possuir acesso controlado e autenticado por usuário, baseado na autenticação integrada com serviço de diretório como Microsoft AD, Open-LDAP, ou similares, podendo ser o mesmo console de administração;

- 2.3.2.11.42.2. Possuir acesso seguro e criptografado de forma a garantir a autenticidade, confidencialidade e integridade dos dados.
- 2.3.2.11.42.3. Permitir a instalação de certificado digital para prover o acesso seguro, e configurar o repositório de certificados confiáveis.
- 2.3.2.11.42.4. Fornecer visualização e ações diferenciadas por perfis de acesso;
- 2.3.2.11.42.5. As visualizações e ações devem ser personalizadas por grupos de usuários, conforme critério do administrador;
- 2.3.2.11.42.6. Deve permitir a configuração via interface gráfica da lista de controle de acesso para limitar o acesso dos grupos de usuários aos recursos da solução, conforme critério do administrador;
- 2.3.2.11.42.7. Deve permitir a segregação de funções dos usuários da solução;
- 2.3.2.11.42.8. Deve permitir a visualização de eventos, alertas e incidentes;
- 2.3.2.11.42.9. Deve permitir a pesquisa nos eventos históricos, fornecendo capacidade de “drill-down”, ou seja, visualizar os detalhes dos eventos, inclusive dado “raw”, quando aplicável, para análise forense e investigação de incidentes;
- 2.3.2.11.43. Deve informar os eventos que compõem um alerta e/ou incidente de segurança de identificado pelas regras de correlação da solução, referenciando estes eventos básicos a partir do evento de alerta/incidente;
- 2.3.2.11.44. Deve permitir nativamente a visualização de painéis (dashboards), relatórios, listas (watchlists) e ter a funcionalidade de inserir e remover dados manualmente;
- 2.3.2.11.45. A solução deve possuir ferramenta de tratamento de incidentes interna ou ser fornecida com solução de tratamento de incidentes de segurança externa integrada, mesmo que de outro fabricante.
- 2.3.2.11.46. O tratamento de incidentes deve permitir a geração e escalção automatizada de casos.
- 2.3.2.11.47. Deverá possuir recurso de workflow automatizado, de forma que ações de criação, alteração e fechamento de casos possam ser realizadas automaticamente, como ações resultantes das regras de correlacionamento
- 2.3.2.11.48. Deve permitir o registro de ações tomadas e planejadas
- 2.3.2.11.49. Deve anexar os eventos relacionados ao caso, assim como relatórios e dashboards de forma a permitir a visualização de todo o histórico da investigação do chamado de segurança.
- 2.3.2.11.50. Deverá se integrar nativamente com a ferramenta de incidentes externos, permitindo que o SIEM abra casos na ferramenta externa diretamente e automaticamente.
- 2.3.2.11.51. Deverá possuir uma base de inteligência de ameaças global que aplica contexto e apoia na priorização de riscos nos eventos gerados. Essa base de inteligência deve ser alimentada em conjunto com uma equipe de pesquisadores que operam em 24/7 monitorando constantemente as ameaças ao redor do mundo.
- 2.3.2.11.52. A correlação de eventos deve ser feita por meio de regras de comportamento pré programadas e implementadas pelo administrador. A correlação deve, minimamente, gerar informação, por meio da identificação de padrões de comportamento, obtidos dos registros enviados pelos ativos computacionais de rede adequados, a fim de:
 - 2.3.2.11.52.1. correlacionar e alertar quanto ao uso impróprio de identidades em serviços de diretórios;

- 2.3.2.11.52.2. detectar comportamentos suspeitos de serem maliciosos;
- 2.3.2.11.52.3. categorizar comportamentos suspeitos quanto à criticidade do alerta;
- 2.3.2.11.52.4. alertar ameaças à proteção dos dados quanto aos requisitos de confidencialidade, integridade e disponibilidade;
- 2.3.2.11.52.5. analisar tráfego de rede para a identificação de ameaças e instruções de remediação;
- 2.3.2.11.52.6. alertar quanto à ocorrência de ataques a serviços web, minimamente, aqueles enumerados no “Open Web Application Security Project” (OWASP);
- 2.3.2.11.52.7. identificar comportamentos maliciosos de aplicações de estações de trabalho, tais como ActiveX, Adobe Flash Player, Java, Javascript;
- 2.3.2.11.52.8. identificar e alertar ataques de autenticação, tais como ataque de força bruta e de dicionário em serviços de rede (p.e. SSH, LDAP, NetBIOS, serviços de diretórios, etc.);
- 2.3.2.11.52.9. identificar atividades de negação de serviço;
- 2.3.2.11.52.10. detectar atuação de programas suspeitos (p.e. programas espiões, cavalos de tróia, rede zumbi – botnet – entre outras);
- 2.3.2.11.52.11. detectar e alertar ataques de rede (p.e. mascaramento de IP, tentativa de sequestro de sessão, etc.);
- 2.3.2.11.52.12. detectar e alertar comportamentos de violação de políticas de segurança (p.e. uso de proxy anônimo, redes P2P e BitTorrent, login em rede Tor, etc.);
- 2.3.2.11.52.13. detectar e alertar demais comportamentos suspeitos que visem a comprometer os requisitos fundamentais de segurança (confidencialidade, integridade e disponibilidade).
- 2.3.2.11.52.14. A solução deve estar adequada a procedimentos legais a fim de:
- 2.3.2.11.52.15. detectar e rastrear comportamentos suspeitos;
- 2.3.2.11.52.16. fornecer base de conhecimento e relatórios para justificação de decisões administrativas que venham a ser necessárias para o incremento de segurança;
- 2.3.2.11.52.17. apoiar procedimentos de análise e correlação das evidências para fins de perícia e apresentação do caso em juízo;
- 2.3.2.11.52.18. produzir as respostas em tempo suficiente para que ações de defesa possam ser postas em prática de maneira efetiva (resposta em tempo real ou quase-real).

