Edital 23/2024

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
23/2024	114702-ENAP-ESCOLA NACIONAL DE ADM. PUBLICA/DF	INGRID MELO POL FERREIRA	11/07/2024 15:39 (v 9.0)

Status

ASSINADO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
V - prestação de serviços, inclusive os técnico-profissionais especializados/Serviço continuado sem dedicação exclusiva de mão de obra		04600002376/2023-45

Informações da Licitação

Pregão Eletrônico nº 90.012/2024

CONTRATANTE (UASG)

Fundação Escola Nacional de Administração Pública - Enap (114702)

OBJETO

O objeto da presente licitação a contratação de solução de tecnologia da informação e comunicação de empresas especializadas no fornecimento de serviços gerenciados de segurança para a ENAP, compreendendo os serviços especificados no item 01 e no item 02, por 12 (doze) meses, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

VALOR TOTAL DA CONTRATAÇÃO

R$ 1.280.166,24 (um milhão e duzentos e oitenta mil e cento e sessenta e seis reais e vinte e quatro centavos).

DATA DA SESSÃO PÚBLICA

Dia **26/07/2024** às **10h (horário de Brasília)**

CRITÉRIO DE JULGAMENTO:

Menor preço por item.

MODO DE DISPUTA:

Aberto.

PREFERÊNCIA ME/EPP/EQUIPARADAS:

Não.

Fundação Escola Nacional de Administração Pública - Enap

PREGÃO ELETRÔNICO Nº 90.012/2024

(Processo Administrativo n° 04600.002376/2023-45)

Torna-se público que a Fundação Escola Nacional de Administração Pública - Enap, por meio da Diretoria de Gestão Interna, sediada no Setor de Áreas Isoladas Sul (SAIS), Área 2A, nesta capital, CNPJ sob nº 00.627.612/0001-09, mediante o Pregoeiro designado pela Portaria Enap nº 101/2024, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 2021, e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

1. Do objeto

1. DO OBJETO

1.1. O objeto da presente licitação a contratação de solução de tecnologia da informação e comunicação de empresas especializadas no fornecimento de serviços gerenciados de segurança para a ENAP, compreendendo os serviços especificados no item 01 e no item 02, por 12 (doze) meses, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será dividida em 02 (dois) itens, conforme tabela constante do Termo de Referência, facultando-se ao licitante a participação em quantos itens forem de seu interesse.

2. Do registro de preços

2. DO REGISTRO DE PREÇOS

2.1. Não se aplica o Registro de Preços.

3. Da participação na licitação

3. DA PARTICIPAÇÃO NA LICITAÇÃO

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

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

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

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

3.4. 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 n.º 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. 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;

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

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

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

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

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

3.7.8. agente público do órgão ou entidade licitante;

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

3.7.10. 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.

3.8. O impedimento de que trata o item 3.7.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

3.9. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 3.7.2 e 3.7.3 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.

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

3.11. O disposto nos itens 3.7.2 e 3.7.3 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.

3.12. 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 14.133/2021.

3.13. A vedação de que trata o item 3.7.8 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. Da apresentação da proposta e dos documentos de habilitação

4. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

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

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

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

4.3.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como 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;

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

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

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

4.4. O 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.

4.5. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° 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 n.º 14.133, de 2021.

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

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

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

4.8. 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.

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

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

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

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

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

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

4.12. O valor final mínimo parametrizado na forma do item 4.10. 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.

4.13. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda

de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

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

5. Do preenchimento da proposta

5. DO PREENCHIMENTO DA PROPOSTA

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

5.1.1. Valor unitário e total do item;

5.1.2. Apresentar a proposta de acordo com o modelo constante no Anexo A do Termo de Referência;

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

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

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

5.5. 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.

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

5.7. Na presente licitação, a Microempresa e a Empresa de Pequeno Porte poderão se beneficiar do regime de tributação pelo Simples Nacional.

5.8. 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.

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

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

5.11. O descumprimento das regras supramencionadas pela Administração por parte dos contratados 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.

6. Da abertura da sessão, classificação das propostas e formulação de lances

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

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

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

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

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

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

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

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

6.8. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de 0,05% (zero virgula zero cinco por cento).

6.9. 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 inexequível.

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

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

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

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

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

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

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

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

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

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

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

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

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

6.18. 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. 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.

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

6.18.2. 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.

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

6.18.4. 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.

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

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

6.19.1.1. 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;

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

6.19.1.3. 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.

6.19.2. Os licitantes classificados que estejam enquadrados no item 6.19.1.1, 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.

6.19.3. Caso a preferência não seja exercida na forma do item 6.19.1.1, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no item 6.19.1.2, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o item 6.19.1.3 caso esse direito não seja exercido.

6.19.4. 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.

6.20. Só poderá haver empate entre propostas iguais (não seguidas de lances).

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

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

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

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

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

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

6.20.2.1. 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;

6.20.2.2. empresas brasileiras;

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

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

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

6.21.2. 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.

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

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

6.21.5. 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.

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

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

7. Da fase de julgamento

7. DA FASE DE JULGAMENTO

7.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 3.7. do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

7.1.1. SICAF;

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

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

7.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

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

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

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

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

7.4. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

7.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com os itens 3.5.1. e 4.5. deste edital.

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

7.7. Será desclassificada a proposta vencedora que:

7.7.1. contiver vícios insanáveis;

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

7.7.3.apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

7.7.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

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

7.8. 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.

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

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

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

7.9. 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.

7.10. 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.

7.10.1. Caso a produtividade for diferente daquela utilizada pela Administração como referência, ou não estiver contida na faixa referencial de produtividade, mas admitida pelo ato convocatório, o licitante deverá apresentar a respectiva comprovação de exequibilidade;

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

7.10.3. Para efeito do subitem anterior, admite-se a adequação técnica da metodologia empregada pela contratada, visando assegurar a execução do objeto, desde que mantidas as condições para a justa remuneração do serviço.

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

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

7.13. 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.

7.14. 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.

7.15. Caso o Termo de Referência exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência, sob pena de não aceitação da proposta.

7.16. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

7.17. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

7.18. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

7.19. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

7.20.Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

8. Da fase de habilitação

8. DA FASE DE HABILITAÇÃO

8.1. 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.

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

8.2. 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.

8.3. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato, 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.

8.4. 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.

8.4.1. 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.

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

8.6. 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.

8.7. 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 (art. 63, I, da Lei nº 14.133/2021).

8.8. 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.

8.9. 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.

8.10. Considerando que na presente contratação a avaliação prévia do local de execução é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, o licitante deve atestar, sob pena de inabilitação, que conhece o local e as condições de realização do serviço, assegurado a ele o direito de realização de vistoria prévia, conforme regras dispostas no item 4.39. e seguintes do Termo de Referência.

8.10.1. O licitante que optar por realizar a vistoria prévia terá disponibilizado pela Administração data e horário exclusivos, a ser agendado no endereço eletrônico cgti@enap.gov.br, de modo que seu agendamento não coincida com o agendamento de outros licitantes.

8.10.2. Caso o licitante opte por não realizar a vistoria, poderá substituir a declaração exigida no presente item por declaração formal assinada pelo seu responsável técnico acerca do conhecimento pleno das condições e peculiaridades da contratação.

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

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

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

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

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

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

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

8.14.1. 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.

8.14.2. Respeitada a exceção do subitem anterior, relativa à regularidade fiscal, quando a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, a verificação ou exigência do presente subitem ocorrerá em relação a todos os licitantes.

8.15. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e IN 73/2022, art. 39, §4º):

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

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

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

8.17. 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 8.16.1.

8.18. 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.

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

9. Da ata de registro de preços

9. DA ATA DE REGISTRO DE PREÇOS

9.1. Não se aplica o Registro de Preços.

10. Da formação do cadastro de reserva

10. DA FORMAÇÃO DO CADASTRO DE RESERVA

10.1. Não se aplica o Registro de Preços.

11. Dos recursos

11. DOS RECURSOS

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

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

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

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

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

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

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

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

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

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

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

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

11.10 Os autos do processo permanecerão com vista franqueada aos interessados, por meio de solicitação no e-mail licitacao@enap.gov.br ou por petição dirigida ou protocolada no endereço SAIS - nº 02-A - Setor Policial Sul - Brasília/DF, seção de Protocolo.

12. Das infrações administrativas e sanções

12. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

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

12.1.1.deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

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

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

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

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

12.1.2.4. deixar de apresentar amostra;

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

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

12.1.3.1. 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;

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

12.1.5. fraudar a licitação;

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

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

12.1.6.2. induzir deliberadamente a erro no julgamento;

12.1.6.3. apresentar amostra falsificada ou deteriorada;

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

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

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

12.2.1. advertência;

12.2.2. multa;

12.2.3. Impedimento de licitar e contratar e

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

12.3. Na aplicação das sanções serão considerados:

12.3.1. a natureza e a gravidade da infração cometida.

12.3.2.as peculiaridades do caso concreto

12.3.3. as circunstâncias agravantes ou atenuantes

12.3.4. os danos que dela provierem para a Administração Pública

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

12.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de **10 (dez) dias** úteis, a contar da comunicação oficial.

12.4.1. Para as infrações previstas nos itens 12.1.1, 12.1.2 e 12.1.3, a multa será de 0,5% a 15% do valor do contrato licitado.

12.4.2. Para as infrações previstas nos itens 12.1.4, 12.1.5, 12.1.6, 12.1.7 e 12.1.8, a multa será de 15% a 30% do valor do contrato licitado.

12.5. 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.

12.6. 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.

12.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 12.1.1, 12.1.2 e 12.1.3, 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.

12.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 12.1.4, 12.1.5, 12.1.6, 12.1.7 e 12.1.8, bem como pelas infrações administrativas previstas nos itens 12.1.1, 12.1.2 e 12.1.3 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 n.º 14.133/2021.

12.9. A recusa injustificada do adjudicatário em assinar o contrato, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 12.1.3, 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.

12.10. 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.

12.11. 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.

12.12. 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.

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

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

13. Da impugnação do edital e do pedido de esclarecimento

13. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

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

13.2. 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.

13.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, pelo e-mail: licitacao@enap.gov.br, ou por petição dirigida ou protocolada no endereço SAIS – nº 02-A – Setor Policial Sul – Brasília/DF, seção de Protocolo.

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

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

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

14. Das disposições gerais

14. DAS DISPOSIÇÕES GERAIS

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

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

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

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

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

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

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

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

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

14.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico www.enap.gov.br.

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

14.11.1. ANEXO I - Termo de Referência

14.11.1.1. ANEXO IA - Modelo de Proposta Comercial

14.11.1.2. ANEXO IB - Modelo de Termo de Compromisso de Sigilo e Segurança da Informação

14.11.1.3. ANEXO IC - Modelo de Termo de Ciência Individual

14.11.1.4. ANEXO ID - Modelo de Termo de Recebimento Provisório

14.11.1.5. ANEXO IE - Modelo de Termo de Recebimento Definitivo

14.11.1.6. ANEXO IF - Modelo de Demonstração de Atendimento aos Requisitos Técnicos dos Itens

14.11.1.7. ANEXO IG - Modelo de Declaração de Vistoria ou Declaração de Opção de Não Realização de Vistoria

14.11.1.8. ANEXO IH - Modelo de Declaração de Cumprimento da Lei Geral de Proteção de Dados

14.11.1.9. ANEXO II - Modelo de Declaração de Conhecimento do Edital

14.11.1.10. ANEXO IJ - Modelo de Ativos de Infraestrutura de TI da ENAP

14.11.1.11. ANEXO IK - Modelo de Descrição da Solução - Ciclo de Vida do Objeto e Especificação do Produto

14.11.1.12. ANEXO IL - Modelo de Ordem de Serviço ou de Fornecimento de Bens

14.11.2. ANEXO II – Apêndice do Anexo I - Estudo Técnico Preliminar

14.11.3. ANEXO III - Minuta de Termo de Contrato

14.11.4. ANEXO IV - Valores Máximos Admissíveis

15. Responsáveis

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

MARCELO FERREIRA HALLAC

Autoridade competente

Assinou eletronicamente em 11/07/2024 às 15:39:33.

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 - Termo de Referencia.pdf (847.58 KB)
- Anexo II - Minuta de Termo de Contrato.pdf (147.16 KB)
- Anexo III - Valores Maximos Admissiveis.pdf (87.24 KB)
- Anexo IV - Estudo Tecnico Preliminar.pdf (745.01 KB)

Anexo I - Termo de Referencia.pdf

Termo de Referência 91/2024

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
91/2024	114702-ENAP-ESCOLA NACIONAL DE ADM. PUBLICA/DF	JULLYANO LINO DA SILVA	07/06/2024 13:27 (v 7.0)

Status

ASSINADO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
V - prestação de serviços, inclusive os técnico-profissionais especializados/Serviço continuado sem dedicação exclusiva de mão de obra		04600.002376/2023-45

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1 Contratação de empresas especializadas no fornecimento de serviços gerenciados de segurança para a ENAP, compreendendo os serviços especificados no item 01 e no item 02, por 12 (doze) meses, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	ESPECIFICAÇÃO	CATSER	MÉTRICA OU UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO MENSAL	VALOR TOTAL PARA 12 MESES
1	Serviço de monitoramento e visibilidade de ataques cibernéticos	27359	Meses	12	R$ 28.965,70	R$ 347.588,44
2	Serviço de **monitoramento, detecção e resposta a incidentes** - 1500 Eventos por segundo (EPS)	27359	Meses	12	R$ 77.714,82	R$ 932.577,84
VALOR TOTAL DA CONTRATAÇÃO PARA 12 MESES						**R$ 1.280.166,28**

1.2 O(s) serviço(s) objeto desta contratação são caracterizados como comuns, uma vez que se trata da contratação de bens e serviços de apoio à gestão da segurança da informação e privacidade na ENAP que podem ser descritos na forma de bens e serviços comuns definidos como padrão e tendo característica de desempenho e qualidade estabelecidos de forma objetiva, ou seja, por meio de especificações usuais de mercado.

1.3 O prazo de vigência da contratação é de 12 meses (máximo de 5 anos) contados do(a) assinatura do contrato, prorrogável para até 05 (cinco) anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

1.3.1 O serviço é enquadrado como continuado tendo em vista que o apoio e manutenção às atividades essenciais e administrativas da Enap, o cumprimento da missão institucional da Contratante e a necessidade de se lidar com os aspectos de segurança da informação na atual realidade cibernética em âmbito mundial dependem dos serviços neste Termo de Referência descritos, sendo a vigência por 12 meses mais vantajosa considerando o Estudo Técnico Preliminar.

1.4 O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

2.1 A descrição da solução como um todo encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência, e também no **ANEXO K - DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO** dos documentos auxiliares deste Termo de Referência.

2.2 A solução de TIC consiste em um conjunto de soluções, divididas em dois itens, componentes de serviços gerenciados de segurança da informação e de segurança cibernética a fim de viabilizar o apoio à gestão de segurança da informação, de riscos cibernéticos e de conformidade baseados nas melhores práticas e frameworks do mercado no âmbito da Escola, bem como operacionalizar o monitoramento e visibilidade de ataques cibernéticos e o tratamento de incidentes de segurança cibernética concernentes aos ativos de Tecnologia da Informação da ENAP.

2.3 A prestação de serviços envolve:

2.3.1 **ITEM 01: Serviço de Monitoramento e Visibilidade de Ataques Cibernéticos** que tem como finalidade aplicar inteligência voltada para a segurança da marca ENAP, com o objetivo de realizar buscas contínuas em diversas camadas da internet, incluindo a Surface, Deep e Dark Web. Essas buscas têm como foco a identificação de informações sensíveis que possam estar sendo discutidas ou comercializadas de forma ilegal, tais como dados confidenciais, informações privilegiadas ou quaisquer outros tipos de conteúdo que possam representar uma ameaça à integridade da ENAP.

2.3.2 **ITEM 02: Serviço de Monitoramento, Detecção e Resposta a Incidentes** que tem como objetivo prover à ENAP mecanismo de visibilidade de logs, rede e informações, capaz de identificar eventos maliciosos, através de correlacionamento de logs e tráfego de rede sob um regime de monitoramento de 1500 eventos por segundo, que possam comprometer os serviços tecnológicos da ENAP.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE

3.1 A presente contratação justifica-se no contexto e pelos motivos abaixo descritos:

3.1.1 A Fundação Escola Nacional da Administração Pública (Enap) é uma escola de governo do Poder Executivo Federal, vinculada ao Ministério da Gestão e da Inovação em Serviços Públicos, conforme dispõe o Decreto nº 11.345, de 1º de Janeiro de 2023. A ENAP desempenha um papel crucial na formação e capacitação de servidores públicos, lidando com informações sensíveis e estratégicas para o Estado brasileiro.

3.1.2 O cenário atual de ameaças cibernéticas apresenta desafios crescentes para as organizações, incluindo instituições governamentais como a ENAP. Ataques cibernéticos sofisticados, como *ransomware, phishing* e *malware* avançado, representam riscos significativos para a confidencialidade, integridade e disponibilidade dos dados e sistemas.

3.1.3 A infraestrutura de Tecnologia da Informação (TI) da ENAP é complexa e heterogênea, abrangendo segurança, rede de comunicação de dados, banco de dados, servidores de rede, sistemas operacionais, sistemas de backup e recursos de armazenamento de dados. Essa complexidade aumenta a superfície de ataque e dificulta a gestão eficiente da segurança da informação utilizando apenas recursos internos.

3.1.4 A ENAP tem intensificado o uso de tecnologias digitais para oferecer serviços à sociedade e apoiar as diferentes modalidades de trabalho dos servidores. Esse contexto demanda um ecossistema de proteção

digital robusto para garantir a continuidade dos serviços, mitigar riscos de perda de informações e danos à imagem institucional, além de fortalecer a percepção de segurança perante usuários internos e a sociedade.

3.1.5 A contratação de Serviços Gerenciados de Segurança da Informação e Segurança Cibernética é essencial para:

- Implementar um sistema de monitoramento e visibilidade de ataques cibernéticos: A identificação proativa de ameaças na Surface, *Deep* e *Dark Web* permite que a ENAP se antecipe a possíveis ataques e proteja sua reputação e informações sensíveis.
- Estabelecer um serviço de monitoramento, detecção e resposta a incidentes: A capacidade de monitorar um grande volume de eventos (1500 eventos por segundo) e correlacionar logs e tráfego de rede é crucial para detectar e responder rapidamente a incidentes de segurança, minimizando seus impactos.
- Aumentar a capacidade da equipe de segurança: A expertise e o conhecimento especializado da empresa contratada complementam as habilidades da equipe interna da ENAP, permitindo uma gestão de segurança mais eficiente e eficaz.

3.1.6 Diante desse cenário, a contratação de Serviços Gerenciados de Segurança da Informação e Segurança Cibernética se apresenta como uma solução estratégica para a ENAP, garantindo a proteção de seus ativos de TI, a continuidade de seus serviços e a segurança das informações sob sua responsabilidade.

3.1.7 Portanto, esta contratação tem como objetivo prover a ENAP de Serviços Gerenciados de Segurança da Informação e Segurança Cibernética necessários ao estabelecimento, à ampliação, à atualização, à manutenção e à melhoria contínua do conjunto de ferramentas, processos e equipes responsáveis pela gestão da segurança da informação e pela execução contínua, conforme a segurança e a privacidade requeridas, dos processos de TIC e de negócio desta Escola.

3.1.8 A Informação se tornou uma ferramenta de fácil acesso e essencial para o desenvolvimento pessoal e coletivo. Porém, essa informação deixou de ser unicamente um recurso de desenvolvimento passando a ser o item mais valioso em uma organização, sendo considerada muitas vezes como patrimônio do órgão no qual ela foi gerada. Diante dessa valorização, ela passou a atrair a atenção de pessoas ou entidades na busca de auferir lucro, posicionar-se melhor no mercado, obter vantagens ou mesmo destruir imagens e reputações. Na sociedade atual, não basta apenas armazenar a informação para futura recuperação, é necessário investir em proteção, uma vez que está sob constante risco e necessita ser adequadamente protegida.

3.1.9 É nesse contexto que a Segurança da Informação se tornou um elemento essencial para a manutenção da idoneidade das instituições e de sua manutenção no mercado.

3.1.10 Diante dessa sociedade da informação, a segurança da informação tem se tornado essencial para a proteção de uma organização, necessitando de uma grande estrutura de operação de segurança dentro dos órgãos e sendo inviável contar somente com o corpo técnico interno das entidades, passando a ser executados por serviços gerenciados de segurança da informação.

3.1.11 A infraestrutura de TIC da ENAP dispõe de uma série de ativos heterogêneos agrupados em: segurança, rede de comunicação de dados, telefonia, banco de dados, servidores de rede, sistemas operacionais, sistemas de backup e recursos de armazenamento de dados que, dada a criticidade dos sistemas hospedados, devem operar em alta disponibilidade e resiliência a falhas, inclusive as de segurança. Tal diversidade eleva exponencialmente a complexidade da gestão de segurança da informação e consequentemente o desafio de fazer frente às ameaças cibernéticas emergentes.

3.1.12 Considerando o crescente uso de recursos tecnológicos pela ENAP as diferentes modalidades de trabalho dos servidores e os novos serviços digitais oferecidos pela Escola à sociedade, fazem com que seja necessária a criação de um ecossistema de proteção digital para a Escola para garantir a continuidade dos serviços de TIC, mitigando riscos de perda de informações, danos à imagem institucional, melhorando a percepção de segurança perante usuários internos e a sociedade.

3.1.13 A ENAP dispõe de um Comitê de Segurança da Informação (Portaria n] 556 de 19 de setembro de 2019 da Escola Nacional de Administração Pública) e executa ações, com caráter *ad hoc* e sistematizadas, de segurança da informação e privacidade de dados (distribuídas pelas diretorias de Gestão Corporativa e Executiva). Entretanto, a Escola ainda não dispõe de equipe técnica especializada e suficientes para a execução de atividades específicas de segurança cibernética, conforme se busca com a contratação dos objetos deste certame.

3.1.14 Ademais, à luz do disposto no art. 48 da Lei 14.133 de 1º de abril de 2021, a terceirização das atividades a serem licitadas e contratadas é completamente viável uma vez que as disposiçãoes deste certame não incorrem em nenhuma das condições de vedação listadas pelo supracitado artigo:

3.1.14.1 As especificações técnicas, os requisitos da contratação e os modelo de gestão propostos neste Termo de Referência não incidem na indicação de pessoas expressamente nominadas para executar direta ou indiretamente o objeto contratado;

3.1.14.2 Os requisitos de formação de equipe e de experiência profissional dispostos neste documento não fixam salário inferior ao definido em lei ou em ato normativo a ser pago pelo contratado;

3.1.14.3 Nos resquitos deste documento, a ENAP não estabelece vínculo de subordinação com funcionário de empresa prestadora de serviço terceirizado;

3.1.14.4 A Escola, conforme os requisitos deste documento, não define forma de pagamento mediante exclusivo reembolso dos salários pagos;

3.1.14.5 A ENAP, como contratante, não avoca para si a prerrogativa de demandar a funcionário de empresa prestadora de serviço terceirizado a execução de tarefas fora do escopo do objeto da contratação;

3.1.14.6 Não há previsão nos documentos deste certame que comporão o edital exigências que constituam intervenção indevida da Administração na gestão interna do contratado.

3.2 Desta forma, considerando a importância que os sistemas e serviços de TI adquiriram para as organizações e a constante diversificação e desenvolvimento de novas ameaças cibernéticas, são mandatórios a constante evolução, o aparelhamento, o aprimoramento dos mecanismos de segurança, bem como o desenvolvimento de equipes e de métodos de segurança cada vez mais complexos.

3.3 O objeto da contratação está previsto no Plano de Contratações Anual 2024, conforme detalhamento a seguir:

1. ID PCA no PNCP: [00627612000109-0-000001/2024];
2. Data de publicação no PNCP: [04/07/2023];
3. Id do item no PCA: [114702-90097/2023]
4. Classe/Grupo: [173 - SERVIÇOS DE CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO ECOMUNICAÇÃO (TIC)];
5. Identificador da Futura Contratação: [Contratação de serviços gerenciados de segurança].

3.4 O objeto da contratação está previsto no Plano de Contratações Anual [2023], conforme consta das informações básicas deste termo de referência.

3.5 O objeto da contratação também está alinhado com a Estratégia de Governo Digital 2023 e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2023-2025 da ENAP, conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
OE6	Promover o melhor ambiente de inovação e a construção colaborativa de soluções para desafios públicos
OE7	Gerir a informação e o conhecimento de forma estratégica
OE14	Prover soluções integradas de tecnologia da informação e comunicação com foco no usuário

ALINHAMENTO AO PDTIC 2023-2025				
Id.N	**Id. Meta**	**Descrição da Meta**	**ID. Ação**	**Descrição da Ação**
N4	M4.4	Prover Soluções de Segurança da Informação	**A4.4.1**	Prover solução integrada de segurança contra vírus, malwares e ransomware
			A4.4.2	Prover solução de antispam para os serviços de e-mail da Enap, incluindo suporte
			A4.4.2	Prover solução para gestão de vulnerabilidades
			A4.4.3	Prover solução de proteção avançada à infraestrutura de TI da Enap
			A4.4.4	Prover modernização contínua da solução de filtro de conteúdo da Enap
			A4.4.5	Prover solução de operação e atendimento a requisição e resposta a incidentes (SOC)
N5	M5	Promover ações de Segurança da Informação e Privacidade de Dados	**A5.1**	Propor revisão e publicação de normativos de Segurança da Informação e Privacidade de dados
			A5.4	Elaborar a Política de Proteção de Dados Pessoais
			A5.5	Elaborar o Plano de Resposta a Incidentes de SI
			A5.6	Realizar campanha de conscientização em Segurança da Informação e Privacidade de dados

			A5.7	Implementar framework de Privacidade e Segurança da Informação

3.6 Por tratar de oferta de serviços públicos digitais, o objeto da contratação será integrado à Plataforma Gov.br, nos termos do Decreto nº 10.332, de 28 de abril de 2020, e suas atualizações, de acordo com as especificações deste Termo de Referência.

4. REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio:

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

4.1.1 A solução de segurança a ser contratada visa, de forma contínua, suportar o gerenciamento, monitoramento, tratamento e proteção aos incidentes de segurança do ambiente tecnológico da ENAP de acordo com as seguintes necessidades de negócio:

4.1.1.1 Prover suporte, monitoramento, operação e gestão de serviços de segurança por meio de soluções próprias ou da ENAP;
4.1.1.2 Prover suporte e administração de ativos e tecnologias de segurança conforme soluções existentes no ambiente de segurança da ENAP;
4.1.1.3 Sustentar e operar todo o parque tecnológico através de um catálogo de serviços pré-estabelecidos pela ENAP por meio de especialistas em segurança dedicados ou por meio do SOC;
4.1.1.4 Documentar e realizar a gestão de respostas aos incidentes de segurança;
4.1.1.5 Prover serviços de governança, risco e conformidade de segurança e privacidade;
4.1.1.6 Prover serviço de prevenção contra vazamento de informações sensíveis para o meio externo;
4.1.1.7 Elaborar planos, programas, workshops, pesquisas e questionários de segurança da informação voltados para melhoria e conscientização de usuários em geral da ENAP;
4.1.1.8 Prover serviços de inteligência aplicados à segurança em busca de informações pertinentes à ENAP;
4.1.1.9 Responder a ataques de forma imediata colocando os responsáveis da ENAP a par da situação de vulnerabilidades, ameaças ou riscos graves à infraestrutura da ENAP;
4.1.1.10 Auxiliar nos problemas relacionados à segurança de ativos de informação com os quais a ENAP estabelece comunicação;
4.1.1.11 Monitorar vulnerabilidades e ameaças em tempo real no que tange à segurança dos ativos de rede e comunicação da ENAP;
4.1.1.12 Garantir a aplicação da Política de Segurança da Informação e Comunicações (POSIC) da ENAP;
4.1.1.13 Prover serviços de operação e gerenciamento de segurança integrados e customizados, capazes de fornecer os níveis de serviço exigidos em contrato em termos de efetividade e prazo;
4.1.1.14 Manter a continuidade dos serviços de segurança atualmente prestados na infraestrutura de TI;
4.1.1.15 Executar as políticas de segurança da informação, públicas, privadas (uso interno da ENAP) e restritas (uso por um grupo restrito);
4.1.1.16 Apoiar as equipes de infraestrutura, sistemas, banco e administração de dados na implantação da esteira de integração contínua do DevSecOPs, no que couber;
4.1.1.17 Elaborar planos e programas de segurança da informação e acesso a dados ou recursos de TI;
4.1.1.18 Proteger a integridade e a confiabilidade dos sistemas de informação contra incidentes de segurança;
4.1.1.19 Minimizar a duração e o impacto de uma eventual violação de segurança dos ativos e informações através de ações imediatas de contenção e erradicação de ameaças;
4.1.1.20 Aplicar a inteligência de proteção contra ataques cibernéticos;
4.1.1.21 Agir proativamente para reduzir a interrupção de serviços em parte ou como um todo, ainda que algum evento de segurança não tenha impactado o usuário final;

4.1.1.22 Realizar testes internos e externos completos e periódicos de segurança e prevenção para verificar pontos de vulnerabilidades na rede e nos sistemas e ambientes de infraestrutura da ENAP;
4.1.1.23 Manter a disponibilidade, desempenho e segurança do ambiente de TI;
4.1.1.24 Realizar a gestão, comunicação e o gerenciamento de riscos de segurança;
4.1.1.25 Coletar, identificar, tratar e efetuar o controle dos riscos mais significativos em cada sistema informacional crítico da ENAP;
4.1.1.26 Identificar vulnerabilidades eventualmente existentes nas diversas soluções e serviços de TI providos, prevenindo a ocorrência de incidentes minimizando os seus impactos;
4.1.1.27 Zelar pela proteção dos dados pessoais de professores, estudantes e cidadãos inseridos nas bases de dados e redes da ENAP por meio de políticas de segurança da informação com a nova Lei Geral de proteção de Dados Pessoais (LGPD);
4.1.1.28 Zelar pela privacidade dos dados pessoais dos cidadãos inseridos nas bases de dados e redes da ENAP;
4.1.1.29 Prevenir qualquer evento de segurança da informação indesejável e inesperado, seja único ou em série, que pode comprometer as operações do negócio e ameaçar a segurança da informação;
4.1.1.30 Apoiar a DGI (Diretoria de Gestão e Inovação) nas tomadas de decisões relacionadas à segurança da informação;
4.1.1.31 Manter a confidencialidade, integridade e disponibilidade do ambiente tecnológico;
4.1.1.32 Garantir que a infraestrutura da rede de dados da ENAP seja escalável e possibilitar um aumento significativo no número de conexões de rede, sem comprometimento da qualidade ou do desempenho devido a ataques cibernético;
4.1.1.33 Garantir a disponibilidade, continuidade e qualidade dos serviços para o cumprimento das atividades finalísticas da ENAP e, consequentemente, o alcance dos resultados desejados para a sociedade;
4.1.1.34 Garantir os meios adequados para que os processos de segurança da informação possam ser aprimorados através da implementação de recursos de proteção adequados.

Requisitos de Capacitação

4.2 Será necessário treinamento à equipe que atuará com a solução. O treinamento deverá ser de no mínimo 6 (seis) horas de duração.

4.3 A CONTRATADA deverá prover capacitação técnica, teórica e prática, de cada item, conforme sua natureza, da solução ofertada à equipe local da ENAP:

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

4.3.2 A capacitação técnica nas disciplinas referentes aos itens ofertados deverá contemplar turmas fechadas, com no máximo 15 (quinze) participantes em cada uma delas.

4.3.3 Os treinamentos devem ser ministrados, sob demanda, nas dependências da ENAP ou conduzidos de forma remota, considerando a duração mínima de 6 horas para cada item, em turnos parciais das 08:00 às 12:00 ou das 14:00 às 18:00, de segunda a sexta-feira, em datas e horários definidos posteriormente pela Escola.

4.3.4 A capacitação técnica provida deverá abordar todos os componentes da solução fornecida, devendo ainda estar de acordo com a utilização da solução instalada no ambiente da ENAP.

4.3.5 Considerando-se as tecnologias disponíveis no ambiente de Tecnologia da Informação da ENAP, verifica-se que, para a execução do objeto dessa pretensa contratação, a empresa a ser contratada deverá dispor de Equipe Técnica especializada e com treinamento e capacitação atualizados nas tecnologias em questão.

4.3.6 Os requisitos de capacitação devem refletir as principais metodologias, tecnologias, produtos e ferramentas que representem maior abrangência para os serviços de TI e soluções de infraestrutura de TI utilizados na ENAP.

4.3.7 A CONTRATADA deverá fornecer, também em meio digital, o material didático de acompanhamento detalhado, original do fabricante quando aplicável, preferencialmente em português, contendo todos os assuntos abordados na capacitação. Entende-se como material didático, apostilas, slides de apresentações, manuais, livros-textos, dentre outros de semelhante natureza, destinados a facilitar ou complementar o aprendizado. Na ausência de publicação em português (Brasil) do material original do fabricante, será aceito material em inglês;

4.3.8 A ENAP reserva-se o direito de realizar a validação técnica e pedagógica do material didático, podendo vir a solicitar à CONTRATADA eventuais correções ou adequações;

4.3.9 Ao término de cada turma, será realizada uma Avaliação de Reação tendo em vista a medição e avaliação da qualidade da capacitação. A ENAP poderá aplicar uma Avaliação de Reação em todos os treinandos, com o objetivo de avaliar a satisfação com a capacitação;

4.3.10 Caso a CONTRATADA, para fins próprios, tenha a necessidade de mensurar outros fatores não previstos na avaliação padrão da ENAP, ela poderá utilizar o seu próprio formulário, porém o mesmo não será utilizado para aprovação da capacitação por parte da ENAP;

4.3.11 Quatro fatores serão objeto de avaliação pelo formulário, conforme descrito abaixo:

4.3.11.1 Instrutoria - Avalia a satisfação dos participantes com relação a atuação do instrutor durante a capacitação, tanto em relação ao seu conhecimento técnico do tema, quanto à sua habilidade didático-pedagógica e de interação com a turma;

4.3.11.2 Material Didático - Avalia a percepção dos participantes sobre a adequação e clareza do material didático utilizado na capacitação;

4.3.11.3 Conteúdo Programático - Avalia a percepção dos treinandos quanto ao equilíbrio entre teoria e prática, nível de profundidade, exemplos de exercícios, aderência e aplicabilidade;

4.3.11.4 Autoavaliação - Avalia a percepção dos participantes quanto à aquisição de novos conhecimentos e habilidades por meio da capacitação oferecida, bem como, a segurança para a sua aplicação e relevância do conteúdo abordado;

4.3.12 Cada fator é composto por um conjunto de itens que deverão ser avaliados por meio da utilização de quatro conceitos, quais sejam: Fraco (0), Regular (1), Bom (2) e Excelente (3);

4.3.13 A capacitação técnica provida pela CONTRATADA poderá ser submetida à aprovação por parte da ENAP;

4.3.14 O resultado da capacitação será considerado INSATISFATÓRIO quando pelo menos uma das situações abaixo ocorrer:

4.3.14.1 Média final da turma igual ou inferior ao conceito regular (1), excluindo-se o fator Auto avaliação;

4.3.14.2 Média do fator Instrutoria igual ou inferior ao conceito regular (1);

4.3.15 A CONTRATADA será obrigada a realizar, sem ônus para a ENAP, nova capacitação para todas as turmas em que ficar configurado como resultado INSATISFATÓRIO. A critério da Escola, o conteúdo poderá ser ajustado e/ou o instrutor substituído para sanar os problemas identificados. A nova capacitação deverá acontecer segundo um novo calendário a ser definido pela ENAP;

4.3.16 Após a conclusão da capacitação, mediante solicitação formal da ENAP, a CONTRATADA deverá fornecer cópia da apresentação utilizada em mídia eletrônica (CD, DVD, PENDRIVE ou link de repositório em nuvem), em formatos padrão de mercado (PDF, DOC, PPT ou HTML);

4.3.17 A ENAP se reserva o direito de reproduzir trechos do material didático utilizado na capacitação, desde que registradas as devidas fontes,para realizar capacitações internas de seus servidores, terceirizados e colaboradores;

4.3.18 A CONTRATADA deverá disponibilizar para os participantes que obtiverem no mínimo 75% de frequência, os certificados de conclusão de curso, em meio eletrônico, ao final de cada turma. Aqueles que apresentarem percentuais inferiores não deverão recebê-lo;

4.3.19 A CONTRATADA deverá enviar à ENAP a lista de presença, assinada pelo instrutor, em que seja comprovada a participação dos treinandos em cada turno de cada dia de capacitação;

4.3.20 Para fins de comprovação dos serviços prestados, visando o faturamento, a CONTRATADA deverá encaminhar à ENAP, em até 5 (cinco) dias úteis após o encerramento de cada turma, os certificados e o documento de presença digitalizados.

4.3.21 As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático, etc.) serão de exclusiva responsabilidade da CONTRATADA;

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

Requisitos Legais

4.4 O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, 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 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis, a saber:

4.4.1 Lei Federal nº 12.846/2013: dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências;

4.4.2 Lei Federal nº 13.709/2018: lei Geral de Proteção de Dados Pessoais;

4.4.3 Lei Complementar nº 123/2006: institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte, e dá outras providências;

4.4.4 Decreto nº 7.174/2010: regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;

4.4.5 Decreto nº 7.579/2011: dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal;

4.4.6 Decreto nº 11.129/2022: regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira;

4.4.7 Decreto 9.507, de 21 de setembro de 2018: dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União;

4.4.8 Instrução Normativa SEGES/MP nº 05, de 26 de maio de 2017: dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional;

4.4.9 Instrução Normativa SEGES/ME Nº 98, de 26 de Dezembro De 2022: estabelece regras e diretrizes para o procedimento de contratação de serviços sob o regime de execução indireta de que dispõe a Lei nº 14.133, de 1º de abril de 2021, no âmbito da Administração Pública federal direta, autárquica e fundacional;

4.4.10 Decreto nº 10.947 de 25 de Janeiro de 2022: regulamenta o inciso VII do caput do art. 12 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o plano de contratações anual e instituir o Sistema de Planejamento e Gerenciamento de Contratações no âmbito da administração pública federal direta, autárquica e fundacional;

4.4.11 Instrução Normativa SGD/ME nº 01, de 4 de abril de 2019: dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

4.4.12 Instrução Normativa nº 03, de 26 de abril de 2018: dispõe sobre regras de funcionamento do Sistema de Cadastramento Unificado de Fornecedores – SICAF, no âmbito do Poder Executivo Federal;

4.4.13 Portaria SGD/MGI nº 1.070, de 1º de junho de 2023: estabelece modelo de contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

4.4.13.1 Sem embargo, este processo não se trata de contratação de posto de trabalho alocado ou de mão de obra com dedicação exclusiva, mas de serviços de segurança da informação para fins de apoio aos processos de gestão de soluções de TIC sob a supervisão exclusiva de servidores lotados na ENAP. A Portaria SGD/MGI nº 1.070, de 2023, portanto, foi referenciada apenas como parâmetro para se descrever as atribuições esperadas, conforme disposto no ANEXO C - CATEGORIAS DE SERVIÇOS da referida portaria, nos requisitos e experiências esperados para o(s) profissional(is) da contratada que atenderão aos requisitos e às especificações dos serviços a serem contratados.

4.4.14 Portaria MPOG/ME Nº 424, de 7 dezembro de 2017: Institui o Índice de Custo de Tecnologia da Informação - ICTI como índice específico a ser considerado nos contratos relacionados à Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração de Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal, observada a periodicidade legal;

4.4.16 Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022: dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

4.5 Ademais, a CONTRATADA deverá se submeter a Política de Segurança da Informação (POSIC) da ENAP, nos termos da Resolução Enap nº 27, de 28 de dezembro de 2021.

Requisitos de Manutenção

4.6 Devido às características da solução, há necessidade de realização de manutenções corretivas, preventivas, adaptativa ou evolutiva pela Contratada, visando à manutenção da disponibilidade da solução e ao aperfeiçoamento de suas funcionalidades;

4.7 Entende-se por requisitos de manutenção a necessidade de continuidade da prestação de serviços de TIC relacionados a segurança cibernética, visando garantir o acesso aos serviços de TIC na ENAP, bem como reduzir ou mitigar a ocorrência de falhas, problemas ou incidentes, conforme detalhado neste Termo de Referência e respectivos Anexos.

Requisitos Temporais

4.8 Os serviços devem ser prestados no prazo máximo de 05 (cinco) dias corridos para as capitais dos estados e Distrito Federal (conforme Local e Endereço da prestação dos serviços na seção 6 - Modelo de Execução Contratual deste Termo de Referência) e de 07 (sete) dias corridos para as demais localidades, 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;

4.9 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.

4.10 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. Serão considerados em dias úteis quando estiverem explicitamente assim definidos.

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

ATIVIDADE	PRAZO
Assinatura do Contrato	Em até 5 dias após a convocação
Reunião de Alinhamento inicial: iniciação do contrato e apresentação do preposto	Em até 10 dias úteis a partir da assinatura do contrato.
Entrega de certificado e/ou declaração para comprovação da qualificação dos técnicos/profissionais que irão executar os serviços.	Durante a reunião de Alinhamento inicial.
Entrega do Plano de Execução pela CONTRATADA.	Em até 14 dias úteis após a reunião de Alinhamento inicial.
Início das atividades propostas.	Em até 07 dias úteis após a entrega do Plano de Execução.
Período de levantamento dos itens 01 e 02.	Em até 03 dias úteis após a entrega do Plano de Execução.
Período de análise das informações obtidas dos itens 01 e 02.	Em até 02 dias úteis após a conclusão da fase de levantamento.
Período de proposições dos itens 01 e 02.	Em até 05 dias úteis após a conclusão da fase de análise.
Execução dos testes externos.	Em até 14 dias úteis após a conclusão da etapa de proposições.
Execução do re-teste.	Em até 07 dias úteis após a conclusão da fase de testes externos.
Reunião final e finalização do projeto.	Após a conclusão dos testes e re-testes, será realizada reunião entre a CONTRATADA e o CONTRATANTE para finalização do projeto em até 14 dias.

4.12 Seguem abaixo requisitos temporais mais detalhados:

4.12.1 O prazo para assinatura do contrato será de até 5 (cinco) dias úteis, contados a partir da data de convocação pela ENAP, podendo ser prorrogado uma vez, por igual período, quando solicitado pela parte e desde que ocorra motivo justificado e aceito pela Escola.

4.12.2 A CONTRATADA terá até 05 (cinco) dias corridos para iniciar a execução do contrato, podendo iniciar antes deste prazo desde que aceito pela DGI/ENAP.

4.12.3 A CONTRATADA deverá apresentar a documentação da equipe a ser habilitada para prestação dos serviços pelo menos 5 (cinco) dias antes do início da efetiva execução do contrato.

4.12.4 A CONTRATADA deverá apresentar uma equipe mínima para realizar atividades de transição contratual, se for o caso, com pelo menos 1 (um) analista do tipo PLENO que deverá participar dos processos de transição.

4.12.5 O evento de início da execução do contrato corresponde ao primeiro dia em que a CONTRATADA assume a responsabilidade operacional dos serviços de segurança, conforme os itens da solução ofertada, da ENAP. Somente a partir deste momento fará jus ao pagamento pelos serviços realizados, que serão calculados de forma proporcional (pró-rata) para o primeiro mês.

4.12.6 O Período de Adaptação Operacional será de 90 (noventa) dias, conforme definições estabelecidas na seção CRITÉRIOS DE MEDIÇÃO E PAGAMENTO deste Termo de Referência.

4.12.7 A CONTRATADA deverá realizar as atividades de Estabilização dos Serviços e Soluções de Segurança durante o Período de Adaptação Operacional.

4.12.8 Durante e após o Período de Adaptação Operacional, a CONTRATADA estará sujeita à aplicação de glosas, de acordo com a subseção "Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento" da seção CRITÉRIOS DE MEDIÇÃO E PAGAMENTO deste documento, conforme não atinja os resultados definidos neste Termo de Referência.

4.12.9 Durante e após o Período de Adaptação Operacional, a CONTRATADA estará sujeita à aplicação das sanções prevista neste Termo de Referência.

4.12.10 Durante o Período de Adaptação Operacional, a CONTRATADA deverá revisar, ajustar e implantar os processos relacionados a Segurança Cibernética e Privacidade de Dados Pessoais.

4.12.11 A partir do início da execução do contrato, inclusive durante o Período de Adaptação Operacional, a CONTRATADA deverá executar os serviços continuados presenciais Sustentação de Operações e Resposta a Requisições de Segurança e de SOC e de Monitoramento do Remoto 24x7x365, fazendo jus ao pagamento mensal por esses serviços.

4.12.12 Os serviços de atendimento descritos no catálogo de serviços relativos aos usuário de TIC (infraestrutura) deverão ser executados nos prazos definidos no acordo de nível de serviço estabelecido na seção CRITÉRIOS DE MEDIÇÃO E PAGAMENTO deste documento.

4.12.13 A descrição e os tipos de serviços constantes no catálogo de serviço poderão sofrer ajustes de acordo com a necessidade da ENAP ao longo da execução do contrato a fim de melhorar processos e comunicação entre as áreas.

4.12.14 A resolução de incidentes de TIC deverá ser tempestiva, conforme a necessidade, de forma a não prejudicar os indicadores de disponibilidade dos serviços de Segurança Cibernética.

Requisitos de Segurança e Privacidade

4.13 A CONTRATADA deverá atender às normas acerca de conformidade técnica e de integridade de dados na Administração Pública Federal, assim como às normas e aos procedimentos de que trata a Resolução Enap nº 27, de 28 de dezembro de 2021 que institui a Política de Segurança da Informação (POSIN) no âmbito da ENAP, sem prejuízo dos demais atos, documentos e normativos expedidos e publicados pela Administração Pública Federal, bem como pela própria ENAP relativos ao sigilo, à segurança e à privacidade das informações e comunicações, além dos respectivos Termos de Compromisso de Ciência previstos nas alíneas “a” e “b” do inciso V do art. 18 da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

4.13.1 A CONTRATADA e seus profissionais deverão observar os preceitos da LGPD (Lei Geral de Proteção de Dados Pessoais), Lei nº 13.709, de 14 de agosto de 2018.

4.13.2 Todos os profissionais da CONTRATADA que irão prestar serviço diretamente para a ENAP, deverão passar por processo específico de habilitação, dentre os quais será verificado o requisito de assinatura e entrega de um instrumento similar a um Termo de Responsabilidade e Ciência (ANEXO I-C – TERMO DE COMPROMISSO DE SIGILO E SEGURANÇA DA INFORMAÇÃO deste TERMO DE REFERÊNCIA) alterável discricionariamente, a qualquer tempo, pela ENAP.

4.13.3 As tarefas e atividades de operação de serviços executadas pela CONTRATADA deverão observar as políticas, normas e procedimentos institucionais de gerenciamento de serviços de TIC e de Segurança da Informação estabelecidas pelo CONTRATANTE, bem como padrões e normativos gerais tais como ANSTI/TIA/EIA, ISO, ABNT e demais normas vigentes no âmbito da Administração Pública Federal.

Requisitos Sociais, Ambientais e Culturais

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

4.14.1 Uma vez que o objeto da pretensa contratação consiste, essencialmente, em prestação de serviços de atendimento e suporte de segurança às equipes de Tecnologia da Informação, como também de suporte de segurança à própria infraestrutura de TI da ENAP, naquilo que couber, os serviços, resultados, relatórios, catálogos, gráficos, prospectos, demonstrativos, entre outros inerentes a serem fornecidos deverão ter documentação (catálogos, manuais, informativos e afins) entregue, preferencialmente, em Língua Portuguesa (Brasil) ou, caso não haja, em Língua Inglesa, e na forma de links de acesso ao sítio de documentação da própria CONTRATANTE, base de conhecimento, sistema de Wiki ou outro que venha a ser definido pela CONTRATANTE.
4.14.2 Os serviços deverão ser prestados de acordo com os critérios de sustentabilidade ambiental contidos na Instrução Normativa nº 01, de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão – SLTI/MPOG, no Guia Nacional de Contratações Sustentáveis (3ª edição, revista, atualizada e ampliada, Abril/2020, Consultoria-Geral da União), e no Decreto nº 7.746/2012, no que couber.
4.14.3 A CONTRATADA deverá cumprir, no que couber, as exigências do inciso XI, art. 7° da Lei 12.305, de 02 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos – PNRS.

Requisitos da Arquitetura Tecnológica

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

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

4.15.2 A CONTRATADA deverá utilizar os padrões de arquitetura definidos pela ENAP e bem como realizar recomendações e análises destas arquiteturas para melhorar a segurança de ativos de infraestrutura e de aplicações por meio de metodologia DevSecOps em todo os ambientes de desenvolvimento de sistemas.

4.15.3 Os serviços prestados pela CONTRATADA devem ser compatíveis com as tecnologias de hardware, software, linguagem de programação, interfaces, entre outros, utilizadas pelo CONTRATANTE, considerando as versões atualmente em uso.

4.15.4 A prestação dos serviços deverá ser realizada a partir do Centro de Operações de Segurança especializado, sendo remoto às instalações da CONTRATANTE e localizado no Brasil.

4.15.5 A CONTRATADA deverá comprovar que possui ao menos, 02 (dois) Centros de Operações de Segurança, redundantes, de modo que a indisponibilidade de um deles não afete nenhum aspecto dos serviços prestados.

4.15.6 A fim de garantir a disponibilidade das ferramentas e soluções utilizadas para a execução do objeto deste Termo de Referência, ambos os Centros de Operações de Segurança devem utilizar as infraestruturas de Data Centers distintas, ou seja, dois ou mais datacenters.

4.15.7 Ao menos um dos Data Centers deve ter as seguintes certificações ou normas, a saber: ABNT NBR ISO/IEC 27001; ABNT NBR ISO/IEC 20000; ABNT NBR ISO/IEC 9001;

4.15.8 A fim de atender o Item 02, O Centro de Operações de Segurança (SOC) deverá atender aos seguintes requisitos mínimos:

4.15.8.1 Utilizar sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas;
4.15.8.2 Filmar toda a área, mantendo as imagens armazenadas por no mínimo 90 (noventa) dias;
4.15.8.3 Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao de Centro de Operações de Segurança, por no mínimo, 90 dias;
4.15.8.4 Possuir solução de monitoramento de disponibilidade e desempenho no Centro de Operações de Segurança;
4.15.8.5 Caso algum dos serviços de gerenciamento e monitoramento não sejam realizados no mesmo espaço físico que o de Centro de Operações de Segurança, todos os requisitos devem ser atendidos em todos os locais de prestação desses serviços;
4.15.8.6 O perímetro do Centro de Operações de Segurança deve ser equipado com sensor de intrusão e alarmes contra acesso indevido, em regime de 24x7x365;
4.15.8.7 Ser vigiado de forma ininterrupta por segurança especializada e armada em regime de 24x7x365;
4.15.8.8 Ter controle de acesso físico ao Centro de Operações de Segurança com pelo menos 2 (dois) dos seguintes fatores de autenticação: Cartão de identificação magnético e; Biometria de leitura de digital ou análise de retina;
4.15.8.9 Possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados por, no mínimo, o correspondente ao prazo do contrato;
4.15.8.10 Ser configurado de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços;
4.20.8.11 Ter sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPS's (unidades de alimentação elétrica contínua) para garantir a transição entre o fornecimento normal de energia e o grupo gerador;
4.15.8.12 Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;
4.15.8.13 O Centro de Operações de Segurança da CONTRATADA deverá possuir processos implementados que garantam a segurança das informações da CONTRATANTE. Estes processos devem estar certificados pelas normas ABNT NBR ISO/IEC 27001. Tal certificação deverá garantir controles rígidos e auditáveis de acesso físico e lógico às informações e processos internos e deverá possuir comprovadamente em seu escopo a área de monitoramento;
4.15.8.14 A CONTRATADA deverá disponibilizar linha telefônica 0800, ou equivalente a ligação local, para abertura e acompanhamento de chamados;
4.15.8.15 Possuir múltiplas conexões independentes para acesso à Internet. Cada conexão para acesso à Internet deve ser capaz de, isoladamente, suportar a operação do Data Center;
4.15.8.16 Caso necessário para a prestação dos serviços, a CONTRATADA deverá providenciar o estabelecimento de VPN para comunicação entre seus Datacenters e os Datacenters do CONTRATANTE;
4.15.8.17 Todas as características exigidas neste item para o Centro de Operações de Segurança poderão ser confirmadas em diligência presencial.

4.15.9 Ademais, os serviços, equipamentos, licenças, subscrições e peças deverão observar integralmente os requisitos de arquitetura tecnológica descritos na especificação técnica dos itens deste Termo de Referência, bem como compatibilidade com *nodes* HPE SimpliVity 380 Gen10 G Node da solução HCI existente e sistemas de virtualização gerais.

4.16 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

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

4.17.1 Para a referida contratação, pode se considerar como implantação a fase de iniciação contratual, na qual, basicamente, a CONTRATADA deverá:

a) Compor e apresentar formalmente para a ENAP a equipe técnica que será responsável pela execução dos serviços, ainda que sem que caracterização de mão de obra com dedicação exclusiva, mas que deverá atender aos requisitos de experiência profissional;

b) Propor e executar processo de transição contratual, do qual devem participar a atual contratada responsável pelo contrato em vigor, a futura contratada e a equipe de fiscalização nomeada da CONTRATANTE;

c) Apresentar cronograma para realizar eventual configuração, ou ajustes iniciais necessários de catálogo de serviços e de baseline nas ferramentas de segurança e de ITSM;

d) Apresentar cronograma para realizar ajustes para os processos de gestão de serviços de Segurança e apresentar em reunião formal para os gestores de TI e equipe de fiscalização.

e) Se for necessário algum tipo de hardware ou equipamento durante a execução contratual, este deverá ser fornecido pela CONTRATADA junto com a licença em nome da ENAP.

4.17.2 Como o objeto do contrato envolve segurança cibernética, o processo de implementação deve estar alinhado aos principais frameworks de boas práticas de gestão de serviços e segurança de TIC em suas versões mais atualizadas durante a vigência do contrato, aplicáveis a cada categoria de serviço, tais como: ITIL, COBIT e PMBOK, ISO/IEC 27001 e ISO/IEC 27002.

4.17.3 No início da execução do contrato a CONTRATADA deverá realizar um levantamento (baseline) da situação de todos ativos de segurança a serem gerenciados de modo a se estabelecer um panorama geral de segurança da informação no ambiente da CONTRATANTE, identificando os riscos, vulnerabilidades ou demais situações que possam comprometer a segurança do Parque Tecnológico da CONTRATANTE, bem como elaborar um planejamento das ações eventualmente necessárias para manter ou adequar o ambiente tecnológico às normas, políticas e melhores práticas de segurança da informação.

4.17.4 Por se tratar na contratação de serviços o requisito para o processo de implantação está intrínseco ao início das atividades contratuais, ou seja, a CONTRATADA deverá fornecer e configurar os softwares para execução das atividades pertinentes ao certame conforme tabela a seguir:

ITEM	DESCRIÇÃO	FERRAMENTAS NECESSÁRIAS PARA EXECUÇÃO DO SERVIÇO (Deverão ser disponibilizados e utilizados pela CONTRATADA para a execução dos serviços)
01	Serviço de monitoramento e visibilidade de ataques cibernéticos	Serviços de Proteção de Riscos Digitais
02	Serviço de monitoramento, detecção e resposta a incidentes - 1500 Eventos por segundo (EPS)	SIEM (Security Information e Event Management) SOAR (Security Orchestration, automation and response)

4.17.5 As subscrições e licenças, quando devidamente previstas, devem ser entregues, instaladas e configuradas no ambiente de hiper convergência (HCI) e virtualização existente pela licitante vencedora. Aderente caso alguma licença dependa de infraestrutura interna para seu pleno funcionamento.

4.17.6 As licenças devem possibilitar o uso de 100% das características aqui detalhadas, assim como proporcionar suporte e atualização de versão dentro do período de vigência contratual;

4.17.7 A CONTRATADA deverá apresentar um Plano de Projeto com, no mínimo, os seguintes conteúdos:

a) Definição do escopo;
b) Definição de quais tarefas deverão ser realizadas para implementação e configuração dos itens;
c) Cronograma de Implantação; e
d) Plano de arquitetura e desenho da solução.

4.17.8 O Plano de Projeto deverá ser aprovada pela CONTRATANTE.

4.17.9 A implementação das licenças contratadas deve ser planejada e executada de modo que não cause interrupções e paralisações não programadas, ou qualquer outro tipo de transtorno ao correto funcionamento do ambiente operacional da CONTRANTE;

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

4.17.11 O serviço de instalação da solução ofertada deverá contemplar no mínimo os seguintes pontos:

a) Todas as etapas de instalação e configuração deverão ser realizadas por técnicos experientes, formados em tecnologia da informação e com experiência mínima de 3 anos na área;
b) Entrega e conferência de licenciamento de acordo com o esperado;
c) Criação de rotinas de monitoramento de componentes que porventura sejam instalados no datacenter da CONTRATANTE;
d) Atualização de software com a última versão disponível e estável dos fabricantes;
e) Configuração dos endereços IP’s para o gerenciamento de produtos instalados conforme políticas de rede da CONTRATANTE;
d) Realização das demais configurações necessárias para o correto funcionamento da solução entregue;
e) Será de responsabilidade da CONTRATADA a correção dos problemas técnicos decorrentes de erros identificados na execução da instalação e configuração das licenças, sejam operacionais ou por problemas de mau funcionamento, responsabilizando-se por todos os procedimentos e custos envolvidos para resolução, sob pena de incorrer em sanções legais cabíveis, sendo garantida a ampla defesa, exceto quando seja comprovado que o problema se deu devido a mau funcionamento de componentes já existentes no ambiente da CONTRATANTE que sejam pré requisitos para o funcionamento dos objetos contratados.
f) Ao término do serviço deve ser fornecido um relatório detalhado (As-Built) contendo todas as configurações realizadas, com comentários sobre os principais comandos e as justificativas das opções de parametrização de modo a facilitar a posterior administração da solução e a continuidade de seu funcionamento;
g) Toda configuração deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada.

Requisitos de Implantação

4.18 Os serviços deverão observar, além dos requisitos de Projeto e Implementação previstos neste Termo de Referência, integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

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

4.18.2 Deverão ser fornecidos todos os componentes necessários para garantia de funcionamento de todos os componentes presentes neste Termo de Referência;

Requisitos de Garantia e Manutenção

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

4.19.1 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, sem custos adicionais durante a execução do contrato.

4.19.2 Os serviços prestados e os produtos, licenças e subscrições adquiridos possuem garantia durante todo o período de vigência contratual.

4.19.3 Todos os recursos que compõe as soluções dos itens 01 e 02 entregues deverão ter garantia de funcionamento e manutenção do fabricante durante toda a vigência do Contrato, sem custos adicionais para a Contratante;

4.19.4 A CONTRATADA garantirá os serviços prestados no período vigente da garantia, sem ônus À CONTRATANTE. Nesse período a CONTRATADA se obriga a corrigir quaisquer defeitos nos produtos ou serviços.

4.19.5 A garantia do produtos, licenças e subscrições deverá abranger todas as atualizações de versões de software (*firmwares*) do produto;

4.19.6 A garantia/suporte deverá atender, no mínimo todas as funcionalidades suportadas pelos componentes da solução, independente de terem sido configurados anteriormente e da política de comercialização do fabricante;

4.19.7 Os defeitos compreendem, mas não se limitam a: imperfeições percebidas no serviço, ausência de artefato de documentação, configurações e qualquer outra ocorrência que impeça o seu funcionamento normal. Tais defeitos poderão ser apurados pelo CONTRATANTE ainda que tenham sido faturados e pagos sem nenhuma restrição, ou seja, a fatura aceita não é documento de garantia de qualidade.

4.19.8 Durante a vigência da garantia, toda a assistência técnica deverá ser prestada para o pleno funcionamento das soluções;

4.19.9 Durante o prazo de garantia a CONTRATADA prestará, quando for o caso, serviços de suporte técnico e/ou de assistência técnica, na forma on-site dentro do horário de trabalho da CONTRATANTE;

4.19.10 Durante o período de vigência da garantia a(s) CONTRATADA(s) deverá(ão) executar correções visando eliminar erros detectados nas soluções que impeçam seu pleno funcionamento de acordo com as especificações listadas neste documento;

4.19.11 Os atendimentos deverão ser prestados por técnico devidamente capacitado e qualificado para executar as atividades, devendo este ser demonstrado, por meio de documento de comprovação de certificação técnica na solução e tecnologia ofertados, no momento da nomeação do PREPOSTO.

4.19.12 Caso a CONTRATADA identifique a necessidade de substituição de solução que apresentem defeitos ou falhas, os mesmos deverão ser substituídos por soluções de qualidade e características técnicas iguais ou superiores aos existentes, desde que compatíveis, com todas as configurações necessárias ao seu funcionamento, e autorizado pela ENAP;

4.19.13 Os serviços deverão ser executados sem impacto na utilização do ambiente de TI da ENAP, de forma que os subsistemas mais críticos deverão ser executados em horário noturno e/ou finais de semana, e autorizado pela ENAP;

4.19.14 A CONTRATADA deverá auxiliar a CONTRATANTE na assistência técnica da solução e deverá abrir para CONTRATANTE os chamados junto ao suporte técnico da fabricante da Solução quando necessário;

4.19.15 A CONTRATADA deverá disponibilizar uma central de atendimento, via telefone, plataforma web ou e-mail, para abertura dos chamados técnicos.