2.3.2.12. PERFIS DE ACESSO

- 2.3.2.12.1. A solução deve permitir diferentes perfis de acesso ao sistema cujas permissões se dividem, minimamente, entre os seguintes perfis:
 - 2.3.2.12.1.1. administrador – para configurar parâmetros do equipamento;
 - 2.3.2.12.1.2. operador – para operar o equipamento e executar ações padronizadas referente aos eventos registrados.
- 2.3.2.12.2. A solução deve permitir, minimamente, a utilização por 20 usuários entre administradores e operadores.
- 2.3.2.12.3. O perfil de administração deve conter, minimamente, as funções de:

- 2.3.2.12.3.1. cadastro, edição e remoção de usuários administradores e operadores;
- 2.3.2.12.3.2. cadastro, edição e remoção de regras de comportamento suspeito;
- 2.3.2.12.3.3. criação, edição e remoção de conectores personalizados;
- 2.3.2.12.3.4. criação, edição e remoção de regras de correlacionamento;
- 2.3.2.12.3.5. funções do perfil operador.
- 2.3.2.12.4. O perfil de operador deve conter, minimamente, as funções de:
 - 2.3.2.12.4.1. visualização de estatísticas de ataques, indicando IP e portas de origem;
 - 2.3.2.12.4.2. número total de eventos suspeitos;
 - 2.3.2.12.4.3. grau de severidade geral dos eventos analisados;
 - 2.3.2.12.4.4. estações de trabalho suspeitas;
 - 2.3.2.12.4.5. categorização por tipo de produto gerador de evento suspeito correlacionado; e
 - 2.3.2.12.4.6. realização de pesquisas de eventos na base de dados, minimamente, por:
 - 2.3.2.12.4.6.1. IP de origem;
 - 2.3.2.12.4.6.2. assinatura de ataque;
 - 2.3.2.12.4.6.3. tipo de sensor;
 - 2.3.2.12.4.6.4. nome de vulnerabilidade;
 - 2.3.2.12.4.6.5. país de origem; e
 - 2.3.2.12.4.6.6. data e horário.
- 2.3.2.13. **INSTALAÇÃO E ADMINISTRAÇÃO DA SOLUÇÃO DE SIEM**
 - 2.3.2.13.1. A contratada deverá implementar e fazer a gestão de toda a solução de SIEM e de todos os seus componentes;
 - 2.3.2.13.2. A contratada será responsável pela migração das regras existentes na solução atual e criação de novas regras de correlação que reflitam as reais necessidades do ambiente do IBGE com o objetivo de identificar possível incidentes de segurança;
 - 2.3.2.13.3. A contratada será responsável pela criação de regras de correlação que reflitam as reais necessidades do ambiente do IBGE com o objetivo de identificar possível incidentes de segurança;
 - 2.3.2.13.4. Criar relatórios e modelos, criar filtros de pesquisa, fazer backups, criar dashboards, gerenciar usuários e utilizar os principais recursos da solução;
 - 2.3.2.13.5. Apresentar plano de instalação e configuração, que deverá contemplar todos os tipos de ativos em produção na rede da contratante.
 - 2.3.2.13.6. Atualizar os sistemas operacionais e demais softwares para a última versão disponível compatível com a solução ofertada.
 - 2.3.2.13.7. Qualquer dano causado às instalações do IBGE ou aos equipamentos nele existentes deve ser reparado pela CONTRATADA conforme recomendação do fabricante ou Representante autorizado do equipamento danificado;
 - 2.3.2.13.8. Os serviços de instalação de coletores nos ambiente do IBGE deverão ser realizados em horário previamente combinado com o IBGE, preferencialmente no horário de expediente normal do IBGE (2ª a 6ª feira, das 8h00min às 18h00min);