4.19.16 A CONTRATADA deverá quando solicitada pela CONTRATANTE emitir relatórios contendo o status de todos os casos abertos, bem como status de RMAs (Registro Mensal de Atendimento), progresso na análise de falhas e emissão de relatórios de assuntos relacionados ao suporte técnico da fabricante da Solução.

4.19.17 Durante a vigência da garantia, a ENAP deverá ter acesso às atualizações de software fornecidas pelo fabricante, assim como receber o suporte técnico por telefone ou sistema eletrônico (internet) para esclarecimento de dúvidas quanto à instalação e/ou configuração do equipamento.

4.19.18 O Suporte Técnico será realizado no regime de 24 horas por dia, 7 dias por semana (24x7x365):

a) O início do atendimento se dará a partir da comunicação do(s) defeito(s) pela ENAP, via serviço telefônico (0800), e-mail e/ou outro meio indicado pela CONTRATADA e aprovado pela ENAP na Reunião Inicial ou em outra subsequente à contratação.
b) Durante a vigência da garantia, a contratada deverá prestar o serviço de forma contínua, sem quaisquer interrupções, atendendo aos níveis de serviço contratado, conforme especificações firmadas neste Termo de Referência e no contrato.

4.19.19 Os serviços de suporte técnico a solução deverá incluir, dentre outros:

a) Orientações sobre uso, configuração e instalação da solução;
b) Questões sobre compatibilidade e interoperabilidade da solução ofertada;
c) Interpretação da documentação da solução ofertada;
d) Orientações para identificar a causa de uma falha;
e) Orientação quanto às melhores práticas para implementação do serviço contratado; e
f) Apoio na recuperação de ambientes em caso de panes ou perda de dados.

4.19.20 Ao término de atendimentos relacionados ao suporte técnico, a CONTRATADA deverá apresentar Relatório de Atendimento contendo data e hora da abertura do chamado, data e hora do início e do término do atendimento, identificação do defeito, nome do técnico responsável pela execução da garantia, providências adotadas e outras informações pertinentes. O Relatório deverá ser validado por técnico da ENAP.

4.19.21 A CONTRATADA deverá substituir, em até 30 (trinta) dias, a solução já instalada por uma nova, sem ônus para a ENAP, quando comprovados defeitos de fabricação, do próprio ou de seus componentes, que comprometa o seu desempenho, nas seguintes hipóteses:

a) caso ocorram 4 (quatro) ou mais defeitos que comprometam seu uso normal, dentro de qualquer intervalo de 30 (trinta) dias;
b) caso a soma dos tempos de paralisação da solução ultrapasse 40 (quarenta) horas, dentro de qualquer intervalo de 30 (trinta) dias.

Requisitos de Experiência Profissional

4.20 Os serviços de instalação, suporte, garantia e treinamento previstos, além de quaisquer outros pertinentes a esta contratação, deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços;

4.20.1 Para o treinamento a contratada deverá comprovar a qualificação do seu profissional que atuará na execução das atividades descritas.

4.20.2 Para a execução do objeto da pretensa contratação, considera-se necessário que a equipe técnica da CONTRATADA satisfaça alguns requisitos mínimos de qualificação e experiência profissional.

4.21 Tendo em vista a complexidade dos serviços a serem executados e o nível de conhecimento exigido para as atividades afetas a tecnologia da informação, é intuitivo afirmar que maior grau de experiência irá resultar em melhores níveis de serviços prestados e menor risco para as atividades institucionais da ENAP.

4.21.1 Uma prática comum do mercado é definir para os perfis profissionais tipos de profissionais com base na qualificação e experiência. É comum a atribuição do tipo de profissional nas categorias: júnior, pleno ou sênior. No mercado de TI não é diferente, e desta forma, a Portaria SGD/MGI nº 1.070 /2023 também adotou a mesma definição de tipos de profissionais, conforme segue:

a) “Profissional Júnior: adequado para exercer atividades de menor complexidade e que exigem menor experiência ou qualificação profissional. Geralmente, não apresenta autonomia para tomadas de decisão operacional;
b) Profissional Pleno: adequado para exercer atividades com um maior grau de complexidade, que requerem uma capacidade maior de análise crítica e resolução de problemas, além de exigir maior experiência ou qualificação profissional;
c) Profissional Sênior: adequado para exercer atividades com grau elevado de complexidade e criticidade, e que requer experiência e qualificação profissional diferenciada;

4.21.2 Definição de Experiência Profissional e Formação de Equipe:

4.21.2.1 Deve-se observar as características e requisitos de cada infraestrutura com vistas a definir os requisitos de experiência profissional necessários para assegurar a qualidade na prestação dos serviços, bem como a definição do tipo mais adequado de perfil profissional.

4.21.2.2 A definição do tipo de profissional (júnior, pleno ou sênior) depende da natureza, criticidade e complexidade dos serviços a serem prestados no âmbito de cada órgão.” (g.n.)

4.21.2.2.1 Também conforme o Mapa de perfis da Portaria SGD/MGI nº 1.070/2023 segue a descrição do Perfil de Gerente de Segurança da Informação que será necessário para essa contratação:

a) Gerente de segurança da informação: profissional com responsabilidade de coordenar e gerenciar a atuação dos demais profissionais de segurança da informação, garantindo a adequada prestação dos serviços, bem como controlando e planejamento operacionalmente as ações dessa equipe. Presta também apoio à tomada de decisão do órgão auxiliando na prospecção de soluções de segurança da informação, fornecimento de informações táticas e operacionais, e proposição de ações de aprimoramento dos serviços de segurança da informação seja preventiva ou reativa.

4.21.2.2.2 Refletido esse padrão de mercado, estão previstos neste Termo de Referência a necessidade da CONTRATADA alocar profissionais do tipo Gerente, Sênior, Pleno para execução dos serviços presenciais e perfis Sênior, Pleno e Júnior para a execução de serviços remotos via SOC 24x7x265, haja vista a complexidade e criticidade do parque computacional da ENAP, e dos serviços de TIC.

Requisitos de Formação da Equipe

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

4.22.1 A prestação de serviços objeto desta contratação depende majoritariamente de profissionais técnicos e qualificados, conforme constata a Portaria SGD/MGI nº 1.070/2023. Portanto, é importante que as licitantes tenham a melhor compreensão possível da abrangência, complexidade e requisitos de entregas e níveis mínimos de serviços exigidos para que possam fazer o correto dimensionamento da equipe e alocações dos perfis e tipos profissionais adequados. Para que haja garantia de qualidade no serviço executado e modernização das metodologias de Gestão de TI, a CONTRATADA deverá manter profissionais qualificados nas áreas funcionais, que deverão ser

gerenciados exclusivamente pelo representante técnico da empresa CONTRATADA, de forma que o CONTRATANTE possa obter o menor tempo de resposta para quaisquer incidentes ocorridos no seu ambiente de Infraestrutura tecnológica, bem como alcançar a excelência nos serviços de tecnologia;

4.22.2 Esses recursos humanos deverão conhecer o funcionamento dos negócios internos da ENAP e executar os procedimentos de acordo com as regras de segurança, sendo possível, para algumas atividades, execução ou operacionalização remota.

4.22.3 As equipes deverão ser dimensionadas pela(s) empresa(s) CONTRATADA(s) de forma a atender as demandas de acordo com os níveis de serviço estabelecidos. Para tanto, salienta-se que essa responsabilidade de formação da equipe de profissionais é exclusiva da empresa CONTRATADA

4.22.4 Será de responsabilidade da CONTRATADA o cumprimento da legislação específica dos profissionais que prestarão o serviço nas dependências da ENAP ou remotamente.

4.22.5 A CONTRATADA deverá fornecer o transporte necessário ao deslocamento dos profissionais até as dependências da ENAP sempre que necessário.

4.22.6 Os profissionais deverão atender às exigências de vestimenta feitas aos servidores da ENAP e portar crachá de identificação, durante toda a prestação do serviço.

4.22.7 Deve-se observar a formação e qualificação dos profissionais a serem empregados na execução do contrato em cada categoria de serviço conforme as especificações técnicas dos itens 01 e 02.

4.22.8 Em relação ao esforço estimado, conforme orienta a Portaria SGD/ME nº 6.432/2021, a CONTRATADA deverá apresentar a formação e os perfis da equipe técnica necessária para o atendimento dos serviços contratados.

4.22.9 As definições e estimativas feitas nessa seção são apenas balizadores para a proposta, e, portanto, a CONTRATADA continua sendo a única responsável pelo dimensionamento adequado da equipe, bem como definição de salários.

4.22.10 As definições e estimativas feitas nessa seção também não configuram alocação de postos de trabalho, nem sequer dedicação exclusiva.

Requisitos de Metodologia de Trabalho

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

4.24 A OS/fornecimento de bens indicará o serviço, a quantidade e a localidade na qual os deverão ser prestados.

4.25 O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 (vinte e quantro) horas por dia e 7 (sete) dias por semana de maneira eletrônica e 8 (oito) horas por dia e 5 (cinco) dias por semana por via telefônica.

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

4.26.1 A metodologia de trabalho será baseada no conceito de delegação de responsabilidade, onde a ENAP é responsável pela gestão e fiscalização do contrato e pela atestação da aderência aos padrões de qualidade exigidos, e a CONTRATADA como responsável pela execução dos serviços e gestão das demandas e dos seus recursos humanos.

4.26.2 Todo o trabalho realizado pela CONTRATADA estará sujeito à avaliação técnica, sendo homologado quando os relatórios dos serviços prestados estiverem de acordo com o padrão de qualidade exigido pela ENAP.

4.26.3 À CONTRATADA caberá sanar as irregularidades apontadas na execução contratual, submetendo entregas ou atividades impugnadas à nova verificação, ficando sobrestado o pagamento até a execução do saneamento necessário, sem prejuízo da aplicação das sanções legais cabíveis.

4.26.4 A CONTRATADA deverá apresentar mensalmente os resultados da prestação dos serviços por meio de reuniões com a CONTRATANTE apresentando relatórios consolidados mensais, relatórios periódicos dos serviços prestados ou quando solicitado pela CONTRATANTE.

4.26.5 A ENAP poderá, a qualquer tempo, sem ônus e dentro de suas conveniências técnicas, modificar padrões técnicos, metodológicos e arquitetura tecnológica.

4.26.6 A CONTRATADA deverá prever a execução de serviços em horários diurnos e noturnos, em fins de semana e feriados, conforme necessidade discriminada nesse TERMO DE REFERÊNCIA e acordado previamente, podendo realizar a compensação de horas dos profissionais através de bancos de horas ou outras modalidades legalmente previstas, desde que os níveis mínimos de serviço não sejam afetados.

4.26.7 Antes do início das atividades, a ENAP irá reunir-se com a CONTRATADA de forma a levantar todas as premissas/adequações para a execução dos serviços. Deve-se prever e explicitar as fases de planejamento, execução e homologação final do atendimento do SOC local e remoto, gerando cronogramas com atividades e responsáveis para subsidiar a fiscalização do contrato.

4.26.8 Todos os serviços deverão ser executados, preferencialmente, sem impactar as atividades rotineiras da ENAP. Os serviços deverão ser precedidos de cronogramas de execução previamente aprovados.

4.26.9 A CONTRATADA deverá criar, manter e atualizar scripts de atendimento, instruções de trabalho e procedimentos operacionais que permitam consultas e alterações quando se fizerem necessárias.

4.26.10 Os materiais a serem utilizados, as obras (se necessárias) e os serviços a serem executados deverão obedecer rigorosamente:

a) A todas as normas e especificações exigidas.
b) Às normas da ABNT pertinentes.
c) Às disposições legais da União.
d) Às prescrições e recomendações dos fabricantes.
e) Às normas internacionais consagradas, na falta de normas da ABNT.

4.26.11 Nenhuma modificação poderá ser feita nas especificações dos projetos aprovados pela ENAP sem autorização expressa do mesmo.

4.26.12 Possíveis indefinições, omissões, falhas ou incorreções das especificações ora fornecidas não poderão constituir pretexto para a CONTRATADA alegar redução de desempenho. Considera-se, inapelavelmente, a CONTRATADA e seus prepostos como altamente especializadas nos serviços em questão e que, por conseguinte, deverá ter considerado as complementações e providências técnicas por acaso omitidos nas especificações, mas implícitos e necessários ao perfeito e completo funcionamento dos serviços descritos neste Termo de Referência.

4.26.13 A ENAP não aceitará, sob nenhum pretexto, a transferência de qualquer responsabilidade da CONTRATADA para outras entidades.

4.26.14 Não serão admitidos estagiários para prestar quaisquer serviços objeto deste instrumento e todos os funcionários da CONTRATADA deverão ser registrados pelo regime CLT ou possuir contratos de prestação de serviços.

4.26.15 A CONTRATADA é responsável por dimensionar, organizar e gerenciar o quantitativo de profissionais em turnos de trabalho necessários para o cumprimento do objeto contratado de acordo com os níveis de serviços exigidos neste Termo de Referência.

4.26.16 A execução do contrato será baseada no modelo no qual a CONTRATANTE é responsável pela gestão do contrato e pela verificação dos resultados esperados e dos níveis de qualidade exigidos frente aos serviços entregues, e a CONTRATADA é a responsável pela execução dos serviços e gestão dos recursos humanos e físicos necessários.

4.26.17 Caso a CONTRATANTE não aprove a execução e/ou a qualidade do serviço, conforme especificado no detalhamento das tarefas, deverá apor comentário e anexar, caso seja necessário para evidenciar, documentos/relatórios que justifiquem a não aprovação, retornando à CONTRATADA para correção/complementação.

4.26.18 A CONTRATADA deverá obrigatoriamente realizar Pesquisas de satisfação com usuários ao final de cada atendimento.

Requisitos de Segurança da Informação e Privacidade

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

4.27.1 A Solução deverá atender aos requisitos de segurança da informação e privacidade, de forma ampla, adotando políticas e boas práticas, de forma a mitigar os riscos.

4.27.2 As atividades da CONTRATADA deverão estar de acordo com as melhores práticas de segurança segundo os frameworks e padrões ITIL v4 ou superior, MITRE ATT&CK®, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 30111 e ISO/IEC 29147, aplicáveis a cada categoria de serviço.

4.27.3 Deverão ser observadas as leis, normas e diretrizes de Governo relacionadas à Segurança da Informação e Comunicações (SIC), em especial atenção ao Decreto n° 9.637/2018, à Instrução Normativa GSI/PR n° 01/2008, e suas normas complementares, à Instrução Normativa Nº 5, de 30 de agosto de 2021, à Lei n° 13.709/2018 e à Política de Segurança da Informação e Comunicações (POSIN) da ENAP, e suas normas complementares.

4.27.4 Deverão ser observadas todas as determinações e orientações contidas nas Diretrizes e Normas de Segurança da ENAP, por meio da POSIN e suas evoluções. Ela apresenta os princípios considerados adequados para o manuseio, controle e proteção das informações contra destruição, modificação, violação, divulgação indevida e acessos não autorizados, sejam acidental ou intencionalmente, visando preservar a integridade, confidencialidade e disponibilidade das informações.

4.27.5 As Soluções deverão contemplar:

a) Implementação de controles necessários para o registro de eventos e incidentes de segurança da informação e privacidade;
b) Implementação e manutenção de controles específicos para registro de eventos e rastreabilidade de forma a manter trilha de auditoria de segurança da informação e privacidade, aderente a disposto em dispositivo legal correlato publicado pelo GSI/PR, de forma a assegurar a rastreabilidade das ações de usuário por meio de logs de transações e de acesso aos sistemas, conforme especificação de requisitos, e gerá-los e disponibilizá-los à ENAP para fins de auditorias e inspeções;
c) Implementação de medidas de salvaguarda para os logs descritos no item anterior, bem como controles específicos para registro das atividades dos administradores e operadores dos sistemas relacionados ao objeto do contrato, de forma que esses não tenham permissão de exclusão ou desativação dos registros (log) de suas próprias atividades;
d) Implementação e manutenção de controles criptográficos para armazenamento, tráfego e tratamento da informação; e
e) Execução periódica de análise de vulnerabilidades na Solução, para detecção de vulnerabilidades técnicas e execução de medidas para seu saneamento ou contenção.

4.27.6 Em relação ao gerenciamento de identidades e registros:

a) Possuir procedimentos de controle de acesso que abordem a transição entre as funções, os limites e controles dos privilégios dos usuários e os controles de utilização das contas de usuários;

b) Impor mecanismo de autenticação que exija tamanho mínimo, complexidade, duração e histórico de senhas de acesso;
c) Suportar tecnologia single sign-on para autenticação;
d) Suportar mecanismos de autenticação multifator ou outra alternativa que aumente o grau de segurança no processo de autenticação de usuários da ENAP no provedor de serviço de nuvem, de acordo com nível de criticidade da informação;
e) Permitir ao órgão ou à entidade gerenciar as próprias identidades, inclusive criação, atualização, exclusão e suspensão no ambiente fornecido pelo provedor de serviço de nuvem; e
f) Atender aos requisitos legais, às melhores práticas de segurança e a outros critérios exigidos pelo órgão ou pela entidade em seus processos de autenticação, controle de acesso, contabilidade e de registro (formato, retenção e acesso);

4.27.7 Estabelecer um canal de comunicação seguro utilizando, no mínimo, *Secure Sockets Layer /Transport Layer Security* (SSL/TLS);

4.27.8 Utilizar um padrão de encriptação seguro, conforme padrão internacional reconhecidamente aceito, que possa ser implementado com chaves de encriptação geradas e armazenadas pela ENAP;

4.27.9 Disponibilizar facilidades que possibilitem a aplicação de uma proteção criptográfica própria da ENAP;

4.27.10 Possuir procedimentos necessários para preservação de evidências, conforme legislação; e Possuir procedimentos em relação ao descarte de ativos de informação e de dados, que assegurem:

a) Sanitizar ou destruir, de modo seguro, os dados existentes nos dispositivos descartados por meio da utilização de métodos que estejam em conformidade com os padrões estabelecidos para a conduta e as melhores práticas;
b) Armazenar, de modo seguro, ativos de informação a serem descartados, em ambiente com acesso físico controlado, com registro de toda movimentação de entrada e de saída de dispositivos.

4.27.11 Contemplar procedimentos e controles adequados para compartilhamento, uso e proteção da informação e os casos de compartilhamento de informações com terceiro devem ser avaliados pela contratante, por intermédio da autoridade competente, a qual caberá autorizar a divulgação do mínimo de informações necessárias para cada compartilhamento, caso julgue apropriado, preservados os casos de sigilo previstos na legislação aplicável e de proteção de dados pessoais disposto pela Lei nº 13.709/2018.

Vistoria

4.28 A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 09 (nove) horas às 18 (dezoito) horas.

4.28.1 A vistoria deverá ser agendada por meio do endereço eletrônico cgti@enap.gov.br devendo ser realizada até 3 (três) dias antes da abertura da licitação, para que haja prazo para o saneamento de possíveis questionamentos.

4.28.2 Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

4.29 Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

4.29.1 A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a licitante vencedora assumir os ônus dos serviços decorrentes.

4.30 Caso o licitante opte por não realizar a vistoria, deverá prestar declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação.

4.31 A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

Sustentabilidade

4.32 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 e suas atualizações, elaborado pela Câmara Nacional de Sustentabilidade da Controladoria Geral da União /Advocacia Geral da União:

4.32.1 Em atendimento à legislação que recomenda a adoção de critérios de sustentabilidade nas especificações dos bens a serem fornecidos e a exigência de práticas sustentáveis por parte das empresas contratadas na execução dos serviços, mormente a Lei nº 14.133/2021 e a Instrução Normativa SLTI nº 1/2010, e demais dispositivos legais pertinentes à matéria, a CONTRATADA deve satisfazer as diretrizes de sustentabilidade expressas no art. 144 daquela Lei, a saber:

a) baixo impacto sobre recursos naturais como flora, fauna, ar, solo e água;
b) preferência para materiais, tecnologias e matérias-primas de origem local;
c) maior eficiência na utilização de recursos naturais como água e energia;
d) maior geração de empregos, preferencialmente com mão de obra local;
e) maior vida útil e menor custo de manutenção do bem e da obra;
f) uso de inovações que reduzam a pressão sobre recursos naturais;
g) origem sustentável dos recursos naturais utilizados nos bens, nos serviços e nas obras; e
h) utilização de produtos florestais madeireiros e não madeireiros originários de manejo florestal sustentável ou de reflorestamento.

4.32.*2* Como consequência, nos instrumentos convocatórios que tenham por objeto o fornecimento de bens, por exemplo, constatada a presença dos requisitos referentes à justificativa e à competitividade referidos no parágrafo anterior, são incluídos critérios de sustentabilidade, os quais passam a integrar as especificações técnicas dos bens.

4.32.*3* No que se refere aos contratos, dentre as obrigações gerais do contratado consta a exigência da adoção de práticas de sustentabilidade na execução dos serviços, de modo a prevenir ações danosas ao meio ambiente, em observância à legislação vigente, principalmente no que se refere aos crimes ambientais, contribuindo para a manutenção de um meio ambiente ecologicamente equilibrado.

4.32.4 Adicionalmente, também é obrigação do contratado orientar e capacitar os prestadores de serviços, fornecendo informações necessárias para a perfeita execução dos serviços, incluindo noções de responsabilidade socioambiental.

4.32.5 Além da adoção dos critérios e práticas de sustentabilidade já mencionados, outros podem ser adotados conforme a natureza do objeto a ser contratado. Neste caso, as exigências e/ou obrigações referentes aos critérios e práticas de sustentabilidade são moldadas às peculiaridades de cada objeto.

Da exigência de carta de solidariedade

4.33 Esta exigência não se aplica a este processo de contratação.

Subcontratação

4.34 Não é admitida a subcontratação do objeto contratual.

4.34.1 Decidiu-se pela vedação de subcontratação por conta da impossibilidade de se definir que o parcelamento do objeto, consolidando o estabelecimento de que a subcontratação não é viável do ponto de vista técnico e financeiro.

4.34.2 Essa decisão visa reduzir o risco de problemas técnicos, financeiros, de gestão e de fiscalização desta contratação que estariam associados a uma possível separação/desmembramento dos serviços técnicos sem a existência de elementos e de maturidade suficientes para garantir a vantajosidade.

Da verificação de amostra do objeto

4.35 Será realizada verificação de amostra do objeto para averiguar se a Solução de TIC apresentada pela Licitante detém os requisitos mínimos necessários para realização dos serviços a serem contratados, de acordo com as funcionalidades, procedimentos e critérios objetivos descritos no ANEXO **I - E-TERMO DE RECEBIMENTO DEFINITIVO**, deste Termo de Referência.

4.35 Serão exigidas amostras do objeto referentes aos seguintes itens:

4.35.1 Todos os itens descritos neste Termo de Referência.

Garantia da Contratação

4.36 Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual e condições descritas nas cláusulas do contrato.

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

4.38 A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 10 dias úteis após a assinatura do contrato.

4.39 O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

Informações relevantes para o dimensionamento e apresentação da proposta

4.40 A demanda do órgão tem como base as seguintes características:

4.40.1 A PROPOSTA de preços deverá ser apresentada de acordo com o modelo ANEXO I-A, contendo o resumo da proposta de preços – observando estritamente a descrição dos itens e os quantitativos listados neste TERMO DE REFERÊNCIA, de forma a garantir a permitir seu adequado julgamento – e a documentação técnica da solução ofertada. A PROPOSTA TÉCNICA E DE PREÇOS deverá ter prazo de validade não inferior a 60 (SESSENTA) DIAS CORRIDOS a partir da data da sessão pública.

4.40.2 Nos preços cotados deverão estar incluídas todas as despesas direta e indiretamente envolvidas na execução dos serviços, tais como: transporte, seguros, salários, encargos sociais, encargos fiscais e taxas comerciais, impostos, taxas de contribuição, tarifas públicas e quaisquer outros custos, quando aplicáveis, necessários ao integral cumprimento do objeto contratado. Deverão estar contidos ainda todos os custos marginais referentes aos profissionais eventualmente designados para a prestação dos serviços, tais como: deslocamentos, hospedagens, treinamentos, etc.

4.40.3 A LICITANTE deverá declarar, no momento de sua PROPOSTA, que possui capacidade técnica adequada para executar o objeto da licitação atendendo aos critérios de qualidade e aos níveis mínimos de serviço exigidos, cumprindo os requisitos especificados para a presente contratação.

4.40.4 A PROPOSTA deverá ser redigida em Língua Portuguesa (pt-BR), salvo quanto às expressões técnicas de uso corrente, sem emendas, rasuras ou entrelinhas, devidamente datada, sendo clara e precisa, sem alternativas de preços ou qualquer outra condição que induza o julgamento a ter mais de um resultado, com todos os preços expressos em REAIS (R$) e declaração expressa de que os serviços ofertados atendem aos requisitos técnicos especificados no TERMO DE REFERÊNCIA.

4.40.5 O LICITANTE é o único responsável pelas informações sobre tributos. Não caberá qualquer reivindicação para majoração de preços em virtude de possíveis equívocos cometidos. Firmado o CONTRATO, será admitida correção/alteração de preços quando houver alteração da respectiva legislação tributária que rege a operação objeto do instrumento contratual OU quando tais alterações se derem após a data estabelecida para apresentação da PROPOSTA.

Requisitos Gerais dos Serviços

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

4.42 O objeto de contratação dos SERVIÇOS GERENCIADOS DE SEGURANÇA consiste na prestação dos seguintes serviços: Item 01: Serviço de monitoramento e visibilidade de ataques cibernéticos e Item 02: Serviço de monitoramento, detecção e resposta a incidentes.

4.43 Os requisitos gerais dos serviços definem os requisitos obrigatórios para todos os serviços que compõem os itens 01 e 02.

4.44 OPERAÇÃO E SUSTENTAÇÃO DE SEGURANÇA CIBERNÉTICA

4.44.1 Tem por objetivo sustentar e operar todas as soluções e serviços de segurança envolvidos neste processo de contratação, trabalhando em conjunto com times de sustentação da CONTRATANTE para agregar inteligência e eficiência.

4.44.2 Principais atividades a serem executadas de forma contínua pela CONTRATADA:

4.44.2.1 Acompanhar a execução dos serviços para o cumprimento dos níveis de serviço estabelecidos;
4.44.2.2 Priorizar os atendimentos críticos, conforme definição da CONTRATANTE;
4.44.2.3 Monitorar de forma permanente e realizar avaliações críticas sobre os produtos e serviços de segurança da CONTRATANTE;
4.44.2.4 Traçar curvas de comportamento, definir a volumetria média de acessos e identificar comportamentos não usuais, visando antecipar a identificação de incidentes de segurança, antes mesmo de impacto nos serviços;
4.44.2.5 Atuar proativamente na antecipação e identificação de incidentes de segurança, antes mesmo do impacto nos serviços;
4.44.2.6 Reagir aos eventos de Segurança da Informação que possam afetar a disponibilidade, integridade e confidencialidade das informações existentes nos sistemas ou serviços de TI da CONTRATANTE;
4.44.2.7 Atuar quando ocorrer a falha dos controles de segurança ou situação previamente desconhecida e que tenha probabilidade de comprometer os sistemas e serviços de TI;
4.44.2.8 Prover os fiscais do contrato com os relatórios técnicos e gerenciais suficientes para a comprovação dos serviços realizados;
4.44.2.9 Supervisionar sua equipe na execução dos serviços executados;
4.44.2.10 Orientar a atuação da equipe técnica em situações críticas de trabalho, bem como interagir com os usuários quando a situação requerer;
4.44.2.11 Fornecer sugestões e auxiliar na construção e manutenção contínua, com o apoio e aprovação da CONTRATANTE, de procedimentos sistematizados e da base de conhecimento, contemplando todas as soluções de problemas resolvidos com respostas padronizadas;
4.44.2.12 Consolidar em manuais de procedimentos e em base de conhecimento todas as soluções adotadas na execução das atividades;
4.44.2.13 Implantar as melhorias solicitadas pelos servidores da CONTRATANTE através das

aberturas de chamados no sistema de gestão de serviços de TI;
4.44.2.14 Sugerir novas tecnologias para modernizar o ambiente tecnológico, buscando subsidiar a equipe da CONTRATANTE na gestão de segurança da informação;
4.44.2.15 Manter atualizado o Configuration Management Database (CMDB) na ferramenta de Gerenciamento de Serviços de TI utilizada pelA CONTRATANTE;
4.44.2.16 Administrar todas as soluções envolvidas na contratação em questão;
4.44.2.17 Abrir chamados técnicos para os serviços de suporte técnico remoto das soluções de hardware e software relacionados à Segurança da Informação no ambiente tecnológico do CONTRATANTE;
4.44.2.18 Realizar as atividades em estrita observância na Política de Segurança da Informação (PSI) e demais normas estipuladas pelo CONTRATANTE;
4.44.2.19 Implantar as melhorias solicitadas pelos servidores do CONTRATANTE;
4.44.2.20 Participar, quando solicitado, de reunião com os gerentes e participantes dos projetos de desenvolvimento e manutenção de sistemas e administração de dados, a fim de prover soluções para projetos/atividades em andamento;
4.44.2.21 Realizar de forma contínua análise de vulnerabilidades, apontando todas as correções que precisam ser realizadas. Tal serviço deve também priorizar aquilo que representa maior criticidade ao ambiente da CONTRATANTE;
4.44.2.22 A CONTRATADA deverá realizar a gestão de privilégios de todas as aplicações executadas nas estações de trabalho e servidores Windows, de forma a permitir que apenas aplicações válidas tenham poder de execução;
4.44.2.23 A CONTRATADA deverá fazer a gestão do controle de acesso a rede de forma contínua, interagindo com o time de redes da CONTRATANTE, de forma a manter processos eficazes de descoberta, classificação e avaliação de postura de dispositivos que acessam a rede, contribuindo também para criação de processos que venham permitir o fácil controle /isolamento de dispositivos que venham a fornecer riscos para o ambiente.

4.44.3 Execução de mudanças de configuração nos ativos sob sua administração

4.44.4 Execução das atividades relativas aos normativos e governança da CONTRATANTE naquilo que for relativo à sua área de atuação.

4.44.5 As atividades abaixo deverão ser realizadas de forma contínua, a fim de manter o processo de melhoria contínua no que tange segurança da informação:

4.44.5.1 Implementação, sustentação e administração da solução de SIEM;
4.44.5.2 Configuração de repositórios e processamento de logs/eventos;
4.44.5.3 Criação/envio de procedimentos para envio de logs para soluções administradas por equipes terceiras;
4.44.5.4 Customização da interpretação dos logs sempre que necessário;
4.44.5.5 Criação/configuração de alertas para cada tipo de log processado;
4.44.5.6 Monitoramento de saúde de recebimento de logs de todas as fontes configuradas para envio;
4.44.5.7 Configuração e disponibilização dos agentes de privilégios;
4.44.5.8 Criação/Manutenção de regras de detecção;
4.44.5.9 Implementação, sustentação e administração da solução de gestão de vulnerabilidades;
4.44.5.10 Implementação, sustentação e administração da solução de controle de acesso à rede;
4.44.5.11 Configurar políticas para análise e correção de posturas indesejadas;
4.44.5.12 Apontar vulnerabilidades por ordem de criticidade e acompanhar o processo de remediação das mesmas.

4.44.6 A CONTRATADA deverá acionar o fabricante das ferramentas sempre que necessário, sem nenhum custo adicional para a CONTRATANTE.

4.44.7 Qualquer atividade técnica, referente aos serviços contratados neste certame que eventualmente não tenham sido listados, também serão de responsabilidade da CONTRATADA.

4.44.8 Fica fora do escopo da CONTRATADA apenas atividades referentes a interações referente às ferramentas de rede e infraestrutura da CONTRATADA, onde os times de sustentação local deverão ser acionados para qualquer tratativa necessária.

4.44.9 A fim de evitar *misinformation combat* (conflito de informações) ante a uma campanha de ataque em curso, independentemente da natureza da CONTRATADA vencedora do item 01 e do do item 02, a integração das duas, respectivas disciplinas contempladas pelos itens (*Cyber Threat Intelligence and Hunting* - Inteligência Cibernética de Caça a Ameaças - e *Cybersecurity Incident Management* - Gerenciamento de Incidentes de Segurança da Informação) deve ser, obrigatoriamente, fortalecida em um ritmo sinérgico de colaboração e produção de resultados sob a pena de sanções ou glosas apropriadas.

4.45 GESTÃO DE INCIDENTES DE SEGURANÇA

4.45.1 Tem por objetivo analisar, remediar, conter e documentar os eventos de segurança da informação que foram transformados em um incidente de segurança da informação. Tal serviço deverá ser executado obedecendo os frameworks NIST e SANS de resposta a incidentes de segurança da informação e boas práticas de mercado.

4.45.2 Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação do CONTRATANTE, levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade.

4.45.3 O início do processo de resposta a incidente de segurança se dará, sempre que um evento adverso for detectado pelas plataformas responsáveis ou através do serviço de monitoramento, porém não se limitando a estes. Poderá o corpo técnico de segurança do CONTRATANTE a qualquer tempo, abrir um incidente de segurança.

4.45.4 Após o incidente de segurança aberto, será de responsabilidade do grupo de resposta a incidente de segurança da CONTRATADA, analisar os logs e artefatos enviados, a fim de no primeiro instante identificar as fontes geradoras de tais logs.

4.45.5 Uma vez realizado as análises iniciais do incidente gerado, o grupo de resposta a incidente de segurança da CONTRATADA, deverá trabalhar para identificar quais foram os principais vetores de ataque ao ambiente do CONTRATANTE.

4.45.6 Como próximo passo o grupo de resposta a incidente de segurança da CONTRATADA, deverá comunicar ao time de segurança da informação do CONTRATANTE as informações iniciais sobre o incidente de segurança gerado, e quais serão as linhas de atuação para solução do incidente.

4.45.7 Juntamente com o CONTRATANTE o grupo de resposta a incidente de segurança da CONTRATADA, deverá definir a severidade do incidente de segurança. A severidade do incidente de segurança da informação será definida através da combinação de urgência e impacto, onde impacto é definido como a medida de criticidade do negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente.

4.45.8 Após análises iniciais do incidente, caberá ao o grupo de resposta a incidente de segurança, realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e/ou artefato (malware).

4.45.9 Todo o processo de análise e resultados obtidos devem ser documentados a todo tempo na ferramenta de gestão de incidentes da segurança da informação, para que o CONTRATANTE acompanhe todos os passos para a solução do incidente.

4.45.10 Uma vez identificado o comportamento e os principais vetores de ataque, o grupo de resposta a incidentes de segurança da CONTRATADA deverá definir e executar uma estratégia para a mitigação e contenção do ataque em questão. Caso seja necessário qualquer tipo de alteração no parque computacional do CONTRATANTE, para contenção e mitigação do incidente, deverá antes ser autorizado tal alteração pelo corpo técnico de segurança do CONTRATANTE.

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

4.45.12 Deve-se reunir os dados coletados durante o processo de tratamento de incidente, para iniciar o processo de análise forense do mesmo, ainda pelo grupo de resposta a incidentes de

segurança. Tal análise deve ser realizada com o objetivo de identificar (pessoas, locais e/ou eventos), correlacionando todas as informações reunidas, e gerando como produto final um laudo sobre o incidente de segurança em questão.

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

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

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

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

4.45.16.1 Pesquisar novos tipos de ataques, vírus, malwares, Botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela CONTRATADA;
4.45.16.2 Criar, em colaboração com a CONTRATANTE, casos de uso (regras) que devem ser implementados no SIEM fornecido;
4.45.16.3 Revisar periodicamente as regras do SIEM, realizando as adaptações e evoluções necessárias;
4.45.16.4 Produzir e entregar informação de inteligência acionável, na forma de procedimentos para triagem de alertas e procedimentos para resposta a incidentes, correspondentes às regras do SIEM;

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

4.45.17.1 Relatórios de ameaças e segurança;
4.45.17.2 Relatórios de Botnets e centros de Comando e Controle;
4.45.17.3 Identificação de exploit kits;
4.45.17.4 Indicadores de ataques “ZeroDays” ;
4.45.17.5 Indicadores de comprometimento, suspeitas e avisos informativos;
4.45.17.6 Inteligência de tendências;
4.45.17.7 Proxies anônimos;
4.45.17.8 Classificação de sites;
4.45.17.9 Endereços de rede TOR.

4.46 VALIDAÇÃO DE SEGURANÇA

4.46.1 Os profissionais alocados deverão realizar testes, a partir da solução de validação de segurança, para verificar se os ativos de segurança estão respondendo a ameaças cibernéticas existentes.

4.46.2 O serviço deve ser capaz de testar a eficiência dos ativos de segurança em ambiente de produção, executando simulações de ataque entre seus componentes de software distribuídos, sem causar danos ou degradação do ambiente.

4.46.3 Tais testes devem ser contínuos a fim de criar uma *baseline* de possíveis modificações nos resultados durante o período contratual.

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

4.46.5 Deve avaliar o nível de segurança fornecido por um grupo de endpoints e ativos de segurança de rede independentemente de fabricante e tecnologia.

4.46.6 Deve executar simulações de ataque entre seus componentes sem iniciar conexões com nenhum servidor, aplicativo ou sistema em produção, a fim de fornecer uma avaliação livre de riscos.

4.46.7 Deve simular ataques, relatar ameaças não bloqueadas e propor medidas de mitigação às ameaças de forma contínua, além de permitir a visualização para cada cenário de ataque;

4.46.8 Para a execução de exploração de vulnerabilidades, Malwares e ataques às aplicações web, devem ser usados “payloads” reais de ataques maliciosos;

4.46.9 Durante a verificação dos controles de segurança de endpoint, devem ser reproduzidos métodos maliciosos usados por APTs (Advanced Persistent Threats) sem que o sistema operacional seja infectado;

4.46.10 Deverão ser realizados testes contínuos de movimentação lateral, de modo a identificar e prevenir possibilidades para atacantes navegarem pela rede corporativa.

4.46.11 Deverão ser realizados testes quanto a efetividades de ataque do tipo command and control, onde o atacante consegue fechar conexão com o centro de controle para efetivação da ação maliciosa.

4.46.12 Deve executar ataques em aplicações Web sobre os protocolos HTTP e HTTPS;

4.46.13 Deve executar ataques de URLs usando protocolo HTTP e HTTPS a partir da Internet ou internamente;

4.46.14 Deverão ser executados testes de acessos a URLs por categorização, de forma a validar a política de acesso web já implementada pela CONTRATANTE.

4.46.15 Deve realizar testes de SMTP, tanto a partir da Internet para o domínio corporativo quanto entre contas de domínios corporativos;

4.46.16 Os testes via SMTP deverão compor campanhas de phishing, de forma a testar a capacidade de resposta dos usuários a ameaças deste gênero.

4.46.17 Deve utilizar técnicas, táticas e procedimentos contidos no MITRE ATT&CK®.

4.46.18 Deve gerar relatórios de todos os ataques realizados, estabelecendo um benchmark de proteção a ser comparado a cada teste, de forma a fornecer relatórios de progresso ou declínio na efetividade das demais tecnologias de proteção em uso.

4.46.19 CANAIS DE COMUNICAÇÃO - Para abertura de solicitações, a CONTRATADA deverá disponibilizar 03 (três) tipos de canais de comunicação, a saber:

Grupo de Tecnologia	Classificação
Linha de telefonia gratuita (0800).	Tipo 1
E-mail com domínio registrado e de propriedade da CONTRATADA.	Tipo 2
Sistema de ITSM do inglês *Information Technology Service Management* (Gerenciamento de Serviços de TI).	Tipo 3

4.46.20 Independente do canal de comunicação utilizado pela ENAP, as solicitações devem ser convergidas, atualizadas, resolvidas e concentradas em um único sistema de ITSM do inglês Information Technology Service Management (Gerenciamento de Serviços de TI). Ou seja, imaginando que a ENAP realize a abertura de uma nova solicitação de serviço via linha telefônica gratuita, no segundo que segue a sua solicitação, a mesma deve constar no sistema de ITSM, assim também deve se proceder com a utilização do canal de comunicação do tipo 2: via e-mail.

4.46.21 Sobre o canal de comunicação do tipo 1: via linha telefonia gratuita (0800), tais ligações obrigatoriamente devem ser atendidas e/ou recepcionadas por uma interface humana, não sendo permitida a utilização de URA (Unidade de Resposta Audível), e/ou qualquer uso de atendimento eletrônico.

4.46.22 Para um eventual cenário de crise, ou seja, onde o negócio fim da ENAP estiver sendo fortemente afetado por um problema envolvendo a segurança da informação, a CONTRATADA deverá disponibilizar uma sala de videoconferência virtual de sua propriedade, onde a qualquer tempo poderá ser utilizada para reuniões emergenciais para tratamento de crises.

4.46.23 Tal sala deve estar disponível via internet e seu acesso deve obrigatoriamente ser criptografado, utilizando protocolo SSL (*Secure Socket Layer*), com certificado digital emitido em nome da CONTRATADA. A CONTRATADA também deve garantir que os canais de comunicação, utilizados pela sala de videoconferência estejam sob protocolos para criptografia dos dados trafegados.

4.46.24 A sala virtual ainda deve ter capacidade para até 10 (dez) pessoas da ENAP simultaneamente, e a fim de evitar eventuais perdas de tempo em momento de crise, a sala deve estar acessível a qualquer tempo, não sendo criada apenas no momento da crise.

4.46.25 Os SERVIÇOS GERENCIADOS DE SEGURANÇA, devem obrigatoriamente serem executados, ofertados, e estarem acessíveis à ENAP em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante todo o período de vigência do contrato.

4.47 GESTÃO DE CATÁLOGO DE SERVIÇO DO AMBIENTE DE SEGURANÇA DA INFORMAÇÃO.

4.47.1 A fim de fornecer uma única fonte de informação sobre os SERVIÇOS GERENCIADOS DE SEGURANÇA, disponíveis para cada grupo de tecnologia dos itens de configuração do parque de segurança da informação da ENAP, se definiu previamente no catálogo de serviços, o qual obrigatoriamente a CONTRATADA deverá ser capaz de entregar. Tal definição pode ser consultada na seção CATÁLOGO DE SERVIÇO e NMS – NÍVEIS MÍNIMOS DE SERVIÇO do presente termo de referência.

4.47.2 É de responsabilidade da CONTRATADA manter, atualizar, revisar, os serviços disponíveis para cada grupo de serviço. As responsabilidades da ENAP estão relacionadas a aprovação de um novo serviço, ou a aposentadoria de um ou mais serviços existentes.

4.47.3 O catálogo de serviço deverá ser mantido e administrado através do sistema de ITSM de responsabilidade da CONTRATADA, estando este disponível de forma online para a ENAP, onde poderá consultar a qualquer tempo os serviços disponíveis. Este sistema deve ser o mesmo descrito no tópico CANAIS DE COMUNICAÇÃO, do presente termo de referência, e obviamente deve seguir os mesmos requisitos técnicos supracitados.

4.47.4 Também se espera que tais revisões de continuidade de um serviço no catálogo de serviços, seja sugerido por parte da CONTRATADA durante a execução do contrato. Todavia, não é de responsabilidade da CONTRATADA a retirada ou inclusão de um serviço, cabendo apenas à ENAP tal ação.

4.48 MODALIDADE DE ATENDIMENTO

4.48.1 A modalidade principal de atendimento será do tipo remota, ou seja, a ser realizada nas dependências da CONTRATADA, obedecendo, obrigatoriamente, os critérios estabelecidos para execução, conforme previstos neste termo de referência.

4.48.2 Eventualmente a ENAP poderá solicitar uma visita técnica, para que um atendimento qualquer possa ser realizado e/ou acompanhado em suas dependências físicas.

4.48.3 Os atendimentos referentes ao objeto contratado, denominado SERVIÇOS GERENCIADOS DE SEGURANÇA é ilimitado durante o período de vigência do contrato, ou seja, não existe limite para quantidade de horas, e/ou quantidade de atendimentos realizados.

4.49 ACESSIBILIDADE E CONFIDENCIALIDADE

4.49.1 Para garantir a qualidade e disponibilidade dos serviços remotos, entre a ENAP e os 02 (dois) Centros de Operações de Segurança da CONTRATADA, deverá haver ao menos dois tipos de conexão digital, sendo do tipo internet ou do tipo MPLS do inglês Multi-Protocol Label Switching para cada Centro de Operações de Segurança.

4.49.2 A conexão digital deve ter velocidade de upload e download mínima de 50 (cinquenta) Mbps, serem contratadas de operadoras e rotas distintas, e devem ser utilizadas única e exclusivamente para prestação dos SERVIÇOS GERENCIADOS DE SEGURANÇA da ENAP.

4.49.3 Especificamente para o tipo de conexão digital internet, necessariamente precisará ter IP dedicado, e não serão aceitos contratos com linksxDSL (executada a tecnologia HDSL). Também a fim de garantir a disponibilidade da conexão, deverá a contratada garantir que tal conexão esteja protegida contra ataques de DDoS do inglês *Distributed Denial of Service*.

4.49.4 Em qualquer que seja o tipo de conexão, será de responsabilidade da CONTRATADA, a contratação junto as devidas operadoras, bem como seus devidos custos durante todo o período de vigência do contrato.

4.49.5 A fim de garantir a segurança do tráfego bidirecional entre a ENAP e os Centros de Operações de Segurança da CONTRATADA, as conexões (Internet e MPLS) devem ser criptografadas. Ou seja, a CONTRATADA deverá estabelecer duas VPN's do inglês *virtual private network*, do tipo site to site, para cada Centro de Operações de Segurança.

4.49.6 A fim de garantir a segurança entre a ENAP e os Centro de Operações de Segurança da CONTRATADA, não será permitido o Centro de Operações de Segurança terceirizado ou consórcio de empresas.

4.49.7 Por outro lado, a CONTRATADA deve revogar todas as credenciais relacionadas a soluções de responsabilidade da CONTRATADA, geridas no item 02, empregadas na prestação de serviços à ENAP, bem como solicitar a revogação destas à ENAP, para soluções de responsabilidade da CONTRATADA, no mesmo dia do encerramento das atividades.

4.49.8 Tais exigências visam proteger a ENAP contra o uso indevido de informações sob sua custódia, por parte de profissional da CONTRATADA, assim como estão em conformidade com boas práticas de gestão e governança de TI.

4.50 CENTRO DE OPERAÇÕES DE CIBERSEGURANÇA:

4.50.1 Os serviços gerenciados de segurança devem ser executados por meio de 02 (dois) Centros de Operações de Segurança redundantes, próprios da CONTRATADA, sendo ambos obrigatoriamente no Brasil, de modo que a indisponibilidade de um deles não afete a prestação dos SERVIÇOS GERENCIADOS DE SEGURANÇA, e a no mínimo 300 (trezentos) km de distância geodésica uma da outra e em estados distintos.

4.50.2 A Redundância de dois SOCs deve garantir que, se houver uma falha em um dos centros de operações de segurança, o outro poderá continuar a proteger a ENAP. Isso ajuda a garantir que a CONTRATADA possa responder rapidamente às ameaças que podem ser contidas pelo serviço contratado.

4.50.3 A geolocalização dos SOCs deve garantir que não ocorra interrupções de serviços devido a desastres naturais ou outros eventos que afetem apenas uma determinada região. Outro fator relevante, está designado a inoperabilidade de um determinado SOC pode interromper o monitoramento de ameaças, deixando o ambiente da ENAP exposto a ataques.

4.50.4 Ambos os centros devem atender os mesmos requisitos mínimos, a saber:

4.50.4.1 Utilizar sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA, e cujas imagens possam ser recuperadas;

4.50.4.2 Filmar toda a área, mantendo as imagens armazenadas por, no mínimo, 90 (noventa) dias;

4.50.4.3 Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao Centro de Operações de Segurança;

4.50.4.4 Possuir solução de monitoramento de disponibilidade e desempenho.

4.50.4.5 O perímetro físico dos Centros de operações de Segurança deve ser equipado com sensor de intrusão e alarmes contra acesso indevido;

4.50.4.6 Ser vigiado de forma ininterrupta por segurança física especializada em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;

4.50.4.7 Ter controle de acesso físico com pelo menos 02 (dois) dos seguintes fatores de autenticação, a saber: cartão de identificação magnético, biometria de leitura digital ou análise de retina;

4.50.4.8 Funcionar em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;

4.50.4.9 Possuir registro de entrada e saída de pessoas, mantido por pelo menos 90 (noventa) dias.

4.50.4.10 Possuir sistemas redundantes para armazenamento de dados e alimentação de energia.

4.50.4.11 Possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados por, no mínimo, durante todo o período de vigência contratual.

4.50.4.12 Ser configurado de forma que a falha de um dos equipamentos, isoladamente, NÃO interrompa a prestação dos serviços;

4.50.4.13 Ter sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPSs do inglês Uninterruptible Power Supply, para garantir a transição entre o fornecimento normal da energia e o grupo gerador;

4.50.4.14 Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;

4.50.4.15 Não possuir campo físico visual externo das suas instalações, a fim de garantir que as informações exibidas em monitores, estejam inacessíveis a leituras e a capturas externas desautorizadas;

4.50.4.16 Possuir ambiente dedicado único e exclusivo para laboratório, onde seja possível reproduzir os incidentes e problemas da ENAP, sem que haja impacto na operação do Centro de Operações de Segurança e/ou do própria ENAP;

4.50.4.17 Possuir no Centro de Operações de Segurança processos consistentes e objetivos de monitoramento e detecção de ameaças, gestão de dispositivos, gestão de incidentes, inteligência de ameaças, investigação de ameaças e gestão de conformidade de segurança.

4.50.4.18 Possuir nativamente solução de SecOps para gerenciamento de incidentes de segurança da informação.

4.50.5 Deverá possuir processos implementados que garantam a segurança das normas ABNT NBR ISO /IEC 27001. Tal certificação deverá garantir controles rígidos e auditáveis de acesso físico e lógico às informações e monitoramento;

4.50.6 Ao menos 01 (um) Centro de Operações de Segurança da CONTRATADA deverá possuir as características das certificações listadas na tabela abaixo. Tais características garantem que a CONTRATADA segue os principais controles de segurança da informação, bem como também possui processos para tratamento de incidentes e problemas bem estabelecidos, além de boa qualidade de atendimento e interface com a ENAP.

4.50.7 Certificações:

Item	Certificações
1	ABNT NBR ISO/IEC 27001

2	ABNT NBR ISO/IEC 20000
3	ABNT NBR ISO/IEC 9001

4.50.8 A fim de garantir a disponibilidade das ferramentas e soluções utilizadas para a execução do objeto do presente termo de referência, ambos os CENTRO DE OPERAÇÕES DE SEGURANÇA devem utilizar as infraestruturas de *datacenters* distintos, ou seja, dois ou mais *datacenters*.

4.50.9 Ao menos um dos Data Centers deve possuir as seguintes certificações ou normas, a saber:

Item	Certificações	Descrição
1	ABNT NBR ISO/IEC 27001, 20000 e 9001	Norma que especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI (Sistema de Gestão de Segurança da Informação) documentado dentro do contexto dos riscos de negócio globais da organização.

4.50.10 O segundo datacenter pode estar situado fora dos ambientes dos CENTROS DE OPERAÇÕES DE SEGURANÇA, e deve possuir as seguintes certificações ou normas, a saber:

Item	Certificações	Descrição
1	ABNT NBR ISO/IEC 27001	Norma que especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI (Sistema de Gestão de Segurança da Informação) documentado dentro do contexto dos riscos de negócio globais da organização.
2	ABNT NBR ISO/IEC 22301	Norma de gestão da continuidade de negócios especifica os requisitos para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um sistema de gestão documentado para se proteger, reduzir a possibilidade de ocorrência, preparar-se, responder, e recuperar-se de incidentes de interrupção quando estes ocorrerem.

4.51 PORTAL DE INDICADORES DE SERVIÇO

4.51.1 O portal de indicadores deverá ser disponibilizado à ENAP deverá contemplando, no mínimo, os requisitos abaixo:

4.51.1.1 A CONTRATADA deverá disponibilizar um sistema em modelo SaaS (do inglês *Software as a Service*), denominado portal de indicadores, para consolidação dos dados gerados pelas soluções que compõem o objeto.

4.51.1.2 O portal deverá estar acessível a CONTRATADA via internet, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, e 365 (trezentos e sessenta e cinco) dias por ano, de maneira segura utilizando protocolo de criptografia SSL.

4.51.1.3 A ENAP terá direito a criação de usuários ilimitados com a função de criação de perfis para cada usuário, disponibilizando assim visões diferentes para cada nível de acesso.

4.51.1.4 Deverá disponibilizar para os usuários da ENAP, a função de mudança de visão gráfica a critério de cada usuário. Isso quer dizer que apesar de um gráfico está disposto em modelo de barras, caso o usuário identifique uma melhor visualização do modelo gráfico em forma de pizza, o sistema deve oferecer tal funcionalidade ou opção.

4.51.2 O portal ainda deverá disponibilizar os seguintes modelos gráficos para os usuários:

4.51.2.1 Gráfico do tipo Pizza
4.51.2.2 Gráfico do tipo Barra
4.51.2.3 Gráfico do tipo linha
4.51.2.4 Gráfico do tipo área
4.51.2.5 Gráfico do tipo funil
4.51.2.6 Gráfico do tipo bolha

4.52 INDICADORES DE RISCO – KRI:

4.52.1 Deverá ser exibido no portal a quantidade de vulnerabilidades que estavam presentes na última auditoria realizada através de gráfico(s) com separação dos tipos/quantidades com a opção de "*Drill Down*", possibilitando assim visualização de forma mais detalhada das vulnerabilidades listadas;

4.52.2 O portal deverá possuir recurso para filtrar apenas as vulnerabilidades relevantes, excluindo as de severidade média e/ou baixa.

4.53 INDICADORES DE META E PERFORMANCE – KGI e KPI:

4.53.1 O portal de indicadores deverá possuir relatório gráfico indicando tempo médio dos atendimentos dos incidentes por fase de Análise, contenção, erradicação e recuperação, possibilitando a filtragem por período:

4.53.1.1 Últimos 15 dias;
4.53.1.2 Últimos 30 dias;
4.53.1.3 Últimos 45 dias;

4.53.2 Deverá possuir gráfico comparativo entre os primeiros e últimos 15 incidentes analisados dentro de período filtrado, mostrando uma linha de tempo qual foi o incidente com o tempo de atendimento menor, maior e o tempo médio.

4.53.3 Deverá ser possível a consulta deste gráfico para cada uma das fases de atendimento (Análise, contenção, erradicação e recuperação).

4.54 INDICADORES POR CATEGORIA:

4.54.1 O Portal de indicadores deverá possuir gráfico que separe e classifique os incidentes de acordo com as categorias existentes no processo de resposta a incidentes, sendo elas no mínimo:

4.54.1.1 Origem do Incidente;
4.54.1.2 Status do Incidente;
4.54.1.3 Prioridade do Incidente;
4.54.1.4 Risco;
4.54.1.5 Grupo de Atendimento;

4.54.2 Todos os indicadores exibidos pelo portal, devem possuir a funcionalidade drill down, para que os usuários possam criar visualizações e filtros dos dados exibidos.

4.54.3 Todos os indicadores exibidos pelo portal, devem ainda possuir funcionalidade de exibição dos dados gerados do gráfico de maneira tabular, a fim de que seja possível aferir os dados brutos.

4.54.4 A qualquer tempo a ENAP poderá solicitar os dados brutos coletados das soluções que compõem o objeto contratado.

4.54.5 Os dados exibidos pelo portal devem representar o ambiente em tempo de execução e de forma automática (real time).

4.54.6 Deverá prover mecanismo para análise de risco e métricas de disponibilidade através de relatórios e dashboards de todas as soluções que compõem o objeto.

4.55 DAS CONDIÇÕES PARA ASSINATURA DO PEDIDO DE FORNECIMENTO:

4.55.1 Quando da convocação para assinatura do Pedido de Fornecimento, no prazo de até 05 (cinco) dias úteis contados da data do recebimento da convocação, prorrogável por igual período, a licitante deverá providenciar, como condição para a assinatura do Pedido de Fornecimento.

4.55.2 A CONTRATADA deverá providenciar, como condição para a assinatura do Pedido de Fornecimento declaração, datada e assinada por seu representante legal, atender plenamente todos os itens do termo de referência.

4.56 DA APRESENTAÇÃO DE CATÁLOGOS

4.56.1 A licitante deverá, antes da disputa pública, juntamente com a proposta, apresentar os manuais, catálogos, folders, ou outros documentos técnicos, ou ainda, links públicos oficiais da solução exigida ou do serviço exigido, para comprovação do atendimento às características técnicas especificadas neste Termo de Referência.

4.56.2 Deverá ser fornecido uma tabela junto à proposta comercial com a comprovação de todos os itens das especificações técnicas indicando documento ou link público com seu devido trecho e página.

4.56.3 No conjunto de documentos apresentados pela licitante (folders/catálogos), para fins de aceitação pela ENAP, deverá vir indicando corretamente, o item, especificação, link ou documento, página e trecho que comprove o atendimento de cada item/subitem das especificações técnicas descritas nos serviços a serem ofertado, conforme modelo abaixo. Será aceito também carta do fabricante com as comprovações, desde que não ultrapasse 5% dos itens técnicos deste termo de referência.

4.56.4 Deverá apresentar com clareza a marca, o modelo, o tipo, a configuração e outras informações aplicáveis e necessárias à perfeita caracterização do dispositivo, serviço ou componente proposto, de forma a permitir a correta identificação deste na documentação técnica apresentada, conforme modelo de comprovação técnica:

Item	Especificação	Link ou Documento	Trecho	Página

4.56.5 A CONTRATADA deveria apresentar carta que demonstre que ela é empresa parceira de todas as soluções ofertadas.

4.56.6 Os documentos serão analisados, para fins de verificação do atendimento às características da solução especificados neste Edital.

4.56.7 A análise das características dos itens ofertados será procedida em cotejo com as especificações técnicas constantes deste instrumento, não sendo admitidos itens com especificações inferiores.

4.56.8 Os itens desprovidos dos documentos relacionados no item anterior, serão passíveis de diligência, podendo, para tanto, a ENAP se valer de todos os meios possíveis, tais como consulta a site diversos, ligações a fabricantes ou exigência de documentos complementares, dentre outros.

4.56.9 Caso os documentos apresentados não sejam aprovados, por não atenderem às especificações previstas neste Edital, o licitante será convocado a apresentar novo item, acompanhado de documentos que atendam às especificações requeridas, no mesmo prazo fixado para apresentação inicial, sem ônus à ENAP, contados da devolução com as instruções ou observações feitas pela ENAP, sob pena de desclassificação.

4.56.10 Caso a 2ª apresentação não atenda às especificações técnicas exigidas neste Edital, a proposta da licitante será considerada inaceitável pelo Pregoeiro, sendo, portanto, desclassificada.

4.56.11 Na hipótese de a proposta da licitante ser desclassificada, por não atendimento das especificações técnicas requeridas, serão convocadas as demais licitantes, obedecendo-se rigorosamente a ordem de classificação das propostas, seguindo-se aos mesmos moldes descritos nos itens anteriores.

4.56.12 A licitante vencedora que vier a ser contratada ficará obrigada ao cumprimento integral de sua proposta, ainda que algum item não tenham sido objeto de verificação na análise do manual/catálogo/folder.

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;

5.1.9 Efetuar as retenções tributárias devidas sobre o valor da fatura de serviços da contratada, em conformidade com o Anexo XI, Item 6 da IN SEGES/MP nº 5 /2017;

5.1.10 Não praticar atos de ingerência na administração da contratada, tais como:

5.1.10.1 exercer o poder de mando sobre os empregados da Contratada, devendo reportar-se somente aos prepostos ou responsáveis por ela indicados, exceto quando o objeto da contratação previr o atendimento direto, tais como nos serviços de recepção e apoio ao usuário;

5.1.10.2 direcionar a contratação de pessoas para trabalhar nas empresas Contratadas;

5.1.10.3 promover ou aceitar o desvio de funções dos trabalhadores da Contratada, mediante a utilização destes em atividades distintas daquelas previstas no objeto da contratação e em relação à função específica para a qual o trabalhador foi contratado;

5.1.10.4 considerar os trabalhadores da contratada como colaboradores eventuais do próprio órgão ou entidade responsável pela contratação, especialmente para efeito de concessão de diárias e passagens.

5.1.10.5 Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato;

5.1.10.6 Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento;

5.1.11 O término da vigência do contrato não exonera a CONTRATADA de sua responsabilidade em promover e assegurar a assistência técnica da garantia, estando sujeita, na hipótese do descumprimento da responsabilidade assumida e mesmo depois de expirada a vigência do contrato, às penalidades previstas neste Termo de Referência, sem prejuízo de eventual responsabilidade civil e penal.

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 responsabilizar-se pelo ônus e a logística da retirada e devolução dos equipamentos para realização de serviços de garantia fora das dependências da CONTRATANTE, bem como da substituição de equipamentos ou software não aceitos;

5.2.10 efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência e seus anexos, bem como naquelas resultantes de sua proposta, devendo já estar inclusos nos valores propostos todos os custos, impostos, taxas e demais encargos pertinentes à execução do objeto do contrato, não sendo aceitas quaisquer modificações, acompanhado da respectiva Nota Fiscal;

5.2.11 garantir o perfeito funcionamento da solução, compreendendo também a instalação e configuração dos equipamentos no local, não cabendo ônus adicional à CONTRATANTE. Entende-se como perfeito funcionamento: compatibilidade do objeto com todas as descrições exigidas deste Termo de Referência e seus anexos, bem como o atendimento às exigências da legislação vigente.