- 2.3.2.13.9. Qualquer atividade que possa colocar em risco o funcionamento normal das unidades do IBGE deverá, necessariamente, ser executada fora do horário do expediente, de 2ª a 6ª feira, entre 6h00min e 8h00min e entre 18h00min e 24h00min, e nos sábados e domingos, das 7h00min às 21h00min, sem custo adicional para o IBGE;
- 2.3.2.13.10. Fornecimento das licenças e execução da instalação ou atualização de todas as novas versões ou releases da solução, incluindo seus softwares e firmwares, disponibilizados pelo fabricante da solução, bem como a aplicação de correções (patches) dos softwares e firmwares da solução nas instalações do IBGE ou de forma remota.

3. SERVIÇOS PARA O ITEM 3

3.1.1. Indicação das atividades e criticidade, para aplicação dos níveis mínimos de serviço :

FASE	CRITICIDADE (Conforme item 7.4 do termo de referência - NMS)
Plano de Resposta aos Incidentes	MÉDIA
Suporte especializado	ALTA
Manutenção preventiva	MÉDIA
Resposta aos incidentes	ALTA
Análise de causa raiz (forense)	BAIXA

3.2. Prevenção e resposta aos incidentes

3.2.1. Plano de Resposta aos Incidentes

- 3.2.1.1. A CONTRATADA deverá elaborar e manter planos de resposta a incidentes de segurança da informação, conforme os critérios abaixo:
- 3.2.1.2. Definição Inicial (Baseline):
- 3.2.1.2.1. A CONTRATADA deverá elaborar planos de resposta para um conjunto inicial de tipos de incidentes prioritários, previamente definidos em conjunto com o IBGE:
- 3.2.1.2.1.1. Quantidade mínima: 10 tipos de incidentes.
- 3.2.1.2.1.2. Os tipos de incidentes deverão ser selecionados com base em critérios como:
- 3.2.1.2.1.2.1. Histórico de ocorrências no IBGE.
- 3.2.1.2.1.2.2. Relevância para o contexto operacional da instituição.
- 3.2.1.2.1.2.3. Impacto potencial sobre os ativos de informação.
- 3.2.1.3. Atualização Periódica:

- 3.2.1.3.1. A cada 6 meses, a CONTRATADA deverá revisar e complementar o conjunto de planos de resposta com base nos incidentes mais recorrentes observados durante a operação do SOC.
- 3.2.1.3.2. Quantidade mínima por ciclo de atualização: 3 novos tipos de incidentes que ainda não possuam plano de resposta formalizado.
- 3.2.1.3.3. A identificação dos incidentes recorrentes deverá ser baseada em:
 - 3.2.1.3.3.1. Relatórios de monitoramento e análise do SOC.
 - 3.2.1.3.3.2. Indicadores de frequência e impacto.
 - 3.2.1.3.3.3. Reuniões de alinhamento com o IBGE.
- 3.2.1.4. Características dos Planos de Resposta:
 - 3.2.1.4.1. Cada plano de resposta deverá conter, no mínimo:
 - 3.2.1.4.1.1. Descrição do tipo de incidente.
 - 3.2.1.4.1.2. Procedimentos técnicos e operacionais para contenção, erradicação e recuperação.
 - 3.2.1.4.1.3. Papéis e responsabilidades envolvidas.
 - 3.2.1.4.1.4. Comunicação interna e externa (quando aplicável).
 - 3.2.1.4.1.5. Indicadores de eficácia e tempo de resposta.

3.2.2. Suporte especializado

- 3.2.2.1. A CONTRATADA deverá prover suporte técnico especializado conforme os requisitos abaixo:
 - 3.2.2.1.1. Canais de Atendimento:
 - 3.2.2.1.1.1. Disponibilizar canais para abertura, acompanhamento e validação de chamados técnicos, operando em regime 24x7x365, com atendimento bilíngue (português e inglês).
 - 3.2.2.1.1.2. Os canais obrigatórios incluem:
 - 3.2.2.1.1.2.1. E-mail;
 - 3.2.2.1.1.2.2. Portal web (cliente);
 - 3.2.2.1.1.2.3. Mensagens instantâneas (ex.: MS Teams);
 - 3.2.2.1.1.2.4. Telefone (0800).
 - 3.2.2.2. Escalação Funcional:
 - 3.2.2.2.1. Possuir processo de escalação funcional, com os seguintes níveis de atendimento:
 - 3.2.2.2.1.1. Nível 1 (N1) – Atendimento inicial e triagem;
 - 3.2.2.2.1.2. Nível 2 (N2) – Suporte técnico especializado;
 - 3.2.2.2.1.3. Nível 3 (N3) – Análise técnica avançada.
 - 3.2.2.2.1.4. O processo deve estar alinhado às melhores práticas descritas pelo ITIL.
 - 3.2.2.3. Análise Técnica Prévia:
 - 3.2.2.3.1. Antes de acionar o suporte dos fabricantes, o Nível 3 (N3) do SOC deverá realizar uma análise técnica documentada do incidente.