5.2.12 fazer a transição contratual, quando for o caso;

5.3 Durante a vigência contratual, e toda a prestação do serviço objeto desta contratação, deverão ser observados e cumpridos os seguintes papéis e responsabilidades dos profissionais:

5.3.1 Patrocinador do Projeto (ENAP): é o gerente da Unidade de Tecnologia da Informação (UTIC), responsável por representar os interesses da ENAP no contexto da presente contratação, pela aprovação da necessidade, dos objetivos e, por fim, pela negociação das ações necessárias para a melhoria da Governança de TI;

5.3.2 Gestor do Contrato (ENAP): é o funcionário formalmente designado pela ENAP E, responsável pelo monitoramento da prestação do serviço ao longo do período de vigência do contrato, pelo controle da evolução dos gastos com o contrato, pela proposição de aditamentos ao contrato, pela participação no planejamento da contratação, pela verificação dos resultados pretendidos, e por garantir que a metodologia adequada seja empregada;

5.3.3 Gerente da Demanda (ENAP): é o funcionário da CGTI/ENAP que aprova a execução do serviço, executa os processos de gerenciamento, monitoramento e controla o andamento de projetos. Auxilia as equipes terceirizadas a remover eventuais obstáculos que possam impedir a equipe de produzir, garantindo o foco no resultado. Zela pela colaboração entre os diferentes papéis e pela melhoria dos processos, atuando sempre como um facilitador. É quem fornece insumos ao Gestor do Contrato quanto à regular execução do serviço prestado, em relação aos níveis de serviço esperados, e às demais disposições contratuais;

5.3.4 Gestor de Negócio (ENAP): é o funcionário da unidade de negócio da ENAP que representa e/ou assessora o demandante do produto. Responsável pela liderança do produto que será desenvolvido, priorizando as funcionalidades que agregam maior valor para o negócio. Tem também o papel de elucidar questões relacionadas ao negócio junto ao Fornecedor de Serviço, como também homologar os produtos entregues.

5.3.5 Gestor de Negócio (ENAP): é o funcionário da unidade de negócio da ENAP que representa e/ou assessora o demandante do produto. Responsável pela liderança do produto que será desenvolvido, priorizando as funcionalidades que agregam maior valor para o negócio. Tem também o papel de elucidar questões relacionadas ao negócio junto ao Fornecedor de Serviço, como também homologar os produtos entregues.

5.3.6 Preposto (CONTRATADA): é o profissional indicado pelo Fornecedor de Serviço para representá-la administrativa e tecnicamente. É o responsável pela coordenação operacional das atividades previstas nos projetos, de forma a solucionar qualquer dúvida, conflito ou desvio técnico que possa comprometer a execução das OS. Deverá ter bons conhecimentos em gestão de projetos para garantir o controle sobre os sinais vitais de cada projeto. Também é responsável pela interlocução com o Gestor do Contrato da ENAP.

6. MODELO DE EXECUÇÃO DO CONTRATO

O Modelo de Execução do Contrato contempla as condições necessárias ao fornecimento da solução de TIC, observando os itens a seguir.

Condições de execução

6.1 A execução do objeto seguirá a seguinte dinâmica:

6.1.1 Início da execução do objeto: 05 (cinco) dias corridos da assinatura do contrato;
6.1.2 Descrição detalhada dos métodos, rotinas, etapas, tecnologias procedimentos, frequência e periodicidade de execução do trabalho: este documento define detalhes da execução dos serviços. Por outro lado, a Contratada deve elaborar e propor Plano de Execução dos Serviços, detalhando a implantação e operação de cada um dos serviços.
6.1.3 Cronograma de realização dos serviços:

6.1.3.1 do item 01:

Item	Cronograma de Atividades da Prestação dos Serviços especializados em Segurança da Informação	Quando ocorre
1	Assinatura do contrato	Dia D
2	Reunião inicial e Apresentação de Plano de Execução dos Serviços	Até 5 (cinco) dias úteis após a assinatura do Contrato, conforme agendamento efetuado pelo Gestor do Contrato
3	Aprovação, pela ENAP, do Plano de Execução dos Serviços	Até 5 (cinco) dias úteis da Apresentação do Plano de Execução dos Serviços
4	Emissão da Ordem de Serviço para os serviços do item 01	Até 5 (cinco) dias úteis da Aprovação, pela ENAP, do Plano de Execução dos Serviços
5	Início da execução dos serviços	Conforme constar na Ordem de Serviços.

6.1.3.2 do item 02:

Item	Cronograma de Atividades da Prestação dos Serviços gerenciados em Segurança da Informação	Quando ocorre
1	Assinatura do contrato	Dia D
2	Reunião inicial e Apresentação de Plano de Execução dos Serviços	Até 5 (cinco) dias úteis após a assinatura do Contrato, conforme agendamento efetuado pelo Gestor do Contrato
3	Aprovação, pela ENAP, do Plano de Execução dos Serviços	Até 5 (cinco) dias úteis da Apresentação do Plano de Execução dos Serviços
4		

	Emissão da Ordem de Serviço para os serviços do item 02	Até 5 (cinco) dias úteis da Aprovação, pela ENAP, do Plano de Execução dos Serviços
5	Início da execução dos serviços	Sob demanda, conforme Ordem de Serviço.

6.1.4 Os serviços devem ser prestados por período integral, ou seja, 7 (sete) dias por semana e 24 (vinte e quatro) horas por dia, enquanto o contrato estiver vigente;
6.1.5 A CONTRATADA deve atentar-se a todos os demais prazos dispostos neste documento.
6.1.6 Documentação Mínima Exigida: a Contratada deverá disponibilizar mensalmente relatórios gerenciais que demonstrem a execução das atividades para que a ENAP possa atestar o provimento dos serviços, consoante disposto na subseção Do Recebimento da seção 8 (CRITÉRIOS DE MEDIÇÃO E PAGAMENTO) constante neste Termo de Referência:

6.1.6.1 Leitura, preenchimento e assinatura do Termo de Ciência expresso pelo ANEXO I-C (MODELO DE TERMO DE CIÊNCIA INDIVIDUAL);
6.1.6.2 Leitura, preenchimento e assinatura do Termo de Compromisso de Manutenção do Sigilo expresso pelo ANEXO I-B (TERMO DE COMPROMISSO DE SIGILO E SEGURANÇA DA INFORMAÇÃO);
6.1.6.3 A entrega da documentação descrita, não exime a LICITANTE/CONTRATADA da entrega das documentações técnicas e habilitatórias do certame.

6.1.7 As condições para a prestação dos serviços são disciplinadas pelas seguintes definições:

6.1.7.1 Independente do item de serviço especificado, todas as soluções e/ou ferramentas utilizadas para prestação do serviço deverão obrigatoriamente seguir os requisitos, a saber:

6.1.7.1.1 Deverá ser obrigatoriamente de propriedade e licenciada em nome CONTRATADA e não serão aceitos serviços entregues por meio de software livre, open-source ou INHOUSE;

6.1.7.1.2 Deverá ser fornecer acesso de leitura, sempre que solicitado, para a ENAP, nas consoles, para auditoria dos serviços prestados, durante toda a vigência do contrato;

6.1.7.1.3 Deverá ser prestado por meio de solução provida através da nuvem do fabricante ou da CONTRATADA;

6.1.7.1.4 Os softwares ofertados devem ser instalados em sua versão mais estável e atualizada e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço. Da mesma maneira, os equipamentos fornecidos para a prestação dos serviços devem estar cobertos por contratos de garantia do fabricante;

6.1.7.1.5 O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade.

Local e horário da prestação dos serviços

6.2 Os serviços serão prestados, via de regra e conforme a natureza dos itens, de maneira presencial (on-site) no ambiente tecnológico da ENAP sendo o ponto de contato com a equipe de Tecnologia da Informação da ENAP, no seguinte endereço Coordenação-Geral de Tecnologia da Informação, localizada no SPO Área especial 2-A - Asa Sul, Ed. ENAP, Brasília - DF, 70610-900.
6.3 Os serviços serão prestados no seguinte horário: 08h às 18h, a princípio, entre segunda-feira e sexta-feira (quando campanhas de ataques ou incidentes não exigirem ações tempestivas e extemporâneas).
6.4 Sempre que solicitado e/ou permitido pela ENAP os serviços poderão ser executados de maneira remota pela CONTRATADA. Desta forma, considerando que os serviços também poderão ser executados

remotamente, a execução das atividades fora das dependências do CONTRATANTE, em nenhuma hipótese, irão gerar custos e obrigações adicionais para pagamento, devendo estes custos serem exclusivos da CONTRATADA.

Materiais a serem disponibilizados

6.5 Para a perfeita execução dos serviços, a Contratada deverá disponibilizar, de forma digital quando couber, os materiais, os equipamentos, as ferramentas, as licenças de software, os acessos, os manuais, os materiais de treinamento e os utensílios necessários, nas quantidades estimadas e qualidades a seguir estabelecidas, promovendo sua substituição quando necessário:

6.5.1 Todos os materiais entregues, disponibilizados e utilizados na transferência de conhecimento, bem como os disponibilizados para consulta, serão concedidos com direito de uso e de reprodução à ENAP, de forma irrestrita, para sua aplicação e uso em treinamentos internos.

Informações relevantes para o dimensionamento da proposta

6.6 A demanda do órgão tem como base as seguintes características:

6.6.1 A PROPOSTA de preços deverá ser apresentada de acordo com o modelo ANEXO I-A (MODELO DE PROPOSTA COMERCIAL), contendo o resumo da proposta de preços – observando estritamente a descrição dos itens e os quantitativos listados no ANEXO I-J (ATIVOS DE INFRAESTRUTURA DE TI DA ENAP) deste TERMO DE REFERÊNCIA, de forma a garantir a permitir seu adequado julgamento – e a documentação técnica da solução ofertada. A PROPOSTA TÉCNICA E DE PREÇOS deverá ter prazo de validade não inferior a 60 (SESSENTA) DIAS CORRIDOS a partir da data da sessão pública;
6.6.2 Nos preços cotados deverão estar incluídas todas as despesas direta e indiretamente envolvidas na execução dos serviços, tais como: transporte, seguros, salários, encargos sociais, encargos fiscais e taxas comerciais, impostos, taxas de contribuição, tarifas públicas e quaisquer outros custos, quando aplicáveis, necessários ao integral cumprimento do objeto contratado. Deverão estar contidos ainda todos os custos marginais referentes aos profissionais eventualmente designados para a prestação dos serviços, tais como: deslocamentos, hospedagens, treinamentos, etc;
6.6.3 A LICITANTE deverá declarar, no momento de sua PROPOSTA, que possui capacidade técnica adequada para executar o objeto da licitação atendendo aos critérios de qualidade e aos níveis mínimos de serviço exigidos, cumprindo os requisitos especificados para a presente contratação;
6.6.4 A PROPOSTA deverá ser redigida em Língua Portuguesa (pt-BR), salvo quanto às expressões técnicas de uso corrente, sem emendas, rasuras ou entrelinhas, devidamente datada, sendo clara e precisa, sem alternativas de preços ou qualquer outra condição que induza o julgamento a ter mais de um resultado, com todos os preços expressos em REAIS (R$) e declaração expressa de que os serviços ofertados atendem aos requisitos técnicos especificados no TERMO DE REFERÊNCIA;
6.6.5 O LICITANTE é o único responsável pelas informações sobre tributos. Não caberá qualquer reivindicação para majoração de preços em virtude de possíveis equívocos cometidos. Firmado o CONTRATO, será admitida correção/alteração de preços quando houver alteração da respectiva legislação tributária que rege a operação objeto do instrumento contratual OU quando tais alterações se derem após a data estabelecida para apresentação da PROPOSTA.

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

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

6.7.1 O início da execução contratual só poderá ocorrer após a apresentação da GARANTIA CONTRATUAL, dentre uma das modalidades definidas no Art. 96, da Lei nº 14.133/2021, em até 05 (cinco) dias úteis da assinatura do CONTRATO.
6.7.2 A inobservância das condições de garantia sujeitará o CONTRATADO às penalidades previstas no Contrato.
6.7.3 A não apresentação do comprovante da garantia, no prazo previsto no caput deste Item, caracteriza descumprimento da obrigação assumida, sujeitando o CONTRATADO às sanções administrativas cabíveis.
6.7.4 O atraso superior a 25 (vinte e cinco) dias autoriza a ENAP a promover a rescisão do Contrato por descumprimento ou cumprimento irregular de suas cláusulas.
6.7.5 A garantia responderá pelo fiel cumprimento das disposições do Contrato, ficando a ENAP

autorizada a executá-la para cobrir o pagamento das obrigações abaixo e de qualquer outra obrigação, inclusive em caso de rescisão:

a) prejuízos advindos do não cumprimento do objeto do Contrato e do não adimplemento das demais obrigações nele previstas;
b) prejuízos causados à ENAP ou a terceiro, decorrentes de culpa ou dolo durante a execução do Contrato;
c) multas moratórias e punitivas aplicadas pela ENAP ao CONTRATADO;
d) obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não adimplidas pelo CONTRATADO.

6.7.6 A perda da garantia em favor da ENAP, por inadimplemento das obrigações contratuais, far-se-á de pleno direito, independentemente de qualquer procedimento judicial e sem prejuízo das demais sanções previstas no Contrato.
6.7.7 Quando houver alteração contratual que implique aumento do preço contratado, a garantia deverá ser integralizada, num prazo máximo de 10 (dez) dias úteis, de modo que corresponda a 5% (cinco por cento) do preço global contratado. No caso de alteração contratual, que configure decréscimo, a alteração na garantia para adequação ao novo valor ocorrerá mediante solicitação do CONTRATADO, respeitado o percentual de 5% (cinco por cento) do novo preço global contratado.
6.7.8 Se o valor da garantia for utilizado pelo CONTRATANTE em pagamento de quaisquer obrigações, inclusive multas contratuais ou indenização a terceiros, o CONTRATADO fica obrigado a fazer a reposição, no prazo máximo de 10 (dez) dias úteis a contar da data do recebimento da comunicação da ENAP.
6.7.9 A garantia prestada ou a parte remanescente somente será liberada ou restituída após 3 (três) meses do término ou rescisão do Contrato, desde que integralmente cumpridas as obrigações assumidas neste Instrumento e que haja a solicitação do CONTRATADO ou a autorização da unidade gestora/fiscalizadora do Contrato.
6.7.10 Será considerada extinta a garantia com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do Contratante, mediante termo circunstanciado, de que o Contratado cumpriu todas as cláusulas do contrato.

Formas de transferência de conhecimento

6.8 A transferência do conhecimento deverá ser realizada observando-se o que segue: toda e qualquer informação produzida no âmbito da execução do objeto do contrato pela CONTRATADA dos serviços será de propriedade da ENAP e fica o CONTRATADO obrigado a documentar e registrar os produtos, serviços e eventos observando as metodologias e ferramentas utilizadas na ENAP;

6.9 Para essa transferência de conhecimento deve-se abordar, no mínimo, os seguintes itens:

1. visão geral de administração e operação da solução;
2. arquitetura da solução: componentes centrais, infraestrutura de rede, configuração e dimensionamento;
3. elementos de segurança: protocolos, criptografia, prevenção de ataques;
4. melhores práticas de segurança e gerenciamento;
5. administração de usuários, grupos e perfis de acesso;
6. procedimentos e rotinas de backup e upgrade da solução;
7. análise de alarmes e troubleshooting;
8. utilização dos canais de suporte técnico disponibilizados;
9. gerenciamento e programação de relatórios;
10. administração de rotinas periódicas para manutenção do ambiente.

6.10 Durante toda execução do contrato e sempre que solicitado pela ENAP, o contratado deverá realizar o repasse de conhecimento diário e formal, quando solicitado, à equipe da ENAP ou empresa por ela designada. Entende-se por conhecimento, todas as informações, documentos, procedimentos, senhas, acessos e processos relacionados ao objeto de execução deste contrato.

6.11 Todos os materiais entregues, disponibilizados e utilizados na transferência de conhecimento, bem como os disponibilizados para consulta, serão concedidos com direito de uso e de reprodução à ENAP, de forma irrestrita, para sua aplicação e uso em treinamentos internos.

6.12 A ENAP não arcará com custos, em hipótese alguma, a exemplo de deslocamento, hospedagem, alimentação ou qualquer outro tipo de custo com o instrutor.

Procedimentos de transição e finalização do contrato

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

EVENTOS DE TRANSIÇÃO CONTRATUAL			
EVENTO	PRAZO DE REFERÊNCIA	DESCRIÇÃO	RESPONSABILIDADE
E1	-	Assinatura do CONTRATO	ENAP/CONTRATADA
E2	E1 + 10 dias	Apresentação da GARANTIA CONTRATUAL	CONTRATADA
E3	E2 + 5 dias	REUNIÃO INICIAL	ENAP/CONTRATADA
E4	E3 + 10 dias	Apresentação do PLANO DE IMPLANTAÇÃO	CONTRATADA
E5	E4 + 10 dias	Início da execução do CONTRATO e implantação da solução	CONTRATADA
E6	E5 + 10 dias	Encerramento da TRANSIÇÃO CONTRATUAL, que coincidirá com o término do período de operação assistida prevista.	CONTRATADA

6.14 Na etapa de transição e finalização contratual, caso da finalização do contrato, seja por rescisão ou por não renovação, o CONTRATADO deverá prestar à ENAP toda a assistência necessária à continuidade dos serviços prestados;

6.14.2 A TRANSIÇÃO CONTRATUAL inicial, a fim de preparar o CONTRATADO a assumir integralmente as obrigações advindas com o CONTRATO, deverá ser viabilizada sem ônus adicional à ENAP, e será baseada em reuniões técnicas e repasse de documentos e/ou manuais específicos das soluções desenvolvidas;

6.14.3 O processo de TRANSIÇÃO CONTRATUAL se inicia a partir do momento em que o CONTRATADO assume as responsabilidades, de forma gradual, pelos serviços prestados, preparando-se para o início efetivo da operação;

6.14.4 A execução dessa etapa de repasse dos serviços deverá ser finalizada em no máximo 30 (trinta) dias corridos a partir do início da prestação dos serviços.

Quantidade mínima de serviços para comparação e controle

6.15 Condição desnecessária porque não será exigida a quantidade mínima de serviços para comparação e controle neste edital, em razão da natureza do objeto.

Mecanismos formais de comunicação

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

6.16.1 Ordem de Serviço: Ordem de Serviço elaborada pela CONTRATANTE, conforme Anexo L - ORDEM DE SERVIÇO OU DE FORNECIMENTO DE BENS constante nos Documentos Auxiliares deste Termo de Referência, e encaminhada via sistema eletrônico SEI, ou por outro meio devidamente acertado na Reunião Inicial no início do contrato;

6.16.2 Ata de Reunião;

6.16.3 Ofício de Comunicação: Ofícios elaborados, por demanda, pela CONTRATANTE para avisar à CONTRATADA, ou vice-versa, de alguma mudança como endereços, telefone de contato ou qualquer informação importante referente aos aspectos legais ou administrativos;

6.16.4 Sistema de abertura de chamados;

6.16.5 Relatórios de Execução dos Serviços Prestados: Conjunto de relatórios elaborados mensalmente pela CONTRATADA e encaminhado ao GESTOR DO CONTRATO;

6.16.6 Relatório de Avaliação Mensal: Relatório elaborado mensalmente pela CONTRATANTE.

6.16.7 Autorização para Faturamento: Autorização emitida pelo GESTOR DO CONTRATO ao PREPOSTO/LÍDER TÉCNICO da CONTRATADA. Este documento contém a autorização para que a CONTRATADA possa efetuar o faturamento.

6.16.8 Relatórios Técnicos de Serviços obrigatórios;

6.16.9 Relatório em que a CONTRATADA descreve sucintamente as atividades executadas durante a execução de suas atividades;

6.16.10 Termo de Recebimento Definitivo: Termo de recebimento definitivo elaborado pela CONTRATANTE e encaminhado via sistema eletrônico SEI, ou por outro meio devidamente acertado na Reunião Inicial, com a função de homologar os serviços e perfis vinculados ao objeto deste Termo de Referência;

6.16.11 Diversos: E-mails elaborados, por demanda, pela CONTRATANTE para avisar à CONTRATADA, ou vice-versa, de qualquer informação importante referente aos aspectos técnicos ou operacionais. Tickets, chamados, requisições e eventos gerados pelas ferramentas computacionais originados e/ou gerenciados pelas soluções automatizadas utilizadas durante a execução contratual;

Formas de Pagamento

6.17 Os critérios de medição e pagamento dos serviços prestados serão tratados em tópico próprio do Modelo de Gestão do Contrato.

Manutenção de Sigilo e Normas de Segurança

6.18 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.

6.19 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 ANEXO I-B – TERMO DE COMPROMISSO DE SIGILO E SEGURANÇA DA INFORMAÇÃO e ANEXO I-C - MODELO DE TERMO DE CIÊNCIA INDIVIDUAL.

Vigência e alterações contratuais

6.20 O prazo de vigência da contratação é de 12 (doze) meses contados da data de assinatura do contrato, prorrogável, caso necessário, por até 5 (cinco) anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

6.21 Para fins de renovação/prorrogação contratual, o GESTOR DO CONTRATO, com base no Histórico de Gestão do Contrato e nos princípios da manutenção da necessidade, economicidade e oportunidade da contratação, deverá encaminhar à Área Administrativa, com pelo menos 60 (SESSENTA) DIAS de antecedência do término do CONTRATO, a respectiva documentação para o aditamento (art. 36 da Instrução Normativa SGD/ME Nº 94 de 23/12/2022).

Da Abrangência e Escopo dos Serviços

6.22 Considerar-se-á, para efeitos desta contratação, todos os recursos necessários para a perfeita execução efetiva da prestação dos serviços.

6.23 O dimensionamento da equipe para a execução adequada do serviço contratado é de responsabilidade exclusiva do Fornecedor de Serviço, devendo ser suficiente para o cumprimento integral dos níveis de serviço exigidos neste Termo de Referência.

6.24 Dependendo da complexidade, criticidade e do prazo do projeto, os serviços poderão ser realizados nas instalações da CONTRATADA ou da ENAP.

6.25 Todos os custos com licenças de simuladores, softwares devem estar contabilizados no valor do serviço, não sendo permitido o pagamento de valores adicionais ou extras, seja a que título for.

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 representante da empresa para adoção de providências que devam ser cumpridas de imediato.

Preposto

7.5 A Contratada 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.

7.5.1 No momento da assinatura do contrato, será exigido da CONTRATADA, a apresentação das documentações do(s) profissionais com perfil de PREPOSTO, as quais devem comprovar as exigências e obrigações descritas neste termo de referência: carteira de trabalho devidamente assinada pela CONTRATADA, para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento conforme TABELA abaixo:

Certificações	Descrição

Ao menos uma das certificações de segurança da informação: **CISSP** (Certified Information Systems Security Professional). **CISM** (Certified Information Security Manager. **CIA** (Certified Intrusion Analyst), **GSEC** (GIAC Security Essentials). **GCIH** (GIAC Incident Handler) **GMON** (GIAC Continuous Monitoring);	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência mínima de 12 (doze) meses em coordenação e gestão de contratos de serviços continuados.

7.6 Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade

Reunião Inicial

7.7 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.
7.8 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 (cinco) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

7.8.1 A pauta desta reunião observará, pelo menos:

7.8.1.1 Presença do representante legal da contratada, que apresentará o seu preposto;
7.8.1.2 Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;
7.8.1.3 esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;
7.8.1.4 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;
7.8.1.5 Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

Fiscalização

7.9 A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput) , nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

Fiscalização Técnica

7.10 O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

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

nº 11.246, de 2022, art. 22, II);
7.10.2 Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);
7.10.3 O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).
7.10.4 No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V).
7.10.5 O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

Fiscalização Administrativa

7.11 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 do contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

7.11.1 Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

Gestor do Contrato

7.12 O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará 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. (Decreto nº 11.246, de 2022, art. 21, IV).

7.13 O gestor do contrato acompanhará 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. (Decreto nº 11.246, de 2022, art. 21, II).

7.14 O gestor do contrato acompanhará a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

7.15 O gestor do contrato emitirá 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. (Decreto nº 11.246, de 2022, art. 21, VIII).

7.16 O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

7.17 O gestor do contrato deverá elaborará relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

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

7.19 Para fins de renovação/prorrogação contratual, o GESTOR DO CONTRATO, com base no Histórico de Gestão do Contrato e nos princípios da manutenção da necessidade, economicidade e oportunidade da contratação, deverá encaminhar à Área Administrativa, com pelo menos 60 (SESSENTA) DIAS de antecedência do término do CONTRATO, a respectiva documentação para o aditamento (art. 36 da Instrução Normativa SGD/ME Nº 94 de 23/12/2022).

Critérios de Aceitação

7.20 O representante do CONTRATANTE deverá ter a qualificação necessária para o acompanhamento e controle da execução dos serviços e do contrato.

7.21 A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência.

7.22 A avaliação dos serviços prestados será feita por meio de indicadores de Níveis de Serviço que refletem o cumprimento de prazos, a disponibilidade dos serviços de Segurança, satisfação e qualidade entre outros aspectos técnicos e de gestão de serviços de Segurança.

7.23 A fiscalização técnica dos contratos avaliará constantemente a execução do contrato, conforme modelo previsto nos Níveis de Serviço, devendo haver o redimensionamento no pagamento com base nos indicadores estabelecidos, sempre que a CONTRATADA:

7.24 Não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou Deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

7.25 Os indicadores e NMS estão detalhados na seção 8 (CRITÉRIOS DE MEDIÇÃO E PAGAMENTO) deste Termo de Referência. Os níveis de serviços estabelecidos poderão ser revisados sempre que houver necessidade, em função do negócio, evolução tecnológica ou, ainda, quando verificada a impropriedade da meta imposta.

7.26 As situações de glosa, se passível de correções, poderão ser realizadas no prazo de 60 (sessenta) dias a contar do prazo de entrega original. Em caso de correção da entrega no prazo, e aceita pela equipe de fiscalização, a CONTRATADA fará jus a reaver 70% (setenta por cento) do valor da glosa.

7.27 Todas as glosas previstas e somadas não poderão ultrapassar 30% (trinta por cento) do valor da fatura mensal.

7.28 A aplicação das glosas, poderá ser feita de forma cumulativa com outras sanções conforme cada caso.

7.29 A CONTRATADA, caso utilize solução própria de ITSM, deverá configurar a extração automatizada de relatórios de indicadores previstos, obtidos a partir das ferramentas de ITSM, de monitoração ou outras que venham a ser adotadas.

7.30 Os mecanismos de extração automatizada de relatórios de indicadores deverão estar disponíveis para que a CGTI/ENAP possa consultar os indicadores a qualquer tempo.

7.31 A CONTRATADA poderá apresentar recurso de glosa para justificar casos fortuitos, contudo, caberá a CONTRATANTE aceitar ou não a justificativa apresentada;

7.32 Os Níveis Mínimos de Serviço (NMS) serão avaliados mensalmente, no processo de fiscalização do contrato, conforme etapas e prazos descritos durante a execução do contrato.

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

8.1 A avaliação da execução do objeto utilizará o Instrumento de Atendimento no Prazo (IAP), conforme o disposto neste item.

IAP – ÍNDICE DE ATENDIMENTO NO PRAZO

Tópico	Descrição
Finalidade	Medir o tempo de atraso na prestação dos serviços constantes na Ordem de Serviço.
Meta a cumprir	IAP igual ou superior a 99 %.
Instrumento de medição	Deve ser aferido por meio de ferramentas, procedimentos de amostragem ou outros procedimentos de inspeção.
Forma de acompanhamento	É apurado pelos fiscais do contrato avaliando a quantidade atendida dentro do prazo em relação à quantidade total atendida no período de referência.
Periodicidade	Mensal
Mecanismo de Cálculo (métrica)	**IAP = 100 * (ΣQtap / ΣQtr)** Onde: IAP = Indicador de atendimento aos prazos do serviço; ΣQtap = Somatório do quantitativo atendido no prazo máximo estabelecido no TR com previsão de encerramento para o período de referência; ΣQtr = Somatório do quantitativo total registrado com previsão de encerramento para o período de referência.
Observações	Obs1: Serão utilizados dias corridos na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.
Início de Vigência	A partir da emissão da OS.
Faixas de ajuste no pagamento e Sanções	IAP >= 90%: sem descontos sobre o valor da fatura mensal. IAP >= 80% e < 90%: 10% de desconto sobre o valor da fatura mensal. IAP >= 70% e < 80%: 20% de desconto sobre o valor da fatura mensal. IAP < 70%: 30% de desconto sobre o valor da fatura mensal.

8.1.1 Os quantitativos das soluções de segurança, a serem disponibilizados para a execução dos serviços, definidos na Tabela (constante na seção 1 - CONDIÇÕES GERAIS DA CONTRATAÇÃO) poderão ser registrados e licenciados, em formato de subscrição, no nome da CONTRATADA e disponibilizadas durante a vigência de todo o contrato.

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

8.2.1 não produzir os resultados acordados;
8.2.2 deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou
8.2.3 deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los 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 Os níveis mínimos de serviço contratados serão registrados, monitorados e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade, condição fundamental para realização dos pagamentos previstos;

8.4.2 De modo a facilitar a compreensão dos Níveis Mínimos de Serviço (NMS) do SERVIÇOS GERENCIADOS DE SEGURANÇA, são apresentadas, a seguir, o método de avaliação da CONTRATADA, a saber:

8.4.2.1 Em cada período avaliado, o cálculo do Percentual de Níveis de Serviço atendidos de acordo com a sua severidade será calculado com a seguinte fórmula:

$$PNSTOTAL = (PNS_{PA} + PNS_{TR})/2 \geq 94\%$$

PNS_{TOTAL} = Percentual de Nível de Serviço

8.4.2.2 A fórmuls do **PNSpa** = Percentual de Nível de Serviço Primeiro Atendimento:

NTAM = Número de Tickets Atendimento Mensal, atendidos no prazo NMS: NTAM= 100% (numero de tickets)
NTPA = Número de Tickets Primeiro Atendimento, não atendidos no prazo NMS:

NTPA(%)= (NTPA * 100)/NTAM

8.4.2.3 A fórmula do **PNStr** = Percentual de Nível de Serviço Tempo de Resolução:

NTSM = Número de Tickets Solucionados Mensal, atendidos no prazo NMS:

NTRM= 100% (numero de atendimentos)

NTNS = Número de Tickets Não Solucionados, no prazo NMS;

8.4.3 O número de tickets classificados em NTNS (Número de Tickets Não Solucionados) e NTPA (Número de Tickets Primeiro Atendimento) serão desconsiderados do cálculo quando:

8.4.3.1 Falta de energia no local de prestação dos serviços;
8.4.3.2 Indisponibilidade da rede lógica da ENAP;
8.4.3.3 Problemas derivados de ocorrências no ambiente da ENAP, onde comprovadamente a indisponibilidade não esteja sendo controlada pela CONTRATADA;
8.4.3.4 Ações necessárias para resolução de problemas que tenham sido autorizadas pela ENAP;
8.4.3.5 Indisponibilidade gerada pela operadora de telecomunicação responsável pelos links e equipamentos do ambiente da ENAP;
8.4.3.6 Fatores externos a prestação de serviços, desde que justificado e acordado com o time de segurança da ENAP;
8.4.3.7 Indisponibilidade do ambiente virtualizado da ENAP, infraestrutura computacional em que parte dos softwares que compõem a solução deve ser instalada;
8.4.3.8 Manutenções programadas pela ENAP;
8.4.3.9 Manutenções programadas pela CONTRATADA, desde que previamente autorizadas pela ENAP;
8.4.3.10 Tickets abertos, cujo prazo de resolução encerre somente no próximo período de faturamento, somente terão calculados os fatores de abatimento, a partir do período seguinte.

8.4.4 Para chamados de severidade Crítica, Alta, Normal ou Baixa, o início dos atendimentos realizados e os prazos de solução estão especificados na tabela a seguir:

REFERÊNCIA	SEVERIDADE	DESCRIÇÃO	PRAZO MÁXIMO PARA PRIMEIRA RESPOSTA DE ATENDIMENTO REMOTO	PRAZO MÁXIMO DA SOLUÇÃO REMOTA
SEVERIDADE- 01	Urgente / Crítica	O serviço está totalmente parado ou inoperante;	Até 2 (duas) horas após a abertura do chamado remoto.	Até 24 (vinte e quatro) horas após abertura do chamado remoto.
SEVERIDADE- 02	Alta	O serviço está ativo, mas com inoperância da maioria de suas funcionalidades, causando um impacto negativo no ambiente de produção	Até 6 (seis) horas após a abertura do chamado remoto	Até 2 (dois) dias após abertura do chamado remoto;
SEVERIDADE- 03	Normal	O serviço está operativo, mas suas funcionalidades são executadas com restrições	Até 8 (oito) horas após a abertura do chamado remoto.	Até 4 (quatro) dias após abertura do chamado remoto.
SEVERIDADE- 04	Baixa	O serviço está operativo e a falha não compromete suas funcionalidades ou questões não tratadas pela documentação	Até 12 (doze) horas após a abertura do chamado remoto.	Até 6 (seis) dias após a abertura do chamado remoto.

8.4.5 Na tabela de severidade dos NMS, abaixo, são especificados os níveis de severidade baseados no catálogo de serviço para cada solução que devem ser seguidos, sob pena de multa, considerando a contagem de tempo em 24x7:

REFERÊNCIA	GRUPO DE SERVIÇO	SERVIÇO DO CATÁLOGO	DESCRIÇÃO	SEVERIDADE DE REFERÊNCIA
NMS-01			Firmware ou software	Urgente / Crítica
NMS-02			Backup de configuração	Baixa
NMS-03			Configuração de sistema	Normal
NMS-04			Configuração de conectividade e segurança	Alta

NMS-05			Ajustes e configurações	Alta
NMS-06			Ajustes e configurações	Normal
NMS-07			Análise	Baixa
NMS-08			Análise	Urgente / Crítica
NMS-09			Análise e remediação	Urgente / Crítica
NMS-10			Monitoramento	Normal
NMS-11			Requisição de suporte para restauração do ambiente	Alta
NMS-12			Firmware ou software	Urgente / Crítica
NMS-13			Backup de configuração	Normal
NMS-14			Configuração de sistema	Normal
NMS-15			Análise	Alta
NMS-16			Ajustes e configurações	Normal
NMS-17			Firmware ou software	Urgente / Crítica
NMS-18			Políticas	Normal
NMS-19			Novas aplicações	Normal
NMS-20			Monitoramento	Normal
NMS-21			Criação, Alteração ou Remoção de política de segurança específica	Normal
NMS-22			Validação dos controles de segurança implementados	Baixa
NMS-23			Relatório de Resumo Mensal de Serviços	Baixa

NMS-25			Reuniões periódicas com proposta de melhoria e evolução da maturidade	Baixa
NMS-26			Relatórios customizados	Baixa
NMS-27			Requisição de suporte para ativação de agente	Baixa
NMS-28			Requisição de suporte para análise de suspeita de anomalia	Alta
NMS-29			Requisição de suporte para correção de impacto	Urgente/Critica
NMS-30			Requisição de suporte para restauração do ambiente	Alta
NMS-31			Abertura de Chamados	Normal
NMS-32			Definir problema na Console SIP	Baixa
NMS-33			Executar Suporte N1	Normal
NMS-34			Escalar para Engenharia do Fabricante	Normal
NMS-35			Acompanhar chamado com o Fabricante	Normal
NMS-36			Criar relatório da resolução do problema	Normal

8.4.6 CHAMADOS EMERGENCIAIS

8.4.6.1 Em caso de indisponibilidade da SERVIÇOS GERENCIADOS DE SEGURANÇA, os chamados abertos para a CONTRATADA deverão ter um grau de severidade a ser definido pelo CONTRATANTE. Para isso, o CONTRATANTE irá avaliar a urgência e a criticidade da demanda. Nesse sentido, os níveis mínimos de serviços deverão ser aferidos conforme a severidade de cada chamado.

8.4.6.2 A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Nível Mínimo de Serviço (NMS) definido em contrato, de modo a resguardar a eficiência e a qualidade da prestação dos serviços.

Do recebimento

8.5 Os serviços serão recebidos provisoriamente, no prazo de 15 *(quinze)* dias úteis, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a , da Lei nº 14.133 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022).

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

8.6 O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. (Art. 22, X, Decreto nº 11.246, de 2022).

8.7 O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. (Art. 23, X, Decreto nº 11.246, de 2022)

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

8.9 Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá 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, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

8.9.1 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;

8.10 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.

8.11 A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021)

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

8.13 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.

8.14 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.

8.15 Os serviços serão recebidos definitivamente no prazo de *10 (dez)* 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:

8.15.1 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 (art. 21, VIII, Decreto nº 11.246, de 2022).

8.15.2 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 à Contratada, por escrito, as respectivas correções;

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

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

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

8.16 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 no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

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

8.18 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

8.19 Serão adotados como procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo:

8.19.1 Após o fim do ciclo mensal de prestação de serviços a CONTRATADA deverá entregar toda a documentação comprobatória do cumprimento da obrigação contratual.

8.19.2 A CONTRATADA deverá emitir, até o décimo dia útil do mês subsequente à realização dos relatórios conforme definido, para cada item, na seção 2 (DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO) deste Termos de Referência ,além de:

8.19.2.1 Relatório Técnico de indicadores de Segurança e Níveis de Serviço: relatório detalhado de cálculo dos indicadores de segurança elaborado por cada uma das categorias de serviços, que demonstrem pelo menos, a saúde dos ambientes, disponibilidade das soluções e serviços de segurança, análise de desempenho, tratativas, as ações proativas e preventivas realizadas, a observância de padrões e diretrizes definidos pela CGTI/ENAP, estatísticas de uso dos recursos e de acessos, resumo de incidentes e problemas, e se houver, propostas de melhorias, além da análise sobre os indicadores de NMS, que apresente a apuração e comentários quanto a execução de novos procedimentos de segurança implementados, contendo a data de emissão do relatório, o número do contrato, mês e ano de referência e a descrição dos serviços prestados contemplando todas as categorias de serviços, com apresentação.

8.19.2.2 Prévia do faturamento: documento sugestivo com detalhamento dos valores a serem faturados em razão da prestação dos serviços, considerando inclusive aplicações de glosas previstas.

8.19.2.3 Documentos acessórios para a fiscalização: relação de profissionais habilitados que demonstre a manutenção dos perfis profissionais solicitados e outras documentações que se fizerem necessárias.

8.19.3 Os relatórios deverão ser entregues em arquivos digitais.

8.19.4 Os serviços serão recebidos da seguinte forma:

8.19.4.1 Provisoriamente, no prazo máximo de 15 (quinze) dias úteis a partir da entrega do Relatório Gerencial, para posterior verificação da conformidade dos produtos e serviços com as especificações técnicas. Será emitido o respectivo Termo de Recebimento Provisório;

8.19.4.2 Definitivamente, no prazo máximo de 90 (noventa) dias úteis a partir da emissão do Termo de Recebimento Provisório, depois de concluída verificação da conformidade dos produtos e serviços com as especificações técnicas, ocasião em que será emitido o respectivo Termo de Recebimento Definitivo.

8.19.5 Qualquer serviço será recusado caso seja entregue em desconformidade com as especificações técnicas constantes deste Termo de Referência e da proposta vencedora, ou caso apresente defeitos, em qualquer de suas partes ou componentes, durante os testes de conformidade e verificação. Nos casos de recusa, o prazo para execução das correções não poderá exceder 20% (vinte por cento) do prazo efetivamente utilizado para corrigir os serviços recusados, sem prejuízo da aplicação cumulativa dos Níveis de Serviço previstos.

8.19.6 O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato, ou, em qualquer época, das garantias concedidas e das responsabilidades assumidas em contrato e por força das disposições legais em vigor.

8.19.7 A ENAP reserva-se ao direito de promover avaliações, inspeções e diligências visando esclarecer quaisquer situações relacionadas à prestação dos serviços contratados, sendo obrigação do CONTRATADO acolhê-las.

Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

8.20 A CONTRATADA estará sujeita, , garantida a prévia defesa, às advertências, retenções, glosas, multas e sanções administrativas pela inobservância das obrigações contratuais elencadas neste documento. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela contratante, conforme a tabela abaixo:

Id	Ocorrência	Glosa / Sanção
1	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de (72) horas úteis.	Multa de (01) % sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela contratante, até o limite de (03) dias úteis.
		Após o limite de (05) dias úteis, aplicar-se-á multa de (03) % do valor total do Contrato.
		Após o 30º (trigésimo) dia de atraso e, a critério da ENAP, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.
2	Não atender ao indicador de nível de serviço IAP (Índice de Atendimento no Prazo)	IAP >= 90%: sem descontos sobre o valor da fatura mensal.
		IAP >= 80% e < 90%: 10% de desconto sobre o valor da fatura mensal.
		IAP >= 70% e < 80%: 20% de desconto sobre o valor da fatura mensal.

		IAP < 70%: 30% de desconto sobre o valor da fatura mensal.
3	Não comparecer, injustificadamente, à Reunião Inicial.	Em caso de reincidência, multa de 0,3% (zero vírgula três por cento) por dia de atraso injustificado sobre o valor da contratação até o limite de 30 (trinta) dias. A partir do 31º (trigésimo primeiro) dia de atraso, o contrato será rescindido.
4	Quando convocado dentro do prazo de validade da sua proposta, não celebrar o Contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não manter a proposta, falhar ou fraudar na execução do Contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.	A CONTRATADA ficará impedida de licitar e contratar com a União, Estados, Distrito Federal e Municípios e, será descredenciada no SICAF, ou nos sistemas de cadastramento de fornecedores a que se refere o Art. 156 da Lei 14.133/2021, sem prejuízo das demais cominações legais.
5	Ter praticado atos ilícitos visando frustrar os objetivos da licitação.	A CONTRATADA será declarada inidônea para licitar e contratar com a Administração.
6	Demonstrar não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
7	Não executar total ou parcialmente os serviços previstos no objeto da contratação.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
8	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por até de 30 dias, sem comunicação formal ao gestor do Contrato.	Multa moratória de 0,5% (zero vírgula cinco por cento) por dia de atraso injustificado sobre o valor da contratação até o limite de 30 (trinta) dias. A partir do 31º (trigésimo primeiro) dia de atraso, o contrato será rescindido. Multa compensatória de 5% (cinco por cento) sobre o valor total do contrato, no caso de inexecução total ou parcial da obrigação assumida, podendo ser cumulada com a multa moratória, desde que o valor cumulado das penalidades não supere o valor total do contrato.
9	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por mais de 30 (trinta) dias, sem comunicação formal ao gestor do contrato.	Contratada será declarada inidônea para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
10	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 40 (quarenta) horas úteis.	Multa de 0,2% (zero vírgula dois por cento) sobre o valor total do Contrato por dia útil de atraso injustificado em prestar as informações por escrito, ou por outro meio quando autorizado pela Contratante, até o limite de 20 dias úteis.

		Após o limite de 20 dias úteis, aplicar-se-á multa de 3% (três por cento) do valor total do Contrato.
11	Provocar intencionalmente a indisponibilidade da prestação dos serviços quanto aos componentes de software (sistemas, portais, funcionalidades, banco de dados, programas, relatórios, consultas, etc).	A CONTRATADA será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 14.133/2021.
12	Permitir intencionalmente o funcionamento dos sistemas de modo adverso ao especificado e às cláusulas contratuais, provocando prejuízo aos usuários dos serviços.	A CONTRATADA será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 14.133/2021.
13	Comprometer intencionalmente a integridade, disponibilidade ou confiabilidade e autenticidade das bases de dados dos sistemas.	A CONTRATADA será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 14.133/2021.
14	Comprometer intencionalmente ou não garantir o sigilo absoluto das informações armazenadas nos sistemas do CONTRATANTE e de todos os processos, rotinas, objetos, informações, documentos e quaisquer outros dados fornecidos pela ENAP.	A CONTRATADA será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 14.133/2021. Multa compensatória correspondente a 15% (cinco por cento) aplicável sobre o preço global do Contrato.
15	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de (05) % do valor total do Contrato.
16	Deixar de executar ou implementar qualquer dos itens previstos para fase de implantação.	Advertência no primeiro mês e 10% (dez por cento) sobre o faturamento mensal para os meses seguintes.
17	Ocorrência de ações danosas ou criminosas cometidas por empregados, prepostos do CONTRATADO, empresas ou pessoas por ele contratadas ou designadas, no exercício das atividades previstas no Contrato que ocasionem prejuízos à ENAP, a seus clientes/usuários de serviços bancários, devidamente comprovados através de decisão judicial (transitada em julgado).	Multa de 5% (cinco por cento), aplicável sobre o preço global do Contrato, mais o valor correspondente ao valor do prejuízo apurado
18	Inobservância do prazo fixado para apresentação ou reposição da garantia contratual.	Multa de 0,1% (um décimo por cento), , aplicável sobre o preço global contratado, por dia de atraso e limitado a 2% (dois por cento)
	Ocorrência faltosa, por hora de atraso, pelo não atendimento dos níveis de serviços relacionados	

19	à assistência e suporte técnico de severidade crítica ou alta, tanto de hardware quanto de software (produção parada ou impactada), previsto na tabela Prazos para execução do projeto descrita nos Requisitos Temporais deste Termo de Referência.	Multa de 5% (cinco por cento), aplicável sobre o valor apurado para pagamento no mês em que se verificar a ocorrência.
20	Aplicável sobre o valor apurado para pagamento no mês em que se verificar a ocorrência faltosa, pelo não atendimento dos níveis de serviços relacionados às atividades descritas nas tabelas de NÍVEL MÍNIMO DE SERVIÇO – NMS desta seção.	Multa de 1% (um por cento) por ocorrência, aplicável sobre o valor apurado para pagamento no mês em que se verificar a ocorrência faltosa
21	Atraso em qualquer uma das fases previstas no item Requisitos Temporais deste Termo de Referência.	Multa de 1% (um por cento) aplicável sobre o valor do faturamento do item em atraso.

8.20.1 Pela inexecução total ou parcial do objeto do Contrato, a ENAP poderá, garantida a prévia defesa, aplicar ao CONTRATADO as seguintes sanções:

8.20.1.1 advertência;

8.20.1.2 multa de 1% (um por cento) por dia de atraso em qualquer uma das fases previstas no item Requisitos Temporais deste Termo de Referência, aplicável sobre o valor do faturamento do item em atraso;

8.20.1.3 multa de 10% (dez por cento), aplicável sobre o preço global contratado, nas demais violações ou descumprimentos de cláusula(s) ou condição(ões) estipulada(s) no Contrato;

8.20.1.4 multa de 10% (dez por cento), aplicável sobre o preço global contratado, em caso de inexecução total do Contrato;

8.20.1.5 suspensão temporária de participar em licitação e impedimento de contratar com a ENAP pelo prazo de até 2 (dois) anos.

8.20.2 Comete infração administrativa nos termos da Lei 14.133/2021, a CONTRATADA que:

8.20.2.1 Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;
8.20.2.2 Ensejar o retardamento da execução do contrato;
8.20.2.3 Falhar ou fraudar na execução do contrato;
8.20.2.4 Comportar-se de modo inidôneo; ou
8.20.2.5 Cometer fraude fiscal.

8.20.3 Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

8.20.3.1 Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;
8.20.3.2 Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;
8.20.3.3 Sanção de impedimento de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;
8.20.3.4 Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir o CONTRATANTE pelos prejuízos causados.

8.20.4 As sanções previstas nos subitens acima poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

8.20.5 A licitante contratada, convocada dentro do prazo de validade da sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedido de licitar e contratar com a União, Estados, Distrito Federal ou Municípios e, será descredenciado no SICAF, ou nos sistemas de cadastramento de fornecedores, conforme disposto na Lei nº 14.133/2021, sem prejuízo das multas previstas no termo de referência e no contrato e das demais cominações legais.

8.20.6 Também ficam sujeitas às penalidades do art. 104, IV da Lei nº 14.133/2021, as empresas ou profissionais que:

8.20.6.1 Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;
8.20.6.2 Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;
8.20.6.3 Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

8.20.7 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 14.133/2021 e, subsidiariamente, a Lei nº 9.784 de 1999.
8.20.8 As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.
8.20.9 Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.
8.20.10 Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.
8.20.11 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.
8.20.12 Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei no 12.846, de 1o de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização (PAR).
8.20.13 A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei no 12.846, de 1o de agosto de 2013, seguirão seu rito normal na unidade administrativa.
8.20.14 O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.
8.20.15 As penalidades serão obrigatoriamente registradas no SICAF.
8.20.16 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 contratado:

8.20.16.1 não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou
8.20.16.2 deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

8.20.17 As sanções de advertência, suspensão e inidoneidade poderão ser aplicadas juntamente com a multa, conforme Capítulo I – DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS do TÍTULO IV – DAS IRREGULARIDADES (arts. 155 a 163 da Lei nº 14.133/2021).
8.20.18 Ao exceder o limite máximo admitido de infrações durante a vigência contratual OU mediante o reiterado descumprimento de critérios de qualidade e/ou níveis mínimos de serviço exigidos OU diante da reiterada aplicação de sanções contratuais, a ENAP deverá avaliar a possibilidade de promover a rescisão do CONTRATO em função da INEXECUÇÃO TOTAL ou PARCIAL do OBJETO, da perda de suas funcionalidades e da comprovada desconformidade com os critérios mínimos de qualidade exigidos – ressalvada a aplicação adicional de outras sanções administrativas cabíveis, respeitados os princípios da razoabilidade, da proporcionalidade, da ampla defesa e do contraditório.

8.20.19 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao CONTRATADO, observando-se o procedimento previsto na Lei nº 14.133/2021.
8.20.20 As multas devidas e/ou prejuízos causados à CONTRATANTE serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.
8.20.21 Caso a CONTRATANTE determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.
8.20.22 Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.
8.20.23 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

8.21 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 o CONTRATADO:

8.21.1 não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou
8.21.2 deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada.

Liquidação

8.22 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, §2º da Instrução Normativa SEGES/ME nº 77/2022.

8.23 O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso 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.

8.24 Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

8.24.1 o prazo de validade;
8.24.2 a data da emissão;
8.24.3 os dados do contrato e do órgão contratante;
8.24.4 o período respectivo de execução do contrato;
8.24.5 o valor a pagar; e
8.24.6 eventual destaque do valor de retenções tributárias cabíveis.

8.25 Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

8.26 A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

8.27 A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas. (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018)

8.28 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.

8.29 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.

8.30 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.

8.31 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

8.32 O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

8.33 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 Índice de Custo da Tecnologia da Informação (ICTI) de correção monetária.

Forma de pagamento

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

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

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

8.37 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.

Antecipação de pagamento

8.39 A presente contratação não permite a antecipação de pagamento.

Cessão de crédito

8.40 É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020, conforme as regras deste presente tópico.

8.40.1 As cessões de crédito não fiduciárias dependerão de prévia aprovação do contratante.

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

8.42 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 14.230, de 25 DE Outubro de 2021, nos termos do Parecer JL-01, de 18 de maio de 2020.

8.43 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 (INSTRUÇÃO NORMATIVA Nº 53, DE 8 DE JULHO DE 2020).

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

9. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECED

Forma de seleção e critério de julgamento da proposta

9.1 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

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

9.2.1 Esse tipo regime de execução, preconizado no art. 6º, inciso XXVIII, Lei nº 14.133, de 2021, coaduna com a natureza dos serviços buscados nesta contratação à medida que satisfaz o caso concreto, esperado para uma operação na qual não se conhece de antemão, com adequado nível de precisão, os quantitativos totais da obra ou serviço e, por isso, a execução das “unidades” se dará de acordo com a necessidade observada, com a realização de medições periódicas a fim de quantificar os serviços efetivamente executados e os correspondentes valores devidos (TCU. Acórdão 1978 /2013-Plenário).

Da Aplicação da Margem de Preferência

9.3 Não será aplicada margem de preferência na presente contratação.

Exigências de habilitação

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

Habilitação jurídica

9.5 **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;

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

9.7 **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;

9.8 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;

9.9 **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.

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

9.11 **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

9.12 **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.

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

Habilitação fiscal, social e trabalhista

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

9.15 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.

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

9.17 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;

9.18 Prova de inscrição no cadastro de contribuintes Distritais/Estaduais relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.19 Prova de regularidade com a Fazenda Distrital/Estadual do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

9.20 Caso o fornecedor seja considerado isento dos tributos Distritais/Estaduais 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.

9.21 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

9.22 Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

9.23 Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

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

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

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

9.24.3 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.

9.24.4 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.

9.25 Caso a empresa licitante 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%* do *valor total estimado da contratação.*

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

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

Qualificação Técnica

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

9.28.1 De acordo com o Acórdão TCU nº 1.851/2015, "para fins de comprovação da qualificação técnica dos licitantes, o TCU tem entendido em reiteradas oportunidades que não se pode estabelecer percentuais mínimos acima de 50% dos quantitativos dos itens de maior relevância".

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

9.29 Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

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

9.30.1 A qualificação técnica será comprovada mediante a apresentação de atestado de capacidade técnica, de no mínimo 12 meses, compatível com o objeto desta licitação.

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

9.30.3 Conforme §2º do art. 67 da Lei nº 14.133, de 2021, “será admitida a exigência de atestados com quantidades mínimas de até 50% (cinquenta por cento) das parcelas de que trata o referido parágrafo, vedadas limitações de tempo e de locais específicos relativas aos atestados”.

9.30.4 Apresentação de atestado(s) de desempenho anterior em atividades pertinentes e compatíveis em características, quantidades e prazos com o objeto desta licitação, emitido(s) por pessoa jurídica de direito público ou privado, demonstrando que foram cumpridas corretamente suas obrigações contratuais, contendo em seu corpo a razão social, endereço completo, telefone e CNPJ/MF, da empresa fornecedora do atestado, bem como a data, assinatura e identificação do assinante, observadas as demais exigências constantes neste edital.

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

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

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

9.33.1 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;

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

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

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

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

9.33.6 Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: a) ata de fundação; b) estatuto social com a ata da assembleia que o aprovou; c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; d) editais de convocação das três últimas assembleias gerais extraordinárias; e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

9.33.7 A 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.

9.34 Considerar-se-á (ão) compatível (is) o(s) atestado(s) que comprove(m) a prestação de SERVIÇOS GERENCIADOS DE SEGURANÇA do item 01 e do item 02 em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, com as seguintes parcelas de maior relevância:

9.34.1 Os Centros de Operação de Segurança (SOCs) devem ser redundantes, próprios da CONTRATADA, sendo ambos obrigatoriamente no Brasil, e estejam – no mínimo – a 300 km (trezentos quilômetros) de distância geodésica uma da outra e em estados distintos, devendo atender – minimamente – os seguintes requisitos:

9.34.1.1 Experiência na prestação em um mesmo contrato de consultoria, operacionalização e entrega de serviço de monitoramento e visibilidade de ataques cibernéticos ou serviço de monitoramento, detecção e resposta a incidentes, nos termos deste edital.

9.34.1.2 No mínimo 1.500 (mil e quinhentos) eventos por segundo (EPS);

9.34.2 Experiência na elaboração de políticas, normas e procedimentos da segurança da informação da ISO 27001 e 27002 em no mínimo 06 políticas, regras e procedimentos. Este item visa atestar a capacidade da licitante para o fornecimento do serviço especificado no Item 02 – Serviço de monitoramento, detecção e resposta a incidentes - 1500 Eventos por segundo (EPS) exigido neste certame.

9.34.3 Experiência em Serviço de conscientização de Segurança, por meio de atestados de conscientização em outras organizações. Este item visa atestar a capacidade da licitante para o fornecimento do serviço especificado no Item 01 - Serviço de monitoramento e visibilidade de ataques cibernéticos exigido neste certame.

9.34.4 Experiência em serviços de Serviço de monitoramento e visibilidade de ataques cibernéticos, fornecendo serviço de inteligência voltada à segurança com buscas na Surface, Deep e Darkweb, de no mínimo, 1000 ativos, dentre eles VIP’s, IP’s, domínios. Este item visa atestar a capacidade da licitante para o fornecimento do serviço especificado no Item 01 - Serviço de monitoramento e visibilidade de ataques cibernéticos, exigidos neste certame.

9.34.5 Experiência em serviços de elaboração de plano de gestão de incidentes cibernéticos e serviço de monitoramento, detecção e resposta a incidentes, utilizando tecnologia de SIEM (Security Information and Event Management) para gerenciamento e correlação de eventos de segurança

através da análise de logs e pacotes, em redes com, no mínimo, 1.500 (mil e quinhentos) EPS. Também deverá ser comprovado a capacidade de realização de um Plano de Resposta a Incidentes e de Assessment & MITRE ATT&CK®. Este item visa atestar a capacidade do licitante para fornecer o serviço especificado no Item 02 - Serviço de monitoramento, detecção e resposta a incidentes exigido neste certame.

9.34.6 Deverá apresentar ISO's descritos no subitem 4.40.6, constante na seção 4 (REQUISITOS DA CONTRATAÇÃO) deste Termo de Referência, a fim de certificar que o SOC/Datacenter possuem padrões/normas de qualidade internacionalmente conhecidos.

9.34.7 Considerar-se-á (ão) compatível (is) o(s) atestado(s) que comprove(m) a prestação de SERVIÇOS GERENCIADOS DE SEGURANÇA do item 02, com as seguintes parcelas de maior relevância:

9.34.7.1 Será aceita a somatória de atestados para comprovação da qualificação técnica, desde que a soma dos itens atenda as quantidades mínimas acima exigidas.

9.34.7.2 Não serão considerados os atestados emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente ou que tenham pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da proponente.

9.34.7.3 Deverá apresentar declaração emitida pelo fabricante da solução, por meio de seu representante legal, específica a este órgão e processo, atestando que a licitante está apta a fornecer e prestar os serviços objetos desta contratação com suas soluções.

9.34.7.4 A LICITANTE deve disponibilizar todas as informações necessárias à comprovação da legitimidade dos atestados ofertados na presente licitação, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, Notas Fiscais/Faturas, Notas de Empenho, endereço atual da ENAP e local em que foram prestados os serviços, sendo que estas e outras informações complementares poderão ser requeridas mediante diligência.

9.34.8 Todas as características e requisitos exigidos neste termo de referência poderão ser confirmados em diligência presencial a ser instruída em tempo oportuno, conforme discricionariedade e critérios da CONTRATANTE.

10. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

10.1 O custo estimado total da contratação é de **R$ 1.280.166,28** (um milhão e duzentos e oitenta mil e cento e sessenta e seis reais e vinte e oito centavos), conforme custos unitários apostos na tabela abaixo:

ITEM	ESPECIFICAÇÃO	CATSER	MÉTRICA OU UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO MENSAL	VALOR TOTAL PARA 12 MESES
1	Serviço de monitoramento e visibilidade de ataques cibernéticos	27359	Meses	12	R$ 28.965,70	R$ 347.588,44
2	Serviço de **monitoramento, detecção e resposta a incidentes** - 1500	27359	Meses	12	R$ 77.714,82	R$ 932.577,84

	Eventos por segundo (EPS)					
VALOR TOTAL DA CONTRATAÇÃO PARA 12 MESES						**R$ 1.280.166,28**

11. ADEQUAÇÃO ORÇAMENTÁRIA

11.1 A contratação será atendida pela seguinte dotação:

1. Gestão/Unidade: Orçamento Enap;
2. Fonte de Recursos: 2000 - Administração da Unidade;
3. Programa de Trabalho: 0002 - Despesas Gerais da Administração;
4. Elemento de Despesa: 3.3.90.40 - Despesas Correntes/Outras Despesas Correntes/Aplicações;
5. Plano Interno: Serviços de Tecnologia da Informação e Comunicação - TIC - Pessoa Jurídica. PI: II1WN;

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

12. 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.

JULLYANO LINO DA SILVA

Integrante Técnico

Assinou eletronicamente em 06/06/2024 às 13:30:08.

RAFAELL DIAS LEITE FELIX

Integrante Requisitante

Assinou eletronicamente em 06/06/2024 às 13:31:13.

JOSIVAN DA SILVA FERREIRA

Integrante Administrativo

Assinou eletronicamente em 07/06/2024 às 13:27:25.

FRANK JAMES DA SILVA PIRES

Autoridade Máxima de TIC

Assinou eletronicamente em 06/06/2024 às 14:00:56.

ALYSSON PEDRO DIAS PINHEIRO

Autoridade competente

Assinou eletronicamente em 06/06/2024 às 16:39:33.

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 - Documentos Auxiliares.pdf (319.45 KB)

Anexo I - Documentos Auxiliares.pdf

A – MODELO DE PROPOSTA COMERCIAL (Prazo: 60 dias)

GRUPO	ITEM	DESCRIÇÃO	QTD	Und	Valor Unitário	Valor Total
01	1	Serviço de monitoramento e visibilidade de ataques cibernéticos	**12**	Meses	R$	R$
VALOR TOTAL GRUPO 01						R$ (Por extenso)
GRUPO	**ITEM**	**DESCRIÇÃO**	**QTD**	**Und**	**Valor Unitário**	**Valor Total**
02	2	Serviço de monitoramento, detecção e resposta a incidentes - 1500 Eventos por segundo (EPS)	**12**	Meses	R$	R$
VALOR TOTAL GRUPO 02						R$ (Por extenso)
VALOR TOTAL						R$ (Por extenso)

IDENTIFICAÇÃO DA EMPRESA LICITANTE		
Razão Social:		
CNPJ:		
Endereço Completo:		
CEP:	Fone:	E-mail:

Demais condições:
a) Ao efetuar essa proposta, esta empresa proponente declara ter tomado pleno conhecimento do Edital, do Termo de Referência e dos demais documentos

integrantes da presente licitação estando ciente das obrigações das partes e das condições de prestação dos serviços.

b) Esta empresa proponente declara que todas as despesas diretas e indiretas envolvidas no provimento dos serviços estão incluídas nos valores desta proposta de preços, que possui capacidade técnico-operacional adequada e que os preços são exequíveis.