- 3.2.2.3.2. Essa etapa visa garantir que o processo de escalação funcional seja seguido corretamente e que o acionamento externo seja justificado.
- 3.2.2.4. Processos de Gerenciamento:
 - 3.2.2.4.1. A CONTRATADA deverá possuir os seguintes processos mapeados e documentados, conforme as melhores práticas do ITIL:
 - 3.2.2.4.1.1. Gerenciamento de incidentes;
 - 3.2.2.4.1.2. Gerenciamento de requisições;
 - 3.2.2.4.1.3. Gerenciamento de eventos;
 - 3.2.2.4.1.4. Gerenciamento de problemas;
 - 3.2.2.4.1.5. Gerenciamento de mudanças;
 - 3.2.2.4.1.6. Tratamento de incidentes críticos.
- 3.2.2.5. Acesso à Plataforma:
 - 3.2.2.5.1. Os administradores de tecnologia do CONTRATANTE terão acesso total à plataforma para fins de auditoria.
 - 3.2.2.5.2. A responsabilidade pela operação diária da solução será integralmente da CONTRATADA.
- 3.2.3. **Manutenção preventiva**
 - 3.2.3.1. Quanto à manutenção preventiva a CONTRATADA deve:
 - 3.2.3.1.1. Atualizar os firmwares e/ou softwares das soluções que compõe a solução e das respectivas consoles de gerenciamento;
 - 3.2.3.1.2. Realizar os ajustes e melhorias constantes, de acordo com as melhores práticas dos fabricantes, as mantendo documentadas e acessíveis no portal do cliente;
 - 3.2.3.1.3. Propor melhorias no ambiente de forma proativa, periodicamente, as mantendo documentadas no portal do cliente e as submetendo para a aprovação da CONTRATANTE.
- 3.2.4. **Resposta aos incidentes**
 - 3.2.4.1. A implantação de controles e ajustes necessários durante um eventual incidente nas ferramentas de segurança no ambiente tecnológico da CONTRATANTE, fora do horário comercial, serão de responsabilidade da CONTRATADA.
 - 3.2.4.2. A implantação dos demais controles e ajustes necessários durante um eventual incidente serão de responsabilidade da CONTRATANTE.
- 3.3. **Análise de causa raiz (forense)**
 - 3.3.1. Para cada incidente identificado deverá ser elaborado e entregue um relatório detalhando minimamente:
 - 3.3.1.1. Os impactos observados;
 - 3.3.1.2. A(s) vulnerabilidade(s) explorada(s);
 - 3.3.1.3. O método de ataque;
 - 3.3.1.4. A origem do ataque.

ANEXO I-B - SISTEMAS DO IBGE AGRUPADOS POR TEMA

Grupo	Sistemas
Censo Demográfico	
	Aplicações GTD
	SAPC
	SIGC Censo Demográfico
	Questionário WEB
Pesquisa Agropecuárias	
	PCA Centralizado
	SIGC Censo Agro
	Projeto de sensoriamento remoto
Pesquisas Domiciliares e Sociais	
	SIGC
	SIGC CNEFE
	SIQ-GERINS
	SIGC Registro Civil
	SISCOD
	POF6 2018
	SIGC PENSE
	SIGC MUNIC
	SIGC PNSB
	SIGC CNEFE
	PNADC
	Amostra Mestra
	SIGC PNDS
	SIGC PeNSE
	ESTADIC
Pesquisas Econômicas	
	PMC - Módulo UE
	PMS - Módulo UE
	SIPEA
	SIGC SNIPC
	SIGC SINAPI
	Painel Pesquisas Conjunturais
	Painel Pesquisas Estruturais por Empresas
	PIMPPF Gerenciador
	CEMPRE
Pesquisas Geociências	
	FMESERVER
	Base Territorial

Sistemas Administrativos	
	BDO
	Central de Atendimento
	SDA
	Eleição Conselho Curados
	Eleição CGPCC
	Novos Servidores
	Acompanhamento servidores
	GED
	SAPC
	Loja Virtual IBGE
	ContacCenter
	BITIC
	BIDECOF
	Movimentados do BNDES
	Auditoria Interna
	Kbasetic
	Trabalho Remoto
	Escritório de Projetos
	Tarifador
	EDATA
	Lista telefônica
	Gestão de riscos
	Cadastro de editais
	Custo deslocamento
	Atendimento IBGE
	CEMPRE Web
Sistemas de Treinamento	
	PCA Centralizado
	IPP
	SIGC MUNIC
	SIGC PNADC
	SIGC Registro Civil
	SIGC SINAPI
	SIGC SNIPC
	SIPEA
	SISCOD
	SIGC VEG
	PCA CENTRALIZADO
	GESTAO DE RISCOS
	SISCOD2
Sites Intranet	
	Intranet IBGE