Local e data: _____, _____ de _____de 2024

_____
Razão Social e CNPJ da Empresa Proponente

_____
Identificação e Assinatura do Representante Legal da Empresa Proponente

Prazo de validade da proposta: ..... (.....) dias, contados da data limite estipulada para a apresentação.

.

INSTRUÇÕES:

1. A descrição e a disposição de itens da proposta de preços devem obedecer ao padrão proposto.
2. Os valores correspondentes a cada item devem ser informados em separado, considerando seus preços unitários e totais (por item).
3. Para a fase de habilitação técnica, anexo à proposta, devem ser apresentados os documentos necessários e suficientes para a comprovação do atendimento aos critérios técnicos de habilitação, conforme definido no TERMO DE REFERÊNCIA.
4. Conforme súmula TCU 254/2010 o Imposto de Renda Pessoa Jurídica (IRPJ) e a Contribuição Social Sobre o Lucro Líquido (CSLL) não devem constar da composição de preços da proposta.
5. À proposta é necessário juntar cópia dos principais documentos da empresa (alteração contratual ou procuração) e do responsável (documento de identidade, CPF ou CNH).
6. Observando o disposto no TERMO DE REFERÊNCIA, a proposta deve ter validade de, no mínimo, 60 (sessenta) dias.

B – TERMO DE COMPROMISSO DE SIGILO E SEGURANÇA DA INFORMAÇÃO

Pelo presente instrumento o , sediado em , CNPJ n° , doravante denominado CONTRATANTE, e, de outro lado, a , sediada em , CNPJ n° , doravante denominado CONTRATADO; CONSIDERANDO que, em razão do CONTRATO N.º doravante denominado CONTRATO PRINCIPAL, o CONTRATADO 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 pelo CONTRATADO, no que diz respeito ao trato de informações sigilosas disponibilizadas pela ENAP 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:

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

   b) 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.

c) 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 enap e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, o CONTRATADO 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 do CONTRATADO;

   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 – O CONTRATADO se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento prévio e expresso da ENAP.

Parágrafo Segundo – O CONTRATADO 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 – O CONTRATADO deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à ENAP dos documentos comprobatórios.
Parágrafo Terceiro – O CONTRATADO obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da ENAP, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela ENAP.

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 – O CONTRATADO 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 ao CONTRATADO, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – O CONTRATADO, 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 ENAP, 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 do CONTRATADO, 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 o CONTRATADO 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, o CONTRATADO, 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. 155 da Lei nº. 14.133/2021.

8. DISPOSIÇÕES GERAIS

   Este TERMO de Confidencialidade é parte integrante e inseparável do

CONTRATO PRINCIPAL.

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

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

Parágrafo Terceiro – Ao assinar o presente instrumento, o CONTRATADO manifesta sua concordância no sentido de que:

I – A ENAP terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades do CONTRATADO;

II – O CONTRATADO deverá disponibilizar, sempre que solicitadas formalmente pela ENAP, 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 o CONTRATADO 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 o CONTRATADO, 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 ENAP elege o foro da cidade de BRASÍLIA/DF, Justiça Federal - Seção Judiciária do Distrito Federal, onde está localizada a sede da ENAP, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

10. ASSINATURAS

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

CONTRATADO	**CONTRATANTE**
<Nome> <Qualificação>	<Nome> <Qualificação>

TESTEMUNHAS	
<Nome> <Qualificação>	<Nome> <Qualificação>

Brasília/DF, ___ de _____ de 2024.

C - MODELO DE TERMO DE CIÊNCIA INDIVIDUAL

TERMO DE CIÊNCIA INDIVIDUAL DO COMPROMISSO DE SIGILO E SEGURANÇA DA INFORMAÇÃO	
IDENTIFICAÇÃO DO CONTRATO	
N° DO CONTRATO: EMPRESA CONTRATADA / CNPJ: OBJETO RESUMIDO: VIGÊNCIA CONTRATUAL:	
TERMOS	
O(s) funcionário(s) abaixo qualificado(s) declara(m) ter pleno conhecimento de sua(s) responsabilidade(s) no que concerne ao sigilo que deve ser mantido sobre as atividades desenvolvidas ou as ações realizadas no âmbito do Contrato Administrativo n° / , bem como sobre todas as informações que eventualmente ou por força de sua(s) função(ões) venha(m) a tomar conhecimento, comprometendo-se a guardar o sigilo necessário nos termos da legislação vigente e a prestar total obediência às normas de segurança da informação vigentes no ambiente do CONTRATANTE ou que venham a ser implantadas a qualquer tempo por este; em conformidade com o TERMO DE COMPROMISSO DE SEGURANÇA DA INFORMAÇÃO firmado entre as partes.	
OBSERVAÇÕES	
DE ACORDO	
E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE CIÊNCIA é assinado pela(s) parte(s) declarante(s) em 02 (duas) vias de igual teor e um só efeito. Brasília (DF), / /	
IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S)	
Nome: Identidade: CPF: Função:	Assinatura:
Nome: Identidade: CPF: Função:	Assinatura:
Observação: Este termo deve ser impresso em papel timbrado do CONTRATADO.	

D - TERMO DE RECEBIMENTO PROVISÓRIO

TERMO DE RECEBIMENTO PROVISÓRIO – COMPRAS DE TIC

INTRODUÇÃO

O Termo de Recebimento Provisório declarará, de forma sumária, que as compras foram entregues, para verificação posterior da conformidade do material com as exigências contratuais, baseada nos requisitos e nos critérios de aceitação definidos no Modelo de Gestão do Contrato.

Referência: Inc. XXI, art.2º, e alínea “i”, inciso II, art. 33 da Instrução Normativa n° 94/2022 SGD/ME

1 – IDENTIFICAÇÃO

CONTRATO Nº:
CONTRATADA/ CNPJ:
N° DA OS:
DATA DA EMISSÃO:

2 – ESPECIFICAÇÃO DOS BEM(S) E VOLUMES DE EXECUÇÃO

SOLUÇÃO DE TIC			
ITEM DO CONTRATO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL POR ITEM

3 – RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea “i”, da IN SGD/ME nº 94/2022, por este instrumento ATESTO que os serviços correspondentes à **<OS>** acima identificada, conforme definido no Modelo de Execução do contrato supracitado, foram executados e **<atende(m)/atende(m) parcialmente/não atende(m)>** às respectivas exigências de caráter técnico discriminadas abaixo. Não obstante, estarão sujeitos à avaliação específica para verificação do atendimento às demais exigências contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato.

Ressaltamos que o recebimento definitivo desses serviços ocorrerá somente após a

verificação desses requisitos e das demais condições contratuais, desde que não se observem inconformidades ou divergências quanto às especificações constantes do Termo de Referência e do Contrato acima identificado que ensejem correções por parte da CONTRATADA. Por fim, reitera-se que o objeto poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

ITEM	ESPECIFICAÇÃO TÉCNICA	ATENDIMENTO	OBSERVAÇÃO
1	<exigências técnicas definidas no TR>	…	……
…	…	…	……

4 – ASSINATURA

_____

Nome do **Fiscal Técnico do Contrato**:

Matrícula:

<LOCAL>, <DIA> de <MÊS>de <ANO>

_____

Nome do **Preposto do Contrato**:

Matrícula:

<LOCAL>, <DIA> de <MÊS>de <ANO>

E - TERMO DE RECEBIMENTO DEFINITIVO

INTRODUÇÃO

O Termo de Recebimento Definitivo declarará formalmente à Contratada que os serviços prestados ou que os bens fornecidos foram devidamente
avaliados e atendem às exigências contratuais, de acordo com os requisitos e critérios de aceitação estabelecidos.

Referência: Inciso XXII, Art. 2º e alínea “h” inciso I do art. 33, da IN SGD/ME Nº 94/2022.

1 – IDENTIFICAÇÃO

CONTRATO/NOTA DE EMPENHO:
CONTRATADA / CNPJ:
Nº DA OS:
DATA DA EMISSÃO:

2 – – ESPECIFICAÇÃO DOS SERVIÇOS E VOLUMES DE EXECUÇÃO

SOLUÇÃO DE TIC <descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>					
ITEM	DESCRIÇÃO	UNIDADE	QTDE/VOLUME	VALOR UNITÁRIO	VALOR TOTAL DO ITEM
VALOR TOTAL ESTIMADO				R$ XX.XXX.XXX,XX (POR EXTENSO)	

3 – ATESTE DE RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea “h”, da IN SGD/ME nº 94/2022, por este instrumento ATESTAMOS que o(s) <serviço(s)/ bem(s)> correspondentes à <OS/OFB> acima identificada foram <prestados/entregues> pela CONTRATADA e ATENDEM às exigências contratuais, discriminadas abaixo, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Contrato acima indicado.

ITEM	ESPECIFICAÇÃO TÉCNICA	ATENDIMENTO	OBSERVAÇÃO
1	<exigências técnicas definidas no TR>	…	……
…	…	…	……

4 – DESCONTOS EFETUADOS E VALOR A LIQUIDAR

De acordo com os critérios de aceitação e demais termos contratuais, <não> há incidência de descontos por desatendimento dos indicadores de níveis de serviços definidos.
<Não foram / Foram> identificadas inconformidades técnicas ou de negócio que ensejam indicação de glosas e sanções, <cuja instrução corre em processo administrativo próprio (nº do processo)>.
Por conseguinte, o valor a liquidar correspondente à <OS/OFB> acima identificada monta em R$ <valor> (<valor por extenso>).

Referência: <Relatório de Fiscalização nº xxxx ou Nota Técnica nº yyyy>.

5 – ASSINATURA

_____

Nome do **Fiscal Técnico do Contrato**:

Matrícula:

<LOCAL>, <DIA> de <MÊS>de <ANO>

_____

Nome do **Fiscal Requisitante do Contrato**:

Matrícula:

<LOCAL>, <DIA> de <MÊS>de <ANO>

6 – AUTORIZAÇÃO PARA FATURAMENTO

Nos termos da alínea “n”, inciso I, art. 33, da IN SGD/ME nº 94/2022, AUTORIZA-SE a CONTRATADA a <faturar os serviços executados / apresentar as notas fiscais dos bens entregues> relativos à supracitada <OS/OFB>, no valor discriminado no item 4, acima.

_____

Nome do **Gestor do Contrato**:

Matrícula:

<LOCAL>, <DIA> de <MÊS>de <ANO>

7 – CIÊNCIA

_____

Nome do **Preposto do Contrato**:

Matrícula:

<LOCAL>, <DIA> de <MÊS>de <ANO>

F - MODELO DE DEMONSTRAÇÃO DE ATENDIMENTO AOS REQUISITOS TÉCNICOS DOS ITENS

ITEM (do edital)	REQUISITO (ponto a ponto)	DESCRIÇÃO DOS REQUISITOS	COMPROVAÇÃO (documento, página, site, etc)

G - DECLARAÇÃO DE VISTORIA OU DECLARAÇÃO OU DE OPÇÃO DE NÃO REALIZAÇÃO DE VISTORIA

DECLARAÇÃO DE REALIZAÇÃO DA VISTORIA TÉCNICA

DECLARAMOS, para fins de participação no Pregão Eletrônico n° ____/2024, que a empresa <Razão Social da Empresa>, registrada no CNPJ/MF <CNPJ>, representada por seu Responsável Técnico abaixo identificado, realizou VISTORIA TÉCNICA nas instalações do DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO tomando ciência de informações e instruções necessárias ao atendimento do objeto da presente licitação e à eventual elaboração de sua PROPOSTA, ao passo que nos comprometemos a manter sob sigilo e a não divulgar as informações e dados a que tivemos acesso por ocasião da VISTORIA TÉCNICA.

DECLARAÇÃO DE OPÇÃO PELA NÃO REALIZAÇÃO DA VISTORIA TÉCNICA

DECLARAMOS, para fins de participação no Pregão Eletrônico n° ____/2024, que a empresa <Razão Social da Empresa>, registrada no CNPJ/MF <CNPJ>, Em conformidade a previsão contida nos Requisitos Gerais do Termo de Referência, manifestamos nossa opção por não realização da Vistoria Técnica.

Brasília/DF, de de 2023.

[assinatura e carimbo]

_____

<Nome completo do emitente>

<Cargo do emitente>

<SIAPE do emitente>

[assinatura]

_____

<Nome completo do representante da Empresa>
<Documento de Identificação>

H - DECLARAÇÃO DE CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS

(Em papel personalizado da empresa)

À ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA

A/C: Sr. Gestor do Contrato
PROCESSO Nº _____/____-___

Prezado Senhor,

Nos termos da Lei 13.709 de 14 de agosto de 2018, DECLARO que tenho pleno conhecimento e cumpro com as obrigações, condições e peculiaridades inerentes à LGPD[1], que assumo total responsabilidade por este fato e seu fiel cumprimento.

_____

Local , data, nome, e assinatura do responsável legal

[1]https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaRequisitosdeSIparaContratacoesdeTI.pdf

I - DECLARAÇÃO DE CONHECIMENTO DO EDITAL

(Em papel personalizado da empresa)

À ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA

A/C: Sr. Pregoeiro (a)
PREGÃO Nº ___/20__
PROCESSO Nº _____/____-___

Prezado Senhor,

Nos termos do item 4.2 do Anexo VII-A da IN SEGES/MP n. 5/2017, DECLARO que tenho pleno conhecimento e concordo com as condições e peculiaridades inerentes à natureza dos serviços contidos no ato convocatório e seus anexos, bem como cumpro plenamente os requisitos de habilitação definidos nos referidos documentos, que assumo total responsabilidade por este fato e que não utilizarei deste para quaisquer questionamentos futuros que ensejam avenças técnicas ou financeiras com a ENAP.

_____

Local , data, nome, e assinatura do responsável legal

J- ATIVOS DE INFRAESTRUTURA DE TI DA ENAP

O ambiente da ENAP apresenta os seguintes ativos de infraestrutura DE ti que deverão ser gerenciados pela CONTRATADA:

ATIVO	QUANTIDADE
Estações de Trabalho	500
Equipamentos servidores	534
Infraestrutura de E-mail G-Suite	1
Infraestrutura de E-mail Microsoft 365	1
Caixas de correio eletrônico	500
Perfis executivos	10
Usuários	500
Aplicações Web	104
Datacenter físico	1
Infraestrutura em Nuvem	4
Ativos digitais (marcas, apps, faixas de endereço IP, contas em redes sociais)	5000

Tabela – Infraestrutura da ENAP

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

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

1.1. A solução de TIC consiste em um conjunto de soluções, divididas em três grupos, componentes de serviços gerenciados de segurança da informação e de segurança cibernética a fim de viabilizar o apoio à gestão de segurança da informação, de riscos cibernéticos e de conformidade baseados nas melhores práticas e frameworks do mercado no âmbito da Escola, bem como entregar serviços de monitoramento e de visibilidade de ataques cibernéticos, além do monitoramento, detecção e tratamento de incidentes de segurança cibernética concernentes aos ativos de Tecnologia da Informação da ENAP.

1.2. A prestação de serviço do Grupo 01 envolve:

1.2.1. **ITEM 01: Serviço de Monitoramento e Visibilidade de Ataques Cibernéticos** que tem como finalidade aplicar inteligência voltada para a segurança da marca ENAP, com o objetivo de realizar buscas contínuas em diversas camadas da internet, incluindo a Surface, Deep e Dark Web. Essas buscas têm como foco a identificação de informações sensíveis que possam estar sendo discutidas ou comercializadas de forma ilegal, tais como dados confidenciais, informações privilegiadas ou quaisquer outros tipos de conteúdo que possam representar uma ameaça à integridade da ENAP.

1.3. A prestação de serviço do Grupo 02 envolve:

1.3.1. **ITEM 02: Serviço de Monitoramento, Detecção e Resposta a Incidentes que** tem como objetivo prover à ENAP mecanismo de visibilidade de logs, rede e informações, capaz de identificar eventos maliciosos, através de correlacionamento de logs e tráfego de rede sob um regime de monitoramento de 1500 eventos por segundo, que possam comprometer os serviços tecnológicos da ENAP.

1.4. **DOS SERVIÇOS ESTRATÉGICOS GERENCIADOS DE SEGURANÇA DO GRUPO 01**

1.4.1. **ITEM 01** – SERVIÇOS MONITORAMENTO E VISIBILIDADE DE ATAQUES CIBERNÉTICOS

1.4.1.1. A CONTRATADA deve realizar o monitoramento contínuo de fontes externas nacionais e internacionais, como Fóruns, Redes Sociais, Mídias Sociais, Nuvens Públicas e Grupos Hackers para identificação de motivações, intenções e atividades de possíveis adversários que possam causar impactos à CONTRATANTE, seja na INTERNET profunda, escura ou de superfície.

1.4.1.2. Os Serviços de Proteção de Riscos Digitais, doravante SPRD, devem suportar quatro grandes pilares: mapeamento, monitoramento, operação e mitigação contemplando plenamente as disciplinas de Threat

Intelligence & Hunting, conforme as boas práticas, frameworks e literatura atualizada.

1.4.1.3. Mapeamento, tem por objetivo coletar, identificar e entender os ativos digitais sob risco.

1.4.1.4. Monitoramento, visa o monitoramento contínuo e ininterrupto dos ativos digitais, com o objetivo de documentar, contextualizar, enriquecer e priorizar os riscos e alertas com capacidade de reportar detalhes de incidentes permitindo a tomada de decisão inteligente em relação a tais riscos.

1.4.1.5. Curadoria, visa ter um time especializado para acompanhar e validar os resultados do monitoramento em agendas recorrentes com o cliente para garantir a melhoria contínua dos resultados, captura melhor do contexto do cliente, eliminando falsos alertas, contribuindo no ajuste de novos contextos de buscas e sugerindo novos ativos para potencializar o monitoramento.

1.4.1.6. Mitigação, visa a reduzir o risco dos ativos digitais, através de:

1.4.1.6.1. Envio de alerta aos clientes via E-mail, Webhook, SMS, Ocorrências/Tickets e WhatsApp.

1.4.1.6.2. Envio de relatórios (executivo e técnico), pelo menos 1 vez por mês.

1.4.1.6.3. Procedimentos de remoção de conteúdo infrator.

1.4.1.6.4. Boletins periódicos de inteligência, contemplando

1.4.1.6.4.1. Envio de boletim quinzenal contendo os seguintes assuntos:

1.4.1.6.4.1.1. Análises de Malwares e Ransomwares com IOCs;

1.4.1.6.4.1.2. Vulnerabilidades descobertas, vulnerabilidades corrigidas e zero-days em ativos e serviços que possam afetar a infraestrutura e/ou funcionamento de empresas;

1.4.1.6.4.1.3. Perfil de atores e grupos maliciosos;

1.4.1.6.4.1.4. Grandes empresas do setor que possam ter sofrido algum tipo de ataque cibernético.

1.4.1.6.4.2. Deverão ser enviados boletins de inteligência ou relatórios de incidentes, disponibilizados nos seguintes idiomas: Português.

1.4.1.7. Todos os serviços descritos pertencem a um único objeto e bloco de contratação denominado **SPRD**. Todas as características e requisitos exigidos neste documento serão confirmadas em diligência presencial.

1.4.1.8. DETALHAMENTO DO OBJETO DA CONTRATAÇÃO: são

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

1.4.1.9. Canais de Suporte

1.4.1.10. Para abertura de solicitações a CONTRATADA deverá possuir formulário dentro da própria plataforma de SPRD.

1.4.1.11. O sistema deverá permitir minimamente a filtragem de chamados de suporte através de status, tipo de chamado e prioridade.

1.4.1.12. Deve permitir ordenar a listagem de chamados por prioridade, status, data (a partir do mais antigo e a partir do mais recente) e por solicitante.

1.4.1.13. O sistema deverá apresentar o histórico dos chamados de suporte permitindo visualizar informações relevantes de sua abertura, tais como status, solicitante, data de abertura, data de cada interação com o chamado e conteúdo das interações.

1.4.1.14. O sistema deve permitir a reabertura de chamados que tenham sido fechados, retornando estes ao status de aberto, reiniciando o atendimento.

1.4.1.15. O sistema da CONTRATADA deverá permitir o acompanhamento de chamados dentro da console do produto, ao invés de apenas solicitações por e-mail. Deve permitir à CONTRATANTE realizar o acompanhamento dos chamados, tal como a adição de comentários, anexos de arquivos e mudança de status diretamente pela console do produto.

1.4.1.16. Horário de Atendimento: os serviços devem obrigatoriamente ser executados, ofertados, e estarem acessíveis ao CONTRATANTE em regime de 24 (vinte quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante todo o período de vigência do contrato.

1.4.1.17. Mapeamento de Ativos:

1.4.1.18. O SPRD deve ser capaz de entregar à CONTRATANTE a visualização de todos os termos/ativos monitorados e permitir o seu

gerenciamento, como por exemplo, sua ativação, desativação, exclusão ou a adição de novos ativos.

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

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

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

1.4.1.21.1. Domínios: Nome que serve para localizar e identificar conjuntos de computadores na internet. O nome de domínio foi concebido com o objetivo de facilitar a memorização dos endereços de computadores na Internet.

1.4.1.21.2. Marcas: A marca registrada, nome fantasia, nome do produto, nome de fachada, razão social, termo ou expressão que identifique o CONTRATANTE.

1.4.1.21.3. BIN (*Bank Identification Number*): Números do cartão de crédito para identificar o banco emissor e a conta do cliente. Os primeiros seis dígitos, liderados pelo primeiro dígito que identifica a bandeira do cartão, são coletivamente conhecidos como o número de identificação do emissor e denominados números de identificação bancária.

1.4.1.21.4. Endereço IP: Endereço de Protocolo da Internet, do inglês Internet Protocol address, é um rótulo numérico atribuído a cada dispositivo conectado a uma rede de computadores que utiliza o Protocolo de Internet para comunicação.

1.4.1.21.5. Pessoa: Informação de identificação pessoal de empregado ou pessoa de interesse para monitoramento de riscos digitais dirigidos à pessoa física.

1.4.1.21.6. APK: Monitora a disponibilidade de aplicativos a partir do package name.

1.4.1.22. O SRPD deve:

1.4.1.22.1. Permitir que o ativo em monitoramento seja apenas desabilitado, para que pare de gerar alertas sem precisar ser excluído da console.

1.4.1.22.2. Apresentar em sua tela de gestão de ativos a lista completa de ativos cadastrados, estejam eles habilitados ou desabilitados, contendo o tipo de ativo, o nome do ativo e a quantidade de eventos que este ativo já recebeu.

1.4.1.22.3. Permitir visualizar em formato resumido a distribuição das quantidades de ativos por severidade, tipo e status.

1.4.1.23. Monitoramento

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

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

1.4.1.26. As informações devem ser apresentadas à CONTRATANTE no formato de evento, contextualizado com o tipo de risco associado de maneira automática, permitindo que a CONTRATANTE parametrize consultas, queries, alertas ou qualquer tipo de ação relacionada de forma deliberada de acordo com cenários desejados. Esta cláusula não dispensa a CONTRATADA de realizar customizações da plataforma para monitoramento, gestão, geração de alertas, e configurações adicionais que não possam ser realizadas pela CONTRATANTE.

1.4.1.27. A solução deve permitir a realização ilimitadas de buscas nos dados coletados das diversas fontes previstas na plataforma, incluindo buscas avançadas com critérios e entidades diferentes;

1.4.1.28. A plataforma deverá fornecer coleta de informações em, no mínimo, 90 (noventa) grupos de Ransomware.

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

1.4.1.29.1. Menção ao cliente, Linguagem Ofensiva, Fraude Cibernética, Exposição de Credenciais, Personificação a um perfil de mídia social, Exposição de chaves, Phishing.

1.4.1.29.2. Correlacionar as informações coletadas, utilizando plataforma de big data para processamento visando normalizar informações, gerando listas acionáveis de inteligência contra ameaças.

1.4.1.29.3. A plataforma deve por exemplo ter a capacidade de ao encontrar um dump de senhas que cite credenciais da CONTRATANTE, apresentar evidência referente apenas a CONTRATANTE ao invés de apresentar o dump completo para que a CONTRATANTE pesquise manualmente.

1.4.1.29.4. Ao verificar por exemplo uma conversa de grupo ou fórum de fraudes menciona a CONTRATANTE, a CONTRATADA deve apresentar somente as mensagens do contexto de risco à CONTRATANTE e não a conversa completa contendo itens que não são relevantes para a CONTRATANTE.

1.4.1.29.5. A plataforma deve ter capacidade de ao ler as informações da Internet que poderão se transformar em um evento, reconhecer no mínimo o que é um(a) CPF, URL, e-mail, comandos normalmente associados a bancos de dados, convite de um chat de mensageria eletrônica, secret key da AWS, API Client ID e Client Secret do Facebook, Google CloudAPI e OAuth key, chave privada, Souce Token, Sendgrid API Key, SonarQube API Key, Twitter client ID, arquivo de configuração do WordPress, menção de Checker com URL, Contas Laras, Currículo Vitae, IPv4, Bin de cartão de crédito.

1.4.1.30. Deverá fornecer coleta de informações para realização de pesquisas em redes sociais e aplicativos, para, no mínimo: Twitter, Facebook, Youtube, Instagram, TikTok, LinkedIn, WhatsApp, Discord, Telegram, Pastebin, Scribd, Apple Store, 4Shared, Google Play, Vimeo, Github, OLX e Mercado Livre.

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

1.4.1.32. Deve ter capacidade para análise de áudio de no mínimo 1 plataforma de mensageria para caso identifique correspondência com os critérios pesquisados, fazer a transcrição de áudio em questão e transformá-lo em evento indicando no mesmo a transcrição do áudio em questão.

1.4.1.33. Na transcrição dos áudios analisados nos vídeos, deverá ser possível destacar informações relevantes de acordo com os ativos digitais definidos pelo CONTRATANTE.

1.4.1.34. O áudio (completo), bem como seus metadados, onde foi encontrado algum resultado, deve ser capturado, identificado e disponibilizado para análise.

1.4.1.35. Realizar análise de conteúdo de imagens (OCR) permitindo que um screenshot contendo uma ameaça a algum dos ativos digitais da

CONTRATANTE seja detectada e notificada.

1.4.1.36. Por exemplo, uma captura de tela de uma credencial do acesso da CONTRATANTE.

1.4.1.37. Todos os incidentes reportados devem conter informações de log sendo possível determinar:

1.4.1.38. O ativo digital ao qual aquele determinado incidente se refere;

1.4.1.39. A data e hora em que houve a coleta da informação;

1.4.1.40. A data e hora em que a informação foi analisada;

1.4.1.41. A data e hora em que a informação se transformou em um risco exibido na console do CONTRATANTE.

1.4.1.42. A prioridade do risco determinada pelo SPRD.

1.4.1.43. O tipo do incidente e a sua origem.

1.4.1.44. O SPRD deve disponibilizar as informações das pesquisas por, no mínimo: intervalo de data, status, severidade, categoria, contexto, metadados e tipo da fonte.

1.4.1.45. Para as quantidades de ativos digitais presentes neste documento, não poderá haver limitação da quantidade de alertas gerados pelo serviço da CONTRATADA.

1.4.1.46. As ocorrências devem possuir um campo de descrição em que os analistas possam contextualizar as informações associadas.

1.4.1.47. Diretamente a partir de um incidente aberto pela ferramenta deve ser possível solicitar o serviço de remoção de conteúdo infrator (takedown) caso o cliente tenha contratado essa opção.

1.4.1.48. O serviço deverá realizar a detecção de domínios registrados que possam oferecer riscos de serem utilizados de forma maliciosa, através do registro de domínios com variações comuns de nome, permutações de caracteres e outros (typosquatting, nomes de domínios similares).

1.4.1.49. Deve possibilitar a descoberta de páginas de phishing ativas utilizando o nome, a marca e a identidade visual da CONTRATADA

1.4.1.50. O serviço deverá realizar a detecção de domínios registrados que possam oferecer riscos de serem utilizados de forma maliciosa, através do registro de domínios com variações comuns de nome, permutações de caracteres e outros (typosquatting, nomes de domínios similares).

1.4.1.51. Deve possibilitar a descoberta de páginas de phishing ativas utilizando o nome, a marca e a identidade visual da CONTRATADA.

1.4.1.52. Deve possibilitar a descoberta de páginas de phishing ativamente, a partir da detecção de clones das aplicações da CONTRATANTE, independentemente de onde estes estejam sendo executados.

1.4.1.53. Deve possuir pelo menos 200 regras pré-definidas para detecção e coleta de eventos de segurança.

1.4.1.54. Permitir a criação e acompanhamento de Incidentes de Segurança, de forma manual ou automática.

1.4.1.55. Possuir a capacidade de criação de interpretadores (coletores) para aplicações proprietárias e/ou não conhecidas, de forma que:

1.4.1.55.1. A Criação seja feita de forma intuitiva e deverá ser realizada dentro da própria ferramenta, via interface web, possibilitando configuração não só pela CONTRATADA como pela própria CONTRATANTE;

1.4.1.55.2. Não seja limitada a 1 coletor por fonte de pesquisa;

1.4.1.55.3. Permitir a aplicação de filtros nos coletores para direcionamento das informações a serem indexadas e monitoradas;

1.4.1.55.4. Deve possuir opção para configuração de periodicidade da coleta;

1.4.1.56. Deve possuir foco no sistema financeiro brasileiro com fontes relevantes relacionadas a grupos de fraudadores.

1.4.1.57. Deve permitir a inclusão e o monitoramento de novos grupos dos aplicativos de mensageria, incluindo grupos que eventualmente sejam solicitados pela CONTRATANTE.

1.4.1.58. Extrair, no mínimo, os seguintes metadados de cada mensagem: autor, aplicativo de origem e data e hora, com precisão de segundos, dos momentos de envio e coleta.

1.4.1.59. Monitorar redes de compartilhamento de textos e a plataforma de compartilhamento de códigos.

1.4.1.60. O serviço não deverá possuir limitação na capacidade de análise de ativos digitais.

1.4.1.61. O módulo de monitoramento deve permitir o uso de regras YARA ou equivalente, inclusive, permitindo o cadastro de regras por solicitação da CONTRATANTE.

1.4.1.62. Para eventos do tipo Informação, não é requerido qualquer tipo

de ação, podendo estes serem apenas mantidos temporariamente na solução para posteriormente serem descartados.

1.4.1.63. Deve existir a garantia por parte da CONTRATADA, que uma interface humana, ou seja, uma analista que pertence ao grupo de monitoramento de ataques, esteja validando e impedindo o envio de falsos positivos para a CONTRATANTE.

1.4.1.64. Deve oferecer canais de comunicação integrados para funcionários do CONTRATANTE, requisitarem e receberem devolutivas de incidentes detectados pela solução.

1.4.1.65. Deve possuir módulo de visualização de eventos, seus tipos e suas respectivas severidades, através de dashboard. Onde possa ser possível filtrar minimamente por período e realizar o download do mesmo em formato PDF, DOCX e HTML.

1.4.1.66. Nos detalhes de todos os eventos apresentados pela solução de SPRD, deve ser possível verificar no mínimo o horário em que o evento foi coletado, o horário em que o evento foi enriquecido e/ou processado, o horário em que o evento foi preparado para análise seja ela manual ou automática, e o horário em que o evento foi disponibilizado na console do produto para consumo da CONTRATANTE.

1.4.1.67. A configuração de alertas deve permitir a criação de notificações granulares a partir dos eventos da plataforma. Entre os critérios que devem estar disponíveis para configuração de alertas estão:

a) Categoria do Evento;

b) Tipo do Evento;

c) Severidade;

d) Filtro de Palavra-Chave.

1.4.1.68. Mitigação

1.4.1.69. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de sites maliciosos, sites que contenham phishing ou sites/domínios que disparem phishing que utilizem o nome, a marca ou a imagem, mesmo que similar (com intuito de confundir), os clientes da CONTRATADA.

1.4.1.70. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de perfis falsos de funcionários (Executivos) e da própria empresa em redes sociais;

1.4.1.71. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer tipos de informação disponíveis e acessíveis que

violem os direitos de uso do CLIENTE ou que permitam burlar os meios de proteção desses direitos;

1.4.1.72. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer tipos de informação disponíveis e acessíveis quando for identificada a tentativa de ataque à reputação da instituição ou ainda a tentativa de captura de credenciais do CLIENTE.

1.4.1.73. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer informações em redes sociais (Facebook, Twittter, Linkedin, Instagram, YouTube etc. que tenham relação com o CLIENTE e não seja autorizado por essa instituição.

1.4.1.74. Possibilitar a realização do serviço de TAKEDOWN para retirar das principais lojas de aplicativos para mobile (Google Play Store, Apple Store, etc.) os aplicativos falsos e maliciosos distribuídos fora das lojas oficiais comumente conhecidas.

1.4.1.75. Possibilitar a realização do serviço de TAKEDOWN para retirar conteúdo com documentos, informações confidenciais, informações de cartões de crédito, divulgações relacionadas a produtos e sistemas do CLIENTE, divulgações relacionadas a clientes e empregados do CLIENTE, além do monitoramento de sites de compartilhamento de arquivos e informações, sites de compartilhamento de textos (Pastebin, Ghostbin, entre outros) presentes na internet superficial.

1.4.1.76. A CONTRATADA deverá emitir um alerta, atualizado conforme andamento, para acompanhamento do processo de TAKEDOWN de cada ocorrência.

1.4.1.77. A CONTRATADA deverá disponibilizar um painel para consulta e análise de ocorrências (em andamento e finalizadas) do serviço de TAKEDOWN. Deve permitir consultas por intervalo de tempo, tipos de ocorrências e demais critérios relevantes na análise das ocorrências.

1.4.1.78. O serviço de TAKEDOWN deverá estar disponível em pacotes mensais.

1.4.1.79. Todo serviço de TAKEDOWN deve ser acompanhado de um especialista, a fim de garantir a assertividade de todo o processo.

1.4.1.80. Características Gerais e Confidencialidade:

1.4.1.81. A CONTRATADA deverá manter total sigilo e confidencialidade dos serviços prestados ao CONTRATANTE no que se refere a não divulgação, por qualquer forma, de toda ou parte das informações ou documentos a ele relativos, e aos quais venha a ter acesso, em

decorrência da prestação dos serviços executados.

1.4.1.82. Eventualmente o CONTRATANTE poderá solicitar uma reunião técnica, a ser realizada remotamente, para que um atendimento qualquer possa ser realizado e/ou acompanhado por um analista, quando a gravidade de um incidente reportado pelo SPRD for classificada como crítica.

1.4.1.83. A plataforma disponibilizada pela CONTRATADA deve oferecer conexão segura através do protocolo HTTPS.

1.4.1.84. O acesso ao SPRD deve possuir métodos de autenticação de múltiplos fatores.

1.4.1.85. A solução deverá:

1.4.1.86. Ser obrigatoriamente de propriedade da CONTRATADA, não poderá ser do tipo open source (software livre), OU

1.4.1.87. A CONTRATADA deverá ser representante formal do fabricante no Brasil.

1.4.1.88. Deverá ser obrigatoriamente de propriedade da CONTRATADA ou licenciado para uso pela CONTRATADA, não poderá ser do tipo open source (software livre).

1.4.1.89. O serviço deverá ser prestado por meio de solução fornecida através da nuvem do fabricante. Nenhum componente da solução poderá ser hospedado ou estar sob responsabilidade da CONTRATANTE.

1.4.1.90. O fabricante deverá possuir equipe de suporte em português.

1.4.1.91. Deve permitir a possibilidade de mudança de idioma do sistema para outras linguagens, tais como Inglês e/ou Espanhol.

1.4.1.92. Deve permitir extração de relatórios completos dos eventos em, no mínimo, formatos PDF, CSV e JSON.

1.4.1.93. Entre os relatórios disponíveis deverá ser possível exportar em um único documento em formato JSON ou CSV, listagem de todas as credenciais expostas da CONTRATANTE contendo no mínimo o ID do evento gerado para aquela credencial, o nome do usuário e a respectiva senha vazada sem anonimização da mesma, a URL e a data e hora do vazamento ou caso não seja possível determinar a data hora do vazamento, informar a data e hora da disponibilização da informação na Internet.

1.4.1.94. A solução deverá permitir que um usuário administrador gerencie os acessos dos demais usuários da CONTRATANTE na

solução.

1.4.1.95. A solução deverá permitir o uso de múltiplos fatores de autenticação, por, pelo menos, e-mail e mais uma das seguintes opções: SMS ou aplicativo de token ou whatsapp.

1.4.1.96. A solução deverá permitir quantidade ilimitada de usuários com acesso à plataforma.

1.4.1.97. A solução deve manter todos os dados e informações da CONTRATANTE, não coletados diretamente de fontes abertas, em território nacional sendo expressamente proibido que estes sejam processados no exterior.

1.4.1.98. Papéis e Responsabilidades

1.4.1.99. Deverá ser empregada na prestação de serviço deste contrato, os seguintes papéis e responsabilidades dos profissionais:

1.4.1.100. Patrocinador do Projeto (CONTRATANTE): é o gerente da Unidade de Tecnologia da Informação, responsável por representar os interesses do CONTRATANTE no contexto da presente contratação, pela aprovação da necessidade, dos objetivos e, por fim, pela negociação das ações necessárias para a melhoria contínua dos serviços.

1.4.1.101. Gestor do Contrato (CONTRATANTE): é o funcionário formalmente designado pelo CONTRATANTE, responsável pelo monitoramento da prestação do serviço ao longo do período de vigência do contrato e pela participação no planejamento da contratação, pela verificação dos resultados pretendidos. É o responsável pelo fornecimento das informações necessárias para a ativação do contrato.

1.4.1.102. Preposto (CONTRATADA): é o profissional indicado pelo Fornecedor de Serviço para representá-la administrativa e tecnicamente. É o responsável pela coordenação operacional das atividades previstas de forma a solucionar qualquer dúvida, conflito ou desvio técnico que possa comprometer a execução do contrato. Deverá ter bons conhecimentos em segurança da informação e também é responsável pela interlocução com o Gestor do Contrato do CONTRATANTE.

1.4.1.103. As qualificações técnicas exigidas para o perfil de PREPOSTO da CONTRATADA:

Certificações	Descrição
Ao menos uma das certificações de segurança da informação: CISSP (Certified Information Systems Security Professional); CISM (Certified Information Security Manager; CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials); GCIH (GIAC Incident Handler) GMON (GIAC Continuous Monitoring);	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência mínima de 5 (cinco) anos em coordenação e gestão de contratos de serviços continuados.

1.5. **DOS SERVIÇOS OPERACIONAIS GERENCIADOS DE SEGURANÇA DO GRUPO 02**

1.5.1. **ITEM 02** – SERVIÇO DE MONITORAMENTO, DETECÇÃO E RESPOSTA A INCIDENTES

1.5.1.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados à ENAP, através de fornecimento de serviços com capacidade de correlacionamento de eventos, para detecção de ameaças direcionadas a CONTRATADA para detecção de comportamento anômalo de serviços, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.

1.5.1.2. APOIO À GESTÃO DA SEGURANÇA DA INFORMAÇÃO

1.5.1.2.1. Perfil do Profissional:

1.5.1.2.1.1. A CONTRATADA deverá disponibilizar, pelo menos, um profissional sênior com as seguintes qualificações:

a)Certificação (ISC)² CISSP ou ISACA CISM;

b) Experiência mínima de 5 anos em gestão da segurança da informação;

c) Conhecimento comprovado de normas e boas práticas de segurança (ISO 27001, ISO 27002, ISO 27005, NIST

Cybersecurity Framework, CIS Controls);

d) Habilidades de comunicação, liderança e relacionamento interpessoal.

1.5.1.2.2. Atividades Esperadas:

1.5.1.2.2.1. Apoio à ENAP na jornada de implantação de um SGSI (Sistema de Gestão de Segurança da Informação) que envolvam:

a) Elaborar um cronograma de implementação do SGSI, alinhado com a ISO/IEC 27001.

b) Definir os escopos do SGSI e identificar os ativos de informação críticos.

c) Realizar análise de riscos de segurança da informação e definir tratamento de riscos.

d) Auxiliar na seleção e implementação de controles de segurança da informação, de acordo com a ISO/IEC 27002.

e) Elaborar documentação do SGSI, incluindo políticas, procedimentos e registros.

f) Preparar a ENAP para a certificação ISO/IEC 27001, se aplicável.

1.5.1.2.2.2. Apoio à ENAP nas atividades de criação/revisão de documentos de segurança da informação que envolvam:

a) Elaborar/revisar o Plano de Gestão de Riscos de Segurança da Informação, alinhado com a ISO/IEC 27005.

b) Elaborar/revisar a Política de Segurança da Informação.

c) Elaborar/revisar o Plano de Gestão de Incidentes Cibernéticos.

d) Elaborar/revisar o Programa de Privacidade de Dados, alinhado com a LGPD.

1.5.1.2.2.3. Assessoria em Projetos de Segurança da Informação da ENAP que envolvam:

a) Participar de projetos de segurança da informação e privacidade de dados.

b) Fornecer análises de risco e recomendações de segurança.

c) Revisar a arquitetura e o design de soluções de segurança.

d) Acompanhar a implementação de projetos de segurança.

1.5.1.2.2.4. Apoio em atividades de Treinamento e Conscientização aos usuários da ENAP que envolvam:

a) Elaborar e ministrar treinamentos de segurança da informação para os colaboradores da ENAP.

b) Desenvolver campanhas de conscientização sobre segurança da informação.

c) Avaliar a eficácia dos programas de treinamento e conscientização.

1.5.1.2.2.5. Apoio executivo no Monitoramento de Ameaças que envolvam:

a) Acompanhar as tendências e ameaças de segurança cibernética.

b) Avaliar o impacto potencial das ameaças na ENAP.

c) Propor e implementar ações de mitigação de riscos.

1.5.1.2.2.6. Geração de Relatórios de Postura de Segurança que envolvam:

a) Elaborar relatórios periódicos sobre a postura de segurança da informação da ENAP.

b) Avaliar a maturidade do SGSI e identificar oportunidades de melhoria.

c) Apresentar os relatórios à gestão da ENAP e discutir as ações recomendadas.

1.5.1.2.3. Carga Horária e Disponibilidade:

1.5.1.2.3.1. O serviço será prestado, em formato híbrido (presencial e remoto), de forma contínua ao longo da vigência do contrato conforme necessidade da ENAP com uma carga horária de 08 horas semanais.

1.5.1.3. GAP ANALYSE

1.5.1.4. A CONTRATADA deverá realizar nos primeiros meses após o início do contrato, a Análise de Superfície (Assessment) baseada em MITRE ATT&CK® no ambiente tecnológico da ENAP para reduzir o risco iminente de incidentes de segurança

1.5.1.5. O assessment de MITRE ATT&CK® identifica as técnicas que os adversários podem usar durante um ataque, bem como conceitos e informações básicas sobre grupos de adversários, para avaliar a postura de segurança dos negócios e dos fornecedores de segurança, nesse processo deverão ser checadas a principais Táticas de ataque, técnicas e subtécnicas;

1.5.1.6. Os entregáveis dessa etapa são:

1.5.1.7. Relatório de GAPs;

1.5.1.8. Infográfico de Maturidade;

1.5.1.9. Artefatos de Avaliação;

1.5.1.10. Avaliação das Técnicas e Sub Técnicas;

1.5.1.11. Matriz de Priorização;

1.5.1.12. Este serviços está condicionado ao PLANO DE GESTÃO DE INCIDENTES CIBERNÉTICOS a ser criado durante a execução do serviço definido na subseção APOIO À GESTÃO DA SEGURANÇA DA INFORMAÇÃO deste item ou em posteriores alterações devidamente aprovadas pela ENAP

1.5.1.13. Para execução deste serviço, a CONTRATADA deverá utilizar e ser capaz de fornecer, operar, sustentar e suportar soluções de

monitoramento que atendam o descritivo técnico a seguir.

1.5.1.14. REQUISITOS GERAIS

1.5.1.15. O serviço técnico especializado inclui no mínimo as seguintes atividades:

1.5.1.16. A CONTRATADA será responsável pela implementação, suporte, administração diária e sustentação de todos os serviços envolvidos neste certame, contemplando qualquer envolvimento em qualquer demanda que tenha relação com as soluções envolvidas.

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

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

1.5.1.19. Entende-se por administração diária, que a CONTRATADA será responsável pela administração de todos os passos técnicos e processos que envolvem os serviços contratados, de forma que as mesmas sejam 100% integradas ao ambiente da CONTRATANTE, porém utilizando a mão de obra da CONTRATADA.

1.5.1.20. Entende-se por sustentação, que a CONTRATADA será responsável pela tratativa de todas as saídas técnicas que envolvem os serviços contratados, sendo responsáveis pela implementação de cada processo, integração ou interação técnica de qualquer natureza envolvendo os serviços contratados.

1.5.1.21. Fica fora do escopo da CONTRATADA, apenas atividades que envolvam interação com as ferramentas de rede e infraestrutura da CONTRATANTE, porém a CONTRATADA ainda fica responsável pela indicação de todas as necessidades de atuação para que os times responsáveis possam desenvolver suas tarefas e atender a novas demandas técnicas elencados pelos serviços contratados

1.5.1.22. A CONTRATADA deverá seguir o processo de mudança estabelecido pelo CONTRATANTE

1.5.1.23. A CONTRATADA deverá implementar conceitos de Threat Hunting, monitorando de forma contínua todos eventos correlacionados.

1.5.1.24. As manutenções preventivas e/ou corretivas, que representem risco de interrupção do(s) serviço(s), deverão ser agendadas e realizadas fora do horário regular, salvo quando expressamente autorizado.

1.5.1.25. As manutenções programadas, que impliquem em extensiva parada do ambiente, serão realizadas durante um final de semana. Tais atividades realizadas fora do horário regular não ensejarão qualquer pagamento adicional em relação ao estabelecido no contrato, portanto a CONTRATADA deverá prever esta situação em sua composição de custos.

1.5.1.26. Todos os serviços de manutenção corretiva e preventiva são considerados de natureza contínua e deverão minimizar a necessidade de parada do ambiente em produção

1.5.1.27. A contrata deverá de forma proativa, analisar políticas e processos de segurança da CONTRATANTE e realizar sugestões de melhoria a serem implementadas em conjunto com todas as equipes envolvidas.

1.5.1.28. Os serviços deverão ser executados por profissionais habilitados, com base em programas de formação e/ ou certificações oficiais dos serviços envolvidos neste Certame

1.5.1.29. A CONTRATADA deverá elaborar e manter atualizados os Planos de Capacidade, de Gerenciamento de Incidentes, de Disponibilidade, de Continuidade e de Recuperação de Desastres para os serviços objeto deste Termo.

1.5.1.30. Os serviços devem ser executados de acordo com normas, procedimentos e técnicas adotadas pela CONTRATANTE.

1.5.1.31. Deverá ser fornecido ao CONTRATANTE acesso à console dos serviços fornecidos para que seja possível o acompanhamento, auditoria e direcionamento de ações no ambiente

1.5.1.32. A CONTRATADA deverá comunicar a CONTRATANTE quanto à ocorrência de qualquer incidente de segurança, seguido de todas as ações de remediação realizadas.

1.5.1.33. Os contatos para notificação de incidentes críticos ou fluxos para aprovação de ações serão documentadas durante o período de implementação.

1.5.1.34. A CONTRATADA deverá assumir atividades de customização de interpretação de logs/eventos que possam não ser interpretados nativamente pelo SIEM. Tais atividades não deverão ter nenhum custo

adicional.

1.5.1.35. A CONTRATADA deverá customizar e disponibilizar dashboards/relatórios solicitados pela CONTRATANTE. Essas visões serão armazenadas na console do SIEM e poderão ser consultadas a qualquer momento. Tais atividades não deverão ter nenhum custo adicional e serão realizadas dentro do horário comercial.

1.5.1.36. Sempre que necessário, a CONTRATADA deverá customizar regras de detecção no SIEM, atendendo boas práticas de segurança da informação e também a demandas específicas da CONTRATANTE.

1.5.1.37. Qualquer atividade realizada fora do horário comercial não deverá atribuir nenhum custo adicional para a CONTRATANTE.7.2.26. Qualquer atualização de plataformas envolvidas na contratação não deverá ter nenhum custo adicional para a CONTRATANTE.

1.5.1.38. A CONTRATADA deverá realizar ações referentes a resposta a incidentes de segurança, envolvendo sempre que necessário responsáveis por soluções administradas por time terceiros, com o objetivo de manter a disponibilidade e qualidade de todos os serviços tecnológicos.

1.5.1.39. Sempre que necessário envolvimento de times terceiros que administram outras soluções da CONTRATANTE, a CONTRATADA deverá enviar os incidentes preenchidos, analisados e contextualizados, apenas para tomada de decisão e/ou execução de ações pontuais.

1.5.1.40. Toda interação com times terceiros deverão ser realizadas por e-mail ou através da ferramenta de chamados da CONTRATANTE, ficando a cargo da CONTRATANTE definir qual meio será adotado.

1.5.1.41. A CONTRATADA deverá ter fluxos de resposta a incidentes bem definidos para os mais variados tipos de incidentes existentes.

1.5.1.42. A CONTRATADA deverá criar relatórios gerenciais a serem apresentados e entregues para a CONTRATANTE mensalmente, em dia a ser definido no período de implementação. Os dados deste relatório poderão ser customizados a pedido da CONTRATANTE, de modo a atender necessidades específicas de negócio. Adicionalmente, os relatórios devem conter índices de resposta a incidentes, indicadores e efetividade de todos os serviços contratados.

1.5.1.43. Todas as ações de resposta a incidentes executadas pela CONTRATADA deverão ser armazenadas em procedimentos operacionais, para consultas sempre que necessário.

1.5.1.44. A contratada deverá detectar e reportar qualquer tipo de incidente que tenha características de reincidência.

1.5.1.45. Serão considerados incidentes de segurança, minimamente, as seguintes ações:

1.5.1.45.1. Aplicações maliciosas detectadas em estações de trabalho e servidores;

1.5.1.45.2. Exploração de vulnerabilidades;

1.5.1.45.3. Uso indevido de credenciais;

1.5.1.45.4. Phishing ou spam;

1.5.1.45.5. Ataques de Força Bruta;

1.5.1.45.6. Execução de códigos ou scripts maliciosos;

1.5.1.45.7. Ataques de saturação;

1.5.1.45.8. Comunicações com IPs ou domínios maliciosos;

1.5.1.45.9. Atividades que tenham o intuito de comprometer a integridade de ativos e entidades da CONTRATANTE;

1.5.1.45.10. Atividades que tenham o intuito de comprometer a confidencialidade de informações da CONTRATANTE;

1.5.1.45.11. Atividades que tenham o intuito de comprometer a disponibilidade dos serviços tecnológicos oferecidos pela CONTRATANTE.

1.5.1.46. A CONTRATADA deverá disponibilizar um canal, por e-mail, possibilitando que a CONTRATANTE comunique qualquer incidente de segurança não detectado por soluções de segurança existentes, para que as devidas investigações sejam realizadas.

1.5.1.47. A CONTRATADA deverá operar todas as plataformas contidas nesta contratação, de forma a realizar todas as atividades pertinentes às mesmas (Exceto ações de infraestrutura específicas administradas pela CONTRATANTE), seguindo melhores práticas recomendadas pelos fabricantes e potencializando ao máximo a capacidade de entrega de cada plataforma.

1.5.1.48. A CONTRATADA deverá entregar um relatório de implementação das soluções (as-built) contidas neste certame, contendo todos os passos realizados para implementação e configuração das soluções.

1.5.1.49. Para o faturamento mensal dos itens, a contratada deverá emitir e apresentar o “Relatório Mensal de Acompanhamento do Contrato”, que

deverá conter, minimamente:

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

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

1.5.1.49.3. Sumários de quantidade de logs ingeridos para cada fonte integrada ao

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

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

1.5.1.49.6. Sumário de toda as vulnerabilidades de segurança encontradas no período do relatório;

1.5.1.49.7. Sumário de todos os e-mails retidos, organizando por camada de proteção;

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

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

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

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

1.5.1.49.12. Resultados dos testes de campanhas de phishing realizadas com os usuários da ENAP;

1.5.1.49.13. Resultados completos de testes de segurança direcionados a solução de WAF em uso pela ENAP;

1.5.1.49.14. Resultados completos referentes ao nível de maturidade de segurança da ENAP baseado nos testes de segurança realizados.

1.5.1.50. REQUISITOS GERAIS SOLUÇÃO DE SIEM

1.5.1.51. Deve ser capaz de gerar detecções baseadas no framework do MITRE ATT&CK® possuindo associações com no mínimo 25 regras de detecções (Táticas, Técnicas ou Procedimentos) de acordo com as fases prevista no framework, de forma que TTP’s de detecções sejam atualizadas regularmente, conforme modificação no FRAMEWORK.

1.5.1.52. A solução deverá unir eventos ao longo do tempo usando modelos Kill Chain para a análise de eventos de maior risco;

1.5.1.53. Deve permitir o Hunting rápido de ameaças por meio da pesquisa em linguagem natural.

1.5.1.54. A ENAP poderá, a qualquer tempo, após a abertura de solicitação prévia, solicitar o acesso direto à console de gerenciamento da solução ofertada pela CONTRATADA, eventos e todas as funcionalidades, no modo somente leitura (read-only).

1.5.1.55. Deverá utilizar análise dos eventos em linha do tempo para facilitar a análise.

1.5.1.56. Deve funcionar, obrigatoriamente, com autenticação de dois fatores nativa.

1.5.1.57. Deve possuir parsing, para interpretação automática de logs.

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

1.5.1.59. ARQUITETURA DA SOLUÇÃO

1.5.1.60. Todas as características abordadas deverão ser atendidas por uma única solução, não sendo permitido a composição de soluções.

1.5.1.61. O serviço deve prover solução de SIEM dimensionada, a princípio, para 1500 EPS para o ambiente da ENAP, provendo a indexação e busca de informações e logs com apresentação das informações em formato técnico e executivo através de painéis orientados a cada finalidade.

1.5.1.62. Não serão aceitas soluções entregues sob estrutura de console compartilhada, devendo o ambiente lógico fornecido, ser de total e exclusivo uso da ENAP;

1.5.1.63. A solução deverá ser extremamente escalável e tolerante a falhas, capaz de ingerir terabytes por dia e suportar a retenção de eventos de segurança por longo período;

1.5.1.64. Deverá estar licenciada, em nome da CONTRATADA, de forma a manter o processamento em tempo real ou realizar o buffer dos eventos, mesmo que o tráfego de eventos ultrapasse o volume licenciado nas horas de pico.

1.5.1.65. Deve ser do tipo Nuvem em Software como um modo de Serviço e ter as certificações SOC 2 TIPO II e ISO 27001;

1.5.1.66. Deve garantir retenção dos logs conforme arquitetura abaixo:

1.5.1.67. 7 dias hot retention;

1.5.1.68. 90 dias warm retention;

1.5.1.69. 365 dias cold retention.

1.5.1.70. Deve ter alta disponibilidade e mecanismos de recuperação de desastres;

1.5.1.71. Deve permitir a filtragem e compressão de dados seletivos em até 90% no ponto de coleta;

1.5.1.72. Deve permitir o gerenciamento da largura de banda para a transmissão de dados entre os coletores e os servidores de gerenciamento;

1.5.1.73. Deve executar o armazenamento em cache local e/ou em buffer nos coletores para garantir que nenhum dado seja perdido em trânsito no caso de um problema de rede ou um pico no volume do evento;

1.5.1.74. Deve oferecer suporte ao mascaramento de dados por meio de controles de acesso granulares baseados em funções, para ofuscar qualquer informação de usuário potencialmente sensível na camada de interface do usuário;

1.5.1.75. Deve suportar controle de acesso baseado em função granular (RBAC) com suporte a administração delegada, tanto para as funcionalidades na interface do usuário quanto acesso aos dados e configurações;

1.5.1.76. Deve incluir uma ferramenta de Security Data Lake baseada em Big Data, uma arquitetura aberta e escalável e com capacidade de coletar e reter dados por períodos estabelecidos para fins de conformidade e investigação;

1.5.1.77. INTEGRAÇÕES

1.5.1.78. Deve oferecer suporte à integração com mais de 500 fontes de eventos usando nativamente no mínimo: métodos de syslog, formatos de log estruturados (CEF, LEEF, JSON, XML), arquivos, bancos de dados (conexão JDBC), conexão API (AWS, Azure, Box, Crowdstrike, SentinelOne, Trend, Symantec, Netskope, Zscaler, Skyhigh, Mcafee, SVN, Splunk, QRadar, Netwitness, Office 365, Okta, Proofpoint, Tenable, Qualys, Rapid7), WMI, consultas LDAP/LDAPS, dados e fluxo (Netflow, sFlow, jFlow), Hadoop, Registros não estruturados (Regex), agentes de terceiros (snare);

1.5.1.79. Deve permitir a integração com diferentes tipos de fontes de dados, como dados de identidade, logs de atividades / transações, logs de eventos de segurança, fluxos de rede, log de aplicativos / soluções de nuvem, permissões de acesso, fontes de inteligência de ameaças;

1.5.1.80. Deve permitir conexão a sistemas externos de gerenciamento de identidade, como Active Directory / LDAP ou soluções de IAM (gestão de identidade), como Sailpoint, CyberArk, para realizar o enriquecimento contextual de eventos adicionando identidade do usuário;

1.5.1.81. Deve ser capaz de se conectar nativamente através de APIs ou outros meios com serviços em nuvem como Amazon Web Services S3, Cloudtrail, CloudWatch, GuardDuty, VPC Flow Logs, BOX, Microsoft Azure, Office 365, Google Apps, Google Cloud, Netskope, ServiceNow, Jira, entre outros.

1.5.1.82. Deve ter uma interface de usuário que permita modificar conectores, analisadores (parsers) existentes ou construir novos analisadores (parsers) na mesma interface de usuário;

1.5.1.83. Deve ter conectores, analisadores (parsers) pré-configurados, prontos para uso, mas que possam ser modificados conforme necessário. A análise, normalização e categorização dos coletores devem ser totalmente personalizáveis na interface do usuário.

1.5.1.84. Deve ter uma API RESTful de serviços para integração bidirecional com outras tecnologias;

1.5.1.85. A CONTRATADA deve fornecer integração com pelo menos 5 fontes de inteligência de ameaças inclusas no valor do serviço ofertado;

1.5.1.86. Deve possuir mascaramento de dados (Data Masking), para proteger informações confidenciais;

1.5.1.87. Deve incluir recursos de workflow nativos e permitir criação e customizáveis para resposta a incidentes de segurança.

1.5.1.88. CAPACIDADES DE INVESTIGAÇÃO

1.5.1.89. Deve realizar o enriquecimento dos eventos com dados contextuais no momento da captura e ingestão de dados e no momento da investigação da ameaça (On Demand), adicionando aos eventos:

1.5.1.90. Identidade do usuário;

1.5.1.91. Contexto;

1.5.1.92. Metadados de ativos;

1.5.1.93. Informações de rede;

1.5.1.94. Localização Geográfica;

1.5.1.95. Dados de inteligência de ameaças.

1.5.1.96. Deve fornecer recursos abrangentes para modelar e ajustar a pontuação de risco com base no perfil do usuário e/ou entidade, gravidade da ameaça e sequência/combinação de eventos que ocorrem durante um período;

1.5.1.97. Deve permitir a modelagem de risco a partir da interface do usuário de acordo com as prioridades da organização;

1.5.1.98. Deve possuir risco score baseado em violação;

1.5.1.99. Deve ter modelos de ameaças que permitam agrupar eventos realizados por um usuário ou entidade que duram dias, semanas, meses e assim por diante. Essas atividades devem ser exibidas como uma cadeia de eliminação com cada evento categorizado em estágios predefinidos.

1.5.1.100. Deve ter algoritmos preditivos para identificar usuários de risco (por exemplo, usuários prestes a deixar a organização);

1.5.1.101. Deve fornecer análises para diferentes tipos de falhas, como relacionadas ao tempo, volume de transferência de dados, origem do evento relacionado, destino do evento relacionado, relacionadas a localização geográfica / velocidade terrestre, bem como rastrear usuários ou outras entidades nas listas de observação;

1.5.1.102. Deve haver técnicas de análise históricas de eventos pelas quais atividades suspeitas que não foram vistas antes possam ser identificadas;

1.5.1.103. Deve possuir técnicas por enumeração que permita criar linhas de base de eventos do mesmo tipo e procurar qualquer desvio do normal;

1.5.1.104. Deve ter técnicas de análise de tráfego para identificar padrões de beaconing, agentes de usuários incomuns, conexões com URLs incomuns, conexões com domínios DGA, entre outras;

1.5.1.105. Deve fornecer a capacidade de definir políticas baseadas em regras para detectar ameaças conhecidas. Essas ameaças conhecidas devem ser usadas como intensificadores de risco e combinadas com as verificações “não assinadas” nos modelos de ameaças;

1.5.1.106. Deve haver modelagem de ameaças que permita a identificação

de ameaças compostas, que se observadas isoladamente podem ser de baixo risco, porém, quando combinadas, são indicativas de um evento de alto risco;

1.5.1.107. Deve reduzir o número de falsos positivos aplicando recursos avançados de feeds de inteligência;

1.5.1.108. VISUALIZAÇÃO E RELATÓRIOS

1.5.1.109. Deve disponibilizar, a qualquer tempo, relatórios de ameaças que forneçam visibilidade da postura de segurança cibernética. Por exemplo: usuários de alto risco, ativos de alto risco, principais ameaças, principais IPs maliciosas, entre outros;

1.5.1.110. Deve disponibilizar, a qualquer tempo, relatórios que forneçam visibilidade sobre as operações de segurança. Por exemplo, para dispositivos VPN, os relatórios devem incluir as melhores sessões de VPN por duração, os principais eventos de saída de dados, a distribuição dos eventos de login por geografia, as principais tentativas de login com falha e assim por diante;

1.5.1.111. Deve disponibilizar, a qualquer tempo, relatórios de conformidade alinhados com requisitos de conformidade específicos, como PCI, SOX, HIPPA, GDPR, ISO27002;

1.5.1.112. Deve disponibilizar, a qualquer tempo, relatórios de resumo executivo de violações, incidentes e operações;

1.5.1.113. Deve disponibilizar relatórios sobre a atividade do usuário;

1.5.1.114. Deve permitir que os dados sejam exibidos com diferentes tipos de gráficos: gráfico de linhas, gráfico de barras, gráfico de pizza, mapa geográfico, tabelas, gráficos de bolhas, gráficos de relacionamento de origem e destino;

1.5.1.115. Deve permitir a visualização de dados que permitam vincular qualquer conjunto de atributos e visualização a relação entre eles;

1.5.1.116. INSTALAÇÃO E ADMINISTRAÇÃO DA SOLUÇÃO DE SIEM

1.5.1.117. A solução de SIEM deve ser implementada, sem limitação de coletores.

1.5.1.118. A ENAP fornecerá a infraestrutura necessária para implementação dos coletores, por se tratar de gateways dentro do ambiente;

1.5.1.119. A CONTRATADA deverá implementar e fazer a gestão de toda a solução de SIEM e de todos os seus componentes;

1.5.1.120. A CONTRATADA será responsável pela criação de regras de correlação que reflitam as reais necessidades do ambiente da ENAP com o objetivo de identificar possíveis incidentes de segurança;

1.5.1.121. Criar relatórios e modelos, criar filtros de pesquisa, fazer backups, criar dashboards, gerenciar usuários e utilizar os principais recursos da solução;

1.5.1.122. Apresentar plano de instalação e configuração, que deverá contemplar todos os tipos de ativos em produção na rede da ENAP.

1.5.1.123. Atualizar a solução e seus componentes para a última versão disponível compatível com a solução ofertada.

1.5.1.124. Os serviços de instalação de coletores nos ambientes da ENAP deverão ser realizados em horário previamente combinado com a ENAP, preferencialmente no horário de expediente normal da ENAP (2ª a 6ª feira, das 8h00min às 18h00min);

1.5.1.125. Qualquer atividade que possa colocar em risco o funcionamento normal das unidades da ENAP 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 a ENAP;

1.5.1.126. 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 da ENAP ou de forma remota.

1.5.1.127. PROCESSO DE MONITORAMENTO, DETECÇÃO E RESPOSTA

1.5.1.128. A CONTRATADA será responsável por implantar, operar e suportar toda a plataforma ofertada;

1.5.1.129. A fim de balizar todo o processo de monitoramento de ataques cibernéticos da ENAP, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir *ipsis litteris*.

1.5.1.130. É sabido que para o sucesso de um monitoramento de ataques cibernético, a primeira definição se deve a que tipo de ocorrência de eventos de segurança, se deseja detectar e tomar algum tipo de ação, logo será de responsabilidade da CONTRATADA como primeiro passo

deste processo, a definição de linha de base de eventos monitorados.

1.5.1.131. Tal definição de linha de base de eventos de segurança monitorados, não deve ser tomada de forma unilateral pela CONTRATADA. A ENAP deverá participar ativamente no processo de construção de forma consultiva. Porém, se ratifica que é de responsabilidade da CONTRATADA a definição, e colocar em operação tal linha de base.

1.5.1.132. Espera-se que a linha de base de eventos de segurança monitorados, seja revista de forma mensal, contudo, não se limitando a este tempo, pois todos os dias novos ataques são projetados no mundo, e se espera que a CONTRATADA tome ciência destes ataques, e por sua vez atualize a linha de base, para que em um cenário onde estes novos ataques sejam direcionados a ENAP, sejam detectados através dos serviços em questão.

1.5.1.133. O produto de um evento é a correlação dos logs gerados pelos itens de configuração do parque da ENAP. Uma vez definida a linha de base de eventos, será também de responsabilidade da CONTRATADA avaliar se todos os insumos para a correta geração do evento, estão sendo enviados corretamente para a ferramenta.

1.5.1.134. Caso a CONTRATADA identifique a ausência dos insumos (eventos) a ser gerado por um item de configuração, será de responsabilidade da CONTRATADA a correção e/ou habilitação de tal insumo dos itens de configuração. Caso o item de configuração não pertencer ao objeto contratado, porém necessário para a correta geração do evento, deverá a CONTRATADA solicitar à ENAP a correção e/ou habilitação de tal insumo no item de configuração em questão.

1.5.1.135. Dar-se-á então o passo de classificação do evento, também de responsabilidade da CONTRATADA. O grupo de monitoramento de ataques da CONTRATADA deve focar as ações nos eventos que são significativos. Logo, tal grupo deve analisar todos os eventos apresentados, classificando-os nos seguintes grupos, a saber:

1.5.1.136. Eventos de Informação: Estes eventos não requerem qualquer ação. São usados para fazer verificação de funcionalidade dos itens de configuração de segurança. Ou seja, tem por objetivo puro e simples, identificar se as ferramentas e soluções estão funcionando dentro do esperado. Estes eventos são também úteis para gerar estatísticas como, por exemplo, porcentagem de hosts com a última vacina de antivírus do dia.

1.5.1.137. Eventos de Aviso: Este grupo de eventos deve ser utilizado quando existe algum comportamento anômalo, se comparado a linha de base de operação padrão do ambiente (serviço ou solução), porém, ainda não gerou algum tipo de impacto ao ambiente (serviço ou solução) do ENAP, como por exemplo fictício: É esperado que exista 1.000 (mil) ataques do tipo port scan bloqueados pelo firewall, porém, na última hora, este número passou para 10.000 (dez mil) ataques, todavia, o firewall ainda continua bloqueando sem que haja degradação da performance do ambiente (serviço, tráfego e/ou solução).

1.5.1.138. Eventos de Exceção: Estes eventos são aqueles que sugere que os pilares de segurança da informação (confidencialidade, integridade e conformidade), foram impactados como, por exemplo: Uma infecção gerada por um malware do tipo ransomware, onde não tenha sido bloqueada pela solução de antivírus da ENAP. Este é o único tipo de evento que pode iniciar o processo de resposta a incidentes de segurança.

1.5.1.139. Uma vez classificado o evento, se inicia o passo de resposta ao mesmo, que também é de responsabilidade da CONTRATADA. As respostas são baseadas nos grupos de classificação de eventos, a saber:

1.5.1.140. Para eventos do tipo informação, não é requerido qualquer tipo de ação, porém, como já mencionado no presente documento, tais eventos são utilizados para verificação do perfeito funcionamento das soluções de segurança. Portanto, a CONTRATADA deverá utilizá-los para tal fim.

1.5.1.141. Para eventos do tipo Aviso, a CONTRATADA deverá garantir que uma interface humana, ou seja, uma analista que pertence ao GRUPO DE MONITORAMENTO DE ATAQUES, esteja validando se tal evento pode se transformar em um evento do tipo exceção, e obviamente tomar as ações cabíveis para identificar a causa raiz da mudança de comportamento do ambiente.

1.5.1.142. Para eventos do tipo Exceção, a CONTRATADA deverá transformar tal evento em um incidente de segurança, realizando, portanto, a abertura na ferramenta de incidente de segurança da informação definida no PROCESSO DE MONITORAMENTO, DETECÇÃO E RESPOSTA, descrito no presente documento. Após a abertura do incidente de segurança, obedecendo os critérios estabelecidos para tal, se encerra a participação do grupo de monitoramento de ataques.

1.5.1.143. Como último passo do processo, a CONTRATADA deve encerrar os eventos após as devidas ações tomadas, conforme definido no parágrafo acima. Eventos podem ter apenas dois tipos de status “aberto” ou “encerrado”, ou seja, após o correto tratamento, o evento deverá ter seu status alterado na ferramenta de “aberto” para “encerrado”.

1.5.1.144. Importante ressaltar que todo o processo de tratamento do evento, independente de qual fase e/ou status, deve ser registrado no módulo de tratamento de eventos da ferramenta. Também é responsabilidade da CONTRATADA a segurança dos eventos, e fica expressamente proibido a remoção de qualquer evento, independentemente de sua classificação e fase de tratamento.

1.5.1.145. PROCESSO DE CAÇADA CONTÍNUA A AMEAÇAS

1.5.1.146. Com o aumento do volume e complexidade das ameaças será exigido que a empresa CONTRATADA execute processos proativos e manuais de caçada de ameaças (Threat Hunting) no ambiente da ENAP. A fim de balizar todo o processo de caçada de ameaças, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir *ipsis litteris*.

1.5.1.147. A CONTRATADA deverá inclusive nos finais de semana e feriados, a:

1.5.1.148. Definir uma hipótese e uma declaração de uma possibilidade de ameaça, tal hipótese deve ser elaborada utilizando como referência novos vetores de ameaças e novas tendências baseadas em inteligência de ameaças e fontes de riscos digitais, informações relevantes coletadas por processos de aprendizagem de máquina e inteligência artificial e investigações de táticas, técnicas e procedimentos criando desta forma uma hipótese de como ameaças podem existir dentro do ambiente e de como encontrá-las;

1.5.1.149. Uma vez que a hipótese tenha sido definida a CONTRATADA deverá realizar um plano de coleta dos eventos dentro das plataformas relevantes de acordo com a hipótese definida;

1.5.1.150. Uma vez que os eventos relevantes estejam disponíveis, a CONTRATADA deverá avaliar a massa de eventos para buscar anomalias associadas a hipótese definida;

1.5.1.151. Caso sejam encontrados eventos maliciosos, estes entram no

processo de resposta a incidentes de segurança da informação, conforme descrito neste documento;

1.5.1.152. Caso não sejam encontrados eventos maliciosos, o processo de caçada é finalizado, sendo repetido no dia seguinte com uma nova hipótese;

1.5.1.153. Todo processo deve ser documentado através da plataforma de ITMS da CONTRATADA, incluindo qual hipótese foi utilizada, quais dados foram analisados e o resultado da análise;

1.5.1.154. GRUPO TÉCNICO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS

1.5.1.155. Através dos seus 02 (dois) centros de operação de segurança, a CONTRATADA deverá manter uma torre de operação denominada GRUPO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS, com objetivo e foco de trabalhar no processo de monitoramento de ataques cibernéticos.

1.5.1.156. Este grupo deverá ser exclusivo para trabalhar no serviço em questão, não podem os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem, com os demais serviços descritos no objeto do presente documento.

1.5.1.157. Todos os profissionais que integram GRUPO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS, devem obrigatoriamente compor o quadro de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho), sendo proibida a terceirização ou subcontratação de tal serviço.

1.5.1.158. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no tópico CATÁLOGO DE SERVIÇO e NMS – NÍVEIS MÍNIMOS DE SERVIÇOS do presente documento.

1.5.1.159. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para executar o processo de monitoramento de ataques cibernéticos da ENAP, a CONTRATADA deverá, obrigatoriamente, compor o GRUPO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS, com 02 (dois) profissionais para cada perfil que segue descrito abaixo:

Perfis	Certificações	Descrição
• Analista de Segurança I	• Certified in Cybersecurity – CC (ISC)	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.
• Analista de Segurança II	• Certified Ethical Hacker	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM. Experiência comprovada de no mínimo 36 (trinta e seis) meses em segurança da informação.
• Analista III	• Certificação da solução a ser utilizada no serviço	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.

Tabela - Certificações Grupo de Monitoramento de ataques.

1.5.1.160. Todos os profissionais deverão possuir diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

1.5.1.161. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS, porém, conforme já foi mencionado neste documento, este(s) deve(m) compor única e exclusivamente o time denominado GRUPO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS.

1.5.1.162. No momento da assinatura do contrato, será exigido da CONTRATADA, as seguintes documentações do(s) profissionais que

participarão do GRUPO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS, os quais devem comprovar as exigências e obrigações descritas neste documento: carteira de trabalho devidamente assinada pela CONTRATADA, para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento

1.5.1.163. ENTREGAS A SEREM REALIZADAS

1.5.1.164. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a ENAP definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma online e em tempo de execução, através do portal de indicadores descrito no tópico de condições gerais para prestação do serviço deste documento, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de eventos correlacionados	Soma de eventos correlacionados	Eventos correlacionados	Eventos correlacionados	Número total de eventos correlacionados
Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	Incidentes	Número total de incidentes abertos
Quantitativo de solicitações por grupo de tecnologia	Soma de solicitações relacionadas aos grupos de tecnologia	Solicitações relacionadas aos grupos de tecnologia	Solicitações	Número total de solicitações relacionadas por grupo de tecnologia
Quantitativo de regras de correlacionamento	Soma do número de regras de correlacionamento	Regras de correlacionamento	Regras de correlacionamento	Número total de regras de correlacionamento
TOP 10 – Regras de correlacionamento	Soma do número de eventos correlacionados por regra de correlacionamento	Eventos correlacionados	Regra de correlacionamento	TOP 10 do número de eventos correlacionados por regra de correlacionamento
TOP 10 – IP de destino de regras de correlacionamento	Soma do número de eventos correlacionados por IP de destino	Eventos correlacionados por IP de destino	IP de destino	TOP do número de eventos correlacionados por IP de destino
TOP 10 – Regras de correlacionamento por país de origem	Soma do número de eventos correlacionados por país de origem	Eventos correlacionados por país de origem	País de origem	TOP do número de eventos correlacionados por país de origem

TOP 10 – Tipos de ataques	Soma do número de ataques correlacionados por tipo de ataque	Eventos correlacionados por ataque	Ataques	TOP 10 por tipo de ataque

1.5.1.165. Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com a presença de profissional que conheça todos os serviços prestados, e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler).

1.5.1.166. Neste contexto, o profissional deve apresentá-lo de forma presencial nas dependências da ENAP, ou de forma virtual, por meio de solução de videoconferência.

L - ORDEM DE SERVIÇO OU DE FORNECIMENTO DE BENS

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

ATENÇÃO!

< Os trechos marcados em vermelho neste documento são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessidade>.

<Conforme **ACÓRDÃO 172/2021 – TCU -PLENÁRIO**, os órgãos e entidades federais têm o dever legal de realizar o planejamento prévio de cada contratação de TIC, inclusive daquelas viabilizadas mediante adesão a ARPs, que vai além do mero preenchimento formal dos artefatos previstos na legislação>.

ORDEM DE SERVIÇO OU DE FORNECIMENTO DE BENS

INTRODUÇÃO
Por intermédio da Ordem de Serviço (OS) ou Ordem de Fornecimento de Bens (OFB) será solicitado formalmente à Contratada a prestação de serviço ou o fornecimento de bens relativos ao objeto do contrato. O encaminhamento das demandas deverá ser planejado visando a garantir que os prazos para entrega final de todos os bens e serviços estejam compreendidos dentro do prazo de vigência contratual. **Referência: Art. 32 IN SGD Nº 94/2022.**

1 – IDENTIFICAÇÃO			
Nº da OS/OFB	xxxx/aaaa	**Data de emissão**	<dd/mm/aaaa>
CONTRATO/NOTA DE EMPENHO nº	xx/aaaa		
Objeto do Contrato	<Descrição do objeto do contrato>		

Contratada	<Nome da contratada>	**CNPJ**	99.999.999/9999-99
Preposto	<Nome do preposto>		
Início vigência	<dd/mm/aaaa>	**Fim vigência**	<dd/mm/aaaa>
ÁREA REQUISITANTE			
Unidade	< Sigla – Nome da unidade>		
Solicitante	<Nome do solicitante>	**E-mail**	xxxxxxxxxxxxx

2 – ESPECIFICAÇÃO DOS BENS/SERVIÇOS E VOLUMES ESTIMADOS					
Item	**Descrição do bem ou serviço**	**Métrica**	**Valor unitário (R$)**	**Qtde/Vol.**	**Valor Total (R$)**
1	…	…	…	…	…
…	…	…	…	…	…
Valor total estimado da OS/OFB					

3 – <INSTRUÇÕES/ESPECIFICAÇÕES> COMPLEMENTARES
<Incluir instruções complementares à execução da OS/OFB>
<Ex.: Contatar a área solicitante para agendamento do horário de entrega>
<Ex.: Conforme consta no Termo de Referência, o recebimento provisório está condicionado à entrega do código no ambiente de homologação, e a documentação do software no repositório oficial de gestão de projetos>

4 – DATAS E PRAZOS PREVISTOS			
Data de Início:	<dd/mm/aaaa>	**Data do Fim:**	<dd/mm/aaaa>
CRONOGRAMA DE EXECUÇÃO/ENTREGA			

Item	**Tarefa/entrega**	**Início**	**Fim**
1		<dd/mm/aaaa>	<dd/mm/aaaa>
…		<dd/mm/aaaa>	<dd/mm/aaaa>

5 – ARTEFATOS / PRODUTOS	
Fornecidos	**A serem gerados e/ou atualizados**

5 – ASSINATURA E ENCAMINHAMENTO DA DEMANDA

Autoriza-se a <execução dos serviços / entrega dos bens> correspondentes à presente <OS/OFB>, no período e nos quantitativos acima identificados.

_____

<Nome >

<Responsável pela demanda/

Fiscal Requisitante>

Matr.: <Nº da matrícula>

_____

<Nome >

Gestor do Contrato

Matr.: <Nº da matrícula>

<Local>, xx de xxxxxxxxx de xxxx

Anexo II - Estudo Tecnico Preliminar.pdf

Estudo Técnico Preliminar 10/2024

1. Informações Básicas

Número do processo: 04600.002376/2023-45

2. Descrição da necessidade

A Fundação Escola Nacional da Administração Pública (Enap) é uma escola de governo do Poder Executivo Federal, vinculada ao Ministério da Gestão e da Inovação em Serviços Públicos, conforme dispõe o Decreto nº 11.345, de 1º de Janeiro de 2023.

Esta contratação tem como objetivo prover a ENAP de Serviços Gerenciados de Segurança da Informação e Segurança Cibernética necessários ao estabelecimento, à ampliação, à atualização, à manutenção e à melhoria contínua do conjunto de ferramentas, processos e equipes responsáveis pela gestão da segurança da informação e pela execução contínua, conforme a segurança e a privacidade requeridas, dos processos de TIC e de negócio desta Escola.

A Informação se tornou uma ferramenta de fácil acesso e essencial para o desenvolvimento pessoal e coletivo. Porém, essa informação deixou de ser unicamente um recurso de desenvolvimento passando a ser o item mais valioso em uma organização, sendo considerada muitas vezes como patrimônio do órgão no qual ela foi gerada. Diante dessa valorização, ela passou a atrair a atenção de pessoas ou entidades na busca de auferir lucro, posicionar-se melhor no mercado, obter vantagens ou mesmo destruir imagens e reputações. Na sociedade atual, não basta apenas armazenar a informação para futura recuperação, é necessário investir em proteção, uma vez que está sob constante risco e necessita ser adequadamente protegida.

É nesse contexto que a Segurança da Informação se tornou um elemento essencial para a manutenção da idoneidade das instituições e de sua manutenção no mercado.

Diante dessa sociedade da informação, a segurança da informação tem se tornado essencial para a proteção de uma organização, necessitando de uma grande estrutura de operação de segurança dentro dos órgãos e sendo inviável contar somente com o corpo técnico interno das entidades, passando a ser executados por serviços gerenciados de segurança da informação.

A infraestrutura de TIC da ENAP dispõe de uma série de ativos heterogêneos agrupados em: segurança, rede de comunicação de dados, telefonia, banco de dados, servidores de rede, sistemas operacionais, sistemas de backup e recursos de armazenamento de dados que, dada a criticidade dos sistemas hospedados, devem operar em alta disponibilidade e resiliência a falhas, inclusive as de segurança. Tal diversidade eleva exponencialmente a complexidade da gestão de segurança da informação e consequentemente o desafio de fazer frente as ameaças cibernéticas emergentes.

Ademais, com o crescente uso de recursos tecnológicos pela ENAP as diferentes modalidades de trabalho dos servidores e os novos serviços digitais oferecidos pela Escola à sociedade, fazem com que seja necessária a criação de um ecossistema de proteção digital para a Escola para garantir a continuidade dos serviços de TIC, mitigando riscos de perda de informações, danos à imagem institucional, melhorando a percepção de segurança perante usuários internos e a sociedade.

Desta forma, considerando a importância que os sistemas e serviços de TI adquiriram para as organizações e a constante diversificação e desenvolvimento de novas ameaças cibernéticas, são obrigatórios a constante evolução, o aparelhamento, o aprimoramento dos mecanismos de segurança, bem como o desenvolvimento de equipes e de métodos de segurança cada vez mais complexos.

3. Área requisitante

Área Requisitante	Responsável
Coordenação-Geral de Tecnologia da Informação	Frank James da Silva Pires
Coordenação de Infraestrutura, Cibersegurança e Serviços de TI	Rafaell Dias Leite Felix

4. Necessidades de Negócio

Esta contratação tem como objetivo atender as seguintes necessidades de negócio:

- Prover suporte, monitoramento, operação e gestão de serviços de segurança por meio de soluções próprias ou da ENAP;
- Prover suporte e administração de ativos e tecnologias de segurança conforme soluções existentes no ambiente de segurança da ENAP;
- Sustentar e operar todo o parque tecnológico através de um catálogo de serviços pré-estabelecidos pela ENAP por meio de especialistas em segurança dedicados ou por meio do SOC;
- Documentar e realizar a gestão de respostas aos incidentes de segurança;
- Prover serviços de governança, risco e conformidade de segurança e privacidade;
- Prover serviço de prevenção contra vazamento de informações sensíveis para o meio externo;
- Elaborar planos, programas, workshops, pesquisas e questionários de segurança da informação voltados para melhoria e conscientização de usuários em geral da ENAP;
- Prover serviços de inteligência aplicados à segurança em busca de informações pertinentes à ENAP;
- Responder a ataques de forma imediata colocando os responsáveis da ENAP a par da situação de vulnerabilidades, ameaças ou riscos graves à infraestrutura da ENAP;
- Auxiliar nos problemas relacionados à segurança de ENDPOINTS externos no qual a ENAP faz comunicação;
- Monitorar vulnerabilidades e ameaças em tempo real no que tange à segurança dos ativos de rede e comunicação da ENAP;
- Garantir a aplicação da Política de Segurança da Informação e Comunicações (POSIN) da ENAP;
- Prover serviços de operação e gerenciamento de segurança integrados e customizados, capazes de fornecer os níveis de serviço exigidos em contrato em termos de efetividade e prazo;
- Manter a continuidade dos serviços de segurança atualmente prestados na infraestrutura de TI;
- Executar as políticas de segurança da informação, públicas, privadas (uso interno da ENAP) e restritas (uso por um grupo restrito);
- Apoiar as equipes de infraestrutura, sistemas, banco e administração de dados na implantação da esteira de integração contínua do DevSecOPs, no que couber;
- Elaborar planos e programas de segurança da informação e acesso a dados ou recursos de TI;
- Proteger a integridade e a confiabilidade dos sistemas de informação contra incidentes de segurança;
- Minimizar a duração e o impacto de uma eventual violação de segurança dos ativos e informações através de ações imediatas de contenção e erradicação de ameaças;
- Garantir a inteligência de proteção contra ataques cibernéticos;
- Agir proativamente para reduzir a interrupção de serviços em parte ou como um todo, ainda que algum evento de segurança não tenha impactado o usuário final;
- Realizar testes internos e externos completos e periódicos de segurança e prevenção para verificar pontos de vulnerabilidades na rede e nos sistemas e ambientes de infraestrutura da ENAP;
- Manter a disponibilidade, desempenho e segurança do ambiente de TI;
- Realizar a gestão, comunicação e o gerenciamento de riscos de segurança;
- Coletar, identificar, tratar e efetuar o controle dos riscos mais significativos em cada sistema informacional crítico da ENAP;
- Identificar vulnerabilidades eventualmente existentes nas diversas soluções e serviços de TI providos, prevenindo a ocorrência de incidentes minimizando os seus impactos;
- Zelar pela proteção dos dados pessoais de professores, estudantes e cidadãos inseridos nas bases de dados e redes da ENAP por meio de políticas de segurança da informação com a nova Lei Geral de proteção de Dados Pessoais (LGPD);
- Zelar pela privacidade dos dados pessoais dos cidadãos inseridos nas bases de dados e redes da ENAP;
- Prevenir qualquer evento de segurança da informação indesejável e inesperado, seja único ou em série, que pode comprometer as operações do negócio e ameaçar a segurança da informação;
- Apoiar a DGI (Diretoria de Gestão Interna) nas tomadas de decisões relacionadas a segurança da informação.

Os impactos negativos decorrentes da não efetivação da presente contratação são:
a) Interrupção na prestação dos serviços, acarretando perdas irreparáveis à administração e a própria missão da ENAP;
b) Indisponibilidade na sustentação ao usuário, sistemas, aplicações, serviços, integrações e portais da ENAP;
c) Interrupção da sustentação, construção, implantação ou uso das soluções de TI da ENAP;
d) Impossibilidade de execução dos serviços essenciais da ENAP.
e) Ausência de capacidade operacional no processo de gestão de riscos aos ativos de TI e processos de negócio da ENAP.

Cabe registrar algumas premissas necessárias e específicas do objeto que devem ser observadas dentro dos objetivos da contratação, são elas: leis, normas e diretrizes de Governo relacionadas à Segurança da Informação e Comunicações (SIC), em especial atenção à Norma Complementar no 14/IN01/DSIC/GSIPR, que estabelece princípios, diretrizes e responsabilidades

relacionados à Segurança da Informação (SI) para o tratamento da informação em ambiente de Computação em Nuvem, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta, ao Decreto Federal n° 3.505/2000, à Instrução Normativa GSI/PR n° 01/2008, e suas normas complementares, à Instrução Normativa Nº 5, de 30 de agosto de 2021, à Lei n° 13.709/2018 e a Resolução Enap nº 27, de 28 de dezembro de 2021 que institui a Política de Segurança da Informação (POSIN) no âmbito da ENAP.

5. Necessidades Tecnológicas

Considerando todos os riscos e necessidades apresentadas, este estudo tem por objetivo analisar os cenários de forma a encontrar a melhor alternativa para atender as necessidades de segurança da informação e privacidade da Escola por meio da contemplação dos seguintes objetivos tecnológicos:

- Prover monitoramento de segurança por meio de coleta, análise e correlacionamento de logs de segurança dos ativos de TI e de soluções de segurança, em tempo real, necessários à correta detecção, classificação e priorização de incidentes de segurança;
- Identificar e prevenir de forma proativa e contínua possíveis vulnerabilidades de segurança da informação, na infraestrutura e aplicações da ENAP, a fim de evitar ataques cibernéticos direcionados à ENAP;
- Proporcionar maior visibilidade do ambiente de segurança às equipes de infra, desenvolvimento de sistemas, arquitetura e banco de dados;
- Monitorar contra ataques cibernéticos de forma proativa e contínua com as devidas respostas e ajustes de segurança;
- Monitorar ativos de segurança contra indisponibilidades;
- Acompanhar, monitorar, administrar e realizar a gestão de ativos de segurança expostos na tabela 9 relativos ao ambiente de segurança da ENAP;
- Atender a necessidade de redundância de Torres externas de monitoramento SOC de acordo com as normas internacionais de segurança;
- Realizar a gestão da segurança das redes cabeadas e sem fio de toda a ENAP;
- Prover serviço de Testes de Invasão (Penetration Testing) na infraestrutura e aplicações da ENAP;
- Manter soluções de segurança sempre atualizadas para conter novas ameaças digitais;
- Coletar eventos e suas correlações com devidos alertas a fim de manter ativos de segurança sempre atualizados contra vulnerabilidades, ataques ou invasões;
- Armazenar o registro de eventos, logs, falhas, incidentes, tratativas e ações corretivas de segurança categorizadas por ativo de TI, ativos de segurança e sistemas;
- Manter a base de conhecimento atualizada e categorizada por níveis de criticidade de risco e gravidade de incidentes;
- Classificar incidentes, mudanças e requisições por ativos de segurança, área (por exemplo: banco de dados, desenvolvimento de sistemas) e sistemas (EVG, SUAP, etc) com respectivas tratativas e correções para futura consulta;
- Realizar periodicamente testes completos de segurança e simulações contra ataques cibernéticos por meio de agendamento prévio após priorização;
- Realizar o monitoramento da deep web, redes sociais e ferramentas de busca com vistas a detectar informações sensíveis ao órgão;
- Utilizar, quando possível, o monitoramento via machine learning e inteligência artificial para a detecção mais eficiente de vulnerabilidades, falhas e riscos;
- Fornecer ferramentas e soluções necessárias para a completa execução do contrato;
- Gerenciar o serviço de VPN e acesso remoto de usuários da ENAP;
- Realizar ações necessárias com o objetivo de detectar e prevenir intrusões nos serviços gerenciados pela CONTRATADA ;
- Realizar análise de ameaças na camada de aplicação;
- Viabilizar a exportação de dados de incidentes, riscos, mudanças e requisições de serviços em caso de transição contratual para uma nova CONTRATADA ;
- Realizar o envio de alertas de segurança de incidentes críticos para a equipe responsável da ENAP;
- Disponibilizar Dashboard com gráficos e estatísticas em formato web de nível gerencial para que a coordenação possa verificar os incidentes relacionados e correlacionados categorizados por endpoint, clustters (datacenter, corporativo, etc.), por ativos de segurança, por aplicação, por exemplo, EVG, SUAP, etc.
- Monitorar e proteger ativos de segurança e rede em relação aos seguintes eventos: SPAM, Botnets e Abuso de site;
- Tráfego de pacotes UDP com endereços IPs falsos;
- Ataques e vulnerabilidades em EndPoints;
- Bloquear Ransomware e vírus maliciosos;
- Vírus e Malwares (gestão de segurança);
- Ataques de SQL Injection;

- Comprometimento de computadores ou redes por vírus;
- Desfiguração (Defacement);
- Desrespeito à POSIN da ENAP e à LGPD;
- Hospedagem não autorizada ou redirecionamento de artefatos ou código malicioso;
- Inclusão remota de arquivos (Remote File Inclusion);
- Ataque DDOS;
- Ataques de engenharia social (Phising);
- Uso abusivo ou indevido de redes sociais para difamação, calúnia, ameaças ou fraudes;
- Uso ou acesso não autorizado a sistemas de dados;Varredura de portas (Port Scan);
- Não exaustivo aos itens acima citados.
- Prover ao ambiente de soluções de segurança da informação atualmente implementado na ENAP, mecanismo de visibilidade de logs, rede e informações, capaz de identificar eventos maliciosos, através de correlacionamento de logs e tráfego de rede, que possam comprometer os serviços tecnológicos da ENAP.
- Prover inteligência de Proteção contra Ataques Cibernéticos e Serviços de pesquisa e desenvolvimento de Inteligência de Proteção contra Ataques Cibernéticos, sendo responsável por:

  a) Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria continua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela CONTRATADA.
  b) Criar, em colaboração com a equipe de infra da ENAP, Casos de Uso (regras), que devem ser implementados na ferramenta SIEM dos serviços de Monitoramento e Resposta a Incidentes.
  c) Revisar periodicamente as regras do SIEM, realizando as adaptações e evoluções necessárias.
  d) Produzir e entregar informação de inteligência acionável, na forma de procedimentos para triagem de alertas e procedimentos para resposta a incidentes, correspondentes às regras do SIEM.
  e) Produzir relatórios completos de indicadores de segurança, de campanhas de Phishing e de Pentests que possam ser acessados por meio de interface web com devidas considerações, tratativas, ações corretivas ou plano de ação;

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

Requisitos de Capacitação

Será necessário treinamento à equipe que atuará com a solução. O treinamento deverá ser de no mínimo 6 (seis) horas de duração.

A CONTRATADA deverá prover capacitação técnica, teórica e prática, de cada item, conforme sua natureza, da solução ofertada à equipe local da ENAP:

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

A capacitação técnica nas disciplinas referentes aos itens ofertados deverá contemplar turmas fechadas, com no máximo 15 (quinze) participantes em cada uma delas.

Os treinamentos devem ser ministrados, sob demanda, nas dependências da ENAP ou conduzidos de forma remota, considerando a duração mínima de 6 horas para cada item, em turnos parciais das 08:00 às 12:00 ou das 14:00 às 18:00, de segunda a sexta-feira, em datas e horários definidos posteriormente pela Escola.

A capacitação técnica provida deverá abordar todos os componentes da solução fornecida, devendo ainda estar de acordo com a utilização da solução instalada no ambiente da ENAP.

Considerando-se as tecnologias disponíveis no ambiente de Tecnologia da Informação da ENAP, verifica-se que, para a execução do objeto dessa pretensa contratação, a empresa a ser contratada deverá dispor de Equipe Técnica especializada e com treinamento e capacitação atualizados nas tecnologias em questão.

Os requisitos de capacitação devem refletir as principais metodologias, tecnologias, produtos e ferramentas que representem maior abrangência para os serviços de TI e soluções de infraestrutura de TI utilizados na ENAP.

A CONTRATADA deverá fornecer, também em meio digital, o material didático de acompanhamento detalhado, original do fabricante quando aplicável, preferencialmente em português, contendo todos os assuntos

abordados na capacitação. Entende-se como material didático, apostilas, slides de apresentações, manuais, livros-textos, dentre outros de semelhante natureza, destinados a facilitar ou complementar o aprendizado. Na ausência de publicação em português (Brasil) do material original do fabricante, será aceito material em inglês;

A ENAP reserva-se o direito de realizar a validação técnica e pedagógica do material didático, podendo vir a solicitar à CONTRATADA eventuais correções ou adequações;

Ao término de cada turma, será realizada uma Avaliação de Reação tendo em vista a medição e avaliação da qualidade da capacitação. A ENAP poderá aplicar uma Avaliação de Reação em todos os treinandos, com o objetivo de avaliar a satisfação com a capacitação;

Caso a CONTRATADA, para fins próprios, tenha a necessidade de mensurar outros fatores não previstos na avaliação padrão da ENAP, ela poderá utilizar o seu próprio formulário, porém o mesmo não será utilizado para aprovação da capacitação por parte da ENAP;

Quatro fatores serão objeto de avaliação pelo formulário, conforme descrito abaixo:

> Instrutoria - Avalia a satisfação dos participantes com relação a atuação do instrutor durante a capacitação, tanto em relação ao seu conhecimento técnico do tema, quanto à sua habilidade didático-pedagógica e de interação com a turma;
>
> Material Didático - Avalia a percepção dos participantes sobre a adequação e clareza do material didático utilizado na capacitação;
>
> Conteúdo Programático - Avalia a percepção dos treinandos quanto ao equilíbrio entre teoria e prática, nível de profundidade, exemplos de exercícios, aderência e aplicabilidade;
>
> Autoavaliação - Avalia a percepção dos participantes quanto à aquisição de novos conhecimentos e habilidades por meio da capacitação oferecida, bem como, a segurança para a sua aplicação e relevância do conteúdo abordado;

Cada fator é composto por um conjunto de itens que deverão ser avaliados por meio da utilização de quatro conceitos, quais sejam: Fraco (0), Regular (1), Bom (2) e Excelente (3);

A capacitação técnica provida pela CONTRATADA poderá ser submetida à aprovação por parte da ENAP;

O resultado da capacitação será considerado INSATISFATÓRIO quando pelo menos uma das situações abaixo ocorrer:

> Média final da turma igual ou inferior ao conceito regular (1), excluindo-se o fator Auto avaliação;
>
> Média do fator Instrutoria igual ou inferior ao conceito regular (1);

A CONTRATADA será obrigada a realizar, sem ônus para a ENAP, nova capacitação para todas as turmas em que ficar configurado como resultado INSATISFATÓRIO. A critério da Escola, o conteúdo poderá ser ajustado e /ou o instrutor substituído para sanar os problemas identificados. A nova capacitação deverá acontecer segundo um novo calendário a ser definido pela ENAP;

Após a conclusão da capacitação, mediante solicitação formal da ENAP, a CONTRATADA deverá fornecer cópia da apresentação utilizada em mídia eletrônica (CD, DVD, PENDRIVE ou link de repositório em nuvem), em formatos padrão de mercado (PDF, DOC, PPT ou HTML);

A ENAP se reserva o direito de reproduzir trechos do material didático utilizado na capacitação, desde que registradas as devidas fontes,para realizar capacitações internas de seus servidores, terceirizados e colaboradores;

A CONTRATADA deverá disponibilizar para os participantes que obtiverem no mínimo 75% de frequência, os certificados de conclusão de curso, em meio eletrônico, ao final de cada turma. Aqueles que apresentarem percentuais inferiores não deverão recebê-lo;

A CONTRATADA deverá enviar à ENAP a lista de presença, assinada pelo instrutor, em que seja comprovada a participação dos treinandos em cada turno de cada dia de capacitação;

Para fins de comprovação dos serviços prestados, visando o faturamento, a CONTRATADA deverá encaminhar à ENAP, em até 5 (cinco) dias úteis após o encerramento de cada turma, os certificados e o documento de presença digitalizados.

As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático, etc.) serão de exclusiva responsabilidade da CONTRATADA;

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

Requisitos Legais

O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, 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 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis, a saber:

Lei Federal nº 12.846/2013: dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências;Lei Federal nº 13.709/2018: lei Geral de Proteção de Dados Pessoais;

Lei Complementar nº 123/2006: institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte, e dá outras providências;

Decreto nº 7.174/2010: regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;

Decreto nº 7.579/2011: dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal;

Decreto nº 11.129/2022: regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira;

Decreto 9.507, de 21 de setembro de 2018: dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União;

Instrução Normativa SEGES/MP nº 05, de 26 de maio de 2017: dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional;

Instrução Normativa SEGES/ME Nº 98, de 26 de Dezembro De 2022: estabelece regras e diretrizes para o procedimento de contratação de serviços sob o regime de execução indireta de que dispõe a Lei nº 14.133, de 1º de abril de 2021, no âmbito da Administração Pública federal direta, autárquica e fundacional;

Decreto nº 10.947 de 25 de Janeiro de 2022: regulamenta o inciso VII do caput do art. 12 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o plano de contratações anual e instituir o Sistema de Planejamento e Gerenciamento de Contratações no âmbito da administração pública federal direta, autárquica e fundacional.

Instrução Normativa SGD/ME nº 01, de 4 de abril de 2019: dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

Instrução Normativa nº 03, de 26 de abril de 2018: dispõe sobre regras de funcionamento do Sistema de Cadastramento Unificado de Fornecedores – SICAF, no âmbito do Poder Executivo Federal;

Portaria SGD/MGI nº 1.070, de 1º de junho de 2023: estabelece modelo de contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

Portaria MPOG/ME Nº 424, de 7 dezembro de 2017: Institui o Índice de Custo de Tecnologia da Informação - ICTI como índice específico a ser considerado nos contratos relacionados à Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração de Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal, observada a periodicidade legal.

Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022: dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

Ademais, a CONTRATADA deverá se submeter a Política de Segurança da Informação (POSIC) da ENAP, nos termos da Resolução Enap nº 27, de 28 de dezembro de 2021.

Requisitos de Manutenção

Devido às características da solução, há necessidade de realização de manutenções corretivas, preventivas, adaptativa ou evolutiva pela Contratada, visando à manutenção da disponibilidade da solução e ao aperfeiçoamento de suas funcionalidades;

Entende-se por requisitos de manutenção a necessidade de continuidade da prestação de serviços de TIC relacionados a segurança cibernética, visando garantir o acesso aos serviços de TIC na ENAP, bem como reduzir ou mitigar a ocorrência de falhas, problemas ou incidentes, conforme detalhado neste documento e seus respectivos Anexos.

Requisitos Temporais

Os serviços devem ser prestados no prazo máximo de 2 (dois) dias corridos para as capitais dos estados e de 5 (cinco) dias corridos para as demais localidades, 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;

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

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. Serão considerados em dias úteis quando estiverem explicitamente assim definidos.

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

ATIVIDADE	PRAZO
Assinatura do Contrato	Em até 5 dias após a convocação
Reunião de Alinhamento inicial: iniciação do contrato e apresentação do preposto	Em até 10 dias úteis a partir da assinatura do contrato.
Entrega de certificado e/ou declaração para comprovação da qualificação dos técnicos /profissionais que irão executar os serviços.	Durante a reunião de Alinhamento inicial.
Entrega do Plano de Execução pela CONTRATADA.	Em até 14 dias úteis após a reunião de Alinhamento inicial.
Início das atividades propostas.	Em até 07 dias úteis após a entrega do Plano de Execução.
Período de levantamento dos itens do Grupo 01, 02 e 03.	Em até 03 dias úteis após a entrega do Plano de Execução.

Período de análise das informações obtidas do Grupo 01, 02 e 03.	Em até 02 dias úteis após a conclusão da fase de levantamento.
Período de proposições dos itens do Grupo 01, 02 e 03.	Em até 05 dias úteis após a conclusão da fase de análise.
Execução dos testes externos.	Em até 14 dias úteis após a conclusão da etapa de proposições.
Execução do re-teste.	Em até 07 dias úteis após a conclusão da fase de testes externos.
Reunião final e finalização do projeto.	Após a conclusão dos testes e re-testes, será realizada reunião entre a CONTRATADA e o CONTRATANTE para finalização do projeto em até 14 dias.

Seguem abaixo requisitos temporais mais detalhados:

O prazo para assinatura do contrato será de até 5 (cinco) dias úteis, contados a partir da data de convocação pela ENAP, podendo ser prorrogado uma vez, por igual período, quando solicitado pela parte e desde que ocorra motivo justificado e aceito pela Escola.

A CONTRATADA terá até 10 dias corridos para iniciar a execução do contrato, podendo iniciar antes deste prazo desde que aceito pela DGI/ENAP.

A CONTRATADA deverá apresentar a documentação da equipe a ser habilitada para prestação dos serviços pelo menos 5 (cinco) dias antes do início da efetiva execução do contrato.

A CONTRATADA deverá apresentar uma equipe mínima para realizar atividades de transição contratual, se for o caso, com pelo menos 1 (um) analista do tipo PLENO que deverá participar dos processos de transição.

O evento de início da execução do contrato corresponde ao primeiro dia em que a CONTRATADA assume a responsabilidade operacional dos serviços de segurança, conforme os itens da solução ofertada, da ENAP. Somente a partir deste momento fará jus ao pagamento pelos serviços realizados, que serão calculados de forma proporcional (pró-rata) para o primeiro mês.

O Período de Adaptação Operacional será de 90 (noventa) dias, conforme definições estabelecidas na seção CRITÉRIOS DE MEDIÇÃO E PAGAMENTO deste documento.

A CONTRATADA deverá realizar as atividades de Estabilização dos Serviços e Soluções de Segurança durante o Período de Adaptação Operacional.

Durante e após o Período de Adaptação Operacional, a CONTRATADA estará sujeita à aplicação de glosas, de acordo com a subseção "Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento" da seção CRITÉRIOS DE MEDIÇÃO E PAGAMENTO deste documento, conforme não atinja os resultados definidos neste documento.

Durante e após o Período de Adaptação Operacional, a CONTRATADA estará sujeita à aplicação das sanções prevista neste documento.

Durante o Período de Adaptação Operacional, a CONTRATADA deverá revisar, ajustar e implantar os processos relacionados a Segurança Cibernética e Privacidade de Dados Pessoais.

A partir do início da execução do contrato, inclusive durante o Período de Adaptação Operacional, a CONTRATADA deverá executar os serviços continuados presenciais Sustentação de Operações e Resposta a Requisições de Segurança e de SOC e de Monitoramento do Remoto 24x7x365, fazendo jus ao pagamento mensal por esses serviços.

Os serviços de atendimento descritos no catálogo de serviços relativos aos usuário de TIC (infraestrutura) deverão ser executados nos prazos definidos no acordo de nível de serviço estabelecido na seção CRITÉRIOS DE MEDIÇÃO E PAGAMENTO deste documento.

A descrição e os tipos de serviços constantes no catálogo de serviço poderão sofrer ajustes de acordo com a necessidade da ENAP ao longo da execução do contrato a fim de melhorar processos e comunicação entre as áreas.

A resolução de incidentes de TIC deverá ser tempestiva, conforme a necessidade, de forma a não prejudicar os indicadores de disponibilidade dos serviços de Segurança Cibernética.

Requisitos de Segurança e Privacidade

A CONTRATADA deverá atender às normas acerca de conformidade técnica e de integridade de dados na Administração Pública Federal, assim como às normas e aos procedimentos de que trata a Resolução Enap nº 27, de 28 de dezembro de 2021 que institui a Política de Segurança da Informação (POSIN) no âmbito da ENAP, sem prejuízo dos demais atos, documentos e normativos expedidos e publicados pela Administração Pública Federal, bem como pela própria ENAP relativos ao sigilo, à segurança e à privacidade das informações e comunicações, além dos respectivos Termos de Compromisso de Ciência previstos nas alíneas “a” e “b” do inciso V do art. 18 da Instrução Normativa nº 01, de 04 de abril de 2019, da SGD/ME.

A CONTRATADA e seus profissionais deverão observar os preceitos da LGPD (Lei Geral de Proteção de Dados Pessoais), Lei nº 13.709, de 14 de agosto de 2018.

Todos os profissionais da CONTRATADA que irão prestar serviço diretamente para a ENAP, deverão passar por processo específico de habilitação, dentre os quais será verificado o requisito de assinatura e entrega de um instrumento similar a um Termo de Responsabilidade e Ciência (**ANEXO C – TERMO DE COMPROMISSO DE SIGILO E SEGURANÇA DA INFORMAÇÃO** a ser inserido no Termo de Referência) alterável discricionariamente, a qualquer tempo, pela ENAP.

As tarefas e atividades de operação de serviços executadas pela CONTRATADA deverão observar as políticas, normas e procedimentos institucionais de gerenciamento de serviços de TIC e de Segurança da Informação estabelecidas pelo CONTRATANTE, bem como padrões e normativos gerais tais como ANSTI/TIA/EIA, ISO, ABNT e demais normas vigentes no âmbito da Administração Pública Federal.

Requisitos Sociais, Ambientais e Culturais

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

Uma vez que o objeto da pretensa contratação consiste, essencialmente, em prestação de serviços de atendimento e suporte de segurança às equipes de Tecnologia da Informação, como também de suporte de segurança à própria infraestrutura de TI da ENAP, naquilo que couber, os serviços, resultados, relatórios, catálogos, gráficos, prospectos, demonstrativos, entre outros inerentes a serem fornecidos deverão ter documentação (catálogos, manuais, informativos e afins) entregue, preferencialmente, em Língua Portuguesa (Brasil) ou, caso não haja, em Língua Inglesa, e na forma de links de acesso ao sítio de documentação da própria CONTRATANTE, base de conhecimento, sistema de Wiki ou outro que venha a ser definido pela CONTRATANTE.
Os serviços deverão ser prestados de acordo com os critérios de sustentabilidade ambiental contidos na Instrução Normativa nº 01, de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão – SLTI/MPOG, no Guia Nacional de Contratações Sustentáveis (3ª edição, revista, atualizada e ampliada, Abril/2020, Consultoria-Geral da União), e no Decreto nº 7.746/2012, no que couber.
4.18.3 A CONTRATADA deverá cumprir, no que couber, as exigências do inciso XI, art. 7° da Lei 12.305, de 02 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos – PNRS.

Requisitos da Arquitetura Tecnológica

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

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.

A CONTRATADA deverá utilizar os padrões de arquitetura definidos pela ENAP e bem como realizar recomendações e análises destas arquiteturas para melhorar a segurança de ativos de infraestrutura e de aplicações por meio de metodologia DevSecOps em todo os ambientes de desenvolvimento de sistemas.

Os serviços prestados pela CONTRATADA devem ser compatíveis com as tecnologias de hardware, software, linguagem de programação, interfaces, entre outros, utilizadas pelo CONTRATANTE, considerando as versões atualmente em uso.

A prestação dos serviços deverá ser realizada a partir do Centro de Operações de Segurança especializado, sendo remoto às instalações da CONTRATANTE e localizado no Brasil.

A CONTRATADA deverá comprovar que possui ao menos, 02 (dois) Centros de Operações de Segurança, redundantes, de modo que a indisponibilidade de um deles não afete nenhum aspecto dos serviços prestados.

A fim de garantir a disponibilidade das ferramentas e soluções utilizadas para a execução do objeto deste documento, ambos os Centros de Operações de Segurança devem utilizar as infraestruturas de Data Centers distintas, ou seja, dois ou mais datacenters.

Ao menos um dos Data Centers deve ter as seguintes certificações ou normas, a saber: ABNT NBR ISO/IEC 27001; ABNT NBR ISO/IEC 20000; ABNT NBR ISO/IEC 9001;

A fim de atender o Item 05, O Centro de Operações de Segurança (SOC) deverá atender aos seguintes requisitos mínimos:

Utilizar sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas;
Filmar toda a área, mantendo as imagens armazenadas por no mínimo 90 (noventa) dias;
Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao de Centro de Operações de Segurança, por no mínimo, 90 dias;
Possuir solução de monitoramento de disponibilidade e desempenho no Centro de Operações de Segurança;
Caso algum dos serviços de gerenciamento e monitoramento não sejam realizados no mesmo espaço físico que o de Centro de Operações de Segurança, todos os requisitos devem ser atendidos em todos os locais de prestação desses serviços;
O perímetro do Centro de Operações de Segurança deve ser equipado com sensor de intrusão e alarmes contra acesso indevido, em regime de 24x7x365;
Ser vigiado de forma ininterrupta por segurança especializada e armada em regime de 24x7x365;
Ter controle de acesso físico ao Centro de Operações de Segurança com pelo menos 2 (dois) dos seguintes fatores de autenticação: Cartão de identificação magnético e; Biometria de leitura de digital ou análise de retina;
Possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados por, no mínimo, o correspondente ao prazo do contrato;
Ser configurado de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços;
Ter sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPS's (unidades de alimentação elétrica contínua) para garantir a transição entre o fornecimento normal de energia e o grupo gerador;
Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;
O Centro de Operações de Segurança da CONTRATADA deverá possuir processos implementados que garantam a segurança das informações da CONTRATANTE. Estes processos devem estar certificados pelas normas ABNT NBR ISO/IEC 27001. Tal certificação deverá garantir controles rígidos e auditáveis de acesso físico e lógico às informações e processos internos e deverá possuir comprovadamente em seu escopo a área de monitoramento;
A CONTRATADA deverá disponibilizar linha telefônica 0800, ou equivalente a ligação local, para abertura e acompanhamento de chamados;
Possuir múltiplas conexões independentes para acesso à Internet. Cada conexão para acesso à Internet deve ser capaz de, isoladamente, suportar a operação do Data Center;
Caso necessário para a prestação dos serviços, a CONTRATADA deverá providenciar o estabelecimento de VPN para comunicação entre seus Datacenters e os Datacenters do

CONTRATANTE;
Todas as características exigidas neste item para o Centro de Operações de Segurança poderão ser confirmadas em diligência presencial.

Ademais, os serviços, equipamentos, licenças, subscrições e peças deverão observar integralmente os requisitos de arquitetura tecnológica descritos na especificação técnica dos itens 03, 04, 05, 06, 07 e 08 deste documento, bem como compatibilidade com *nodes* HPE SimpliVity 380 Gen10 G Node da solução HCI existente e sistemas de virtualização gerais.

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

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

Para a referida contratação, pode se considerar como implantação a fase de iniciação contratual, na qual, basicamente, a CONTRATADA deverá:

a) Compor e apresentar formalmente para a ENAP a equipe técnica que será responsável pela execução dos serviços, ainda que sem que caracterização de mão de obra com dedicação exclusiva, mas que deverá atender aos requisitos de experiência profissional;

b) Propor e executar processo de transição contratual, do qual devem participar a atual contratada responsável pelo contrato em vigor, a futura contratada e a equipe de fiscalização nomeada da CONTRATANTE;

c) Apresentar cronograma para realizar eventual configuração, ou ajustes iniciais necessários de catálogo de serviços e de baseline nas ferramentas de segurança e de ITSM;

d) Apresentar cronograma para realizar ajustes para os processos de gestão de serviços de Segurança e apresentar em reunião formal para os gestores de TI e equipe de fiscalização.

e) Se for necessário algum tipo de hardware ou equipamento durante a execução contratual, este deverá ser fornecido pela CONTRATADA junto com a licença em nome da ENAP.

Como o objeto do contrato envolve segurança cibernética, o processo de implementação deve estar alinhado aos principais frameworks de boas práticas de gestão de serviços e segurança de TIC em suas versões mais atualizadas durante a vigência do contrato, aplicáveis a cada categoria de serviço, tais como: ITIL, COBIT e PMBOK, ISO/IEC 27001 e ISO/IEC 27002.

No início da execução do contrato a CONTRATADA deverá realizar um levantamento (baseline) da situação de todos ativos de segurança a serem gerenciados de modo a se estabelecer um panorama geral de segurança da informação no ambiente da CONTRATANTE, identificando os riscos, vulnerabilidades ou demais situações que possam comprometer a segurança do Parque Tecnológico da CONTRATANTE, bem como elaborar um planejamento das ações eventualmente necessárias para manter ou adequar o ambiente tecnológico às normas, políticas e melhores práticas de segurança da informação.

Por se tratar na contratação de serviços o requisito para o processo de implantação está intrínseco ao início das atividades contratuais, ou seja, a CONTRATADA deverá fornecer e configurar os softwares para execução das atividades pertinentes ao certame conforme tabela a seguir:

ITEM	DESCRIÇÃO	FERRAMENTAS NECESSÁRIAS PARA EXECUÇÃO DO SERVIÇO (Deverão ser disponibilizados e utilizados pela CONTRATADA para a execução dos serviços)

GRUPO 01		
01	Serviços especializados em Segurança da Informação (Gerenciamento de Riscos, de Políticas, Planos e Procedimentos de Segurança da Informação)	Serviço de Apoio e Suporte em Governança, Risco & Conformidade, além de apoio nas disciplinas de continuidade de negócios e recuperação de desastres
02	Serviço de conscientização de Segurança	Programa e campanhas de Conscientização/Anti-phishing/Anti-Engenharia Social
GRUPO 02		
03	Serviço de monitoramento e visibilidade de ataques cibernéticos	Serviços de Proteção de Riscos Digitais
GRUPO 03		
04	Serviço de gestão de vulnerabilidade com priorização de riscos ao negócio para ativos de rede e aplicações web – ativos de rede ou aplicações Web	Ferramenta de Vulnerability Management
05	Serviço de monitoramento, detecção e resposta a incidentes - Eventos por segundo (EPS)	SIEM (Security Information e Event Management) SOAR (Security Orchestration, automation and response)
06	Serviço gerenciado de detecção e resposta para endpoints	XDR (Extended detection and response)
07	Serviço gerenciado de proteção de avançada de e-mail – 500 usuários	Ferramenta gerenciada de Advanced E-mail Security
08	Serviço de simulação de ataques cibernéticos	Serviços de Pentesting/Red Team

As subscrições e licenças previstas nos itens 01 e 02, quando oportuno e adequado ao pleno funcionamento, devem ser entregues, instaladas e configuradas no ambiente de hiper convergência (HCI) e virtualização existente pela licitante vencedora. Aderente caso alguma licença dependa de infraestrutura interna para seu pleno funcionamento.

As licenças devem possibilitar o uso de 100% das características aqui detalhadas, assim como proporcionar suporte e atualização de versão dentro do período de vigência contratual;

A CONTRATADA deverá apresentar um Plano de Projeto com, no mínimo, os seguintes conteúdos:

a) Definição do escopo;
b) Definição de quais tarefas deverão ser realizadas para implementação e configuração dos itens;

c) Cronograma de Implantação; e
d) Plano de arquitetura e desenho da solução.

O Plano de Projeto deverá ser aprovada pela CONTRATANTE.

A implementação das licenças contratadas deve ser planejada e executada de modo que não cause interrupções e paralisações não programadas, ou qualquer outro tipo de transtorno ao correto funcionamento do ambiente operacional da CONTRANTE;

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

O serviço de instalação da solução ofertada deverá contemplar no mínimo os seguintes pontos:

a) Todas as etapas de instalação e configuração deverão ser realizadas por técnicos experientes, formados em tecnologia da informação e com experiência mínima de 3 anos na área;
b) Entrega e conferência de licenciamento de acordo com o esperado;
c) Criação de rotinas de monitoramento de componentes que porventura sejam instalados no datacenter da CONTRATANTE;
d) Atualização de software com a última versão disponível e estável dos fabricantes;
e) Configuração dos endereços IP’s para o gerenciamento de produtos instalados conforme políticas de rede da CONTRATANTE;
d) Realização das demais configurações necessárias para o correto funcionamento da solução entregue;
e) Será de responsabilidade da CONTRATADA a correção dos problemas técnicos decorrentes de erros identificados na execução da instalação e configuração das licenças, sejam operacionais ou por problemas de mau funcionamento, responsabilizando-se por todos os procedimentos e custos envolvidos para resolução, sob pena de incorrer em sanções legais cabíveis, sendo garantida a ampla defesa, exceto quando seja comprovado que o problema se deu devido a mau funcionamento de componentes já existentes no ambiente da CONTRATANTE que sejam pré requisitos para o funcionamento dos objetos contratados.
f) Ao término do serviço deve ser fornecido um relatório detalhado (As-Built) contendo todas as configurações realizadas, com comentários sobre os principais comandos e as justificativas das opções de parametrização de modo a facilitar a posterior administração da solução e a continuidade de seu funcionamento;
g) Toda configuração deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada.

Requisitos de Implantação

Os serviços deverão observar, além dos requisitos de Projeto e Implementação previstos neste documento, integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

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

Deverão ser fornecidos todos os componentes necessários para garantia de funcionamento de todos os componentes presentes neste documento;

Requisitos de Garantia e Manutenção

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

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, sem custos adicionais durante a execução do contrato.

Os serviços prestados e os produtos, licenças e subscrições adquiridos possuem garantia durante todo o período de vigência contratual.

Todos os recursos que compõe as soluções dos grupos 01, 02 e 03 entregues deverão ter garantia de funcionamento e manutenção do fabricante durante toda a vigência do Contrato, sem custos adicionais para a Contratante;

A CONTRATADA garantirá os serviços prestados no período vigente da garantia, sem ônus À CONTRATANTE. Nesse período a CONTRATADA se obriga a corrigir quaisquer defeitos nos produtos ou serviços.

A garantia do produtos, licenças e subscrições deverá abranger todas as atualizações de versões de software (firmwares) do produto;

A garantia/suporte deverá atender, no mínimo todas as funcionalidades suportadas pelos componentes da solução, independente de terem sido configurados anteriormente e da política de comercialização do fabricante;

Os defeitos compreendem, mas não se limitam a: imperfeições percebidas no serviço, ausência de artefato de documentação, configurações e qualquer outra ocorrência que impeça o seu funcionamento normal. Tais defeitos poderão ser apurados pelo CONTRATANTE ainda que tenham sido faturados e pagos sem nenhuma restrição, ou seja, a fatura aceita não é documento de garantia de qualidade.

Durante a vigência da garantia, toda a assistência técnica deverá ser prestada para o pleno funcionamento das soluções;

Durante o prazo de garantia a CONTRATADA prestará, quando for o caso, serviços de suporte técnico e/ou de assistência técnica, na forma on-site dentro do horário de trabalho da CONTRATANTE;

Durante o período de vigência da garantia a(s) CONTRATADA(s) deverá(ão) executar correções visando eliminar erros detectados nas soluções que impeçam seu pleno funcionamento de acordo com as especificações listadas neste documento;

Os atendimentos deverão ser prestados por técnico devidamente capacitado e qualificado para executar as atividades, devendo este ser demonstrado, por meio de documento de comprovação de certificação técnica na solução e tecnologia ofertados, no momento da nomeação do PREPOSTO.

Caso a CONTRATADA identifique a necessidade de substituição de solução que apresentem defeitos ou falhas, os mesmos deverão ser substituídos por soluções de qualidade e características técnicas iguais ou superiores aos existentes, desde que compatíveis, com todas as configurações necessárias ao seu funcionamento, e autorizado pela ENAP;

Os serviços deverão ser executados sem impacto na utilização do ambiente de TI da ENAP, de forma que os subsistemas mais críticos deverão ser executados em horário noturno e/ou finais de semana, e autorizado pela ENAP;

A CONTRATADA deverá auxiliar a CONTRATANTE na assistência técnica da solução e deverá abrir para CONTRATANTE os chamados junto ao suporte técnico da fabricante da Solução quando necessário;

A CONTRATADA deverá disponibilizar uma central de atendimento, via telefone, plataforma web ou e-mail, para abertura dos chamados técnicos.

A CONTRATADA deverá quando solicitada pela CONTRATANTE emitir relatórios contendo o status de todos os casos abertos, bem como status de RMAs (Registro Mensal de Atendimento), progresso na análise de falhas e emissão de relatórios de assuntos relacionados ao suporte técnico da fabricante da Solução.