	Intranet CDDI
	Intranet DGC
	Intranet DE
	Intranet DI
	Intranet DPE
	Intranet Presidência
	Intranet AL
	Intranet AM
	Intranet BA
	Intranet CE
	Intranet DF
	Intranet ES
	Intranet GO
	Intranet MG
	Intranet MT
	Intranet PB
	Intranet PR
	Intranet RJ
	Intranet RO
	Intranet RS
	Intranet SC
	Intranet SP
	Intranet TO
Sites Internet	
	Escola Virtual
	ENCE
	IBGE
	Quarentena
	WEBMAIL IBGE
	SIDRA
	Metadado
	BME
Aplicação Desktop	
	Apps Extranet IBGE
	Ultimus
	SAS Enterprise Guide
	SUPORTE TIC

ANEXO I-C - DESCRIÇÃO DO AMBIENTE COMPUTACIONAL DO IBGE

A Instituto Brasileiro de Geografia e Estatística (IBGE) possui em julho de 2021, segundo o SDA, 4.342 servidores públicos e 5.942 contratos temporários distribuídos por todos os Estados da Federação e no Distrito Federal. O ambiente computacional possui estações de trabalho, notebooks, impressoras, servidores, switches de rede, storage, firewall, wi-fi access points, sistemas de backup, smartphones, tablets e outros.

As tabelas abaixo ilustram o ambiente atual da IBGE (https://www.ibge.gov.br/np_download/novoportal/documentos_institucionais/PDTI_2023_2024.pdf) .



Documento assinado eletronicamente por FLAVIA MARINHO DE LIMA, Coordenador, em 4 de Março de 2026, às 12:11:18, horário de Brasília, com fundamento legal no § 3º do Art. 4º do Decreto Nº 10.543, de 13 de Novembro de 2020.



A autenticidade deste documento pode ser conferida no site <https://transparenciasda.ibge.gov.br/docs/validador.jsf> informando o código verificador 4829893608081213136 e o código CRC 617C2A5B.



Documento assinado eletronicamente por JUSSARA ROBERTA DE FREITAS SILVA, Gerente Nível II, em 4 de Março de 2026, às 14:31:08, horário de Brasília, com fundamento legal no § 3º do Art. 4º do Decreto Nº 10.543, de 13 de Novembro de 2020.



A autenticidade deste documento pode ser conferida no site <https://transparenciasda.ibge.gov.br/docs/validador.jsf> informando o código verificador 9171752104361018001 e o código CRC 3B7F6915.



Documento assinado eletronicamente por MARCOS VINICIUS FERREIRA MAZONI, Diretor, em 4 de Março de 2026, às 17:08:53, horário de Brasília, com fundamento legal no § 3º do Art. 4º do Decreto Nº 10.543, de 13 de Novembro de 2020.



A autenticidade deste documento pode ser conferida no site <https://transparenciasda.ibge.gov.br/docs/validador.jsf> informando o código verificador 7320457122253851551 e o código CRC 6B295FA3.

IBGE-FUN.INST.BRAS.GEOGRAFIA E ESTATISTICA

Contrato 3/2026

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
3/2026	114601-IBGE-FUN.INST.BRAS.GEOGRAFIA E ESTATISTICA	WEBBER TAVARES DE CARVALHO	20/03/2026 12:05 (v 0.5)
Status	CONCLUIDO		

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Serviços de TIC		03603.000077/2025-45

IBGE

(Processo Administrativo nº 03603.000077/2025-45)

CONTRATO ADMINISTRATIVO Nº **xx/xxxx**, QUE FAZEM ENTRE SI A UNIÃO, POR INTERMÉDIO DO (A) E

A Fundação Instituto Brasileiro de Geografia e Estatística - IBGE, com sede na Avenida Franklin Roosevelt, 166, Centro, na cidade do Rio de Janeiro/RJ, inscrita no CNPJ sob o nº 33.787.094/0001-40, neste ato representado(a) pelo(a) **[cargo e nome]**, nomeado(a) pela Portaria nº **XX**, de **[dia]** de **[mês]** de **[ano]**, publicada no DOU de **[dia]** de **[mês]** de **[ano]**, portador da Matrícula Funcional nº **[nº matrícula]**, doravante denominado CONTRATANTE, e o(a) **[CONTRATADO]**, inscrito(a) no CNPJ/MF sob o nº **[CNPJ]**, sediado(a) na **[endereço]**, na cidade de **[cidade]/[UF]**, doravante designado CONTRATADO, neste ato representado(a) por **[nome e função no CONTRATADO]**, conforme **[atos constitutivos da empresa] OU [procuração apresentada nos autos]**, tendo em vista o que consta no Processo nº **03603.000077/2025-45** e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente do(a) Pregão Eletrônico nº 90006/2026, mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a contratação de solução de tecnologia da informação e comunicação de empresa especializada para execução de serviços técnicos contínuos referente ao Serviço Gerenciado de Segurança da Informação de forma REMOTA, pelo período de 24 (vinte e quatro) meses, conforme condições estabelecidas no presente Termo de Referência, podendo ser renovado até o limite da lei, nas condições estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