Durante a vigência da garantia, a ENAP deverá ter acesso às atualizações de software fornecidas pelo fabricante, assim como receber o suporte técnico por telefone ou sistema eletrônico (internet) para esclarecimento de dúvidas quanto à instalação e/ou configuração do equipamento.

O Suporte Técnico será realizado no regime de 24 horas por dia, 7 dias por semana (24x7x365):

a) O início do atendimento se dará a partir da comunicação do(s) defeito(s) pela ENAP, via serviço telefônico (0800), e-mail e/ou outro meio indicado pela CONTRATADA e aprovado pela ENAP na Reunião Inicial ou em outra subsequente à contratação.
b) Durante a vigência da garantia, a contratada deverá prestar o serviço de forma contínua, sem quaisquer interrupções, atendendo aos níveis de serviço contratado, conforme especificações firmadas neste documento e no contrato.

Os serviços de suporte técnico a solução deverá incluir, dentre outros:

a) Orientações sobre uso, configuração e instalação da solução;
b) Questões sobre compatibilidade e interoperabilidade da solução ofertada;
c) Interpretação da documentação da solução ofertada;
d) Orientações para identificar a causa de uma falha;
e) Orientação quanto às melhores práticas para implementação do serviço contratado; e
f) Apoio na recuperação de ambientes em caso de panes ou perda de dados.

Ao término de atendimentos relacionados ao suporte técnico, a CONTRATADA deverá apresentar Relatório de Atendimento contendo data e hora da abertura do chamado, data e hora do início e do término do atendimento, identificação do defeito, nome do técnico responsável pela execução da garantia, providências adotadas e outras informações pertinentes. O Relatório deverá ser validado por técnico da ENAP.

A CONTRATADA deverá substituir, em até 30 (trinta) dias, a solução já instalada por uma nova, sem ônus para a ENAP, quando comprovados defeitos de fabricação, do próprio ou de seus componentes, que comprometa o seu desempenho, nas seguintes hipóteses:

a) caso ocorram 4 (quatro) ou mais defeitos que comprometam seu uso normal, dentro de qualquer intervalo de 30 (trinta) dias;
b) caso a soma dos tempos de paralisação da solução ultrapasse 40 (quarenta) horas, dentro de qualquer intervalo de 30 (trinta) dias.

Requisitos de Experiência Profissional

4.27 Os serviços de instalação, suporte, garantia e treinamento previstos, além de quaisquer outros pertinentes a esta contratação, deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços;

4.27.1 Para o treinamento a contratada deverá comprovar a qualificação do seu profissional que atuará na execução das atividades descritas.

4.27.2 Para a execução do objeto da pretensa contratação, considera-se necessário que a equipe técnica da CONTRATADA satisfaça alguns requisitos mínimos de qualificação e experiência profissional.

4.28 Tendo em vista a complexidade dos serviços a serem executados e o nível de conhecimento exigido para as atividades afetas a tecnologia da informação, é intuitivo afirmar que maior grau de experiência irá resultar em melhores níveis de serviços prestados e menor risco para as atividades institucionais da ENAP.

4.28.1 Uma prática comum do mercado é definir para os perfis profissionais tipos de profissionais com base na qualificação e experiência. É comum a atribuição do tipo de profissional nas categorias: júnior, pleno ou sênior. No mercado de TI não é diferente, e desta forma, a Portaria SGD/MGI nº 1.070, de 1º de junho de 2023 também adotou a mesma definição de tipos de profissionais, conforme segue:

a) “Profissional Júnior: adequado para exercer atividades de menor complexidade e que exigem menor experiência ou qualificação profissional. Geralmente, não apresenta autonomia para tomadas de decisão operacional;
b) Profissional Pleno: adequado para exercer atividades com um maior grau de complexidade, que requerem uma capacidade maior de análise crítica e resolução de problemas, além de exigir maior experiência ou qualificação profissional;
c) Profissional Sênior: adequado para exercer atividades com grau elevado de complexidade e criticidade, e que requer experiência e qualificação profissional diferenciada;

4.28.2 Definição de Experiência Profissional e Formação de Equipe:

4.28.2.1 Deve-se observar as características e requisitos de cada infraestrutura com vistas a definir os requisitos de experiência profissional necessários para assegurar a qualidade na prestação dos serviços, bem como a definição do tipo mais adequado de perfil profissional.

4.28.2.2 A definição do tipo de profissional (júnior, pleno ou sênior) depende da natureza, criticidade e complexidade dos serviços a serem prestados no âmbito de cada órgão.” (g.n.)

4.28.2.2.1 Também conforme o Mapa de perfis da Portaria SGD/MGI nº 1.070, de 1º de junho de 2023 segue a descrição do Perfil de Gerente de Segurança da Informação que será necessário para essa contratação:

a) Gerente de segurança da informação: profissional com responsabilidade de coordenar e gerenciar a atuação dos demais profissionais de segurança da informação, garantindo a adequada prestação dos serviços, bem como controlando e planejamento operacionalmente as ações dessa equipe. Presta também apoio à tomada de decisão do órgão auxiliando na prospecção de soluções de segurança da informação, fornecimento de informações táticas e operacionais, e proposição de ações de aprimoramento dos serviços de segurança da informação seja preventiva ou reativa.

4.28.2.2.2 Refletido esse padrão de mercado, estão previstos neste documento a necessidade da CONTRATADA alocar profissionais do tipo Gerente, Sênior, Pleno para execução dos serviços presenciais e perfis Sênior, Pleno e Júnior para a execução de serviços remotos via SOC 24x7x265, haja vista a complexidade e criticidade do parque computacional da ENAP, e dos serviços de TIC.

Requisitos de Formação da Equipe

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

A prestação de serviços objeto desta contratação depende majoritariamente de profissionais técnicos e qualificados, conforme constata a Portaria SGD/MGI nº 1.070, de 1º de junho de 2023. Portanto, é importante que as licitantes tenham a melhor compreensão possível da abrangência, complexidade e requisitos de entregas e níveis mínimos de serviços exigidos para que possam fazer o correto dimensionamento da equipe e alocações dos perfis e tipos profissionais adequados. Para que haja garantia de qualidade no serviço executado e modernização das metodologias de Gestão de TI, a CONTRATADA deverá manter profissionais qualificados nas áreas funcionais, que deverão ser gerenciados exclusivamente pelo representante técnico da empresa CONTRATADA, de forma que o CONTRATANTE possa obter o menor tempo de resposta para quaisquer incidentes ocorridos no seu ambiente de Infraestrutura tecnológica, bem como alcançar a excelência nos serviços de tecnologia;

Esses recursos humanos deverão conhecer o funcionamento dos negócios internos da ENAP e executar os procedimentos de acordo com as regras de segurança, sendo possível, para algumas atividades, execução ou operacionalização remota.

As equipes deverão ser dimensionadas pela(s) empresa(s) CONTRATADA(s) de forma a atender as demandas de acordo com os níveis de serviço estabelecidos. Para tanto, salienta-se que essa responsabilidade de formação da equipe de profissionais é exclusiva da empresa CONTRATADA

Será de responsabilidade da CONTRATADA o cumprimento da legislação específica dos profissionais que prestarão o serviço nas dependências da ENAP ou remotamente.

A CONTRATADA deverá fornecer o transporte necessário ao deslocamento dos profissionais até as dependências da ENAP sempre que necessário.

Os profissionais deverão atender às exigências de vestimenta feitas aos servidores da ENAP e portar crachá de identificação, durante toda a prestação do serviço.

Deve-se observar a formação e qualificação dos profissionais a serem empregados na execução do contrato em cada categoria de serviço conforme as especificações técnicas dos itens dos grupos 01, 02 e 03.

Em relação ao esforço estimado, conforme orienta a Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, a CONTRATADA deverá apresentar a formação e os perfis da equipe técnica necessária para o atendimento dos serviços contratados.

O mapa de pesquisa salarial de referência para serviços de operação de infraestrutura e atendimento ao usuário, publicado na Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, e atualizado pela Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, foi a referência utilizada para estimativa de custos desta contratação.

As definições e estimativas feitas nessa seção são apenas balizadores para a proposta, e, portanto, a CONTRATADA contínua sendo a única responsável pelo dimensionamento adequado da equipe, bem como definição de salários.

As definições e estimativas feitas nessa seção também não configuram alocação de postos de trabalho, nem sequer dedicação exclusiva.

Requisitos de Metodologia de Trabalho

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

A OS/fornecimento de bens indicará o serviço, a quantidade e a localidade na qual os deverão ser prestados.

O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 (vinte e quantro) horas por dia e 7 (sete) dias por semana de maneira eletrônica e 8 (oito) horas por dia e 5 (cinco) dias por semana por via telefônica.

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

A metodologia de trabalho será baseada no conceito de delegação de responsabilidade, onde a ENAP é responsável pela gestão e fiscalização do contrato e pela atestação da aderência aos padrões de qualidade exigidos, e a CONTRATADA como responsável pela execução dos serviços e gestão das demandas e dos seus recursos humanos.

Todo o trabalho realizado pela CONTRATADA estará sujeito à avaliação técnica, sendo homologado quando os relatórios dos serviços prestados estiverem de acordo com o padrão de qualidade exigido pela ENAP.

À CONTRATADA caberá sanar as irregularidades apontadas na execução contratual, submetendo entregas ou atividades impugnadas à nova verificação, ficando sobrestado o pagamento até a execução do saneamento necessário, sem prejuízo da aplicação das sanções legais cabíveis.

A CONTRATADA deverá apresentar mensalmente os resultados da prestação dos serviços por meio de reuniões com a CONTRATANTE apresentando relatórios consolidados mensais, relatórios periódicos dos serviços prestados ou quando solicitado pela CONTRATANTE.

A ENAP poderá, a qualquer tempo, sem ônus e dentro de suas conveniências técnicas, modificar padrões técnicos, metodológicos e arquitetura tecnológica.

A CONTRATADA deverá prever a execução de serviços em horários diurnos e noturnos, em fins de semana e feriados, conforme necessidade discriminada neste documento e acordado previamente, podendo realizar a compensação de horas dos profissionais através de bancos de horas ou outras modalidades legalmente previstas, desde que os níveis mínimos de serviço não sejam afetados.

Antes do início das atividades, a ENAP irá reunir-se com a CONTRATADA de forma a levantar todas as premissas /adequações para a execução dos serviços. Deve-se prever e explicitar as fases de planejamento, execução e homologação final do atendimento do SOC local e remoto, gerando cronogramas com atividades e responsáveis para subsidiar a fiscalização do contrato.

Todos os serviços deverão ser executados, preferencialmente, sem impactar as atividades rotineiras da ENAP. Os serviços deverão ser precedidos de cronogramas de execução previamente aprovados.

A CONTRATADA deverá criar, manter e atualizar scripts de atendimento, instruções de trabalho e procedimentos operacionais que permitam consultas e alterações quando se fizerem necessárias.

Os materiais a serem utilizados, as obras (se necessárias) e os serviços a serem executados deverão obedecer rigorosamente:

a) A todas as normas e especificações exigidas.
b) Às normas da ABNT pertinentes.
c) Às disposições legais da União.
d) Às prescrições e recomendações dos fabricantes.
e) Às normas internacionais consagradas, na falta de normas da ABNT.

Nenhuma modificação poderá ser feita nas especificações dos projetos aprovados pela ENAP sem autorização expressa do mesmo.

Possíveis indefinições, omissões, falhas ou incorreções das especificações ora fornecidas não poderão constituir pretexto para a CONTRATADA alegar redução de desempenho. Considera-se, inapelavelmente, a CONTRATADA e seus prepostos como altamente especializadas nos serviços em questão e que, por conseguinte, deverá ter considerado as complementações e providências técnicas por acaso omitidos nas especificações, mas implícitos e necessários ao perfeito e completo funcionamento dos serviços descritos neste documento.

A ENAP não aceitará, sob nenhum pretexto, a transferência de qualquer responsabilidade da CONTRATADA para outras entidades.

Não serão admitidos estagiários para prestar quaisquer serviços objeto deste instrumento e todos os funcionários da CONTRATADA deverão ser registrados pelo regime CLT ou possuir contratos de prestação de serviços.

A CONTRATADA é responsável por dimensionar, organizar e gerenciar o quantitativo de profissionais em turnos de trabalho necessários para o cumprimento do objeto contratado de acordo com os níveis de serviços exigidos neste documento.

A execução do contrato será baseada no modelo no qual a CONTRATANTE é responsável pela gestão do contrato e pela verificação dos resultados esperados e dos níveis de qualidade exigidos frente aos serviços entregues, e a CONTRATADA é a responsável pela execução dos serviços e gestão dos recursos humanos e físicos necessários.

Caso a CONTRATANTE não aprove a execução e/ou a qualidade do serviço, conforme especificado no detalhamento das tarefas, deverá apor comentário e anexar, caso seja necessário para evidenciar, documentos/relatórios que justifiquem a não aprovação, retornando à CONTRATADA para correção/complementação.

A CONTRATADA deverá obrigatoriamente realizar Pesquisas de satisfação com usuários ao final de cada atendimento.

Requisitos de Segurança da Informação e Privacidade

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

A Solução deverá atender aos requisitos de segurança da informação e privacidade, de forma ampla, adotando políticas e boas práticas, de forma a mitigar os riscos.

As atividades da CONTRATADA deverão estar de acordo com as melhores práticas de segurança segundo os frameworks e padrões ITIL v4 ou superior, MITRE ATT&CK®, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 30111 e ISO/IEC 29147, aplicáveis a cada categoria de serviço.

Deverão ser observadas as leis, normas e diretrizes de Governo relacionadas à Segurança da Informação e Comunicações (SIC), em especial atenção ao Decreto Federal n° 3.505/2000, à Instrução Normativa GSI/PR n° 01/2008, e suas normas complementares, à Instrução Normativa Nº 5, de 30 de agosto de 2021, à Lei n° 13.709 /2018 e à Política de Segurança da Informação e Comunicações (POSIN) da ENAP, e suas normas complementares.

Deverão ser observadas todas as determinações e orientações contidas nas Diretrizes e Normas de Segurança da ENAP, por meio da POSIN e suas evoluções. Ela apresenta os princípios considerados adequados para o manuseio, controle e proteção das informações contra destruição, modificação, violação, divulgação indevida e acessos não autorizados, sejam acidental ou intencionalmente, visando preservar a integridade, confidencialidade e disponibilidade das informações.

As Soluções deverão contemplar:

a) Implementação de controles necessários para o registro de eventos e incidentes de segurança da informação e privacidade;
b) Implementação e manutenção de controles específicos para registro de eventos e rastreabilidade de forma a manter trilha de auditoria de segurança da informação e privacidade, aderente a disposto em dispositivo legal correlato publicado pelo GSI/PR, de forma a assegurar a rastreabilidade das ações de usuário por meio de logs de transações e de acesso aos sistemas, conforme especificação de requisitos, e gerá-los e disponibilizá-los à ENAP para fins de auditorias e inspeções;
c) Implementação de medidas de salvaguarda para os logs descritos no item anterior, bem como controles específicos para registro das atividades dos administradores e operadores dos sistemas

relacionados ao objeto do contrato, de forma que esses não tenham permissão de exclusão ou desativação dos registros (log) de suas próprias atividades;
d) Implementação e manutenção de controles criptográficos para armazenamento, tráfego e tratamento da informação; e
e) Execução periódica de análise de vulnerabilidades na Solução, para detecção de vulnerabilidades técnicas e execução de medidas para seu saneamento ou contenção.

Em relação ao gerenciamento de identidades e registros:

a) Possuir procedimentos de controle de acesso que abordem a transição entre as funções, os limites e controles dos privilégios dos usuários e os controles de utilização das contas de usuários;
b) Impor mecanismo de autenticação que exija tamanho mínimo, complexidade, duração e histórico de senhas de acesso;
c) Suportar tecnologia single sign-on para autenticação;
d) Suportar mecanismos de autenticação multifator ou outra alternativa que aumente o grau de segurança no processo de autenticação de usuários da ENAP no provedor de serviço de nuvem, de acordo com nível de criticidade da informação;
e) Permitir ao órgão ou à entidade gerenciar as próprias identidades, inclusive criação, atualização, exclusão e suspensão no ambiente fornecido pelo provedor de serviço de nuvem; e
f) Atender aos requisitos legais, às melhores práticas de segurança e a outros critérios exigidos pelo órgão ou pela entidade em seus processos de autenticação, controle de acesso, contabilidade e de registro (formato, retenção e acesso);

Estabelecer um canal de comunicação seguro utilizando, no mínimo, Secure Sockets Layer/Transport Layer Security (SSL/TLS);

Utilizar um padrão de encriptação seguro, conforme padrão internacional reconhecidamente aceito, que possa ser implementado com chaves de encriptação geradas e armazenadas pela ENAP;

Disponibilizar facilidades que possibilitem a aplicação de uma proteção criptográfica própria da ENAP;

Possuir procedimentos necessários para preservação de evidências, conforme legislação; e Possuir procedimentos em relação ao descarte de ativos de informação e de dados, que assegurem:

a) Sanitizar ou destruir, de modo seguro, os dados existentes nos dispositivos descartados por meio da utilização de métodos que estejam em conformidade com os padrões estabelecidos para a conduta e as melhores práticas;
b) Armazenar, de modo seguro, ativos de informação a serem descartados, em ambiente com acesso físico controlado, com registro de toda movimentação de entrada e de saída de dispositivos.

Contemplar procedimentos e controles adequados para compartilhamento, uso e proteção da informação e os casos de compartilhamento de informações com terceiro devem ser avaliados pela contratante, por intermédio da autoridade competente, a qual caberá autorizar a divulgação do mínimo de informações necessárias para cada compartilhamento, caso julgue apropriado, preservados os casos de sigilo previstos na legislação aplicável e de proteção de dados pessoais disposto pela Lei nº 13.709/2018.

Vistoria

A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 08 (oito) horas às 17 (dezessete) horas.

Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

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

A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a licitante vencedora assumir os ônus dos serviços decorrentes.

Caso o licitante opte por não realizar a vistoria, deverá prestar declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação.

A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

Sustentabilidade

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 e suas atualizações, elaborado pela Câmara Nacional de Sustentabilidade da Controladoria Geral da União/Advocacia Geral da União:

Em atendimento à legislação que recomenda a adoção de critérios de sustentabilidade nas especificações dos bens a serem fornecidos e a exigência de práticas sustentáveis por parte das empresas contratadas na execução dos serviços, mormente o Decreto nº 7.746/2012 e a Instrução Normativa SLTI nº 1/2010, e demais dispositivos legais pertinentes à matéria, a CONTRATADA deve satisfazer as diretrizes de sustentabilidade expressas no art. 4º daquele Decreto, a saber:

a) baixo impacto sobre recursos naturais como flora, fauna, ar, solo e água;
b) preferência para materiais, tecnologias e matérias-primas de origem local;
c) maior eficiência na utilização de recursos naturais como água e energia;
d) maior geração de empregos, preferencialmente com mão de obra local;
e) maior vida útil e menor custo de manutenção do bem e da obra;
f) uso de inovações que reduzam a pressão sobre recursos naturais;
g) origem sustentável dos recursos naturais utilizados nos bens, nos serviços e nas obras; e
h) utilização de produtos florestais madeireiros e não madeireiros originários de manejo florestal sustentável ou de reflorestamento.

Como consequência, nos instrumentos convocatórios que tenham por objeto o fornecimento de bens, por exemplo, constatada a presença dos requisitos referentes à justificativa e à competitividade referidos no parágrafo anterior, são incluídos critérios de sustentabilidade, os quais passam a integrar as especificações técnicas dos bens.

No que se refere aos contratos, dentre as obrigações gerais do contratado consta a exigência da adoção de práticas de sustentabilidade na execução dos serviços, de modo a prevenir ações danosas ao meio ambiente, em observância à legislação vigente, principalmente no que se refere aos crimes ambientais, contribuindo para a manutenção de um meio ambiente ecologicamente equilibrado.

Adicionalmente, também é obrigação do contratado orientar e capacitar os prestadores de serviços, fornecendo informações necessárias para a perfeita execução dos serviços, incluindo noções de responsabilidade socioambiental.

Além da adoção dos critérios e práticas de sustentabilidade já mencionados, outros podem ser adotados conforme a natureza do objeto a ser contratado. Neste caso, as exigências e/ou obrigações referentes aos critérios e práticas de sustentabilidade são moldadas às peculiaridades de cada objeto.

Indicação de marcas ou modelos (Art. 41, inciso I, da Lei nº 14.133, de 2021):

Não se aplica ao objeto da contratação.

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

Não se aplica ao objeto da contratação.

Da exigência de carta de solidariedade

Em caso de fornecedor, revendedor ou distribuidor, será exigida carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato.

Subcontratação

Não é admitida a subcontratação do objeto contratual.

Decidiu-se pela vedação de subcontratação por conta da impossibilidade de se definir que o parcelamento do objeto, o estabelecimento de que a subcontratação é viável do ponto de vista técnico e financeiro.

Essa decisão visa reduzir o risco de problemas técnicos, financeiros, de gestão e de fiscalização desta contratação que estariam associados a uma possível separação/desmembramento dos serviços técnicos sem a existência de elementos e de maturidade suficientes para garantir a vantajosidade.

Da verificação de amostra do objeto

Será realizada verificação de amostra do objeto para averiguar se a Solução de TIC apresentada pela Licitante detém os requisitos mínimos necessários para realização dos serviços a serem contratados, de acordo com as funcionalidades, procedimentos e critérios objetivos descritos no ANEXO **E - TERMO DE RECEBIMENTO DEFINITIVO**, a ser inserido no Termo de Referência.

Serão exigidas amostras do objeto referentes aos seguintes itens:

Todos, exceto o Item 01 - Serviços especializados em Segurança da Informação (Gerenciamento de Riscos, de Políticas, Planos e Procedimentos de Segurança da Informação)

Garantia da Contratação

Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual e condições descritas nas cláusulas do contrato.
Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.
A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 10 dias úteis após a assinatura do contrato.
O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

Informações relevantes para o [dimensionamento E/OU apresentação] da proposta

A demanda do órgão tem como base as seguintes características:

A PROPOSTA de preços deverá ser apresentada de acordo com o modelo **ANEXO A - MODELO DE PROPOSTA COMERCIAL (Prazo: 60 dias)** a ser inserido no Termo de Referência, contendo o resumo da proposta de preços – observando estritamente a descrição dos itens e os quantitativos listados neste documento, de forma a garantir a permitir seu adequado julgamento – e a documentação técnica da solução ofertada. A PROPOSTA TÉCNICA E DE PREÇOS deverá ter prazo de validade não inferior a 60 (SESSENTA) DIAS CORRIDOS a partir da data da sessão pública.

Nos preços cotados deverão estar incluídas todas as despesas direta e indiretamente envolvidas na execução dos serviços, tais como: transporte, seguros, salários, encargos sociais, encargos fiscais e taxas comerciais, impostos, taxas de contribuição, tarifas públicas e quaisquer outros custos, quando aplicáveis, necessários ao integral cumprimento do objeto contratado. Deverão estar contidos ainda todos os custos marginais referentes aos profissionais eventualmente designados para a prestação dos serviços, tais como: deslocamentos, hospedagens, treinamentos, etc.

A LICITANTE deverá declarar, no momento de sua PROPOSTA, que possui capacidade técnica adequada para executar o objeto da licitação atendendo aos critérios de qualidade e aos níveis mínimos de serviço exigidos, cumprindo os requisitos especificados para a presente contratação.

A PROPOSTA deverá ser redigida em Língua Portuguesa (pt-BR), salvo quanto às expressões técnicas de uso corrente, sem emendas, rasuras ou entrelinhas, devidamente datada, sendo clara e precisa, sem alternativas de preços ou qualquer outra condição que induza o julgamento a ter mais de um resultado, com todos os preços expressos em REAIS (R$) e declaração expressa de que os serviços ofertados atendem aos requisitos técnicos especificados neste documento.

O LICITANTE é o único responsável pelas informações sobre tributos. Não caberá qualquer reivindicação para majoração de preços em virtude de possíveis equívocos cometidos. Firmado o CONTRATO, será admitida correção/alteração de preços quando houver alteração da respectiva legislação tributária que rege a operação objeto do instrumento contratual OU quando tais alterações se derem após a data estabelecida para apresentação da PROPOSTA.

Requisitos Gerais dos Serviços

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

O objeto de contratação dos SERVIÇOS GERENCIADOS DE SEGURANÇA consiste na prestação dos seguintes serviços: Item 01: Serviços especializados em Segurança da Informação (Gerenciamento de Riscos, de Políticas, Planos e Procedimentos de Segurança da Informação); Item 02: Serviço de conscientização de Segurança; Item 03: Serviço de monitoramento e visibilidade de ataques cibernéticos; Item 04: Serviço de gestão de vulnerabilidade com priorização de riscos ao negócio para ativos de rede e aplicações web; Item 05: Serviço de monitoramento, detecção e resposta a incidentes; Item 06: Serviço gerenciado de detecção e resposta para endpoints; Item 07: Serviço gerenciado de proteção de avançada de e-mail; Item 08: Serviço de simulação de ataques cibernéticos.

Os requisitos gerais dos serviços definem os requisitos obrigatórios para todos os serviços que compõem o GRUPO 01, GRUPO 02 e o GRUPO 03.

OPERAÇÃO E SUSTENTAÇÃO DE SEGURANÇA CIBERNÉTICA

Tem por objetivo sustentar e operar todas as soluções e serviços de segurança envolvidos neste processo de contratação, trabalhando em conjunto com times de sustentação da CONTRATANTE para agregar inteligência e eficiência.

Principais atividades a serem executadas de forma contínua pela CONTRATADA:

Acompanhar a execução dos serviços para o cumprimento dos níveis de serviço estabelecidos;
Priorizar os atendimentos críticos, conforme definição da CONTRATANTE;
Monitorar de forma permanente e realizar avaliações críticas sobre os produtos e serviços de segurança da CONTRATANTE;
Traçar curvas de comportamento, definir a volumetria média de acessos e identificar comportamentos não usuais, visando antecipar a identificação de incidentes de segurança, antes mesmo de impacto nos serviços;
Atuar proativamente na antecipação e identificação de incidentes de segurança, antes mesmo do impacto nos serviços;
Reagir aos eventos de Segurança da Informação que possam afetar a disponibilidade, integridade e confidencialidade das informações existentes nos sistemas ou serviços de TI da CONTRATANTE;
Atuar quando ocorrer a falha dos controles de segurança ou situação previamente desconhecida e que tenha probabilidade de comprometer os sistemas e serviços de TI;
Prover os fiscais do contrato com os relatórios técnicos e gerenciais suficientes para a comprovação dos serviços realizados;
Supervisionar sua equipe na execução dos serviços executados;
Orientar a atuação da equipe técnica em situações críticas de trabalho, bem como interagir com os usuários quando a situação requerer;
Fornecer sugestões e auxiliar na construção e manutenção contínua, com o apoio e aprovação da CONTRATANTE, de procedimentos sistematizados e da base de conhecimento, contemplando todas as soluções de problemas resolvidos com respostas padronizadas;
Consolidar em manuais de procedimentos e em base de conhecimento todas as soluções adotadas na execução das atividades;
Implantar as melhorias solicitadas pelos servidores da CONTRATANTE através das aberturas de chamados no sistema de gestão de serviços de TI;
Sugerir novas tecnologias para modernizar o ambiente tecnológico, buscando subsidiar a equipe da CONTRATANTE na gestão de segurança da informação;
Manter atualizado o Configuration Management Database (CMDB) na ferramenta de Gerenciamento de Serviços de TI utilizada pelA CONTRATANTE;
Administrar todas as soluções envolvidas na contratação em questão;
Abrir chamados técnicos para os serviços de suporte técnico remoto das soluções de hardware e software relacionados à Segurança da Informação no ambiente tecnológico do CONTRATANTE;
Realizar as atividades em estrita observância na Política de Segurança da Informação (PSI) e demais normas estipuladas pelo CONTRATANTE;
Implantar as melhorias solicitadas pelos servidores do CONTRATANTE;
Participar, quando solicitado, de reunião com os gerentes e participantes dos projetos de desenvolvimento e manutenção de sistemas e administração de dados, a fim de prover soluções para projetos/atividades em andamento;

Realizar de forma contínua análise de vulnerabilidades, apontando todas as correções que precisam ser realizadas. Tal serviço deve também priorizar aquilo que representa maior criticidade ao ambiente da CONTRATANTE;
A CONTRATADA deverá realizar a gestão de privilégios de todas as aplicações executadas nas estações de trabalho e servidores Windows, de forma a permitir que apenas aplicações válidas tenham poder de execução;
A CONTRATADA deverá fazer a gestão do controle de acesso a rede de forma contínua, interagindo com o time de redes da CONTRATANTE, de forma a manter processos eficazes de descoberta, classificação e avaliação de postura de dispositivos que acessam a rede, contribuindo também para criação de processos que venham permitir o fácil controle/isolamento de dispositivos que venham a fornecer riscos para o ambiente.

Execução de mudanças de configuração nos ativos sob sua administração

Execução das atividades relativas aos normativos e governança da CONTRATANTE naquilo que for relativo à sua área de atuação.

As atividades abaixo deverão ser realizadas de forma contínua, a fim de manter o processo de melhoria contínua no que tange segurança da informação:

Implementação, sustentação e administração da solução de SIEM;
Configuração de repositórios e processamento de logs/eventos;
Criação/envio de procedimentos para envio de logs para soluções administradas por equipes terceiras;
Customização da interpretação dos logs sempre que necessário;
Criação/configuração de alertas para cada tipo de log processado;
Monitoramento de saúde de recebimento de logs de todas as fontes configuradas para envio;
Configuração e disponibilização dos agentes de privilégios;
Criação/Manutenção de regras de detecção;
Implementação, sustentação e administração da solução de gestão de vulnerabilidades;
Implementação, sustentação e administração da solução de controle de acesso à rede;
Configurar políticas para análise e correção de posturas indesejadas;
Apontar vulnerabilidades por ordem de criticidade e acompanhar o processo de remediação das mesmas.

A CONTRATADA deverá acionar o fabricante das ferramentas sempre que necessário, sem nenhum custo adicional para a CONTRATANTE.

Qualquer atividade técnica, referente aos serviços contratados neste certame que eventualmente não tenham sido listados, também serão de responsabilidade da CONTRATADA.

Fica fora do escopo da CONTRATADA apenas atividades referentes a interações referente às ferramentas de rede e infraestrutura da CONTRATADA, onde os times de sustentação local deverão ser acionados para qualquer tratativa necessária.

A fim de evitar misinformation combat ante a uma campanha de ataque em curso, independentemente da natureza da CONTRATADA vencedora do Item 03 do Grupo 02 e do Item 05 do Grupo 03, a integração das duas, respectivas disciplinas contempladas pelos itens (Threat Hunting e Incident Handling) deve ser, obrigatoriamente, fortalecida em um ritmo sinérgico de colaboração e produção de resultados sob a pena de sanções ou glosas apropriadas.

GESTÃO DE VULNERABILIDADES DE SEGURANÇA

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

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

No caso de vulnerabilidades envolvidas em sistemas o Windows, a CONTRATADA deverá interagir com o time que administra a solução de correção de atualizações já utilizada pela CONTRATANTE para revisar todas as ações já em prática, de forma a estabelecer um fluxo saudável de atualizações de segurança recorrentes no ambiente.7.4.4. No caso de correções de vulnerabilidades em softwares não cobertos pelo software de gestão de patches já em uso pela CONTRATANTE, a CONTRATADA deverá sugerir opções disponíveis para resolução definitiva do problema

Para vulnerabilidades encontradas em sistemas WEB e servidores sustentados pela CONTRATADA, o time técnico da CONTRATANTE deverá interagir com o time responsável já atuante no ambiente para apresentar a vulnerabilidade, apontar os caminhos de resolução, aplicar a correção em conjunto e acompanhar o processo de validação do serviço hospedado no ativo em questão.

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

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

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

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

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

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

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

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

GESTÃO DE INCIDENTES DE SEGURANÇA

Tem por objetivo analisar, remediar, conter e documentar os eventos de segurança da informação que foram transformados em um incidente de segurança da informação. Tal serviço deverá ser executado obedecendo os frameworks NIST e SANS de resposta a incidentes de segurança da informação e boas práticas de mercado.

Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação do CONTRATANTE, levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade.

O início do processo de resposta a incidente de segurança se dará, sempre que um evento adverso for detectado pelas plataformas responsáveis ou através do serviço de monitoramento, porém não se limitando a estes. Poderá o corpo técnico de segurança do CONTRATANTE a qualquer tempo, abrir um incidente de segurança.

Após o incidente de segurança aberto, será de responsabilidade do grupo de resposta a incidente de segurança da CONTRATADA, analisar os logs e artefatos enviados, a fim de no primeiro instante identificar as fontes geradoras de tais logs.

Uma vez realizado as análises iniciais do incidente gerado, o grupo de resposta a incidente de segurança da CONTRATADA, deverá trabalhar para identificar quais foram os principais vetores de ataque ao ambiente do CONTRATANTE.

Como próximo passo o grupo de resposta a incidente de segurança da CONTRATADA, deverá comunicar ao time de segurança da informação do CONTRATANTE as informações iniciais sobre o incidente de segurança gerado, e quais serão as linhas de atuação para solução do incidente.

Juntamente com o CONTRATANTE o grupo de resposta a incidente de segurança da CONTRATADA, deverá definir a severidade do incidente de segurança. A severidade do incidente de segurança da informação será definida através da combinação de urgência e impacto, onde impacto é definido como a medida de criticidade do negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente.

Após análises iniciais do incidente, caberá ao o grupo de resposta a incidente de segurança, realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e/ou artefato (malware).

Todo o processo de análise e resultados obtidos devem ser documentados a todo tempo na ferramenta de gestão de incidentes da segurança da informação, para que o CONTRATANTE acompanhe todos os passos para a solução do incidente.

Uma vez identificado o comportamento e os principais vetores de ataque, o grupo de resposta a incidentes de segurança da CONTRATADA deverá definir e executar uma estratégia para a mitigação e contenção do ataque em questão. Caso seja necessário qualquer tipo de alteração no parque computacional do CONTRATANTE, para contenção e mitigação do incidente, deverá antes ser autorizado tal alteração pelo corpo técnico de segurança do CONTRATANTE.

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

Deve-se reunir os dados coletados durante o processo de tratamento de incidente, para iniciar o processo de análise forense do mesmo, ainda pelo grupo de resposta a incidentes de segurança. Tal análise deve ser realizada com o objetivo de identificar (pessoas, locais e/ou eventos), correlacionando todas as informações reunidas, e gerando como produto final um laudo sobre o incidente de segurança em questão.

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

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

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

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

Pesquisar novos tipos de ataques, vírus, malwares, Botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela CONTRATADA;
Criar, em colaboração com a CONTRATANTE, casos de uso (regras) que devem ser implementados no SIEM fornecido;
Revisar periodicamente as regras do SIEM, realizando as adaptações e evoluções necessárias;
Produzir e entregar informação de inteligência acionável, na forma de procedimentos para triagem de alertas e procedimentos para resposta a incidentes, correspondentes às regras do SIEM;

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

Relatórios de ameaças e segurança;
Relatórios de Botnets e centros de Comando e Controle;
Identificação de exploit kits;
Indicadores de ataques “ZeroDays” ;
Indicadores de comprometimento, suspeitas e avisos informativos;
Inteligência de tendências;
Proxies anônimos;
Classificação de sites;
Endereços de rede TOR.

VALIDAÇÃO DE SEGURANÇA

Os profissionais alocados deverão realizar testes, a partir da solução de validação de segurança, para verificar se os ativos de segurança estão respondendo a ameaças cibernéticas existentes.

O serviço deve ser capaz de testar a eficiência dos ativos de segurança em ambiente de produção, executando simulações de ataque entre seus componentes de software distribuídos, sem causar danos ou degradação do ambiente.

Tais testes devem ser contínuos a fim de criar uma baseline de possíveis modificações nos resultados durante o período contratual.

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

Deve avaliar o nível de segurança fornecido por um grupo de endpoints e ativos de segurança de rede independentemente de fabricante e tecnologia.

Deve executar simulações de ataque entre seus componentes sem iniciar conexões com nenhum servidor, aplicativo ou sistema em produção, a fim de fornecer uma avaliação livre de riscos.

Deve simular ataques, relatar ameaças não bloqueadas e propor medidas de mitigação às ameaças de forma contínua, além de permitir a visualização para cada cenário de ataque;

Para a execução de exploração de vulnerabilidades, Malwares e ataques às aplicações web, devem ser usados “payloads” reais de ataques maliciosos;

Durante a verificação dos controles de segurança de endpoint, devem ser reproduzidos métodos maliciosos usados por APTs (Advanced Persistent Threats) sem que o sistema operacional seja infectado;

Deverão ser realizados testes contínuos de movimentação lateral, de modo a identificar e prevenir possibilidades para atacantes navegarem pela rede corporativa.

Deverão ser realizados testes quanto a efetividades de ataque do tipo command and control, onde o atacante consegue fechar conexão com o centro de controle para efetivação da ação maliciosa.

Deve executar ataques em aplicações Web sobre os protocolos HTTP e HTTPS;

Deve executar ataques de URLs usando protocolo HTTP e HTTPS a partir da Internet ou internamente;

Deverão ser executados testes de acessos a URLs por categorização, de forma a validar a política de acesso web já implementada pela CONTRATANTE.

Deve realizar testes de SMTP, tanto a partir da Internet para o domínio corporativo quanto entre contas de domínios corporativos;

Os testes via SMTP deverão compor campanhas de phishing, de forma a testar a capacidade de resposta dos usuários a ameaças deste gênero.

Deve utilizar técnicas, táticas e procedimentos contidos no MITRE ATT&CK®.

Deve gerar relatórios de todos os ataques realizados, estabelecendo um benchmark de proteção a ser comparado a cada teste, de forma a fornecer relatórios de progresso ou declínio na efetividade das demais tecnologias de proteção em uso.

CANAIS DE COMUNICAÇÃO - Para abertura de solicitações, a CONTRATADA deverá disponibilizar 03 (três) tipos de canais de comunicação, a saber:

Grupo de Tecnologia	Classificação
Linha de telefonia gratuita (0800).	Tipo 1
E-mail com domínio registrado e de propriedade da CONTRATADA.	Tipo 2

Sistema de ITSM do inglês *Information Technology Service Management* (Gerenciamento de Serviços de TI).	Tipo 3

Independente do canal de comunicação utilizado pela ENAP, as solicitações devem ser convergidas, atualizadas, resolvidas e concentradas em um único sistema de ITSM do inglês Information Technology Service Management (Gerenciamento de Serviços de TI). Ou seja, imaginando que a ENAP realize a abertura de uma nova solicitação de serviço via linha telefônica gratuita, no segundo que segue a sua solicitação, a mesma deve constar no sistema de ITSM, assim também deve se proceder com a utilização do canal de comunicação do tipo 2: via e-mail.

Sobre o canal de comunicação do tipo 1: via linha telefonia gratuita (0800), tais ligações obrigatoriamente devem ser atendidas e/ou recepcionadas por uma interface humana, não sendo permitida a utilização de URA (Unidade de Resposta Audível), e/ou qualquer uso de atendimento eletrônico.

Para um eventual cenário de crise, ou seja, onde o negócio fim da ENAP estiver sendo fortemente afetado por um problema envolvendo a segurança da informação, a CONTRATADA deverá disponibilizar uma sala de videoconferência virtual de sua propriedade, onde a qualquer tempo poderá ser utilizada para reuniões emergenciais para tratamento de crises.

Tal sala deve estar disponível via internet e seu acesso deve obrigatoriamente ser criptografado, utilizando protocolo SSL (Secure Socket Layer), com certificado digital emitido em nome da CONTRATADA. A CONTRATADA também deve garantir que os canais de comunicação, utilizados pela sala de videoconferência estejam sob protocolos para criptografia dos dados trafegados.

A sala virtual ainda deve ter capacidade para até 10 (dez) pessoas da ENAP simultaneamente, e a fim de evitar eventuais perdas de tempo em momento de crise, a sala deve estar acessível a qualquer tempo, não sendo criada apenas no momento da crise.

Os SERVIÇOS GERENCIADOS DE SEGURANÇA, devem obrigatoriamente serem executados, ofertados, e estarem acessíveis à ENAP em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante todo o período de vigência do contrato.

GESTÃO DE CATÁLOGO DE SERVIÇO DO AMBIENTE DE SEGURANÇA DA INFORMAÇÃO.

A fim de fornecer uma única fonte de informação sobre os SERVIÇOS GERENCIADOS DE SEGURANÇA, disponíveis para cada grupo de tecnologia dos itens de configuração do parque de segurança da informação da ENAP, se definiu previamente no catálogo de serviços, o qual obrigatoriamente a CONTRATADA deverá ser capaz de entregar. Tal definição pode ser consultada através do item 10. CATÁLOGO DE SERVIÇO e NMS – NÍVEIS MÍNIMOS DE SERVIÇO do presente documento.

É de responsabilidade da CONTRATADA manter, atualizar, revisar, os serviços disponíveis para cada grupo de serviço. As responsabilidades da ENAP estão relacionadas a aprovação de um novo serviço, ou a aposentadoria de um ou mais serviços existentes.

O catálogo de serviço deverá ser mantido e administrado através do sistema de ITSM de responsabilidade da CONTRATADA, estando este disponível de forma online para a ENAP, onde poderá consultar a qualquer tempo os serviços disponíveis. Este sistema deve ser o mesmo descrito no tópico CANAIS DE COMUNICAÇÃO, do presente documento, e obviamente deve seguir os mesmos requisitos técnicos supracitados.

Também se espera que tais revisões de continuidade de um serviço no catálogo de serviços, seja sugerido por parte da CONTRATADA durante a execução do contrato. Todavia, não é de responsabilidade da CONTRATADA a retirada ou inclusão de um serviço, cabendo apenas à ENAP tal ação.

MODALIDADE DE ATENDIMENTO

A modalidade principal de atendimento será do tipo remota, ou seja, a ser realizada nas dependências da CONTRATADA, obedecendo, obrigatoriamente, os critérios estabelecidos para execução, conforme previstos neste documento.

Eventualmente a ENAP poderá solicitar uma visita técnica, para que um atendimento qualquer possa ser realizado e/ou acompanhado em suas dependências físicas.

Os atendimentos referentes ao objeto contratado, denominado SERVIÇOS GERENCIADOS DE SEGURANÇA é ilimitado durante o período de vigência do contrato, ou seja, não existe limite para quantidade de horas, e/ou quantidade de atendimentos realizados.

ACESSIBILIDADE E CONFIDENCIALIDADE

Para garantir a qualidade e disponibilidade dos serviços remotos, entre a ENAP e os 02 (dois) Centros de Operações de Segurança da CONTRATADA, deverá haver ao menos dois tipos de conexão digital, sendo do tipo internet ou do tipo MPLS do inglês Multi-Protocol Label Switching para cada Centro de Operações de Segurança.

A conexão digital deve ter velocidade de upload e download mínima de 50 (cinquenta) Mbps, serem contratadas de operadoras e rotas distintas, e devem ser utilizadas única e exclusivamente para prestação dos SERVIÇOS GERENCIADOS DE SEGURANÇA da ENAP.

Especificamente para o tipo de conexão digital internet, necessariamente precisará ter IP dedicado, e não serão aceitos contratos com linksxDSL (executada a tecnologia HDSL). Também a fim de garantir a disponibilidade da conexão, deverá a contratada garantir que tal conexão esteja protegida contra ataques de DDoS do inglês Distributed Denial of Service.

Em qualquer que seja o tipo de conexão, será de responsabilidade da CONTRATADA, a contratação junto as devidas operadoras, bem como seus devidos custos durante todo o período de vigência do contrato.

A fim de garantir a segurança do tráfego bidirecional entre a ENAP e os Centros de Operações de Segurança da CONTRATADA, as conexões (Internet e MPLS) devem ser criptografadas. Ou seja, a CONTRATADA deverá estabelecer duas VPN’s do inglês virtual private network, do tipo site to site, para cada Centro de Operações de Segurança.

A fim de garantir a segurança entre a ENAP e os Centro de Operações de Segurança da CONTRATADA, não será permitido o Centro de Operações de Segurança terceirizado ou consórcio de empresas.

Por outro lado, a CONTRATADA deve revogar todas as credenciais relacionadas a soluções de responsabilidade da CONTRATADA, geridas no item 01, empregadas na prestação de serviços à ENAP, bem como solicitar a revogação destas à ENAP, para soluções de responsabilidade da CONTRATADA, no mesmo dia do encerramento das atividades.

Tais exigências visam proteger a ENAP contra o uso indevido de informações sob sua custódia, por parte de profissional da CONTRATADA, assim como estão em conformidade com boas práticas de gestão e governança de TI.

CENTRO DE OPERAÇÕES DE CIBERSEGURANÇA:

Os serviços gerenciados de segurança devem ser executados por meio de 02 (dois) Centros de Operações de Segurança redundantes, próprios da CONTRATADA, sendo ambos obrigatoriamente no Brasil, de modo que a indisponibilidade de um deles não afete a prestação dos SERVIÇOS GERENCIADOS DE SEGURANÇA, e a no mínimo 300 (trezentos) km de distância geodésica uma da outra e em estados distintos.

A Redundância de dois SOCs deve garantir que, se houver uma falha em um dos centros de operações de segurança, o outro poderá continuar a proteger a ENAP. Isso ajuda a garantir que a CONTRATADA possa responder rapidamente às ameaças que podem ser contidas pelo serviço contratado.

A geolocalização dos SOCs deve garantir que não ocorra interrupções de serviços devido a desastres naturais ou outros eventos que afetem apenas uma determinada região. Outro fator relevante, está designado a inoperabilidade de um determinado SOC pode interromper o monitoramento de ameaças, deixando o ambiente da ENAP exposto a ataques.

Ambos os centros devem atender os mesmos requisitos mínimos, a saber:

Utilizar sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA, e cujas imagens possam ser recuperadas;

Filmar toda a área, mantendo as imagens armazenadas por, no mínimo, 90 (noventa) dias;

Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao Centro de Operações de Segurança;

Possuir solução de monitoramento de disponibilidade e desempenho.

O perímetro físico dos Centros de operações de Segurança deve ser equipado com sensor de intrusão e alarmes contra acesso indevido;

Ser vigiado de forma ininterrupta por segurança física especializada em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;

Ter controle de acesso físico com pelo menos 02 (dois) dos seguintes fatores de autenticação, a saber: cartão de identificação magnético, biometria de leitura digital ou análise de retina;

Funcionar em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;

Possuir registro de entrada e saída de pessoas, mantido por pelo menos 90 (noventa) dias.

Possuir sistemas redundantes para armazenamento de dados e alimentação de energia.

Possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados por, no mínimo, durante todo o período de vigência contratual.

Ser configurado de forma que a falha de um dos equipamentos, isoladamente, NÃO interrompa a prestação dos serviços;

Ter sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPSs do inglês Uninterruptible Power Supply, para garantir a transição entre o fornecimento normal da energia e o grupo gerador;

Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;

Não possuir campo físico visual externo das suas instalações, a fim de garantir que as informações exibidas em monitores, estejam inacessíveis a leituras e a capturas externas desautorizadas;

Possuir ambiente dedicado único e exclusivo para laboratório, onde seja possível reproduzir os incidentes e problemas da ENAP, sem que haja impacto na operação do Centro de Operações de Segurança e/ou do própria ENAP;

Possuir no Centro de Operações de Segurança processos consistentes e objetivos de monitoramento e detecção de ameaças, gestão de dispositivos, gestão de incidentes, inteligência de ameaças, investigação de ameaças e gestão de conformidade de segurança.

Possuir nativamente solução de SecOps para gerenciamento de incidentes de segurança da informação.

Deverá possuir processos implementados que garantam a segurança das normas ABNT NBR ISO/IEC 27001. Tal certificação deverá garantir controles rígidos e auditáveis de acesso físico e lógico às informações e monitoramento;

Ao menos 01 (um) Centro de Operações de Segurança da CONTRATADA deverá possuir as características das certificações listadas na tabela abaixo. Tais características garantem que a CONTRATADA segue os principais controles de segurança da informação, bem como também possui processos para tratamento de incidentes e problemas bem estabelecidos, além de boa qualidade de atendimento e interface com a ENAP.

Certificações:

Item	Certificações
1	ABNT NBR ISO/IEC 27001

2	ABNT NBR ISO/IEC 20000
3	ABNT NBR ISO/IEC 9001

A fim de garantir a disponibilidade das ferramentas e soluções utilizadas para a execução do objeto do presente documento, ambos os CENTRO DE OPERAÇÕES DE SEGURANÇA devem utilizar as infraestruturas de Data Centers distintos, ou seja, dois ou mais datacenters.

Ao menos um dos Data Centers deve possuir as seguintes certificações ou normas, a saber:

Item	Certificações	Descrição
1	ABNT NBR ISO/IEC 27001, 20000 e 9001	Norma que especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI (Sistema de Gestão de Segurança da Informação) documentado dentro do contexto dos riscos de negócio globais da organização.

O segundo datacenter pode estar situado fora dos ambientes dos CENTROS DE OPERAÇÕES DE SEGURANÇA, e deve possuir as seguintes certificações ou normas, a saber:

Item	Certificações	Descrição
1	ABNT NBR ISO/IEC 27001	Norma que especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI (Sistema de Gestão de Segurança da Informação) documentado dentro do contexto dos riscos de negócio globais da organização.
2	ABNT NBR ISO/IEC 22301	Norma de gestão da continuidade de negócios especifica os requisitos para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um sistema de gestão documentado para se proteger, reduzir a possibilidade de ocorrência, preparar-se, responder, e recuperar-se de incidentes de interrupção quando estes ocorrerem.

CONDIÇÕES PARA PRESTAÇÃO DOS SERVIÇOS:

Independente do grupo de serviço especificados, todas as soluções e/ou ferramentas utilizadas para prestação do serviço deverão obrigatoriamente seguir os requisitos, a saber:

Deverá ser obrigatoriamente de propriedade e licenciada em nome CONTRATADA e não serão aceitos serviços entregues por meio de software livre, open-source ou INHOUSE.
Deverá ser fornecer acesso de leitura, sempre que solicitado, para a ENAP, nas consoles, para auditoria dos serviços prestados, durante toda a vigência do contrato;
Deverá ser prestado por meio de solução provida através da nuvem do fabricante ou da CONTRATADA.
Os softwares ofertados devem ser instalados em sua versão mais estável e atualizada e estar cobertos por

contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço. Da mesma maneira, os equipamentos fornecidos para a prestação dos serviços devem estar cobertos por contratos de garantia do fabricante;
O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade.

PORTAL DE INDICADORES DE SERVIÇO

O portal de indicadores deverá ser disponibilizado à ENAP deverá contemplando, no mínimo, os requisitos abaixo:

A CONTRATADA deverá disponibilizar um sistema em modelo SaaS (do inglês Software as a Service), denominado portal de indicadores, para consolidação dos dados gerados pelas soluções que compõem o objeto.

O portal deverá estar acessível a CONTRATADA via internet, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, e 365 (trezentos e sessenta e cinco) dias por ano, de maneira segura utilizando protocolo de criptografia SSL.

A ENAP terá direito a criação de usuários ilimitados com a função de criação de perfis para cada usuário, disponibilizando assim visões diferentes para cada nível de acesso.

Deverá disponibilizar para os usuários da ENAP, a função de mudança de visão gráfica a critério de cada usuário. Isso quer dizer que apesar de um gráfico está disposto em modelo de barras, caso o usuário identifique uma melhor visualização do modelo gráfico em forma de pizza, o sistema deve oferecer tal funcionalidade ou opção.

O portal ainda deverá disponibilizar os seguintes modelos gráficos para os usuários:

Gráfico do tipo Pizza
Gráfico do tipo Barra
Gráfico do tipo linha
Gráfico do tipo área
Gráfico do tipo funil
Gráfico do tipo bolha

INDICADORES DE RISCO – KRI:

Deverá ser exibido no portal a quantidade de vulnerabilidades que estavam presentes na última auditoria realizada através de gráfico(s) com separação dos tipos/quantidades com a opção de “Drill Down”, possibilitando assim visualização de forma mais detalhada das vulnerabilidades listadas;

O portal deverá possuir recurso para filtrar apenas as vulnerabilidades relevantes, excluindo as de severidade média e/ou baixa.

INDICADORES DE META E PERFORMANCE – KGI e KPI:

O portal de indicadores deverá possuir relatório gráfico indicando tempo médio dos atendimentos dos incidentes por fase de Análise, contenção, erradicação e recuperação, possibilitando a filtragem por período:

Últimos 15 dias;
Últimos 30 dias;
Últimos 45 dias;

Deverá possuir gráfico comparativo entre os primeiros e últimos 15 incidentes analisados dentro de período filtrado, mostrando uma linha de tempo qual foi o incidente com o tempo de atendimento menor, maior e o tempo médio.

Deverá ser possível a consulta deste gráfico para cada uma das fases de atendimento (Análise, contenção, erradicação e recuperação).

INDICADORES POR CATEGORIA:

O Portal de indicadores deverá possuir gráfico que separe e classifique os incidentes de acordo com as categorias existentes no processo de resposta a incidentes, sendo elas no mínimo:

Origem do Incidente;
Status do Incidente;
Prioridade do Incidente;
Risco;
Grupo de Atendimento;

Todos os indicadores exibidos pelo portal, devem possuir a funcionalidade drill down, para que os usuários possam criar visualizações e filtros dos dados exibidos.

Todos os indicadores exibidos pelo portal, devem ainda possuir funcionalidade de exibição dos dados gerados do gráfico de maneira tabular, a fim de que seja possível aferir os dados brutos.

A qualquer tempo a ENAP poderá solicitar os dados brutos coletados das soluções que compõem o objeto contratado.

Os dados exibidos pelo portal devem representar o ambiente em tempo de execução e de forma automática (real time).

Deverá prover mecanismo para análise de risco e métricas de disponibilidade através de relatórios e dashboards de todas as soluções que compõem o objeto.

DAS CONDIÇÕES PARA ASSINATURA DO PEDIDO DE FORNECIMENTO:

Quando da convocação para assinatura do Pedido de Fornecimento, no prazo de até 05 (cinco) dias úteis contados da data do recebimento da convocação, prorrogável por igual período, a licitante deverá providenciar, como condição para a assinatura do Pedido de Fornecimento.

A CONTRATADA deverá providenciar, como condição para a assinatura do Pedido de Fornecimento declaração, datada e assinada por seu representante legal, atender plenamente todos os itens do documento.

DA APRESENTAÇÃO DE CATÁLOGOS

A licitante deverá, antes da disputa pública, juntamente com a proposta, apresentar os manuais, catálogos, folders, ou outros documentos técnicos, ou ainda, links públicos oficiais da solução exigida ou do serviço exigido, para comprovação do atendimento às características técnicas especificadas neste documento.

Deverá ser fornecido uma tabela junto à proposta comercial com a comprovação de todos os itens das especificações técnicas indicando documento ou link público com seu devido trecho e página.

No conjunto de documentos apresentados pela licitante (folders/catálogos), para fins de aceitação pela ENAP, deverá vir indicando corretamente, o item, especificação, link ou documento, página e trecho que comprove o atendimento de cada item/subitem das especificações técnicas descritas nos serviços a serem ofertado, conforme modelo abaixo. Será aceito também carta do fabricante com as comprovações, desde que não ultrapasse 5% dos itens técnicos deste documento.

Deverá apresentar com clareza a marca, o modelo, o tipo, a configuração e outras informações aplicáveis e necessárias à perfeita caracterização do dispositivo, serviço ou componente proposto, de forma a permitir a correta identificação deste na documentação técnica apresentada, conforme modelo de comprovação técnica:

Item	**Especificação**	**Link ou Documento**	**Trecho**	**Página**

A CONTRATADA deveria apresentar carta que demonstre que ela é empresa parceira de todas as soluções ofertadas.

Os documentos serão analisados, para fins de verificação do atendimento às características da solução especificados neste Edital.

A análise das características dos itens ofertados será procedida em cotejo com as especificações técnicas constantes deste instrumento, não sendo admitidos itens com especificações inferiores.

Os itens desprovidos dos documentos relacionados no item anterior, serão passíveis de diligência, podendo, para tanto, a ENAP se valer de todos os meios possíveis, tais como consulta a site diversos, ligações a fabricantes ou exigência de documentos complementares, dentre outros.

Caso os documentos apresentados não sejam aprovados, por não atenderem às especificações previstas neste Edital, o licitante será convocado a apresentar novo item, acompanhado de documentos que atendam às especificações requeridas, no mesmo prazo fixado para apresentação inicial, sem ônus à ENAP, contados da devolução com as instruções ou observações feitas pela ENAP, sob pena de desclassificação.

Caso a 2ª apresentação não atenda às especificações técnicas exigidas neste Edital, a proposta da licitante será considerada inaceitável pelo Pregoeiro, sendo, portanto, desclassificada.

Na hipótese de a proposta da licitante ser desclassificada, por não atendimento das especificações técnicas requeridas, serão convocadas as demais licitantes, obedecendo-se rigorosamente a ordem de classificação das propostas, seguindo-se aos mesmos moldes descritos nos itens anteriores.

A licitante vencedora que vier a ser contratada ficará obrigada ao cumprimento integral de sua proposta, ainda que algum item não tenham sido objeto de verificação na análise do manual/catálogo/folder.

QUALIFICAÇÃO TÉCNICA

De acordo com o Acórdão TCU nº 1.851/2015, "para fins de comprovação da qualificação técnica dos licitantes, o TCU tem entendido em reiteradas oportunidades que não se pode estabelecer percentuais mínimos acima de 50% dos quantitativos dos itens de maior relevância".

Apresentação de atestado(s) de desempenho anterior em atividades pertinentes e compatíveis em características, quantidades e prazos com o objeto desta licitação, emitido(s) por pessoa jurídica de direito público ou privado, demonstrando que foram cumpridas corretamente suas obrigações contratuais, contendo em seu corpo a razão social, endereço completo, telefone e CNPJ/MF, da empresa fornecedora do atestado, bem como a data, assinatura e identificação do assinante, observadas as demais exigências constantes neste edital.

Considerar-se-á (ão) compatível (is) o(s) atestado(s) que comprove(m) a prestação de SERVIÇOS GERENCIADOS DE SEGURANÇA do Grupo 02 e do Grupo 03 em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, com as seguintes parcelas de maior relevância:

Os Centros de Operação de Segurança (SOCs) devem ser redundantes, próprios da CONTRATADA, sendo ambos obrigatoriamente no Brasil, e estejam – no mínimo – a 300 km (trezentos quilômetros) de distância geodésica uma da outra e em estados distintos, devendo atender – minimamente – os seguintes requisitos:

Experiência na prestação em um mesmo contrato de consultoria de gerenciamento de riscos, de políticas e procedimentos; serviço de conscientização de segurança; serviço de gestão de vulnerabilidade de riscos em ativos de rede e aplicações web; serviço de monitoramento e visibilidade de ataques cibernéticos; consultoria de plano de resposta a incidentes; serviço de monitoramento, detecção e resposta a incidentes; serviço gerenciado de detecção e resposta para endpoints; serviço gerenciado de proteção de avançada de e-mail; serviço de simulação de ataques cibernéticos.
No mínimo de 225 (duzentos e vinte e cinco) servidores;
No mínimo de 235 (duzentos e trinta e cinco) desktops;
No mínimo de 500 (quinhentos)usuários;
No mínimo 3.000 (mil) eventos por segundo (EPS);

Experiência na elaboração de políticas, normas e procedimentos da segurança da informação da ISO 27001 e 27002 em no mínimo 06 políticas, regras e procedimentos. Este item visa atestar a capacidade da licitante para o fornecimento do serviço especificado no **Item 01 – Serviços especializados em Segurança da Informação (Gerenciamento de Riscos, de Políticas, Planos e Procedimentos de Segurança da Informação)** exigido neste certame.

Experiência em Serviço de conscientização de Segurança, por meio de atestados de conscientização em outras organizações. Este item visa atestar a capacidade da licitante para o fornecimento do serviço especificado no **Item 02 - Serviço de conscientização de Segurança** exigido neste certame.

Experiência em serviços de Serviço de monitoramento e visibilidade de ataques cibernéticos, fornecendo serviço de inteligência voltada à segurança com buscas na Surface, Deep e Darkweb, de no mínimo, 1000 ativos, dentre eles VIP's, IP's, domínios. Este item visa atestar a capacidade da licitante para o fornecimento do serviço especificado no **Item 03 - Serviço de monitoramento e visibilidade de ataques cibernéticos**, exigidos neste certame.

Experiência em serviços de **elaboração de plano de gestão de incidentes cibernéticos e serviço de monitoramento, detecção e resposta a incidentes**, utilizando tecnologia de SIEM (Security Information and Event Management) para gerenciamento e correlação de eventos de segurança através da análise de logs e pacotes, em redes com, no mínimo, 1.000 (mil) EPS. Também deverá ser comprovado a capacidade de realização de um Plano de Resposta a Incidentes e de Assessment & MITRE ATT&CK®. Este item visa atestar a capacidade do licitante para fornecer o serviço especificado no **Item 01 - Serviços especializados em Segurança da Informação (Gerenciamento de Riscos, de Políticas, Planos e Procedimentos de Segurança da Informação)** e **Item 05 - Serviço de monitoramento, detecção e resposta a incidentes exigidos neste certame**.

Experiência em serviços de serviço de gestão de vulnerabilidade de riscos em ativos de rede e aplicações web, por meio do fornecimento, instalação, prestação de serviços de suporte, administração e operação da solução para no mínimo, 235 (duzentos e trinta e cinco) ativos de TI. Este item visa atestar a capacidade da licitante para o fornecimento do serviço especificado no. Este item visa atestar a capacidade da licitante para o fornecimento do serviço especificado no **Item 04 - serviço de gestão de vulnerabilidade de riscos em ativos de rede e aplicações web**, exigido neste certame.

Experiência em Serviço gerenciado de detecção e resposta para endpoints, com as seguintes características:

> No mínimo de 300 (duzentos e vinte e cinco) servidores;
> No mínimo 200 (duzentos e trinta e cinco) desktops;
> No mínimo 500 (quinhentos) usuários. Este item visa atestar a capacidade do licitante para fornecer o serviço especificado no **Item 06 - Serviço gerenciado de detecção e resposta para endpoints**, exigidos neste certame.

Experiência em Serviço gerenciado de proteção avançada de e-mail, fornecendo serviço de proteção de e-mail de no mínimo 250 (quinhentas) caixas de e-mail. Este item visa atestar a capacidade do licitante para fornecer o serviço especificado no **Item 07 - Serviço gerenciado de proteção de avançada de e-mail**, exigidos neste certame.

Experiência em Serviço de simulação de ataques cibernéticos, fornecendo serviço de inteligência e simulação de ataques cibernéticos. Este item visa atestar a capacidade da licitante para o fornecimento do serviço especificado no **Item 08 - Serviço de simulação de ataques cibernéticos**, exigidos neste certame.

Deverá apresentar ISO's descritos no item 3.1.7. para certifica que o SOC/Datacenter possuem padrões /normas de qualidade internacionalmente conhecidos.

Considerar-se-á (ão) compatível (is) o(s) atestado(s) que comprove(m) a prestação de SERVIÇOS GERENCIADOS DE SEGURANÇA do Grupo 03, com as seguintes parcelas de maior relevância:

> Será aceita a somatória de atestados para comprovação da qualificação técnica, desde que a soma dos itens atenda as quantidades mínimas acima exigidas.
>
> Não serão considerados os atestados emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente ou que tenham pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da proponente;
>
> Deverá apresentar declaração emitida pelo fabricante da solução, por meio de seu representante legal, específica a este órgão e processo, atestando que a licitante está apta a fornecer e prestar os serviços objetos desta contratação com suas soluções.

A LICITANTE deve disponibilizar todas as informações necessárias à comprovação da legitimidade dos atestados ofertados na presente licitação, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, Notas Fiscais/Faturas, Notas de Empenho, endereço atual da ENAP e local em que foram prestados os serviços, sendo que estas e outras informações complementares poderão ser requeridas mediante diligência.

Todas as características e requisitos exigidos neste documento poderão ser confirmados em diligência presencial a ser instruída em tempo oportuno, conforme discricionariedade e critérios da CONTRATANTE.

7. Estimativa da demanda - quantidade de bens e serviços

Os serviços gerenciados de segurança da informação contemplando o serviço de Consultoria de Gerenciamento de Riscos, de Políticas e Procedimentos, o Serviço de conscientização de Segurança, o Serviço de monitoramento e visibilidade de ataques cibernéticos, o serviço de Consultoria de plano de resposta a incidentes, o Serviço de gestão de vulnerabilidade com priorização de riscos ao negócio para ativos de rede e aplicações web, o Serviço de monitoramento, detecção e resposta a incidentes, o Serviço gerenciado de detecção e resposta para endpoints, o Serviço gerenciado de proteção de avançada de e-mail e o Serviço de simulação de ataques cibernéticos são uma necessidade urgente, e se justifica com base no contexto atual da Escola, que tem o dever de performar um monitoramento inteligente e disponibilizar testes que permitam conhecer e avaliar a experiência do usuário com os serviços ofertados.

Tecnicamente, pelo cenário complexo atual no que tange à segurança cibernética e às orientações gerais do Governo Federal, a cada dia que passa surgem inúmeros artefatos maliciosos, vulnerabilidades conhecidas, técnicas comuns de ataque, entre outros.

À medida que os avanços tecnológicos fornecem novos meios de realizar/facilitar atividades cotidianas, agentes mal-intencionados trabalham para explorar e se aproveitar de brechas ocasionadas também por serviços de tecnologia que muitas vezes não são notadas.

Abordar o tema segurança cibernética há alguns anos já era algo extremamente relevante, porém, sempre se fez necessária uma contextualização profunda frente às necessidades de proteção. Atualmente, pode-se afirmar que o mundo vive literalmente uma guerra cibernética e muitos especialistas apontam que "os ataques cibernéticos estão se tornando mais frequentes – e a questão agora não é mais saber se 2023 vai registrar um recorde de violações de dados, mas sim o quão alto será esse número." (https://fastcompanybrasil.com/tech/2023-foi-o-pior-ano-em-termos-de-ciberataques-e-ainda-nem-chegou-ao-fim/).

Tal afirmação se sustenta pelo avanço na utilização de meios digitais e tecnológicos para as mais variadas funções e setores da cadeia corporativa, seja privada ou governamental, o que torna o ataque cibernético algo extremamente rentável para o atacante.

Quando se estuda o ambiente de empresas privadas, podemos observar uma série de ataques cibernéticos recentes que lograram êxito, causando prejuízos em larga escala.

Quando abordamos o cenário governamental, se torna possível observar um cenário semelhante de ataques (https://www.cisoadvisor.com.br/setor-de-governo-e-o-segundo-mais-atacado-no-brasil/), dentre eles:

- GDF (Governo do Distrito Federal): https://g1.globo.com/df/distrito-federal/noticia/2020/11/05/governo-do-df-tira-sistemas-online-do-ar-apos-ataque-hacker.ghtml
- Ministério da Saúde 2020: https://www.poder360.com.br/governo/ministerio-da-saude-identifica-virus-na-rede-do-datasus/
- Ministério da Saúde 2021: https://www.cnnbrasil.com.br/nacional/site-do-ministerio-da-saude-sofre-ataque-hacker-durante-madrugada-e-sai-do-ar/
- CNJ (Conselho Nacional de Justiça): https://www.conjur.com.br/2019-abr-01/cnj-sofre-ataque-hacker-dados-milhares-pessoas-vazam
- STN (Secretaria do Tesouro Nacional): https://www.uol.com.br/tilt/noticias/redacao/2021/08/16/tesouro-sofre-ataque-do-tipo-ransomware-o-que-e-isso.htm
- STJ (Superior Tribunal de Justiça): https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04112020-Em-razao-de-ataque-cibernetico--STJ-funcionara-em-regime-de-plantao-ate-o-dia-9.aspx
- TRF1 (Tribunal Regional de Brasília): https://www.cisoadvisor.com.br/invasao-de-rede-tira-do-ar-tribunal-federal-regional-de-brasilia/
- TJRS (Tribunal de Justiça do Rio Grande do Sul): https://www.cisoadvisor.com.br/tribunal-de-justica-do-rio-grande-do-sul-prejudicado-em-ataque-de-ransomware/
- Incidentes de segurança cibernética no Governo (https://agenciabrasil.ebc.com.br/radioagencia-nacional/seguranca/audio/2022-01/governo-sofreu-quase-cinco-mil-incidentes-ciberneticos-em-2021)

Observando os casos, nota-se claramente como o incidente cibernético afeta diretamente a vida do cidadão, impedindo muitas das vezes que ele faça compras ou utilize serviços de empresas privadas ou governamentais que são essenciais. Além da vertente monetária, nota-se também um número grande de ataques cibernéticos de cunho político (https://www.uol.com.br/tilt/noticias /redacao/2022/01/20/ataques-ciberneticos-como-arma-politica.htm).

Outro aspecto importante referente ao cenário atual de combate a ataques cibernéticos, é o fato de que nos últimos três anos o aumento na adoção do trabalho remoto foi a principal alternativa seguida pela grande maioria dos órgãos do Governo Federal para manter a execução das atividades de trabalho, e ao mesmo tempo diminuir os riscos de transmissão do coronavírus(COVID-19). Diante deste cenário a solução encontrada para permitir o acesso remoto aos colaboradores de modo a permitir a continuidade das atividades foi a implementação em larga escala de Redes Virtuais Privadas (Virtual Private Networks - VPN).

As Redes Privadas Virtuais (VPNs) permitem que os usuários se conectem remotamente a uma rede corporativa através de um túnel criptografado. Utilizando este túnel, os usuários podem aproveitar os serviços e proteções normalmente oferecidos aos usuários que estão dentro do perímetro corporativo (SEDE ou filial), como: ferramentas de colaboração, sistemas internos, repositórios de documentos confidenciais, firewalls e gateways de perímetro etc.

Entretanto, ao mesmo tempo em que o acesso via VPN viabiliza o trabalho remoto e fornece acesso a recursos privados, o abuso deste recurso vem sendo usado com grande frequência para ações maliciosas ou mesmo ataques direcionados às redes Internas das Instituições governamentais. Recentemente o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), lançou um alerta (https://www.gov.br/ctir/pt-br/assuntos/alertas-e recomendacoes/alertas/2022/alerta-08-2022) sobre os abusos em Redes Virtuais Privadas (VPN). Os abusos se dão devido à superfície de ataque que é ocasionado pela VPN, uma vez que para conceder os acessos ao usuário, ela insere o mesmo dentro da rede corporativa, possibilitando uma série ações maliciosas, após o acesso ser estabelecido.

Atualmente existem mais de 600 vulnerabilidades associadas a tecnologias de rede privada virtual (VPN) presentes no banco de CVE (Common Vulnerabilities and Exposures - https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=vpn). A tecnologia tem sido um alvo crescente e constante e vem sendo utilizada como vetor para ações maliciosas ou mesmo ataques direcionados às redes internas das instituições. Diversos Alertas foram emitidos pela NSA (National Security Agency https://media.defense.gov/2019 /Oct/07/2002191601/-1/-1/0/Mitigating%20Recent%20VPN%20Vulnerabilities%20%20Copy.pdf) sobre a exploração ativa dessas vulnerabilidades por ameaças avançadas em todo o planeta.

A exemplo destes ataques recentes podemos ilustrar o ataque ao Oleoduto Colonial Pipeline (https://g1.globo.com/economia /noticia/2021/06/09/senha-roubada-permitiu-que-hackers-atacassem-oleodutos-da-colonial pipeline-diz-empresa.ghtml), uma invasão crítica que interrompeu o fornecimento de combustível para todo o sudeste dos Estados Unidos em maio de 2020. O Presidente da Colonial Pipeline informou que o ataque ocorreu usando um sistema de rede privada virtual (VPN).

De acordo com o último levantamento realizado, a ENAP possui um total de 5000 (cinco mil) ativos digitais, sendo aproximadamente 500 (quinhentas) estações de trabalho, caixas de correio eletrônico e credenciais de usuários, 534 (quinhentos) equipamentos servidores físicos e virtuais e 4 (quatro) infraestruturas em nuvem e 1 (um) datacenter físico. O atendimento a toda essa estrutura possui forte necessidade de segurança cibernética.

Diante desse contexto, com a crescente demanda de usuários acessando o ambiente computacional de forma remota e com a evolução cada vez maior de migração dos dados para o ambiente de nuvem que a ENAP vem realizando (assinaturas de contratos de prestação de serviços em nuvem), faz-se cada vez mais necessária a busca por obter maior controle e segurança dos dados, a fim de evitar perdas de informações sensíveis e ataques cibernéticos através da contratação de uma solução integrada para proteção de usuários e visibilidade da superfície estendida de ataques, com resolução contínua de vulnerabilidades e priorização e correlação dos eventos de segurança, possibilitando a integração e todas as proteções em uma única visão.

A solução permitirá à ENAP registrar e monitorar os comportamentos dos usuários localizados dentro e fora do ambiente corporativo, oferecendo capacidade de controle de políticas de download, upload e compartilhamento de dados em aplicações de nuvem gerenciadas como Office 365, e em aplicações de nuvem não gerenciadas (Google Drive, Dropbox, WeTransfer, etc), e em dispositivos corporativos ou pessoais, assim como a descoberta e resolução contínua de vulnerabilidades de segurança, correlacionamento e priorização de eventos de segurança, simulações contínuas de ataque, aliado a serviços especializados para resposta a incidentes de segurança em meios digitais.

Tais iniciativas irão ampliar a camada de defesa cibernética da ENAP de forma considerável, bem como a elevação da maturidade de segurança da informação e privacidade na Escola a partir da contemplação estratégica de serviços de consultoria e gestão de riscos, elaboração de planos, políticas e procedimentos de segurança e da contemplação operacional (gestão de incidentes de segurança, simulação de ataques, proteção de email e de endpoints) a partir dos objetos propostos por esta contratação.

Nesse contexto observam-se também os impactos causados por ataques cibernéticos recentes contra instituições e órgãos do Governo, causando interrupção dos serviços e sistemas, afetando a disponibilidade e integridade das informações: 5.17.1. https://www.uol.com.br/tilt/noticias/redacao/2022/04/06/ataque-hacker-trf3-prazos-o-que-aconteceu.htm;5.17.2. https://www.tecmundo.com.br/seguranca/238738-sites-ministerio-saude-saem-do-ar-tentativa-invasao.htm.

Ainda nesse sentido, é importante trazer à pauta importantes recomendações normativas e de boas práticas trazidas pela Secretaria de Governo Digital – SGD, no que tange a Gestão de Vulnerabilidades e Segurança da Informação como um todo:

- Art.12, inciso IV, alínea “d” da Instrução Normativa no 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;
- CTIR Gov (Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo) (https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/);
- Guia do Framework de Segurança - CIS Controle 03: Gestão Contínua de Vulnerabilidade;
- CIS Controls v8 - Controle 07: Gestão contínua de vulnerabilidade;
- ABNT NBR ISO/IEC 27002 - 12.6 Gestão de vulnerabilidades técnicas.

Depreende-se das referências supracitadas uma crescente preocupação com a gestão de vulnerabilidades e atualização de patches, inclusive com a necessidade de utilização de softwares de forma a automatizar as rotinas de gerenciamento e atualização de patches nos diversos ambientes da Escola.

Ademais, constatou-se que o atual padrão e tendência do mercado de Threat Intelligence é a venda e contratação separada entre solução de monitoramento de ameaças externas para com serviços de gerenciamento de risco interno e planos de gestão de incidentes, conforme apontado nos diversos editais de órgãos governamentais publicados e realizados nos últimos anos. Tal separação contribui para a garantia de que os recursos e os esforços sejam direcionados exclusivamente para cada um dos casos. Desta forma, a interdependência entre esses dois serviços, sob o ponto de vista de auditoria, permite que a ENAP tenha sempre duas perspectivas de segurança a todo momento, com entregas mais especializadas.

O item 01 exige que a solução de monitoramento ganhadora deverá possuir API para integração. Acredita-se que essa integração (via API REST ou SDK) seja suficiente para a conversa entre as equipes, dado que a mesma consegue ser integrada com SIEMs, soluções de gerenciamento de ticket e ferramentas de BI, por exemplo, permitindo a rápida comunicação dos achados e a interação entre as equipes necessárias para as tratativas, prezando pela colaboração e a cooperação para o sucesso mútuo.

Dados os pontos apresentados acima, e visando promover uma maior competitividade entre as principais soluções e empresas de CTI existentes no mercado, bem como os padrões de contratação vistos hoje no mercado nacional, sejam de instituições públicas ou privadas, a contratação do serviço de monitoramento e visibilidade de ataques cibernéticos e SOC deve permanecer separada.

Nesse contexto, frente à necessidade de estruturação, operação e resolução contínua de vulnerabilidades e priorização/correlação dos incidentes de segurança, seguem detalhadas as pretendidas soluções que compõem os serviços gerenciados de segurança:

A prestação de serviços do Grupo 01 envolve:

- ITEM 01: Serviços especializados em Segurança da Informação (Gerenciamento de Riscos, de Políticas e Procedimentos de Segurança da Informação e Plano de Gestão de Incidentes) que tem por objetivo fortalecer a segurança da informação da ENAP, assegurando a confidencialidade, integridade e disponibilidade dos dados por meio da criação de diretrizes claras e procedimentos eficazes de gestão de segurança da informação especializados para desenvolver, implementar políticas, planos e procedimentos baseados, dentre outras boas práticas, nas normas ISO 27001 e ISO 27002. Este item abrange também o objetivo específico de de arquitetar a concepção de atividades de gestão de incidentes cibernéticos baseado nas características organizacionais e políticas da ENAP e aliado ao Serviço de Monitoramento, Detecção e Resposta a Incidente (Item 05).
- ITEM 02: Serviço de Conscientização de Segurança com o objetivo de promover a conscientização de segurança e a adoção de práticas seguras para proteger informações, sistemas e recursos contra ameaças cibernéticas, riscos físicos e outras formas de danos. Isso se aplica tanto a nível pessoal quanto organizacional.

A prestação de serviços do Grupo 02 envolve:

- ITEM 03: Serviço de Monitoramento e Visibilidade de Ataques Cibernéticos que tem como finalidade aplicar inteligência voltada para a segurança da ENAP, com o objetivo de realizar buscas contínuas em diversas camadas da internet, incluindo a Surface, Deep e Dark Web. Essas buscas têm como foco a identificação de informações sensíveis que possam estar sendo discutidas ou comercializadas de forma ilegal, tais como dados confidenciais, informações privilegiadas ou quaisquer outros tipos de conteúdo que possam representar uma ameaça à integridade da ENAP.

A prestação de serviços do Grupo 03 envolve:

- ITEM 04: Serviço de Gestão de Vulnerabilidade com Priorização de Riscos ao Negócio, Gestão de Patch para Ativos de Rede e Aplicação Web que tem por objetivo, de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação, na infraestrutura e aplicações da ENAP, a fim de evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas. O serviço também contempla gestão de vulnerabilidade;
- ITEM 05: Serviço de Monitoramento, Detecção e Resposta a Incidentes que tem como objetivo prover à ENAP mecanismo de visibilidade de logs, rede e informações, capaz de identificar eventos maliciosos, através de correlacionamento de logs e tráfego de rede, que possam comprometer os serviços tecnológicos da ENAP;
- ITEM 06: Serviço Gerenciado de Detecção e Resposta para Endpoints que tem como objetivo fornecer uma visão ampliada e integrada do ambiente de TI da ENAP, permitindo a detecção e resposta eficazes a ameaças cibernéticas e protegendo seus ativos e dados contra ataques maliciosos;
- ITEM 07: Serviço Gerenciado de Proteção Avançada de E-mail que tem como objetivo principal proteger a ENAP contra ameaças relacionadas a e-mails, como phishing, malware, spam e outras formas de ataques cibernéticos direcionados através de mensagens eletrônicas. Ele oferece uma camada adicional de segurança para garantir que os e-mails recebidos e enviados pela organização estejam livres de ameaças e sejam autênticos;
- ITEM 08: Serviço de simulação de ataques cibernéticos que tem como objetivo avaliar a segurança dos sistemas e redes da ENAP por meio da simulação de um ataque controlado e realista, visando identificar possíveis vulnerabilidades e aprimorar as defesas de segurança da instituição utilizando as táticas, técnicas e processos do Mitre ATT&CK®.

A sistematizção das soluções e o quantitativo estimado para esta demanda, baseado nas necessidades elencadas, encontram-se nas tabelas abaixo:

GRUPO	ITEM	DESCRIÇÃO	QTD
1	1	Serviços especializados em Segurança da Informação (Gerenciamento de Riscos, de Políticas, Planos e Procedimentos de Segurança da Informação)	**1 Serviço Unitário**
	2	Serviço de conscientização de Segurança	**500 Usuários**
VALOR TOTAL GRUPO 01			
2	3	Serviço de monitoramento e visibilidade de ataques cibernéticos	**1 Marca**
VALOR TOTAL GRUPO 02			
3	4	Serviço de gestão de vulnerabilidade com priorização de riscos ao negócio e gestão de patch para ativos de rede e aplicações web	**640 ativos**
	5	Serviço de monitoramento, detecção e resposta a incidentes	**1500 Eventos por segundo (EPS)**
	6	Serviço gerenciado de detecção e resposta para endpoints	**1036 ativos**
	7	Serviço gerenciado de proteção de avançada de e-mail	**500 caixas de email**
	8	Serviço de simulação de ataques cibernéticos	**9 ataques simultâneos**
VALOR TOTAL GRUPO 03			

A tabela abaixo descreve o atual cenário da infraestrutura de TI da ENAP:

ATIVO	QUANTIDADE
Estações de Trabalho	500
Equipamentos servidores	534
Infraestrutura de E-mail G-Suite	1
Infraestrutura de E-mail Microsoft 365	1
Caixas de correio eletrônico	500
Perfis executivos	10
Usuários	500
Aplicações Web	104
Datacenter físico	1
Infraestrutura em Nuvem	4
Ativos digitais (marcas, apps, faixas de endereço IP, contas em redes sociais)	5000

No atual cenário da ENAP, não existe um número de funcionários/colaboradores suficientes e preparados para a sustentação de todas as soluções necessárias para o alcance dos objetivos e satisfação das necessidades em segurança cibernética, por isso o estudo dos cenários busca, além das ferramentas, serviços gerenciados e especializados de apoio à gestão da segurança da informação e operação dos processos de segurança cibernética.

8. Levantamento de soluções

Geralmente, os SOC's são unidades compartilhadas, portanto instituir uma estrutura similar fisicamente no ambiente da ENAP com todas as soluções e ferramentas de segurança necessárias requer um gigantesco investimento por parte da ENAP para manter todos esses serviços e profissionais de forma dedicada e exclusiva 24x7x365, além do investimento em equipamentos, treinamentos, atualizações e capacitação de profissionais certificados.

Até a elaboração deste ETP, não foi encontrado no Portal do Software público, ferramenta voltada para a segurança cibernética que atenda a necessidade da ENAP ou software público que esteja atualizado contra novos ataques e vulnerabilidades em tempo real.

Acrescentamos que utilizar solução de outros órgãos não atende aos requisitos específicos da ENAP, haja vista que serviços de segurança exigem um conjunto de serviços de segurança e inteligência especializados, bem como de monitoramento de forma integrada e em tempo real por equipe especializada em segurança, além de serviços e softwares específicos de monitoramento contra ataques cibernéticos, de gestão de vulnerabilidades, de resposta a incidentes e requisições, de risco e conformidade, de testes de invasão, de descoberta e mapeamento de dados sensíveis, de inteligência aplicado à segurança, bem como de serviços especializados 24x7x365 em segurança que exigem um know-how e curva de aprendizado muito elevada.

No âmbito de espaço físico, não há necessidade de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual no que se refere à equipe presencial responsável pela Sustentação de Operações e Resposta a Requisições de Segurança.

Utilizar alternativas de mercado de forma separada também não atende as necessidades da ENAP porque requer a contratação de diferentes serviços de segurança, o que acarretaria em um maior custo e uma maior complexidade para se realizar a gestão e fiscalização de diferentes contratos, especialmente, se for levado em consideração o elevado volume de contratos existentes e o atual déficit de servidores atualmente na Coordenação de Infraestrutura, Cibersegurança e Serviços de TI (COINF) que atualmente conta com apenas com 4 (quatro) servidores sendo apenas 2 (dois) dedicados à segurança da informação.

Por se tratar de serviços que dependem exclusivamente da alocação de mão de obra especializada, e considerando que a atual configuração da equipe da DGI (Diretoria de Gestão Interna) da ENAP, conforme previsto na Resolução Enap nº 41, de 16 de maio de 2023 que aprova o Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC 2023-2025 - da ENAP (https://www.in.gov.br/web/dou/-/resolucao-enap-n-41-de-16-de-maio-de-2023-483960603), demanda uma execução indireta de tais serviços (Provisão solução de operação e atendimento a requisição e resposta a incidentes - SOC - e provisão de solução de proteção avançada à infraestrutura de TI da Enap), a única solução possível é a contratação junto ao mercado especializado.

A aquisição na forma de prestação de serviços como é feita no contrato atual (com exceção dos serviços evolutivos sob demanda), é uma solução viável considerando que a nova portaria de contratação de soluções de tecnologia da informação SGD /ME 6.432 de 15 de junho de 2021 SEI (1052531), recomenda utilizar o pagamento fixo mensal para contratação de serviços e monitoramento de segurança.

Portanto, em relação à força de trabalho e aos modelos contratuais, levantou-se os seguintes cenários:

Id	Solução	Descrição da Solução
1	Utilização de servidores efetivos	UTILIZAR SERVIDORES EFETIVOS DA COINF (COORDENAÇÃO DE INFRAESTRUTURA, CIBERSEGURANÇA E SERVIÇOS DE TI) PARA REALIZAÇÃO DO MONITORAMENTO, GESTÃO, OPERAÇÃO E SUSTENTAÇÃO DOS SERVIÇOS DE SEGURANÇA DA INFORMAÇÃO DA ENAP. Atualmente, a COINF (Coordenação de Infraestrutura, Cibersegurança e Serviços de TI) não dispõe, nem de quantitativo, nem de perfis suficientes para prestar o serviço de segurança 24x7x365 a contento, devido ao gigantesco volume de ativos de segurança necessários que a ENAP possui e que precisam ser protegidos com eficiência segundo as normas de segurança, bem como para executar o monitoramento de incidentes conforme o modelo de central de operação de segurança SOC, com tempo de resposta hábil para o tratamento de incidentes de segurança compatível com a necessidade do órgão. Além disso, a ENAP precisaria contratar ferramentas de segurança adicionais de monitoramento e gerenciamento de eventos de segurança que precisaria ser constantemente atualizada necessitando de capacitação, treinamento e especialização específica, o que se seria inviável diante da enorme quantidade de requisições e de ativos de segurança a serem controlados atualmente considerando o tamanho do porte do parque tecnológico do órgão e a relevância de suas atividades finalísticas para a sociedade. Nesse modelo não é possível executar o Pentesting, entre os outros serviços das demais categorias, que é um serviço crítico para os projetos estratégicos da ENAP, pois esses testes de invasão requerem

		ferramentas e equipe de segurança altamente especializada com habilidades bastante específicas, que atualmente a ENAP não dispõe em seu quadro de servidores.
2	Utilização de postos de trabalho de dedicação exclusiva	CONTRATAR POSTOS FIXOS DE TRABALHO PARA PRESTAR OS SERVIÇOS DE SEGURANÇA COM DEDICAÇÃO EXCLUSIVA. A PORTARIA SGD/ME Nº 6.432, DE 15 DE JUNHO DE 2021, Art 2, §1 e §2 impede a utilização do modelo de dedicação exclusiva de mão de obra por postos de trabalho sendo vedado ao CONTRATANTE realizar a distribuição, controle, fiscalização ou supervisão dos recursos humanos da CONTRATADA, a exemplo de quantidade de perfis, base salarial, jornada, frequência ou outros critérios relacionados à alocação de mão de obra.
3	Utilização de serviços por UST - unidade de serviços técnicos - ou similares	CONTRATAR SERVIÇOS DE INFRAESTRUTURA DE TIC PARA SEGURANÇA DA INFORMAÇÃO BASEADO EM UST (UNIDADE DE SERVIÇOS TÉCNICOS) QUE LEVA EM CONSIDERAÇÃO A COMPLEXIDADE DAS TAREFAS, A PRIORIDADE E A CRITICIDADE PARA PRECIFICAÇÃO. O referido modelo consiste na definição prévia: i) de todas as tarefas a serem executadas; ii) dos resultados esperados; iii) dos padrões de qualidade exigidos; e iv) dos procedimentos e qualificações necessárias à execução dos serviços em conformidade com os adotados pela organização de maneira a permitir a análise comparativa posterior entre o planejado e o executado. O TCU, após analisar algumas contratações baseadas nessa metodologia de medição, resultado de Fiscalizações de Orientação Centralizada – FOC, publicou o Acórdão 2037/2019 – Plenário, onde identificou problemas e recomenda, dentre alguns pontos, que: “a métrica UST deve ser evitada para a contratação de serviços de suporte contínuo de infraestrutura de TIC”, e que deve-se “avaliar, durante o planejamento da contratação do serviço de TIC, alternativas à métrica UST, bem como documentar as justificativas da escolha”.
4	Manutenção do ambiente atual	MANUTENÇÃO ORGÂNICA DO AMBIENTE, DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO E DA OPERAÇÃO DE SEGURANÇA CIBERNÉTICA ATUAIS DA ENAP.
5	Implantação de solução integrada para proteção de usuários e visibilidade da superfície estendida de ataques, com resolução contínua de vulnerabilidades e priorização e correlação dos eventos de segurança em ambientes On-Premises	CONTRATAR SERVIÇOS DE SEGURANÇA DA INFORMAÇÃO EM AMBIENTE ON-PREMISES. Cenário que visa a implantação de solução integrada para proteção de usuários e visibilidade da superfície estendida de ataques, com resolução contÍnua de vulnerabilidades e priorização e correlação dos eventos de segurança em ambientes *On-Premises*.
		CONTRATAR SERVIÇOS DE FORMA INTEGRADA EM CONJUNTO COM MÃO DE OBRA ESPECIALIZADA LOCAL PARA PROVER OS SERVIÇOS TÉCNICOS ESPECIALIZADOS DE SUPORTE, MONITORAMENTO E GERENCIAMENTO DE SEGURANÇA VIA SOC.

6	Contratação de Serviços Gerenciados de Segurança Cibernética por meio de pagamento fixo mensal vinculado ao atendimento de níveis mínimos de serviços	Esta solução engloba o SOC (Security Operations Center) e um MSSP (Managed Security Services Provider), que operam remotamente e também, de forma presencial, através de uma equipe de técnicos especializados em segurança que atuariam localmente na sede da ENAP. Quando a administração pública passa a contar com os serviços do MSSP, ela deixa de se preocupar com a gestão de suas soluções de proteção de dados e, com isso, consegue uma significativa redução de gastos com licenças, hardwares e softwares. Para essa solução, mantém-se o atendimento de chamados técnicos mediante Níveis Mínimos de Serviço a serem cumpridos de forma conjunta com os serviços prestados pelo SOC e MSSP. Por outro lado, se os serviços não atenderem os Níveis Mínimos de Serviço especificados, o pagamento pode sofrer redução conforme critérios técnicos estabelecidos em edital.

Identificação das Soluções.

9. Análise comparativa de soluções

A escolha pela solução ocorreu sobre os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação e pelas recomendações dos órgãos de controle. No portal do software público não foi possível encontrar solução capaz de proteger os ativos de segurança do órgão de acordo com o já exposto neste estudo.

Conforme análises realizadas, apesar da Solução 1 apresentar-se a mais econômica, pois não requer gasto com mão de obra, ela esbarra no problema da falta de servidores efetivos e de ferramentas adicionais que a ENAP não dispõe. Caso se optasse por essa solução, a ENAP precisaria adquirir outras soluções de segurança que não estão no ROL de ferramentas de segurança da Escola como, dentre outros, software para Gestão de Vulnerabilidades, o Security Information and Event Management (SIEM) para a coleta e monitoramento de log de eventos identificando ameaças em tempo real.
Ademais, até o momento o portal do software público não dispõe deste tipo de solução, portanto, esta solução foi descartada.

Também ficou evidenciado não ser possível aplicar a Solução 2 (Contratação de serviços por postos de trabalho) e a Solução 3 (Contratação de serviços que utiliza a métrica de UST) por atendimento às recomendações dos órgãos de controle.

As alternativas 4 (Cenário de manutenção do ambiente atual) e 5 (Cenário de implantação de solução integrada para proteção de usuários e visibilidade da superfície estendida de ataques, com resolução contínua de vulnerabilidades e priorização e correlação dos eventos de segurança em ambientes On-Premises) são consideradas inviáveis.

Segue a análise tabular das soluções:

Análise comparativa e qualitativa das soluções identificadas.

Solução	Vantagens	Desvantagens
Utilização de servidores efetivos	Manutenção do de conhecimento adquirido durante a operação das soluções existentes. Ausência de custeio extra de mão de obra.	Baixa capacidade em quantitativo de servidores e de soluções disponíveis. Contratação inevitável de um rol grande de subscrições de ferramentas sem apoio gerencial e operacional. Alta complexidade de administração e de curva de aprendizado.
Utilização de postos de trabalho de	Compartilhamento	Não atendimento às recomendações dos

dedicação exclusiva	de priorização de força de trabalho	órgãos de controle.
Utilização de serviços por UST - unidade de serviços técnicos - ou similares	Transferência de riscos. Adição de força de trabaho para a operação de segurança cibernética.	Não atendimento às recomendações dos órgãos de controle.
Manutenção do ambiente atual	Soluções já gerenciadas pela equipe de tecnologia; Infraestrutura já existente; Não é necessário iniciar novo processo licitatório.	Extrema complexidade de criação e aplicação de políticas de controle de dados; Falta de funcionalidades avançadas; Necessidade de integração com outras ferramentas para controle e auditoria; Falta de proteção contra novas ameaças em nuvem; Não identifica ou bloqueia grandes ataques cibernéticos; Impacto na máquina dos usuários gerando impacto no desempenho do colaborador; Falta de capacidade de bloqueio para ameaças avançadas; Falta de iniciativas voltadas diretamente para detecção e bloqueio de ransomware; Falta de visibilidade e capacidade de correção de vulnerabilidades de segurança; Falta de um framework integrado de segurança voltado para resposta a incidentes de segurança; Baixa capacidade de resposta a incidentes que eventualmente já tenham ocorrido.
Implantação de solução integrada para proteção de usuários e visibilidade da superfície estendida de ataques, com	Dados sensíveis serão analisados	Necessidade de implementação de appliances físico ou virtual dentro do ambiente de Data Center, comprometendo a escalabilidade da solução; Atualmente a maior parte do tráfego de redes é criptografado sendo necessário habilitar funcionalidade de SSL decryption no NGFW, o que compromete o desempenho de rede,

resolução contínua de vulnerabilidades e priorização e correlação dos eventos de segurança em ambientes On-Premises	sem infraestrutura de terceiros.	devido a necessidade de utilização de recursos de processamento do equipamento; Adquirir solução para funcionalidade de decriptação e orquestração de SSL; Perda de conhecimento adquirido na solução existente, uma vez que haverá a necessidade de treinamento de toda a equipe de técnica; Elaboração de projeto para contratação de uma nova solução.
Contratação de Serviços Gerenciados de Segurança Cibernética por meio de pagamento fixo mensal vinculado ao atendimento de níveis mínimos de serviços	A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública. Sem necessidade de instalação de infraestrutura local; Sem impacto nas máquinas dos usuários; Decriptografia do tráfego SSL com escalabilidade; Funcionalidades avançadas de controle e visibilidade de tráfego; Proteção contra ransomware e malwares modernos; Visibilidade automática de vulnerabilidades de segurança; Correção automática de vulnerabilidades de segurança; Integração de todas as visões de segurança em uma única plataforma;	Perda de conhecimento adquirido na solução existente, uma vez que haverá a necessidade de treinamento de toda a equipe de técnica; Elaboração de projeto para contratação de uma nova solução.

	Disponibilização de um framework para descoberta, triagem e resolução de incidentes de segurança; Aplicação de inteligência de ameaças contextual em todos os eventos de segurança da rede corporativa; Automatização de testes de segurança em toda a infraestrutura de proteção; Ampliação da camada de proteção dos usuários que utilizam e-mail corporativo.	

10. Registro de soluções consideradas inviáveis

Conforme §1º do inciso V do art. 11 da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022 regida pela Lei nº 14.133, de 2021, as soluções identificadas e consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação, dispensando-se a realização dos respectivos cálculos de custo total de propriedade.

Em função dos serviços corresponderem exclusivamente à alocação de mão de obra especializada, e serem abrangidos pela Portaria SGD/ME No 6.432, de 15 de junho de 2021 SEI (1052531), e suas atualizações, a solução a ser considerada foi a Contratação de Serviços Gerenciados de Segurança da Informação por meio de pagamento fixo mensal vinculado ao atendimento de níveis mínimos de serviços.

Em relação à força de trabalho, as alternativas 1 (Utilização de servidores efetivos), 2 (Utilização de postos de trabalho de dedicação exclusiva) e 3 (Serviços por UST - unidade de serviços técnicos - ou similares) foram consideradas inviáveis, devido às restrições legais (Portaria 6.432), técnicas e a ausência completa de parâmetros confiáveis de custos para comparação e composição da estimativa de custos (TCO), portanto, dispensamos a realização das correspondentes estimativas de custos dessas soluções.

Em relação ao modelo contratual, após levantamento das possíveis soluções, a equipe de planejamento da contratação, concluiu que as alternativas 4 (Cenário de manutenção do ambiente atual) e 5 (Cenário de implantação de solução integrada para proteção de usuários e visibilidade da superfície estendida de ataques, com resolução contínua de vulnerabilidades e priorização e correlação dos eventos de segurança em ambientes *On-Premises*) são consideradas inviáveis.

Dessa forma, com base no § 1º do art. 11 da IN 94/2022 da SGD/ME, as soluções identificadas e consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação (breve descrição e justificativa), dispensando-se a realização dos respectivos cálculos de custo total de propriedade.

11. Análise comparativa de custos (TCO)

Não se aplica, pois apenas 1 (uma) solução se mostrou viável não sendo possível realizar comparação com outra, conforme previsto no art. 11, § 1º da Instrução Normativa nº 94, de 23 de dezembro de 2022. "§ 1º As soluções identificadas no inciso II consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação, dispensando-se a realização dos respectivos cálculos de custo total de propriedade." Como somente a Solução 6 foi considerada viável, portanto não há necessidade de se realizar o Cálculo dos Custos Totais de Propriedade.

Apesar disso, por meio de pesquisa de preços, seguindo as normas da Instrução Normativa SEGES/ME nº 65, de 07 de julho de 2021, chegou-se ao valor estimado da contratação para a Solução 6, conforme descrito no documento SEI 0777770, contido no processo SEI 04600.002376/2023-45, ao objeto de contratação de empresa especializada para fornecimento de serviços gerenciados de segurança da informação para a Fundação Escola Nacional de Administração Pública – Enap, bem como fornecimento de soluções, ferramentas e e treinamento para os servidores da Escola, por Sistema de Registro de Preços, conforme condições, quantidades e exigências estabelecidas neste edital.

Por meio de pesquisa de preços (SEI 0777769), foram considerados processos da Administração Pública, similares ao objeto desta contratação, e pesquisa de preços com fornecedores (SEI 0777768) a fim de se aplicar um cálculo do valor unitário das pesquisas e propostas sob a metodologia de escolha do menor valor entre a média e a mediana do valor mensal, definindo assim, o valor base do pregão.

A metodologia supracitada foi escolhida para considerar os métodos mais comuns de mercado (média e mediana) e eliminar possíveis distorções em decorrência de valores extremos, para reduzir o risco de valores inexequíveis.

A base monetária dos valores encontrados e dos valores estimados, conforme apresentados na tabela a seguir, é a moeda Real Brasileiro (BRL) representada pelo símbolo R$:

Item	1	2	3	4	5	6	7	8
Descrição	**Serviços especializados em Segurança da Informação**	**Serviço de conscientização de Segurança**	**Serviço de monitoramento e visibilidade de ataques cibernéticos**	**Serviço de gestão de vulnerabilidade**	**Serviço de monitoramento, detecção e resposta a incidentes**	**Serviço gerenciado de detecção e resposta para endpoints**	**Serviço gerenciado de proteção de avançada de e-mail**	**Serviço de simulação de ataques cibernéticos**
CATSER/CATMAT	27340	27340	27359	27006	27359	27006	27006	27359
Unidade	Serviço unitário	Meses	Meses	Meses	Meses	Meses	Meses	Meses
Quantidade	1	12	12	12	12	12	12	12
MRE PREGÃO 03/2023	726835,59			30284,82	87565,93			19093,7
STJ PREGÃO 13/2023	448.990,00							
FUNDACAO OSWALDO CRUZ/RJ PREGÃO 11/2023						33333,33		
AGU PREGÃO 03/2023							78750	
SUPERINTENDÊNCIA ESTADUAL DE COMPRAS E LICITAÇÕES DE RONDÔNIA PREGÃO 161/2023						38.333,33	5.729,75	
TSE/AM PREGÃO 39/2023		4194,44						
BASA PREGÃO Nº 56/2022		9465,6						
MJ PREGÃO 21/2021								14583,33
TRT/SP PREGÃO 141/2023				35413,56				
TRT 17ª Região PREGÃO Nº 03/2023					45000			
Proposta RSec Group			35083,33					
Proposta Apura			35000					
Proposta ISH	1.316.490,75	16683,03	16813,78	45238,54	100578,53	52908,11	49473,09	30708,17

Como relatado na seção "12. Descrição da Solução de TIC a ser Contratada" deste Estudo Técnico Preliminar, ante as necessidades de negócio e as necessidades tecnológicas já descritas neste documento, o levantamento de soluções, bem como a

análise comparativa das soluções, que indicou as soluções viáveis, foram baseados na *Cybersecurity Mesh Architecture* (CSMA), uma abordagem moderna de segurança cibernética que se concentra na criação de um ecossistema de segurança distribuído e flexível, preconizada pelo Gartner <https://www.gartner.com/en/information-technology/glossary/cybersecurity-mesh>.

As soluções propostas se encaixam na CSMA pelos seguintes motivos:

a) Camada de Segurança de Identidade: O serviço de monitoramento e visibilidade de ataques cibernéticos pode ser considerado parte da camada de segurança de identidade, pois busca proteger a reputação e as informações sensíveis da ENAP.

b) Camada de Segurança de Dados: O serviço de monitoramento, detecção e resposta a incidentes se encaixa na camada de segurança de dados, pois visa proteger os dados da ENAP contra acesso não autorizado e vazamentos.

c) Camada de Segurança de Infraestrutura: A gestão de vulnerabilidades pode ser considerada parte da camada de segurança de infraestrutura, pois visa proteger os sistemas e aplicações da ENAP contra ataques.

Destaca-se, todavia, que o ano de 2024 reservou para a ENAP uma realidade orçamentária impeditiva para a contratação de todos os itens estudados e objetos de cotação de preços em processos de contratação governamentais similares e de propostas de preços por empresas pré-proponentes aptas a entregarem tais soluções.

Os itens 02 (Serviço de conscientização de Segurança para até 500 usuários), 04 (Serviço de gestão de vulnerabilidade com priorização de riscos ao negócio para ativos de rede e aplicações web) e 08 (Serviço de simulação de ataques cibernéticos) serão removidos do Termo de Referência e serão objetos de contratação futura sob uma realidade orçamentária mais oportuna. O item 01, dadas as suas necessidade, importância e essencialidade, foi substituído por um serviço embutido no item 05.

Ademais, outro processo de contratação em estágio mais avançado (SEI 04600.000850/2024-85), como bônus, oferece serviços de *Endpoint Security* (proteção de computadores e equipamentos servidores), *Data Leak Prevention* (Prevenção a Perda de Dados), *Email Security* (Segurança de Caixas de Correio Eletrônico) que sombreariam os itens 06 (Serviço gerenciado de detecção e resposta para endpoints) e 07 (Serviço gerenciado de proteção de avançada de e-mail).

Os itens 03 (Serviço de monitoramento e visibilidade de ataques cibernéticos) e 05 (Serviço de monitoramento, detecção e resposta a incidentes) foram os únicos que permaneceram como objeto de contratação deste edital em função de necessidades de negócio, definição do corpo gestor e de sua capacidade de elevarem a maturidade de segurança da informação e segurança cibernética da Escola. Além disso, todo o estudo realizado neste processo será mantido e inventariado como fonte de consulta para futuras oportunidades tanto de aderência à *Cybersecurity Mesh Architecture* (CSMA) quanto para a implantaçao de um Sistema de Gestão de Segurança da Informação na ENAP.

O detalhamento técnico da solução a ser contratada, então, contempla apenas os itens escolhidos (03 e 05 que se tornarão os itens 01 e 02 no Termo de Referência), a saber:

Grupo 01				
ITEM	**ESPECIFICAÇÃO**	**CATSER**	**MÉTRICA OU UNIDADE DE MEDIDA**	**QUANTIDADE**
1	Serviço de monitoramento e visibilidade de ataques cibernéticos	27359	Meses	12
Grupo 02				
2	Serviço de **monitoramento,**		Meses	

	detecção e resposta a incidentes - 1500 Eventos por segundo (EPS)	27359		12

Além disso, considerando a supracitada circunstância orçamentária da Escola, o período de execução foi definido como 12 meses e não 5 anos como inicialmente se planejara.

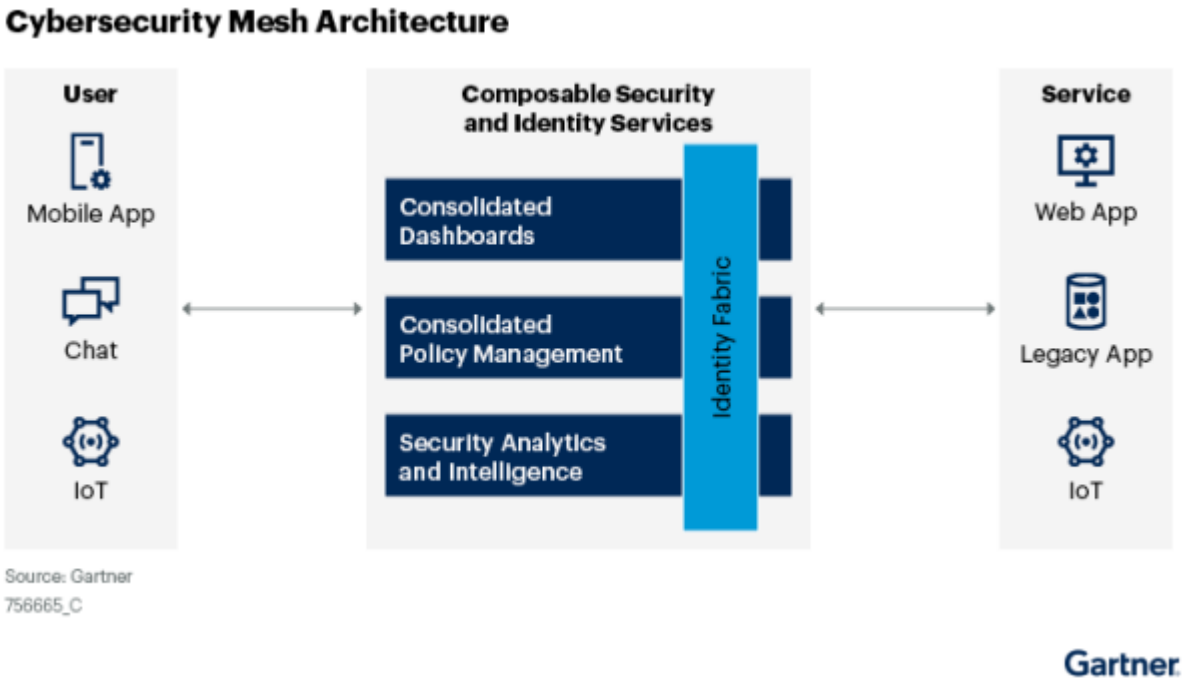
Portanto, dadas as considerações de escolha dos itens, e aplicando-se a metodologia utilizada, chegou-se aos seguintes valores:

Item	Média Unitária	Mediana Unitária	Valor Total Estimado (Menor Valor Unitário entre Média e Mediana)
1	R$ 28.965,70	R$ 35.000,00	R$ 347.588,44
Valor Estimado para os itens do Grupo 01			R$ 347.588,44
2	R$ 77.714,82	R$ 87.565,93	R$ 932.577,84
Valor Estimado para os itens do Grupo 02			R$ 932.577,84
VALOR TOTAL ESTIMADO			R$ 1.280.166,28

Portanto, o valor total da pesquisa foi estimado em **R$ 1.280.166,28 (um milhão e duzentos e oitenta mil e cento e sessenta e seis reais e vinte e oito centavos)**.

12. Descrição da solução de TIC a ser contratada

Ante as necessidades de negócio e as necessidades tecnológicas já descritas neste documento, o levantamento de soluções, bem como a análise comparativa das soluções, que indicou as soluções viáveis, foram baseados na *Cybersecurity Mesh Architecture* (CSMA), uma abordagem moderna de segurança cibernética que se concentra na criação de um ecossistema de segurança distribuído e flexível, preconizada pelo Gartner <https://www.gartner.com/en/information-technology/glossary/cybersecurity-mesh>. A CSMA permite que as organizações protejam seus ativos digitais, independentemente de onde eles estejam localizados, seja na nuvem, no data center ou em dispositivos endpoint, conforme exibido na figura a seguir:



As soluções que a ENAP estudou para esta contratação convergem com diversos pontos de convergência com os princípios da CSMA:

1. Descentralização:

   A solução da ENAP se divide em três grupos de serviços, cada um com foco em uma área específica da segurança cibernética. Essa descentralização alinha-se com a CSMA, que defende a distribuição da segurança em camadas e a implementação de controles específicos para cada tipo de ativo.

1. Visibilidade e Análise:

   Tanto o serviço de monitoramento e visibilidade de ataques cibernéticos quanto o serviço de monitoramento, detecção e resposta a incidentes enfatizam a coleta e análise de dados de diferentes fontes. Essa abordagem é fundamental para a CSMA, que se baseia na visibilidade centralizada e na análise de dados para identificar e responder a ameaças de forma eficiente.

1. Automação e Orquestração:

A solução da ENAP busca automatizar processos de segurança, como a detecção de incidentes e a gestão de vulnerabilidades. A automação e orquestração são elementos-chave da CSMA, permitindo que as organizações respondam rapidamente a ameaças e reduzam o tempo de reação.

1. Segurança Zero Trust:

   A ênfase na proteção de informações sensíveis e na criação de um ecossistema de proteção digital sugere que a ENAP está buscando uma abordagem de segurança Zero Trust. A CSMA é compatível com o Zero Trust, pois permite que as organizações implementem controles de acesso granular e verifiquem continuamente a identidade de usuários e dispositivos.

As soluções propostas se encaixam na CSMA pelos seguintes motivos:
a) Camada de Segurança de Identidade: O serviço de monitoramento e visibilidade de ataques cibernéticos pode ser considerado parte da camada de segurança de identidade, pois busca proteger a reputação e as informações sensíveis da ENAP.
b) Camada de Segurança de Dados: O serviço de monitoramento, detecção e resposta a incidentes se encaixa na camada de segurança de dados, pois visa proteger os dados da ENAP contra acesso não autorizado e vazamentos.

c) Camada de Segurança de Infraestrutura: A gestão de vulnerabilidades pode ser considerada parte da camada de segurança de infraestrutura, pois visa proteger os sistemas e aplicações da ENAP contra ataques.

Destaca-se, todavia, que o ano de 2024 reservou para a ENAP uma realidade orçamentária impeditiva para a contratação de todos os itens estudados e objetos de cotação de preços em processos de contratação governamentais similares e de propostas de preços por empresas pré-proponentes aptas a entregarem tais soluções.

Os itens 02 (Serviço de conscientização de Segurança para até 500 usuários), 04 (Serviço de gestão de vulnerabilidade com priorização de riscos ao negócio para ativos de rede e aplicações web) e 08 (Serviço de simulação de ataques cibernéticos) serão removidos do Termo de Referência e serão objetos de contratação futura sob uma realidade orçamentária mais oportuna. O item 01, dadas as suas necessidade, importância e essencialidade, foi substituído por um serviço embutido no item 05.

Ademais, outro processo de contratação em estágio mais avançado (SEI 04600.000850/2024-85), como bônus, oferece serviços de *Endpoint Security* (proteção de computadores e equipamentos servidores), *Data Leak Prevention* (Prevenção a Perda de Dados), *Email Security* (Segurança de Caixas de Correio Eletrônico) que sombreariam os itens 06 (Serviço gerenciado de detecção e resposta para endpoints) e 07 (Serviço gerenciado de proteção de avançada de e-mail).

Os itens 03 (Serviço de monitoramento e visibilidade de ataques cibernéticos) e 05 (Serviço de monitoramento, detecção e resposta a incidentes) foram os únicos que permaneceram como objeto de contratação deste edital em função de necessidades de negócio, definição do corpo gestor e de sua capacidade de elevarem a maturidade de segurança da informação e segurança cibernética da Escola. Além disso, todo o estudo realizado neste processo será mantido e inventariado como fonte de consulta para futuras oportunidades tanto de aderência à *Cybersecurity Mesh Architecture* (CSMA) quanto para a implantaçao de um Sistema de Gestão de Segurança da Informação na ENAP.

Portanto, os os itens selecionados (03 e 05), para permanecerem como objeto de contratação, tornar-se-ão os itens 01 e 02, componentes, cada um, de grupo isolado, no Termo de Referência, conforme resumido na tabela abaixo:

Grupo 01							
ITEM	**ESPECIFICAÇÃO**	**CATSER**	**MÉTRICA OU UNIDADE DE MEDIDA**	**CÓD. PMC-TIC**	**QUANTIDADE**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	Serviço de monitoramento e visibilidade de ataques cibernéticos	27359	Meses		12		
Grupo 02							
2	Serviço de **monitoramento, detecção e resposta a incidentes** - 1500 Eventos por segundo (EPS)	27359	Meses		12		

O detalhamento técnico da solução, somente com os itens escolhidos , encontra-se descrito no **ANEXO I - Caderno de Especificações Técnicas** (DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO), deste Estudo Técnico Preliminar.

13. Estimativa de custo total da contratação

Valor (R$): 1.280.166,20

Para uma precisa estimativa de valores do objeto desta contratação, a equipe de planejamento, utilizou como parâmetro legal a Instrução Normativa SEGES /ME Nº 65, de 7 de Julho de 2021, como fonte de pesquisa e utilizou:

8.1.1. Os incisos I e II do Art, Painel de Preços (http://paineldeprecos.planejamento.gov.br), aquisições e contratações similares de outros entes públicos, no qual está demonstrado no Mapa Comparativo de Preços com a composição da média de mercado.

8.1.2. Para compor uma melhor estimativa de mercado, e de acordo com o inciso IV do Art. 5º, realizamos pedidos de preços junto aos fornecedores, mediante contato direto para apresentação de orçamentos prévios, no qual se obteve uma média de valor mais coerente com a realidade de mercado do objeto deste processo licitatório, conforme disposto no Mapa Comparativo (SEI 0715727).

8.2. Com isso, o valor estimado da contratação é de **1.280.166,28 (um milhão e duzentos e oitenta mil e cento e sessenta e seis reais e vinte e oito centavos).**

14. Justificativa técnica da escolha da solução

Solução: Contratação de Serviços Gerenciados de Segurança Cibernética por meio de pagamento fixo mensal vinculado ao atendimento de níveis mínimos de serviços.

Descrição: CONTRATAR SERVIÇOS DE FORMA INTEGRADA EM CONJUNTO COM MÃO DE OBRA ESPECIALIZADA LOCAL PARA PROVER OS SERVIÇOS TÉCNICOS ESPECIALIZADOS DE SUPORTE, MONITORAMENTO E GERENCIAMENTO DE SEGURANÇA VIA SOC.

Esta solução engloba o SOC (*Security Operations Center*) e um MSSP (Managed Security Services Provider), que operam remotamente e também, de forma presencial, através de uma equipe de técnicos especializados em segurança que atuariam localmente na sede da ENAP.

Quando a administração pública passa a contar com os serviços do MSSP, ela deixa de se preocupar com a gestão de suas soluções de proteção de dados e, com isso, consegue uma significativa redução de gastos com licenças, hardwares e softwares.

Para essa solução, mantém-se o atendimento de chamados técnicos mediante Níveis Mínimos de Serviço a serem cumpridos de forma conjunta com os serviços prestados pelo SOC e MSSP. Por outro lado, se os serviços não atenderem os Níveis Mínimos de Serviço especificados, o pagamento pode sofrer redução conforme critérios técnicos estabelecidos em edital.

Justificativa: Esta solução foi a escolhida por ser a mais abrangente e integrada (Contratação de Serviços Gerenciados de Segurança Cibernética por meio de pagamento fixo mensal vinculado ao atendimento de níveis mínimos de serviços), baseada na disponibilidade do parque computacional existente em conjunto com o SOC (Security Operations Center - SOC) 24x7x365 e equipe especializada de operação in loco e remota fornecida pela CONTRATADA , que permite à ENAP otimizar os recursos de infraestrutura, obter uma maior qualidade e sinergia no atendimento dos incidentes e chamados de segurança pelas equipes responsáveis.

Nesse modelo de contratação, não há necessidade de gastos adicionais com hardware e infraestrutura. Espera-se que com esta forma de contratação ocorra a redução da quantidade de problemas de segurança no parque computacional porque a uma única empresa será responsável por atender todos os serviços de segurança melhorando a qualidade no atendimento e diminuindo falhas de comunicação ao se contratar empresas diferentes para objeto de mesma natureza.

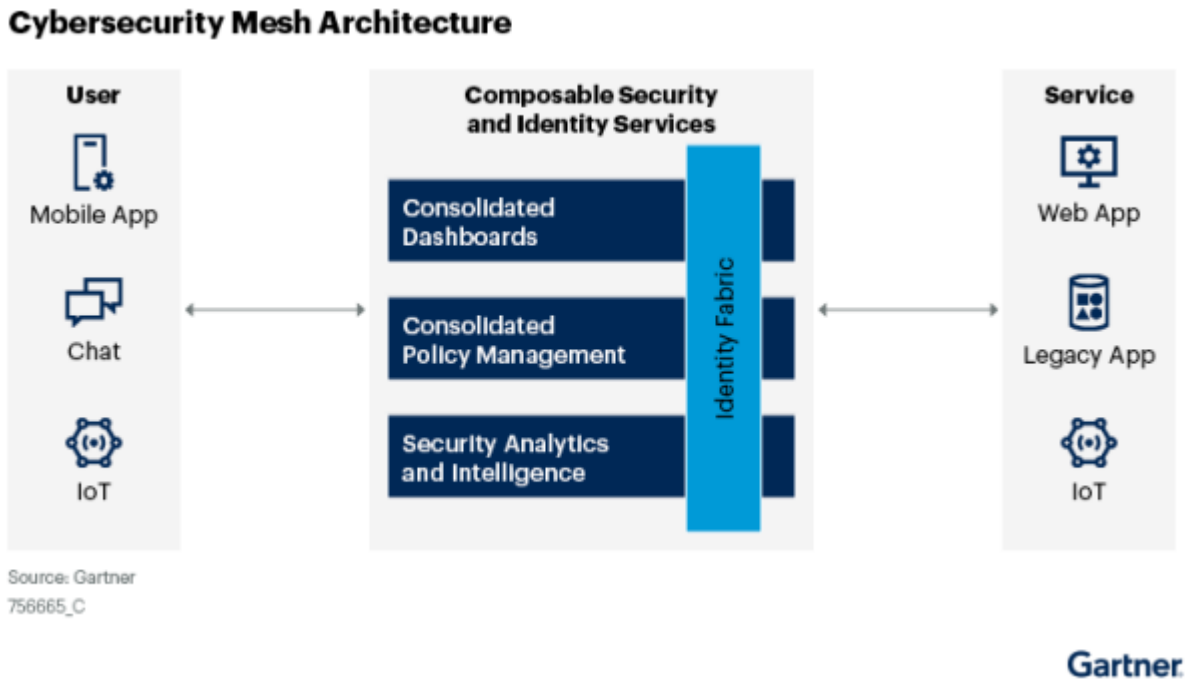
Além disso, a diminuição do volume de incidentes e problemas implica diretamente na redução do risco da CONTRATADA sofrer sanções administrativas, evitando-se assim a possibilidade da sua desqualificação durante a execução do contrato. Outra vantagem na adoção deste modelo é a previsibilidade de faturamento permitindo um melhor planejamento financeiro das partes, a simplificação da gestão e da fiscalização contratual e a melhoria contínua dos serviços prestados.

Acrescenta-se que o catálogo de serviços que define a descrição e os requisitos dos itens constante neste edital, estabelece uma baseline de serviços que poderão ser executados e que poderá ser ajustado posteriormente durante a execução contratual, facilitando a melhoria contínua da qualidade dos serviços prestados.

Considerando o tamanho do parque computacional da ENAP, os seus projetos e ativos estratégicos e o número de usuários (internos e externos, principalmente estudantes), os serviços de segurança a serem contratados devem priorizar, quando couber, uma parte da equipe de segurança para o trabalho presencial durante o horário comercial e atendimento emergencial fora deste horário, como também no regime de sobreaviso.

Quanto ao modelo de remuneração dos serviços, o art. 2o da Portaria SGD/ME No 6.432, de 15 de junho de 2021, estabelece que a contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação deverá ser realizada por meio de modelo de pagamento fixo mensal, vinculada exclusivamente ao atendimento de níveis mínimos de serviços previamente estabelecidos. Deste modo, o único modelo de remuneração possível a ser adotado é o de pagamento fixo mensal, vinculado ao atendimento de níveis mínimos de serviços.

Ante as necessidades de negócio e as necessidades tecnológicas já descritas neste documento, o levantamento de soluções, bem como a análise comparativa das soluções, que indicou as soluções viáveis, foram baseados na *Cybersecurity Mesh Architecture* (CSMA), uma abordagem moderna de segurança cibernética que se concentra na criação de um ecossistema de segurança distribuído e flexível, preconizada pelo Gartner <https://www.gartner.com/en/information-technology/glossary/cybersecurity-mesh>. A CSMA permite que as organizações protejam seus ativos digitais, independentemente de onde eles estejam localizados, seja na nuvem, no data center ou em dispositivos endpoint, conforme exibido na figura a seguir:



As soluções que a ENAP estudou para esta contratação convergem com diversos pontos de convergência com os princípios da CSMA:

1. Descentralização:

   A solução da ENAP se divide em três grupos de serviços, cada um com foco em uma área específica da segurança cibernética. Essa descentralização alinha-se com a CSMA, que defende a distribuição da segurança em camadas e a implementação de controles específicos para cada tipo de ativo.