--	--	--	--	--	--	--	--

GRUPO	ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO MENSAL ESTIMADO	VALOR TOTAL ESTIMADO
1	1	Gestão de Riscos - Processo integrado envolvendo a Gestão de Vulnerabilidades, Gestão de Riscos, Compliance e Monitoração de Marca	27014	Mês	24		
	2	Gestão de Incidentes - Processo integrado envolvendo a Análise de Incidentes Globais e o Monitoramento de Incidentes	27014	Mês	24		
	3	Resposta aos Incidentes - Processo integrado envolvendo a prevenção, bloqueio e resposta aos incidentes, bem como a análise de sua causa raiz	27014	Mês	24		
		Total					

1.3. Vinculam esta contratação, independentemente de transcrição:

- 1.3.1. O Termo de Referência;
- 1.3.2. O Edital da Licitação;
- 1.3.3. A Proposta do contratado;
- 1.3.4. Eventuais anexos dos documentos supracitados

2. CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 24 (vinte e quatro) meses contados da assinatura do contrato, prorrogável sucessivamente por até 10 anos, na forma dos arts. 106 e 107 da Lei nº 14.133, de 2021.

2.2. A prorrogação de que trata esse item é condicionada à avaliação, por parte do Gestor do Contrato, da vantajosidade da prorrogação, a qual deverá ser realizada motivadamente, com base no Histórico de Gestão do Contrato, nos princípios da manutenção da necessidade, economicidade e oportunidade da contratação e nos demais aspectos que forem julgados relevantes, atentando, ainda, para o cumprimento dos seguintes requisitos:

2.3. Estar formalmente demonstrado no processo que a forma de prestação dos serviços tem natureza continuada;

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

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

2.3.3. Haja manifestação expressa do CONTRATADO informando o interesse na prorrogação;

2.3.4. Seja comprovado que o CONTRATADO mantém as condições iniciais de habilitação; e

2.3.5. Não haja registro no Cadastro Informativo de créditos não quitados do setor público federal (Cadin).

2.4 O CONTRATADO não tem direito subjetivo à prorrogação contratual.

2.5. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

2.6. Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a renovação.

2.7. O contrato não poderá ser prorrogado quando o CONTRATADO tiver sido penalizado nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

3. CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

4. CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. As regras sobre a subcontratação do objeto são aquelas estabelecidas no Termo de Referência, anexo a este Contrato.

5. CLÁUSULA QUINTA - PREÇO

5.1. O valor mensal da contratação é de R\$ xxxxxx (xxxxxxxxx), perfazendo o valor total de R\$ xxxxxx (xxxxxxxxx).

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

6. CLÁUSULA SEXTA - PAGAMENTO

6.1. O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

7. CLÁUSULA SÉTIMA - REAJUSTE

7.1. As regras acerca do reajuste do valor contratual são aquelas definidas no Termo de Referência, anexo a este Contrato.

8. CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE

8.1. São obrigações do CONTRATANTE:

8.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo CONTRATADO, de acordo com o contrato e seus anexos;

8.1.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.1.3. Notificar o CONTRATADO, por escrito, sobre vícios, defeitos, incorreções, imperfeições, falhas ou irregularidades verificadas na execução do objeto contratual, fixando prazo para que seja substituído, reparado ou corrigido, total ou parcialmente, às suas expensas, certificando-se de que as soluções por ele propostas sejam as mais adequadas;

8.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo CONTRATADO;

8.1.5. Comunicar a empresa para emissão de Nota Fiscal relativa à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;

8.1.6. Efetuar o pagamento ao CONTRATADO do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

8.1.7. Aplicar ao CONTRATADO as sanções previstas na lei e neste Contrato;

8.1.8. Não praticar atos de ingerência na administração do CONTRATADO, tais como:

8.1.8.1. indicar pessoas expressamente nominadas para executar direta ou indiretamente o objeto contratado;

8.1.8.2. fixar salário inferior ao definido em lei ou em ato normativo a ser pago pelo CONTRATADO;

8.1.8.3. estabelecer vínculo de subordinação com funcionário do CONTRATADO;

8.1.8.4. definir forma de pagamento mediante exclusivo reembolso dos salários pagos;

8.1.8.5. demandar a funcionário do CONTRATADO a execução de tarefas fora do escopo do objeto da contratação; e

8.1.8.6. prever exigências que constituam intervenção indevida da Administração na gestão interna do CONTRATADO.

8.1.9. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo CONTRATADO;

8.1.10. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste;

8.1.10.1. A Administração terá o prazo de 30 (trinta) dias, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

8.1.11. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo CONTRATADO no prazo máximo de 30 (trinta) dias;

8.1.12. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais;

8.1.13. Comunicar o CONTRATADO na hipótese de posterior alteração do projeto pelo CONTRATANTE, no caso do art. 93, §2º, da Lei nº 14.133, de 2021.

8.2. A Administração não responderá por quaisquer compromissos assumidos pelo CONTRATADO com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do CONTRATADO, de seus empregados, prepostos ou subordinados.

9. CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO

9.1. O CONTRATADO deve cumprir todas as obrigações constantes deste Contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

9.2. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior e prestar todo esclarecimento ou informação por eles solicitados;

9.3. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os bens e serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

9.4. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo CONTRATANTE, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;

9.5. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o CONTRATADO deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos:

9.5.1. prova de regularidade relativa à Seguridade Social;

9.5.2. certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;

9.5.3. certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do CONTRATADO;

9.5.4. Certidão de Regularidade do FGTS – CRF; e

9.5.5. Certidão Negativa de Débitos Trabalhistas – CNDT.

- 9.6. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao CONTRATANTE e não poderá onerar o objeto do contrato;
- 9.7. Comunicar ao Fiscal do contrato tempestivamente, observada a urgência da situação, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto contratual, não ultrapassando o prazo de 24 (vinte e quatro) horas;
- 9.8. Paralisar, por determinação do CONTRATANTE, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros;
- 9.9. Manter, durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;
- 9.10. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação;
- 9.11. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas;
- 9.12. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;
- 9.13. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021;
- 9.14. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do CONTRATANTE;
- 9.15. Alocar os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados;
- 9.16. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos;
- 9.17. Fornecer todos os materiais, equipamentos, ferramentas e utensílios demandados, em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação de regência;
- 9.18. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local de execução do objeto e nas melhores condições de segurança, higiene e disciplina;
- 9.19. Submeter previamente, por escrito, ao CONTRATANTE, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere;
- 9.20. Cumprir as normas de proteção ao trabalho, inclusive aquelas relativas à segurança e à saúde no trabalho;
- 9.21. Não submeter os trabalhadores a condições degradantes de trabalho, jornadas exaustivas, servidão por dívida ou trabalhos forçados;
- 9.22. Não permitir a utilização de qualquer trabalho do menor de dezesesseis anos de idade, exceto na condição de aprendiz para os maiores de quatorze anos de idade, observada a legislação pertinente;
- 9.23. Não submeter o menor de dezoito anos de idade à realização de trabalho noturno e em condições perigosas e insalubres e à realização de atividades constantes na Lista de Piores Formas de Trabalho Infantil, aprovada pelo Decreto nº 6.481, de 12 de junho de 2008;

9.24. Receber e dar o tratamento adequado a denúncias de discriminação, violência e assédio no ambiente de trabalho;

9.25. Manter preposto aceito pela Administração no local da obra ou do serviço para representá-lo na execução do contrato;

9.25.1. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

9.26. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do CONTRATANTE ou de agente público que tenha desempenhado função na licitação ou que atue na fiscalização ou gestão do contrato, nos termos do art. 48, parágrafo único, da Lei nº 14.133, de 2021;

9.27. Prestar todo esclarecimento ou informação solicitada pelo CONTRATANTE ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do contrato;

9.28. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato;

9.29. Assegurar aos seus trabalhadores ambiente de trabalho e instalações em condições adequadas ao cumprimento das normas de saúde, segurança e bem-estar no trabalho;

9.30. Fornecer equipamentos de proteção individual (EPI) e equipamentos de proteção coletiva (EPC), quando for o caso;

9.31. Garantir o acesso do CONTRATANTE, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do contrato;

9.32. Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram o Termo de Referência, no prazo determinado;

9.33. Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração;

9.34. Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo o CONTRATADO relatar ao CONTRATANTE toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função;

10. CLÁUSULA DÉCIMA - OBRIGAÇÕES PERTINENTES À LGPD

10.1. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

10.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

10.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

10.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.

10.5. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

10.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

10.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

10.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

10.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

10.10. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

10.10.1. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.

10.11. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

10.12. Os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser comunicados à autoridade nacional.

11. CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO

11.1. Será exigida a prestação de garantia na presente contratação, conforme regras constantes do Termo de Referência.

12. CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

12.1. As regras acerca de infrações e sanções administrativas referentes à execução do contrato são aquelas definidas no Termo de Referência, anexo a este Contrato.

13. CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL

13.1. O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

13.2. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o contratante, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

13.3. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

13.4. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

13.5. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no art. 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

13.5.1. Nesta hipótese, aplicam-se também os arts. 138 e 139 da mesma Lei.

13.5.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

13.5.3. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

13.6. O termo de extinção, sempre que possível, será precedido de:

13.6.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

13.6.2. Relação dos pagamentos já efetuados e ainda devidos;

13.6.3. Indenizações e multas.

13.7. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório.

13.8. O CONTRATANTE poderá ainda:

13.8.1. nos casos de obrigação de pagamento de multa pelo CONTRATADO, reter a garantia prestada a ser executada, conforme legislação que rege a matéria; e

13.8.2. nos casos em que houver necessidade de ressarcimento de prejuízos causados à Administração, nos termos do inciso IV do art. 139 da Lei n.º 14.133, de 2021, reter os eventuais créditos existentes em favor do CONTRATADO decorrentes do contrato.

13.9. O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou na contratação direta ou que atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

14. CLÁUSULA DÉCIMA QUARTA – ALTERAÇÕES

14.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

14.2. O CONTRATADO é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

14.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

14.4. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do CONTRATANTE, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês.

14.5. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

15. CLÁUSULA DÉCIMA QUINTA – DOTAÇÃO ORÇAMENTÁRIA

15.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União deste exercício, na dotação abaixo discriminada:

- I) Gestão/Unidade: [...];
- II) Fonte de Recursos: [...];
- III) Programa de Trabalho: [...];
- IV) Elemento de Despesa: [...];
- V) Plano Interno: [...];
- VI) Nota de Empenho: [...];

15.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

16. CLÁUSULA DÉCIMA SEXTA – DOS CASOS OMISSOS

16.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

17. CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

17.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, *caput*, da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

18. CLÁUSULA DÉCIMA OITAVA– FORO

18.1. Fica eleito o Foro da Justiça Federal no Estado do Rio de Janeiro, Seção Judiciária do Rio de Janeiro para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

Rio de Janeiro, na data da assinatura eletrônica.

Representante legal do CONTRATANTE

Representante legal do CONTRATADO

TESTEMUNHAS:

1-

19. Responsáveis

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

CLAUDIA GOULART DE SIQUEIRA

Pregoeiro

ANEXO III
MODELO DE PROPOSTA COMERCIAL
FUNDAÇÃO INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA – IBGE
PREGÃO Nº 9000X/2025
(Processo Administrativo nº 03603.000077/2025-45)

PROCESSO: 03603.000077/2025-45						
EMPRESA:						
ENDEREÇO:						
CEP:						
TEL:						
FAX:						
INSCRIÇÃO ESTADUAL						
Grupo	Item	DESCRIÇÃO	UND.	QTD.	VALOR UNITÁRIO	VALOR TOTAL
1	1	Gestão de Riscos - Processo integrado envolvendo a Gestão de Vulnerabilidades, Gestão de Riscos, Compliance e Monitoração de Marca	Mês	24		
	2	Gestão de Incidentes - Processo integrado envolvendo a Análise de Incidentes Globais e o Monitoramento de Incidentes	Mês	24		
	3	Resposta aos Incidentes - Processo integrado envolvendo a prevenção, bloqueio e resposta aos incidentes, bem como a análise de sua causa raiz	Mês	24		
TOTAL						
IMPORTA A PRESENTE PROPOSTA NO VALOR DE:						
DECLARAMOS de que os preços contidos na proposta incluem todos os custos e despesas, tais como custos diretos e indiretos, tributos incidentes, taxa de administração, materiais, serviços, encargos sociais, trabalhistas, seguros, lucro e outros necessários ao cumprimento integral do objeto deste Edital e inteira submissão às condições de fornecimento constantes do Pregão nº 9000X/2025.						
PRAZO DE ENTREGA: Conforme Anexo I do Edital			VALIDADE DA PROPOSTA: 60 (sessenta) dias corridos. Rio de Janeiro, _____ de _____ de 2025.			
GARANTIA: Conforme ANEXO I do Edital						
LOCAL DE ENTREGA E EXECUÇÃO DO SERVIÇO: Conforme Anexo I do Edital			ASSINATURA E CARIMBO DO RESPONSÁVEL PELA PROPOSTA:			
CONDIÇÕES DE PAGAMENTO: Conforme Anexo I do Edital						

DADOS BANCÁRIOS DA EMPRESA:

Banco:

Agência:

Conta:

Praça:

DADOS DO REPRESENTANTE LEGAL DA EMPRESA PARA FINS DE ASSINATURA DO CONTRATO:

Nome: Estado Civil:

Domicílio:

Cargo:

E-mail :