1. Visibilidade e Análise:

   Tanto o serviço de monitoramento e visibilidade de ataques cibernéticos quanto o serviço de monitoramento, detecção e resposta a incidentes enfatizam a coleta e análise de dados de diferentes fontes. Essa abordagem é fundamental para a CSMA, que se baseia na visibilidade centralizada e na análise de dados para identificar e responder a ameaças de forma eficiente.

1. Automação e Orquestração:

A solução da ENAP busca automatizar processos de segurança, como a detecção de incidentes e a gestão de vulnerabilidades. A automação e orquestração são elementos-chave da CSMA, permitindo que as organizações respondam rapidamente a ameaças e reduzam o tempo de reação.

1. Segurança Zero Trust:

A ênfase na proteção de informações sensíveis e na criação de um ecossistema de proteção digital sugere que a ENAP está buscando uma abordagem de segurança Zero Trust. A CSMA é compatível com o Zero Trust, pois permite que as organizações implementem controles de acesso granular e verifiquem continuamente a identidade de usuários e dispositivos.

As soluções propostas se encaixam na CSMA pelos seguintes motivos:
a) Camada de Segurança de Identidade: O serviço de monitoramento e visibilidade de ataques cibernéticos pode ser considerado parte da camada de segurança de identidade, pois busca proteger a reputação e as informações sensíveis da ENAP.
b) Camada de Segurança de Dados: O serviço de monitoramento, detecção e resposta a incidentes se encaixa na camada de segurança de dados, pois visa proteger os dados da ENAP contra acesso não autorizado e vazamentos.
c) Camada de Segurança de Infraestrutura: A gestão de vulnerabilidades pode ser considerada parte da camada de segurança de infraestrutura, pois visa proteger os sistemas e aplicações da ENAP contra ataques.

Destaca-se, todavia, que o ano de 2024 reservou para a ENAP uma realidade orçamentária impeditiva para a contratação de todos os itens estudados e objetos de cotação de preços em processos de contratação governamentais similares e de propostas de preços por empresas pré-proponentes aptas a entregarem tais soluções.

Os itens 02 (Serviço de conscientização de Segurança para até 500 usuários), 04 (Serviço de gestão de vulnerabilidade com priorização de riscos ao negócio para ativos de rede e aplicações web) e 08 (Serviço de simulação de ataques cibernéticos) serão removidos do Termo de Referência e serão objetos de contratação futura sob uma realidade orçamentária mais oportuna. O item 01, dadas as suas necessidade, importância e essencialidade, foi substituído por um serviço embutido no item 05.

Ademais, outro processo de contratação em estágio mais avançado (SEi 04600.000850/2024-85), como bônus, oferece serviços de *Endpoint Security* (proteção de computadores e equipamentos servidores), *Data Leak Prevention* (Prevenção a Perda de Dados), *Email Security* (Segurança de Caixas de Correio Eletrônico) que sombreariam os itens 06 (Serviço gerenciado de detecção e resposta para endpoints) e 07 (Serviço gerenciado de proteção de avançada de e-mail).

Os itens 03 (Serviço de monitoramento e visibilidade de ataques cibernéticos) e 05 (Serviço de monitoramento, detecção e resposta a incidentes) foram os únicos que permaneceram como objeto de contratação deste edital em função de necessidades de negócio, definição do corpo gestor e de sua capacidade de elevarem a maturidade de segurança da informação e segurança cibernética da Escola. Além disso, todo o estudo realizado neste processo será mantido e inventariado como fonte de consulta para futuras oportunidades tanto de aderência à *Cybersecurity Mesh Architecture* (CSMA) quanto para a implantaçao de um Sistema de Gestão de Segurança da Informação na ENAP.

Portanto, os os itens selecionados (03 e 05), para permanecerem como objeto de contratação, tornar-se-ão os itens 01 e 02, componentes, cada um, de grupo isolado, no Termo de Referência, conforme resumido na tabela abaixo:

Grupo 01							
ITEM	**ESPECIFICAÇÃO**	**CATSER**	**MÉTRICA OU UNIDADE DE MEDIDA**	**CÓD. PMC-TIC**	**QUANTIDADE**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	Serviço de monitoramento e visibilidade de	27359	Meses		12		

	ataques cibernéticos						
Grupo 02							
2	Serviço de **monitoramento, detecção e resposta a incidentes** - 1500 Eventos por segundo (EPS)	27359	Meses		12		

15. Justificativa econômica da escolha da solução

A escolha do objeto de serviços de segurança da informação integrada em ambiente em nuvem e de forma gerenciada pode ser fundamentada sob uma análise econômica e financeira alinhada à Instrução Normativa SGD/ME Nº 94/2022, que estabelece diretrizes para a contratação de serviços de TI no âmbito do Governo Federal, e preconiza a busca por soluções tecnológicas inovadoras e eficientes, promovendo a modernização da infraestrutura e a economia de recursos públicos.

A Contratação de Serviços Gerenciados de Segurança Cibernética por meio de pagamento fixo mensal vinculado ao atendimento de níveis mínimos de serviços, baseada na disponibilidade do parque computacional existente em conjunto com o SOC (*Security Operations Center* - SOC) 24x7x365 e equipe especializada de operação in loco ou remota fornecida pela CONTRATADA, permite à ENAP otimizar os recursos de infraestrutura, obter uma maior qualidade e sinergia no atendimento dos incidentes e chamados de segurança pelas equipes responsáveis.

Nesse modelo de contratação, não há necessidade de gastos adicionais com hardware e infraestrutura. Espera-se que com esta forma de contratação ocorra a redução da quantidade de problemas de segurança no parque computacional porque a uma única empresa será responsável por atender todos os serviços de segurança melhorando a qualidade no atendimento e diminuindo falhas de comunicação ao se contratar empresas diferentes para objeto de mesma natureza.

A contratação das soluções objetiva manter os serviços de TI sempre disponíveis para seus usuários da ENAP, prestando atendimento adequado e satisfatório, possibilitando o pleno desenvolvimento de suas atividades, bem como adequado monitoramento e suporte destinados ao ambiente tecnológico da ENAP, buscando prevenir e corrigir falhas para garantir a disponibilidade, confidencialidade e integridade das informações e da estrutura desse ambiente de proteção.

Destaca-se que a diminuição do volume de incidentes e problemas implica diretamente na redução do risco da CONTRATADA sofrer sanções administrativas, evitando-se assim a possibilidade da sua desqualificação durante a execução do contrato. Outra vantagem na adoção deste modelo é a previsibilidade de faturamento permitindo um melhor planejamento financeiro das partes, a simplificação da gestão e da fiscalização contratual e a melhoria contínua dos serviços prestados.

Quanto ao modelo de remuneração dos serviços, o art. 2º da Portaria SGD/ME Nº 6.432, de 15 de junho de 2021, estabelece que a contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação deverá ser realizada por meio de modelo de pagamento fixo mensal, vinculada exclusivamente ao atendimento de níveis mínimos de serviços previamente estabelecidos. Deste modo, o único modelo de remuneração possível a ser adotado é o de pagamento fixo mensal, vinculado ao atendimento de níveis mínimos de serviços.

Dessa forma, a adoção de serviços de segurança da informação em ambiente de nuvem e de forma gerenciada se alinha com a IN SGD/ME No 94/2022, cumprindo os requisitos de eficiência, economia e modernização estabelecidos pela normativa, e ainda contribui para a sustentabilidade financeira da ENAP ao otimizar investimentos e custos operacionais.

Cumpre informar que a contratação será realizada com a adoção do Sistema de Registro de Preços - SRP. Com isso, considerando a quantidade e tipos de itens que compõem a solução, a equipe técnica entende que haverá vantagens e benefícios econômicos, a exemplo da não variação dos preços, bem como as entregas parceladas.

16. Benefícios a serem alcançados com a contratação

A escolha das soluções baseou-se nos aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação e pelas recomendações dos órgãos de controle. No portal do software público, não foi possível encontrar solução capaz de proteger os ativos de segurança da Escola.

Conforme análises realizadas, a ENAP enfrenta um cenário de falta de servidores efetivos suficientes para a gestão da segurança da informação e operação da segurança cibernética e de ferramentas adicionais para a execução de tais atividades. Caso se optasse pela aquisição apenas das subscrições das soluções, a ENAP precisaria adquirir ferramentas sem a capacidade de operá-las como, por exemplo, software para Gestão de Vulnerabilidades, solução de simulação de ataques cibernéticos, solução de visibilidade de ataques cibernéticos, o Security Information and Event Management (SIEM) para a coleta e monitoramento de log de eventos identificando ameaças em tempo real, dentre outras.

Portanto, dentre os principais resultados a serem alcançados com esta contratação, destaca-se:
a) Aumento da maturidade em segurança da informação e o gerenciamento dos dados para aplicações em nuvem;
b) Ampliação da capacidade de descoberta e correção de vulnerabilidades de segurança;
c) Possibilidade de rápida correlação de eventos de segurança e resposta a incidentes;
d) Possibilidade a automatização de testes de segurança;
e) Implementação de técnicas que permitam a inibição de ataques às caixas de e-mail corporativos;
f) Incorporação de novas e eficientes tecnologias de segurança nas soluções de TI;
g) Auditoria e visibilidade dos dados corporativos;
h) Proteção contra ransomware;
i) Elevação da qualidade dos serviços e maturidade de segurança da informação;
j) Prevenção incipiente da perda de dados.
k) Apoio especializado na gestão da segurança da informação da Escola.

17. Providências a serem Adotadas

<ALTERAR>

No âmbito de espaço físico, não há a necessidade de adequação do ambiente da Escola para viabilizar a execução contratual no que se refere à equipe presencial responsável pela Sustentação de Operações e Resposta a Requisições de Segurança.

No âmbito tecnológico, as adequações, frente às soluções buscadas por esta contratação, são mínimas e pouco invasivas (instalação de agentes e configuração de apontamento de endereços de rede).

Portanto, faz-se necessária a elaboração do Plano de Implantação da solução compreendendo a instalação e configuração.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

A contratação de serviços gerenciados de segurança da informação e segurança cibernética para a criação/revisão de planos e políticas de segurança da informação, proteção de usuários e ativos de TI (caixas de correio eletrônico e endpoints), bem como a visibilidade e testes da superfície de ataques da Escola, com resolução contínua de vulnerabilidades e priorização e correlação dos eventos de segurança, além da gestão operacional de incidentes de segurança cibernética mostra-se viável e atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e os riscos administráveis.

Com base nas informações levantadas ao longo do estudo técnico preliminar, os integrantes requisitante e técnico, da equipe de planejamento, declaram que a contratação é viável, do ponto de vista técnico e econômico, sendo relevante e essencial para o desenvolvimento das atividades e trabalhos realizados pela Escola Nacional de Adminstração Pública.

O presente estudo técnico preliminar foi elaborado em harmonia com a Instrução IN SGD/ME no 94/2022 e Instrução Normativa SEGES/ME no 65/2021, da Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da aquisição/contratação.

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.

JULLYANO LINO DA SILVA

Integrante Técnico

Assinou eletronicamente em 24/04/2024 às 17:24:51.

RAFAELL DIAS LEITE FELIX

Integrante Requisitante

Assinou eletronicamente em 24/04/2024 às 17:12:55.

FRANK JAMES DA SILVA PIRES

Autoridade Máxima de TIC

Assinou eletronicamente em 24/04/2024 às 21:38:36.

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 - Caderno de Especificações Técnicas.pdf (239.02 KB)

Anexo I - Caderno de Especificações Técnicas.pdf

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

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

1.1. A solução de TIC consiste em um conjunto de soluções, divididas em três grupos, componentes de serviços gerenciados de segurança da informação e de segurança cibernética a fim de viabilizar o apoio à gestão de segurança da informação, de riscos cibernéticos e de conformidade baseados nas melhores práticas e frameworks do mercado no âmbito da Escola, bem como entregar serviços de monitoramento e de visibilidade de ataques cibernéticos, além do monitoramento, detecção e tratamento de incidentes de segurança cibernética concernentes aos ativos de Tecnologia da Informação da ENAP.

1.2. A prestação de serviço do Grupo 01 envolve:

1.2.1. **ITEM 01: Serviço de Monitoramento e Visibilidade de Ataques Cibernéticos** que tem como finalidade aplicar inteligência voltada para a segurança da marca ENAP, com o objetivo de realizar buscas contínuas em diversas camadas da internet, incluindo a Surface, Deep e Dark Web. Essas buscas têm como foco a identificação de informações sensíveis que possam estar sendo discutidas ou comercializadas de forma ilegal, tais como dados confidenciais, informações privilegiadas ou quaisquer outros tipos de conteúdo que possam representar uma ameaça à integridade da ENAP.

1.3. A prestação de serviço do Grupo 02 envolve:

1.3.1. **ITEM 02: Serviço de Monitoramento, Detecção e Resposta a Incidentes que** tem como objetivo prover à ENAP mecanismo de visibilidade de logs, rede e informações, capaz de identificar eventos maliciosos, através de correlacionamento de logs e tráfego de rede sob um regime de monitoramento de 1500 eventos por segundo, que possam comprometer os serviços tecnológicos da ENAP.

1.4. **DOS SERVIÇOS ESTRATÉGICOS GERENCIADOS DE SEGURANÇA DO GRUPO 01**

1.4.1. **ITEM 01** – SERVIÇOS MONITORAMENTO E VISIBILIDADE DE ATAQUES CIBERNÉTICOS

1.4.1.1.1. A CONTRATADA deve realizar o monitoramento contínuo de fontes externas

nacionais e internacionais, como Fóruns, Redes Sociais, Mídias Sociais, Nuvens Públicas e Grupos Hackers para identificação de motivações, intenções e atividades de possíveis adversários que possam causar impactos à CONTRATANTE, seja na INTERNET profunda, escura ou de superfície.

1.4.1.1.2. Os Serviços de Proteção de Riscos Digitais, doravante SPRD, devem suportar quatro grandes pilares: mapeamento, monitoramento, operação e mitigação contemplando plenamente as disciplinas de Threat Intelligence & Hunting, conforme as boas práticas, frameworks e literatura atualizada.

1.4.1.1.3. Mapeamento, tem por objetivo coletar, identificar e entender os ativos digitais sob risco.

1.4.1.1.4. Monitoramento, visa o monitoramento contínuo e ininterrupto dos ativos digitais, com o objetivo de documentar, contextualizar, enriquecer e priorizar os riscos e alertas com capacidade de reportar detalhes de incidentes permitindo a tomada de decisão inteligente em relação a tais riscos.

1.4.1.1.5. Curadoria, visa ter um time especializado para acompanhar e validar os resultados do monitoramento em agendas recorrentes com o cliente para garantir a melhoria contínua dos resultados, captura melhor do contexto do cliente, eliminando falsos alertas, contribuindo no ajuste de novos contextos de buscas e sugerindo novos ativos para potencializar o monitoramento.

1.4.1.1.6. Mitigação, visa a reduzir o risco dos ativos digitais, através de:

1.4.1.1.6.1. Envio de alerta aos clientes via E-mail, Webhook, SMS, Ocorrências/Tickets e WhatsApp.

1.4.1.1.6.2. Envio de relatórios (executivo e técnico), pelo menos 1 vez por mês.

1.4.1.1.6.3. Procedimentos de remoção de conteúdo infrator.

1.4.1.1.6.4. Boletins periódicos de inteligência, contemplando

1.4.1.1.6.4.1. Envio de boletim quinzenal contendo os seguintes assuntos:

1.4.1.1.6.4.1.1. Análises de Malwares e Ransomwares com IOCs;

1.4.1.1.6.4.1.2. Vulnerabilidades descobertas, vulnerabilidades corrigidas e zero-days em ativos e serviços que possam afetar a infraestrutura e/ou funcionamento de empresas;

1.4.1.1.6.4.1.3. Perfil de atores e grupos maliciosos;

1.4.1.1.6.4.1.4. Grandes empresas do setor que possam ter sofrido algum tipo de ataque cibernético.

1.4.1.1.6.4.2. Deverão ser enviados boletins de inteligência ou relatórios de incidentes, disponibilizados nos seguintes idiomas: Português.

1.4.1.1.7. Todos os serviços descritos pertencem a um único objeto e bloco de contratação denominado **SPRD**. Todas as características e requisitos exigidos neste documento serão confirmadas em diligência presencial.

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

1.4.1.1.9. Canais de Suporte

1.4.1.1.10. Para abertura de solicitações a CONTRATADA deverá possuir formulário dentro da própria plataforma de SPRD.

1.4.1.1.11. O sistema deverá permitir minimamente a filtragem de chamados de suporte através de status, tipo de chamado e prioridade.

1.4.1.1.12. Deve permitir ordenar a listagem de chamados por prioridade, status, data (a partir do mais antigo e a partir do mais recente) e por solicitante.

1.4.1.1.13. O sistema deverá apresentar o histórico dos chamados de suporte permitindo visualizar informações relevantes de sua abertura, tais como status, solicitante, data de abertura, data de cada interação com o chamado e conteúdo das interações.

1.4.1.1.14. O sistema deve permitir a reabertura de chamados que tenham sido fechados, retornando estes ao status de aberto, reiniciando o atendimento.

1.4.1.1.15. O sistema da CONTRATADA deverá permitir o acompanhamento de chamados dentro da console do produto, ao invés de apenas solicitações por e-mail. Deve permitir à CONTRATANTE realizar o acompanhamento dos chamados, tal como a adição de comentários, anexos de arquivos e mudança de status diretamente pela console do produto.

1.4.1.1.16. Horário de Atendimento: os serviços devem obrigatoriamente ser executados, ofertados, e estarem acessíveis ao CONTRATANTE em regime de 24 (vinte quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante todo o período de vigência do contrato.

1.4.1.1.17. Mapeamento de Ativos:

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

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

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

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

1.4.1.1.21.1. Domínios: Nome que serve para localizar e identificar conjuntos de computadores na internet. O nome de domínio foi concebido com o objetivo de facilitar a memorização dos endereços de computadores na Internet.

1.4.1.1.21.2. Marcas: A marca registrada, nome fantasia, nome do produto, nome de fachada, razão social, termo ou expressão que identifique o CONTRATANTE.

1.4.1.1.21.3. BIN (*Bank Identification Number*): Números do cartão de crédito para identificar o banco emissor e a conta do cliente. Os primeiros seis dígitos, liderados pelo primeiro dígito que identifica a bandeira do cartão, são coletivamente conhecidos como o número de identificação do emissor e denominados números de identificação bancária.

1.4.1.1.21.4. Endereço IP: Endereço de Protocolo da Internet, do inglês Internet Protocol address, é um rótulo numérico atribuído a cada dispositivo conectado a uma rede de computadores que utiliza o Protocolo de Internet para comunicação.

1.4.1.1.21.5. Pessoa: Informação de identificação

pessoal de empregado ou pessoa de interesse para monitoramento de riscos digitais dirigidos à pessoa física.

1.4.1.1.21.6. APK: Monitora a disponibilidade de aplicativos a partir do package name.

1.4.1.1.22. O SRPD deve:

1.4.1.1.22.1. Permitir que o ativo em monitoramento seja apenas desabilitado, para que pare de gerar alertas sem precisar ser excluído da console.

1.4.1.1.22.2. Apresentar em sua tela de gestão de ativos a lista completa de ativos cadastrados, estejam eles habilitados ou desabilitados, contendo o tipo de ativo, o nome do ativo e a quantidade de eventos que este ativo já recebeu.

1.4.1.1.22.3. Permitir visualizar em formato resumido a distribuição das quantidades de ativos por severidade, tipo e status.

1.4.1.1.23. Monitoramento

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

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

1.4.1.1.26. As informações devem ser apresentadas à

CONTRATANTE no formato de evento, contextualizado com o tipo de risco associado de maneira automática, permitindo que a CONTRATANTE parametrize consultas, queries, alertas ou qualquer tipo de ação relacionada de forma deliberada de acordo com cenários desejados. Esta cláusula não dispensa a CONTRATADA de realizar customizações da plataforma para monitoramento, gestão, geração de alertas, e configurações adicionais que não possam ser realizadas pela CONTRATANTE.

1.4.1.1.27. A solução deve permitir a realização ilimitadas de buscas nos dados coletados das diversas fontes previstas na plataforma, incluindo buscas avançadas com critérios e entidades diferentes;

1.4.1.1.28. A plataforma deverá fornecer coleta de informações em, no mínimo, 90 (noventa) grupos de Ransomware.

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

1.4.1.1.29.1. Menção ao cliente, Linguagem Ofensiva, Fraude Cibernética, Exposição de Credenciais, Personificação a um perfil de mídia social, Exposição de chaves, Phishing.

1.4.1.1.29.2. Correlacionar as informações coletadas, utilizando plataforma de big data para processamento visando normalizar informações, gerando listas acionáveis de inteligência contra ameaças.

1.4.1.1.29.3. A plataforma deve por exemplo ter a capacidade de ao encontrar um dump de senhas que cite credenciais da CONTRATANTE, apresentar evidência referente apenas a CONTRATANTE ao invés

de apresentar o dump completo para que a CONTRATANTE pesquise manualmente.

1.4.1.1.29.4. Ao verificar por exemplo uma conversa de grupo ou fórum de fraudes menciona a CONTRATANTE, a CONTRATADA deve apresentar somente as mensagens do contexto de risco à CONTRATANTE e não a conversa completa contendo itens que não são relevantes para a CONTRATANTE.

1.4.1.1.29.5. A plataforma deve ter capacidade de ao ler as informações da Internet que poderão se transformar em um evento, reconhecer no mínimo o que é um(a) CPF, URL, e-mail, comandos normalmente associados a bancos de dados, convite de um chat de mensageria eletrônica, secret key da AWS, API Client ID e Client Secret do Facebook, Google CloudAPI e OAuth key, chave privada, Souce Token, Sendgrid API Key, SonarQube API Key, Twitter client ID, arquivo de configuração do WordPress, menção de Checker com URL, Contas Laras, Currículo Vitae, IPv4, Bin de cartão de crédito.

1.4.1.1.30. Deverá fornecer coleta de informações para realização de pesquisas em redes sociais e aplicativos, para, no mínimo: Twitter, Facebook, Youtube, Instagram, TikTok, LinkedIn, WhatsApp, Discord, Telegram, Pastebin, Scribd, Apple Store, 4Shared, Google Play, Vimeo, Github, OLX e Mercado Livre.

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

1.4.1.1.32. Deve ter capacidade para análise de áudio de no mínimo 1 plataforma de mensageria para caso identifique correspondência com os critérios pesquisados, fazer a transcrição de áudio em questão e transformá-lo em evento indicando no mesmo a transcrição do áudio em questão.

1.4.1.1.33. Na transcrição dos áudios analisados nos vídeos, deverá ser possível destacar informações relevantes de acordo com os ativos digitais definidos pelo CONTRATANTE.

1.4.1.1.34. O áudio (completo), bem como seus metadados, onde foi encontrado algum resultado, deve ser capturado, identificado e disponibilizado para análise.

1.4.1.1.35. Realizar análise de conteúdo de imagens (OCR) permitindo que um screenshot contendo uma ameaça a algum dos ativos digitais da CONTRATANTE seja detectada e notificada.

1.4.1.1.36. Por exemplo, uma captura de tela de uma credencial do acesso da CONTRATANTE.

1.4.1.1.37. Todos os incidentes reportados devem conter informações de log sendo possível determinar:

1.4.1.1.38. O ativo digital ao qual aquele determinado incidente se refere;

1.4.1.1.39. A data e hora em que houve a coleta da informação;

1.4.1.1.40. A data e hora em que a informação foi analisada;

1.4.1.1.41. A data e hora em que a informação se transformou em um risco exibido na console do CONTRATANTE.

1.4.1.1.42. A prioridade do risco determinada pelo SPRD.

1.4.1.1.43. O tipo do incidente e a sua origem.

1.4.1.1.44. O SPRD deve disponibilizar as informações das pesquisas por, no mínimo: intervalo de data, status, severidade, categoria, contexto, metadados e tipo da fonte.

1.4.1.1.45. Para as quantidades de ativos digitais presentes neste documento, não poderá haver limitação da quantidade de alertas gerados pelo

serviço da CONTRATADA.

1.4.1.1.46. As ocorrências devem possuir um campo de descrição em que os analistas possam contextualizar as informações associadas.

1.4.1.1.47. Diretamente a partir de um incidente aberto pela ferramenta deve ser possível solicitar o serviço de remoção de conteúdo infrator (takedown) caso o cliente tenha contratado essa opção.

1.4.1.1.48. O serviço deverá realizar a detecção de domínios registrados que possam oferecer riscos de serem utilizados de forma maliciosa, através do registro de domínios com variações comuns de nome, permutações de caracteres e outros (typosquatting, nomes de domínios similares).

1.4.1.1.49. Deve possibilitar a descoberta de páginas de phishing ativas utilizando o nome, a marca e a identidade visual da CONTRATADA

1.4.1.1.50. O serviço deverá realizar a detecção de domínios registrados que possam oferecer riscos de serem utilizados de forma maliciosa, através do registro de domínios com variações comuns de nome, permutações de caracteres e outros (typosquatting, nomes de domínios similares).

1.4.1.1.51. Deve possibilitar a descoberta de páginas de phishing ativas utilizando o nome, a marca e a identidade visual da CONTRATADA.

1.4.1.1.52. Deve possibilitar a descoberta de páginas de phishing ativamente, a partir da detecção de clones das aplicações da CONTRATANTE, independentemente de onde estes estejam sendo executados.

1.4.1.1.53. Deve possuir pelo menos 200 regras pré-definidas para detecção e coleta de eventos de segurança.

1.4.1.1.54. Permitir a criação e acompanhamento de Incidentes de Segurança, de forma manual ou automática.

1.4.1.1.55. Possuir a capacidade de criação de interpretadores (coletores) para aplicações proprietárias e/ou não conhecidas, de forma que:

1.4.1.1.55.1. A Criação seja feita de forma intuitiva e deverá ser realizada dentro da própria ferramenta, via interface web, possibilitando configuração não só pela CONTRATADA como pela própria CONTRATANTE;

1.4.1.1.55.2. Não seja limitada a 1 coletor por fonte de pesquisa;

1.4.1.1.55.3. Permitir a aplicação de filtros nos coletores para direcionamento das informações a serem indexadas e monitoradas;

1.4.1.1.55.4. Deve possuir opção para configuração de periodicidade da coleta;

1.4.1.1.56. Deve possuir foco no sistema financeiro brasileiro com fontes relevantes relacionadas a grupos de fraudadores.

1.4.1.1.57. Deve permitir a inclusão e o monitoramento de novos grupos dos aplicativos de mensageria, incluindo grupos que eventualmente sejam solicitados pela CONTRATANTE.

1.4.1.1.58. Extrair, no mínimo, os seguintes metadados de cada mensagem: autor, aplicativo de origem e data e hora, com precisão de segundos, dos momentos de envio e coleta.

1.4.1.1.59. Monitorar redes de compartilhamento de textos e a plataforma de compartilhamento de códigos.

1.4.1.1.60. O serviço não deverá possuir limitação na capacidade de análise de ativos digitais.

1.4.1.1.61. O módulo de monitoramento deve permitir o uso de regras YARA ou equivalente, inclusive, permitindo o cadastro de regras por solicitação da CONTRATANTE.

1.4.1.1.62. Para eventos do tipo Informação, não é requerido qualquer tipo de ação, podendo estes serem apenas mantidos temporariamente na solução para posteriormente serem descartados.

1.4.1.1.63. Deve existir a garantia por parte da CONTRATADA, que uma interface humana, ou seja, uma analista que pertence ao grupo de monitoramento de ataques, esteja validando e impedindo o envio de falsos positivos para a CONTRATANTE.

1.4.1.1.64. Deve oferecer canais de comunicação integrados para funcionários do CONTRATANTE, requisitarem e receberem devolutivas de incidentes detectados pela solução.

1.4.1.1.65. Deve possuir módulo de visualização de eventos, seus tipos e suas respectivas severidades, através de dashboard. Onde possa ser possível filtrar minimamente por período e realizar o download do mesmo em formato PDF, DOCX e HTML.

1.4.1.1.66. Nos detalhes de todos os eventos apresentados pela solução de SPRD, deve ser possível verificar no mínimo o horário em que o evento foi coletado, o horário em que o evento foi enriquecido e/ou processado, o horário em que o evento foi preparado para análise seja ela manual ou automática, e o horário em que o evento foi disponibilizado na console do produto para consumo da CONTRATANTE.

1.4.1.1.67. A configuração de alertas deve permitir a criação de notificações granulares a partir dos eventos da plataforma. Entre os critérios que devem estar disponíveis para configuração de alertas estão:

a) Categoria do Evento;

b) Tipo do Evento;

c) Severidade;

d) Filtro de Palavra-Chave.

1.4.1.1.68. Mitigação

1.4.1.1.69. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de sites maliciosos, sites que contenham phishing ou sites/domínios que disparem phishing que utilizem o nome, a marca ou a imagem, mesmo que similar (com intuito de confundir), os clientes da CONTRATADA.

1.4.1.1.70. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de perfis falsos de funcionários (Executivos) e da própria empresa em redes sociais;

1.4.1.1.71. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer tipos de informação disponíveis e acessíveis que violem os direitos de uso do CLIENTE ou que permitam burlar os meios de proteção desses direitos;

1.4.1.1.72. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer tipos de informação disponíveis e acessíveis quando for identificada a tentativa de ataque à reputação da instituição ou ainda a tentativa de captura de credenciais do CLIENTE.

1.4.1.1.73. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer informações em redes sociais (Facebook, Twittter, Linkedin, Instagram, YouTube etc. que tenham relação com o CLIENTE e não seja autorizado por essa instituição.

1.4.1.1.74. Possibilitar a realização do serviço de TAKEDOWN para retirar das principais lojas de aplicativos para mobile (Google Play Store, Apple Store, etc.) os aplicativos falsos e maliciosos distribuídos fora das lojas oficiais comumente conhecidas.

1.4.1.1.75. Possibilitar a realização do serviço de TAKEDOWN para retirar conteúdo com documentos, informações confidenciais, informações de cartões de crédito, divulgações

relacionadas a produtos e sistemas do CLIENTE, divulgações relacionadas a clientes e empregados do CLIENTE, além do monitoramento de sites de compartilhamento de arquivos e informações, sites de compartilhamento de textos (Pastebin, Ghostbin, entre outros) presentes na internet superficial.

1.4.1.1.76. A CONTRATADA deverá emitir um alerta, atualizado conforme andamento, para acompanhamento do processo de TAKEDOWN de cada ocorrência.

1.4.1.1.77. A CONTRATADA deverá disponibilizar um painel para consulta e análise de ocorrências (em andamento e finalizadas) do serviço de TAKEDOWN. Deve permitir consultas por intervalo de tempo, tipos de ocorrências e demais critérios relevantes na análise das ocorrências.

1.4.1.1.78. O serviço de TAKEDOWN deverá estar disponível em pacotes mensais.

1.4.1.1.79. Todo serviço de TAKEDOWN deve ser acompanhado de um especialista, a fim de garantir a assertividade de todo o processo.

1.4.1.1.80. Características Gerais e Confidencialidade:

1.4.1.1.81. A CONTRATADA deverá manter total sigilo e confidencialidade dos serviços prestados ao CONTRATANTE no que se refere a não divulgação, por qualquer forma, de toda ou parte das informações ou documentos a ele relativos, e aos quais venha a ter acesso, em decorrência da prestação dos serviços executados.

1.4.1.1.82. Eventualmente o CONTRATANTE poderá solicitar uma reunião técnica, a ser realizada remotamente, para que um atendimento qualquer possa ser realizado e/ou acompanhado por um analista, quando a gravidade de um incidente reportado pelo SPRD for classificada como crítica.

1.4.1.1.83. A plataforma disponibilizada pela CONTRATADA deve oferecer conexão segura através do protocolo HTTPS.

1.4.1.1.84. O acesso ao SPRD deve possuir métodos de autenticação de múltiplos fatores.

1.4.1.1.85. A solução deverá:

1.4.1.1.86. Ser obrigatoriamente de propriedade da CONTRATADA, não poderá ser do tipo open source (software livre), OU

1.4.1.1.87. A CONTRATADA deverá ser representante formal do fabricante no Brasil.

1.4.1.1.88. Deverá ser obrigatoriamente de propriedade da CONTRATADA ou licenciado para uso pela CONTRATADA, não poderá ser do tipo open source (software livre).

1.4.1.1.89. O serviço deverá ser prestado por meio de solução fornecida através da nuvem do fabricante. Nenhum componente da solução poderá ser hospedado ou estar sob responsabilidade da CONTRATANTE.

1.4.1.1.90. O fabricante deverá possuir equipe de suporte em português.

1.4.1.1.91. Deve permitir a possibilidade de mudança de idioma do sistema para outras linguagens, tais como Inglês e Espanhol.

1.4.1.1.92. Deve permitir extração de relatórios completos dos eventos em, no mínimo, formatos PDF, CSV e JSON.

1.4.1.1.93. Entre os relatórios disponíveis deverá ser possível exportar em um único documento em formato JSON ou CSV, listagem de todas as credenciais expostas da CONTRATANTE contendo no mínimo o ID do evento gerado para aquela credencial, o nome do usuário e a respectiva senha vazada sem anonimização da mesma, a URL e a data e hora do vazamento ou caso não seja possível determinar a data hora do vazamento, informar a data e hora da disponibilização da informação na Internet.

1.4.1.1.94. A solução deverá permitir que um usuário

administrador gerencie os acessos dos demais usuários da CONTRATANTE na solução.

1.4.1.1.95. A solução deverá permitir o uso de múltiplos fatores de autenticação, por, pelo menos, e-mail e mais uma das seguintes opções: SMS ou aplicativo de token ou whatsapp.

1.4.1.1.96. A solução deverá permitir quantidade ilimitada de usuários com acesso à plataforma.

1.4.1.1.97. A solução deve manter todos os dados e informações da CONTRATANTE, não coletados diretamente de fontes abertas, em território nacional sendo expressamente proibido que estes sejam processados no exterior.

1.4.1.1.98. Papéis e Responsabilidades

1.4.1.1.99. Deverá ser empregada na prestação de serviço deste contrato, os seguintes papéis e responsabilidades dos profissionais:

1.4.1.1.100. Patrocinador do Projeto (CONTRATANTE): é o gerente da Unidade de Tecnologia da Informação, responsável por representar os interesses do CONTRATANTE no contexto da presente contratação, pela aprovação da necessidade, dos objetivos e, por fim, pela negociação das ações necessárias para a melhoria contínua dos serviços.

1.4.1.1.101. Gestor do Contrato (CONTRATANTE): é o funcionário formalmente designado pelo CONTRATANTE, responsável pelo monitoramento da prestação do serviço ao longo do período de vigência do contrato e pela participação no planejamento da contratação, pela verificação dos resultados pretendidos. É o responsável pelo fornecimento das informações necessárias para a ativação do contrato.

1.4.1.1.102. Preposto (CONTRATADA): é o profissional indicado pelo Fornecedor de Serviço para representá-la administrativa e tecnicamente. É o responsável pela coordenação operacional das atividades previstas de forma a solucionar qualquer

dúvida, conflito ou desvio técnico que possa comprometer a execução do contrato. Deverá ter bons conhecimentos em segurança da informação e também é responsável pela interlocução com o Gestor do Contrato do CONTRATANTE.

1.4.1.1.103. As qualificações técnicas exigidas para o perfil de PREPOSTO da CONTRATADA:

Certificações	Descrição
Ao menos uma das certificações de segurança da informação: CISSP (Certified Information Systems Security Professional); CISM (Certified Information Security Manager; CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials); GCIH (GIAC Incident Handler) GMON (GIAC Continuous Monitoring);	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência mínima de 5 (cinco) anos em coordenação e gestão de contratos de serviços continuados.

1.5. **DOS SERVIÇOS OPERACIONAIS GERENCIADOS DE SEGURANÇA DO GRUPO 02**

1.5.1. **ITEM 02** – SERVIÇO DE MONITORAMENTO, DETECÇÃO E RESPOSTA A INCIDENTES

1.5.1.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados à ENAP, através de fornecimento de serviços com capacidade de correlacionamento de eventos, para detecção de ameaças direcionadas a CONTRATADA para detecção de comportamento anômalo de serviços, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de

gestão de eventos.

1.5.1.2. APOIO À GESTÃO DA SEGURANÇA DA INFORMAÇÃO

1.5.1.2.1. Perfil do Profissional:

1.5.1.2.1.1. A CONTRATADA deverá disponibilizar, pelo menos, um profissional sênior com as seguintes qualificações:

a)Certificação (ISC)² CISSP ou ISACA CISM;

b) Experiência mínima de 5 anos em gestão da segurança da informação;

c) Conhecimento comprovado de normas e boas práticas de segurança (ISO 27001, ISO 27002, ISO 27005, NIST Cybersecurity Framework, CIS Controls);

d) Habilidades de comunicação, liderança e relacionamento interpessoal.

1.5.1.2.2. Atividades Esperadas:

1.5.1.2.2.1. Apoio à ENAP na jornada de implantação de um SGSI (Sistema de Gestão de Segurança da Informação) que envolvam:

a) Elaborar um cronograma de implementação do SGSI, alinhado com a ISO/IEC 27001.

b) Definir os escopos do SGSI e identificar os ativos de informação críticos.

c) Realizar análise de riscos de segurança da informação e definir tratamento de riscos.

d) Auxiliar na seleção e implementação de controles de segurança da informação, de acordo com a ISO/IEC 27002.

e) Elaborar documentação do SGSI, incluindo políticas, procedimentos e registros.

f) Preparar a ENAP para a certificação ISO/IEC 27001, se aplicável.

1.5.1.2.2.2. Apoio à ENAP nas atividades de criação/revisão de documentos de segurança da informação que envolvam:

a) Elaborar/revisar o Plano de Gestão de Riscos de Segurança da Informação, alinhado com a ISO/IEC 27005.

b) Elaborar/revisar a Política de

Segurança da Informação.

c) Elaborar/revisar o Plano de Gestão de Incidentes Cibernéticos.

d) Elaborar/revisar o Programa de Privacidade de Dados, alinhado com a LGPD.

1.5.1.2.2.3. Assessoria em Projetos de Segurança da Informação da ENAP que envolvam:

a) Participar de projetos de segurança da informação e privacidade de dados.

b) Fornecer análises de risco e recomendações de segurança.

c) Revisar a arquitetura e o design de soluções de segurança.

d) Acompanhar a implementação de projetos de segurança.

1.5.1.2.2.4. Apoio em atividades de Treinamento e Conscientização aos usuários da ENAP que envolvam:

a) Elaborar e ministrar treinamentos de segurança da informação para os colaboradores da ENAP.

b) Desenvolver campanhas de conscientização sobre segurança da informação.

c) Avaliar a eficácia dos programas de treinamento e conscientização.

1.5.1.2.2.5. Apoio executivo no Monitoramento de Ameaças que envolvam:

a) Acompanhar as tendências e ameaças de segurança cibernética.

b) Avaliar o impacto potencial das ameaças na ENAP.

c) Propor e implementar ações de mitigação de riscos.

1.5.1.2.2.6. Geração de Relatórios de Postura de Segurança que envolvam:

a) Elaborar relatórios periódicos sobre a postura de segurança da informação da ENAP.

b) Avaliar a maturidade do SGSI e identificar oportunidades de melhoria.

c) Apresentar os relatórios à gestão da ENAP e discutir as ações recomendadas.

1.5.1.2.3. Carga Horária e Disponibilidade:

1.5.1.2.3.1. O serviço será prestado, em formato híbrido (presencial e remoto), de forma

contínua ao longo da vigência do contrato conforme necessidade da ENAP com uma carga horária de 08 horas semanais.

1.5.1.3. GAP ANALYSE

1.5.1.4. A CONTRATADA deverá realizar nos primeiros meses após o início do contrato, a Análise de Superfície (Assessment) baseada em MITRE ATT&CK® no ambiente tecnológico da ENAP para reduzir o risco iminente de incidentes de segurança

1.5.1.5. O assessment de MITRE ATT&CK® identifica as técnicas que os adversários podem usar durante um ataque, bem como conceitos e informações básicas sobre grupos de adversários, para avaliar a postura de segurança dos negócios e dos fornecedores de segurança, nesse processo deverão ser checadas a principais Táticas de ataque, técnicas e subtécnicas;

1.5.1.6. Os entregáveis dessa etapa são:

1.5.1.7. Relatório de GAPs;

1.5.1.8. Infográfico de Maturidade;

1.5.1.9. Artefatos de Avaliação;

1.5.1.10. Avaliação das Técnicas e Sub Técnicas;

1.5.1.11. Matriz de Priorização;

1.5.1.12. Este serviços está condicionado ao PLANO DE GESTÃO DE INCIDENTES CIBERNÉTICOS a ser criado durante a execução do serviço definido na subseção APOIO À GESTÃO DA SEGURANÇA DA INFORMAÇÃO deste item ou em posteriores alterações devidamente aprovadas pela ENAP

1.5.1.13. Para execução deste serviço, a CONTRATADA deverá utilizar e ser capaz de fornecer, operar, sustentar e suportar soluções de monitoramento que atendam o descritivo

técnico a seguir.

1.5.1.14. REQUISITOS GERAIS

1.5.1.15. O serviço técnico especializado inclui no mínimo as seguintes atividades:

1.5.1.16. A CONTRATADA será responsável pela implementação, suporte, administração diária e sustentação de todos os serviços envolvidos neste certame, contemplando qualquer envolvimento em qualquer demanda que tenha relação com as soluções envolvidas.

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

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

1.5.1.19. Entende-se por administração diária, que a CONTRATADA será responsável pela administração de todos os passos técnicos e processos que envolvem os serviços contratados, de forma que as mesmas sejam 100% integradas ao ambiente da CONTRATANTE, porém utilizando a mão de obra da CONTRATADA.

1.5.1.20. Entende-se por sustentação, que a CONTRATADA será responsável pela tratativa de todas as saídas técnicas que envolvem os serviços contratados, sendo responsáveis pela implementação de cada processo, integração ou interação técnica de qualquer natureza envolvendo os serviços contratados.

1.5.1.21. Fica fora do escopo da CONTRATADA,

apenas atividades que envolvam interação com as ferramentas de rede e infraestrutura da CONTRATANTE, porém a CONTRATADA ainda fica responsável pela indicação de todas as necessidades de atuação para que os times responsáveis possam desenvolver suas tarefas e atender a novas demandas técnicas elencados pelos serviços contratados

1.5.1.22. A CONTRATADA deverá seguir o processo de mudança estabelecido pelo CONTRATANTE

1.5.1.23. A CONTRATADA deverá implementar conceitos de Threat Hunting, monitorando de forma contínua todos eventos correlacionados.

1.5.1.24. As manutenções preventivas e/ou corretivas, que representem risco de interrupção do(s) serviço(s), deverão ser agendadas e realizadas fora do horário regular, salvo quando expressamente autorizado.

1.5.1.25. As manutenções programadas, que impliquem em extensiva parada do ambiente, serão realizadas durante um final de semana. Tais atividades realizadas fora do horário regular não ensejarão qualquer pagamento adicional em relação ao estabelecido no contrato, portanto a CONTRATADA deverá prever esta situação em sua composição de custos.

1.5.1.26. Todos os serviços de manutenção corretiva e preventiva são considerados de natureza contínua e deverão minimizar a necessidade de parada do ambiente em produção

1.5.1.27. A contrata deverá de forma proativa, analisar políticas e processos de segurança da CONTRATANTE e realizar sugestões de melhoria a serem implementadas em conjunto com todas as equipes envolvidas.

1.5.1.28. Os serviços deverão ser executados por

profissionais habilitados, com base em programas de formação e/ ou certificações oficiais dos serviços envolvidos neste Certame

1.5.1.29. A CONTRATADA deverá elaborar e manter atualizados os Planos de Capacidade, de Gerenciamento de Incidentes, de Disponibilidade, de Continuidade e de Recuperação de Desastres para os serviços objeto deste Termo.

1.5.1.30. Os serviços devem ser executados de acordo com normas, procedimentos e técnicas adotadas pela CONTRATANTE.

1.5.1.31. Deverá ser fornecido ao CONTRATANTE acesso à console dos serviços fornecidos para que seja possível o acompanhamento, auditoria e direcionamento de ações no ambiente

1.5.1.32. A CONTRATADA deverá comunicar a CONTRATANTE quanto à ocorrência de qualquer incidente de segurança, seguido de todas as ações de remediação realizadas.

1.5.1.33. Os contatos para notificação de incidentes críticos ou fluxos para aprovação de ações serão documentadas durante o período de implementação.

1.5.1.34. A CONTRATADA deverá assumir atividades de customização de interpretação de logs/eventos que possam não ser interpretados nativamente pelo SIEM. Tais atividades não deverão ter nenhum custo adicional.

1.5.1.35. A CONTRATADA deverá customizar e disponibilizar dashboards/relatórios solicitados pela CONTRATANTE. Essas visões serão armazenadas na console do SIEM e poderão ser consultadas a qualquer momento. Tais atividades não deverão ter nenhum custo adicional e serão realizadas dentro do horário comercial.

1.5.1.36. Sempre que necessário, a CONTRATADA deverá customizar regras de detecção no SIEM, atendendo boas práticas de segurança da informação e também a demandas específicas da CONTRATANTE.

1.5.1.37. Qualquer atividade realizada fora do horário comercial não deverá atribuir nenhum custo adicional para a CONTRATANTE.7.2.26. Qualquer atualização de plataformas envolvidas na contratação não deverá ter nenhum custo adicional para a CONTRATANTE.

1.5.1.38. A CONTRATADA deverá realizar ações referentes a resposta a incidentes de segurança, envolvendo sempre que necessário responsáveis por soluções administradas por time terceiros, com o objetivo de manter a disponibilidade e qualidade de todos os serviços tecnológicos.

1.5.1.39. Sempre que necessário envolvimento de times terceiros que administram outras soluções da CONTRATANTE, a CONTRATADA deverá enviar os incidentes preenchidos, analisados e contextualizados, apenas para tomada de decisão e/ou execução de ações pontuais.

1.5.1.40. Toda interação com times terceiros deverão ser realizadas por e-mail ou através da ferramenta de chamados da CONTRATANTE, ficando a cargo da CONTRATANTE definir qual meio será adotado.

1.5.1.41. A CONTRATADA deverá ter fluxos de resposta a incidentes bem definidos para os mais variados tipos de incidentes existentes.

1.5.1.42. A CONTRATADA deverá criar relatórios gerenciais a serem apresentados e entregues para a CONTRATANTE mensalmente, em dia a ser definido no período de implementação. Os dados deste relatório poderão ser customizados

a pedido da CONTRATANTE, de modo a atender necessidades específicas de negócio. Adicionalmente, os relatórios devem conter índices de resposta a incidentes, indicadores e efetividade de todos os serviços contratados.

1.5.1.43. Todas as ações de resposta a incidentes executadas pela CONTRATADA deverão ser armazenadas em procedimentos operacionais, para consultas sempre que necessário.

1.5.1.44. A contratada deverá detectar e reportar qualquer tipo de incidente que tenha características de reincidência.

1.5.1.45. Serão considerados incidentes de segurança, minimamente, as seguintes ações:

1.5.1.45.1. Aplicações maliciosas detectadas em estações de trabalho e servidores;

1.5.1.45.2. Exploração de vulnerabilidades;

1.5.1.45.3. Uso indevido de credenciais;

1.5.1.45.4. Phishing ou spam;

1.5.1.45.5. Ataques de Força Bruta;

1.5.1.45.6. Execução de códigos ou scripts maliciosos;

1.5.1.45.7. Ataques de saturação;

1.5.1.45.8. Comunicações com IPs ou domínios maliciosos;

1.5.1.45.9. Atividades que tenham o intuito de comprometer a integridade de ativos e entidades da CONTRATANTE;

1.5.1.45.10. Atividades que tenham o intuito de comprometer a confidencialidade de informações da CONTRATANTE;

1.5.1.45.11. Atividades que tenham o intuito de comprometer a disponibilidade dos serviços tecnológicos oferecidos pela CONTRATANTE.

1.5.1.46. A CONTRATADA deverá disponibilizar

um canal, por e-mail, possibilitando que a CONTRATANTE comunique qualquer incidente de segurança não detectado por soluções de segurança existentes, para que as devidas investigações sejam realizadas.

1.5.1.47. A CONTRATADA deverá operar todas as plataformas contidas nesta contratação, de forma a realizar todas as atividades pertinentes às mesmas (Exceto ações de infraestrutura específicas administradas pela CONTRATANTE), seguindo melhores práticas recomendadas pelos fabricantes e potencializando ao máximo a capacidade de entrega de cada plataforma.

1.5.1.48. A CONTRATADA deverá entregar um relatório de implementação das soluções (as-built) contidas neste certame, contendo todos os passos realizados para implementação e configuração das soluções.

1.5.1.49. Para o faturamento mensal dos itens, a contratada deverá emitir e apresentar o “Relatório Mensal de Acompanhamento do Contrato”, que deverá conter, minimamente:

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

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

1.5.1.49.3. Sumários de quantidade de logs ingeridos para cada fonte integrada ao

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

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

1.5.1.49.6. Sumário de toda as vulnerabilidades de

segurança encontradas no período do relatório;

1.5.1.49.7. Sumário de todos os e-mails retidos, organizando por camada de proteção;

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

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

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

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

1.5.1.49.12. Resultados dos testes de campanhas de phishing realizadas com os usuários da ENAP;

1.5.1.49.13. Resultados completos de testes de segurança direcionados a solução de WAF em uso pela ENAP;

1.5.1.49.14. Resultados completos referentes ao nível de maturidade de segurança da ENAP baseado nos testes de segurança realizados.

1.5.1.50. REQUISITOS GERAIS SOLUÇÃO DE SIEM

1.5.1.51. Deve ser capaz de gerar detecções baseadas no framework do MITRE ATT&CK® possuindo associações com no mínimo 25 regras de detecções (Táticas, Técnicas ou Procedimentos) de acordo com as fases prevista no framework, de forma que TTP’s de detecções sejam atualizadas regularmente, conforme modificação no FRAMEWORK.

1.5.1.52. A solução deverá unir eventos ao longo do tempo usando modelos Kill Chain para a análise de eventos de maior risco;

1.5.1.53. Deve permitir o Hunting rápido de

ameaças por meio da pesquisa em linguagem natural.

1.5.1.54. A ENAP poderá, a qualquer tempo, após a abertura de solicitação prévia, solicitar o acesso direto à console de gerenciamento da solução ofertada pela CONTRATADA, eventos e todas as funcionalidades, no modo somente leitura (read-only).

1.5.1.55. Deverá utilizar análise dos eventos em linha do tempo para facilitar a análise.

1.5.1.56. Deve funcionar, obrigatoriamente, com autenticação de dois fatores nativa.

1.5.1.57. Deve possuir parsing, para interpretação automática de logs.

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

1.5.1.59. ARQUITETURA DA SOLUÇÃO

1.5.1.60. Todas as características abordadas deverão ser atendidas por uma única solução, não sendo permitido a composição de soluções.

1.5.1.61. O serviço deve prover solução de SIEM dimensionada, a princípio, para 1500 EPS para o ambiente da ENAP, provendo a indexação e busca de informações e logs com apresentação das informações em formato técnico e executivo através de painéis orientados a cada finalidade.

1.5.1.62. Não serão aceitas soluções entregues sob estrutura de console compartilhada, devendo o ambiente lógico fornecido, ser de total e exclusivo uso da ENAP;

1.5.1.63. A solução deverá ser extremamente escalável e tolerante a falhas, capaz de ingerir terabytes por dia e suportar a retenção de eventos de segurança por longo período;

1.5.1.64. Deverá estar licenciada, em nome da

CONTRATADA, de forma a manter o processamento em tempo real ou realizar o buffer dos eventos, mesmo que o tráfego de eventos ultrapasse o volume licenciado nas horas de pico.

1.5.1.65. Deve ser do tipo Nuvem em Software como um modo de Serviço e ter as certificações SOC 2 TIPO II e ISO 27001;

1.5.1.66. Deve garantir retenção dos logs conforme arquitetura abaixo:

1.5.1.67. 7 dias hot retention;

1.5.1.68. 90 dias warm retention;

1.5.1.69. 365 dias cold retention.

1.5.1.70. Deve ter alta disponibilidade e mecanismos de recuperação de desastres;

1.5.1.71. Deve permitir a filtragem e compressão de dados seletivos em até 90% no ponto de coleta;

1.5.1.72. Deve permitir o gerenciamento da largura de banda para a transmissão de dados entre os coletores e os servidores de gerenciamento;

1.5.1.73. Deve executar o armazenamento em cache local e/ou em buffer nos coletores para garantir que nenhum dado seja perdido em trânsito no caso de um problema de rede ou um pico no volume do evento;

1.5.1.74. Deve oferecer suporte ao mascaramento de dados por meio de controles de acesso granulares baseados em funções, para ofuscar qualquer informação de usuário potencialmente sensível na camada de interface do usuário;

1.5.1.75. Deve suportar controle de acesso baseado em função granular (RBAC) com suporte a administração delegada, tanto para as

funcionalidades na interface do usuário quanto acesso aos dados e configurações;

1.5.1.76. Deve incluir uma ferramenta de Security Data Lake baseada em Big Data, uma arquitetura aberta e escalável e com capacidade de coletar e reter dados por períodos estabelecidos para fins de conformidade e investigação;

1.5.1.77. INTEGRAÇÕES

1.5.1.78. Deve oferecer suporte à integração com mais de 500 fontes de eventos usando nativamente no mínimo: métodos de syslog, formatos de log estruturados (CEF, LEEF, JSON, XML), arquivos, bancos de dados (conexão JDBC), conexão API (AWS, Azure, Box, Crowdstrike, SentinelOne, Trend, Symantec, Netskope, Zscaler, Skyhigh, Mcafee, SVN, Splunk, QRadar, Netwitness, Office 365, Okta, Proofpoint, Tenable, Qualys, Rapid7), WMI, consultas LDAP/LDAPS, dados e fluxo (Netflow, sFlow, jFlow), Hadoop, Registros não estruturados (Regex), agentes de terceiros (snare);

1.5.1.79. Deve permitir a integração com diferentes tipos de fontes de dados, como dados de identidade, logs de atividades / transações, logs de eventos de segurança, fluxos de rede, log de aplicativos / soluções de nuvem, permissões de acesso, fontes de inteligência de ameaças;

1.5.1.80. Deve permitir conexão a sistemas externos de gerenciamento de identidade, como Active Directory / LDAP ou soluções de IAM (gestão de identidade), como Sailpoint, CyberArk, para realizar o enriquecimento contextual de eventos adicionando identidade do usuário;

1.5.1.81. Deve ser capaz de se conectar

nativamente através de APIs ou outros meios com serviços em nuvem como Amazon Web Services S3, Cloudtrail, CloudWatch, GuardDuty, VPC Flow Logs, BOX, Microsoft Azure, Office 365, Google Apps, Google Cloud, Netskope, ServiceNow, Jira, entre outros.

1.5.1.82. Deve ter uma interface de usuário que permita modificar conectores, analisadores (parsers) existentes ou construir novos analisadores (parsers) na mesma interface de usuário;

1.5.1.83. Deve ter conectores, analisadores (parsers) pré-configurados, prontos para uso, mas que possam ser modificados conforme necessário. A análise, normalização e categorização dos coletores devem ser totalmente personalizáveis na interface do usuário.

1.5.1.84. Deve ter uma API RESTful de serviços para integração bidirecional com outras tecnologias;

1.5.1.85. A CONTRATADA deve fornecer integração com pelo menos 5 fontes de inteligência de ameaças inclusas no valor do serviço ofertado;

1.5.1.86. Deve possuir mascaramento de dados (Data Masking), para proteger informações confidenciais;

1.5.1.87. Deve incluir recursos de workflow nativos e permitir criação e customizáveis para resposta a incidentes de segurança.

1.5.1.88. CAPACIDADES DE INVESTIGAÇÃO

1.5.1.89. Deve realizar o enriquecimento dos eventos com dados contextuais no momento da captura e ingestão de dados e no momento da investigação da ameaça (On Demand), adicionando aos eventos:

1.5.1.90. Identidade do usuário;

1.5.1.91. Contexto;

1.5.1.92. Metadados de ativos;

1.5.1.93. Informações de rede;

1.5.1.94. Localização Geográfica;

1.5.1.95. Dados de inteligência de ameaças.

1.5.1.96. Deve fornecer recursos abrangentes para modelar e ajustar a pontuação de risco com base no perfil do usuário e/ou entidade, gravidade da ameaça e sequência/combinação de eventos que ocorrem durante um período;

1.5.1.97. Deve permitir a modelagem de risco a partir da interface do usuário de acordo com as prioridades da organização;

1.5.1.98. Deve possuir risco score baseado em violação;

1.5.1.99. Deve ter modelos de ameaças que permitam agrupar eventos realizados por um usuário ou entidade que duram dias, semanas, meses e assim por diante. Essas atividades devem ser exibidas como uma cadeia de eliminação com cada evento categorizado em estágios predefinidos.

1.5.1.100. Deve ter algoritmos preditivos para identificar usuários de risco (por exemplo, usuários prestes a deixar a organização);

1.5.1.101. Deve fornecer análises para diferentes tipos de falhas, como relacionadas ao tempo, volume de transferência de dados, origem do evento relacionado, destino do evento relacionado, relacionadas a localização geográfica / velocidade terrestre, bem como rastrear usuários ou outras entidades nas listas de observação;

1.5.1.102. Deve haver técnicas de análise históricas de eventos pelas quais atividades

suspeitas que não foram vistas antes possam ser identificadas;

1.5.1.103. Deve possuir técnicas por enumeração que permita criar linhas de base de eventos do mesmo tipo e procurar qualquer desvio do normal;

1.5.1.104. Deve ter técnicas de análise de tráfego para identificar padrões de beaconing, agentes de usuários incomuns, conexões com URLs incomuns, conexões com domínios DGA, entre outras;

1.5.1.105. Deve fornecer a capacidade de definir políticas baseadas em regras para detectar ameaças conhecidas. Essas ameaças conhecidas devem ser usadas como intensificadores de risco e combinadas com as verificações “não assinadas” nos modelos de ameaças;

1.5.1.106. Deve haver modelagem de ameaças que permita a identificação de ameaças compostas, que se observadas isoladamente podem ser de baixo risco, porém, quando combinadas, são indicativas de um evento de alto risco;

1.5.1.107. Deve reduzir o número de falsos positivos aplicando recursos avançados de feeds de inteligência;

1.5.1.108. VISUALIZAÇÃO E RELATÓRIOS

1.5.1.109. Deve disponibilizar, a qualquer tempo, relatórios de ameaças que forneçam visibilidade da postura de segurança cibernética. Por exemplo: usuários de alto risco, ativos de alto risco, principais ameaças, principais IPs maliciosas, entre outros;

1.5.1.110. Deve disponibilizar, a qualquer tempo, relatórios que forneçam visibilidade sobre as operações de segurança. Por exemplo, para dispositivos VPN, os relatórios devem incluir as

melhores sessões de VPN por duração, os principais eventos de saída de dados, a distribuição dos eventos de login por geografia, as principais tentativas de login com falha e assim por diante;

1.5.1.111. Deve disponibilizar, a qualquer tempo, relatórios de conformidade alinhados com requisitos de conformidade específicos, como PCI, SOX, HIPPA, GDPR, ISO27002;

1.5.1.112. Deve disponibilizar, a qualquer tempo, relatórios de resumo executivo de violações, incidentes e operações;

1.5.1.113. Deve disponibilizar relatórios sobre a atividade do usuário;

1.5.1.114. Deve permitir que os dados sejam exibidos com diferentes tipos de gráficos: gráfico de linhas, gráfico de barras, gráfico de pizza, mapa geográfico, tabelas, gráficos de bolhas, gráficos de relacionamento de origem e destino;

1.5.1.115. Deve permitir a visualização de dados que permitam vincular qualquer conjunto de atributos e visualização a relação entre eles;

1.5.1.116. INSTALAÇÃO E ADMINISTRAÇÃO DA SOLUÇÃO DE SIEM

1.5.1.117. A solução de SIEM deve ser implementada, sem limitação de coletores.

1.5.1.118. A ENAP fornecerá a infraestrutura necessária para implementação dos coletores, por se tratar de gateways dentro do ambiente;

1.5.1.119. A CONTRATADA deverá implementar e fazer a gestão de toda a solução de SIEM e de todos os seus componentes;

1.5.1.120. A CONTRATADA será responsável pela criação de regras de correlação que reflitam as reais necessidades do ambiente da ENAP com o objetivo de identificar possíveis incidentes de segurança;

1.5.1.121. Criar relatórios e modelos, criar filtros de pesquisa, fazer backups, criar dashboards, gerenciar usuários e utilizar os principais recursos da solução;

1.5.1.122. Apresentar plano de instalação e configuração, que deverá contemplar todos os tipos de ativos em produção na rede da ENAP.

1.5.1.123. Atualizar a solução e seus componentes para a última versão disponível compatível com a solução ofertada.

1.5.1.124. Os serviços de instalação de coletores nos ambientes da ENAP deverão ser realizados em horário previamente combinado com a ENAP, preferencialmente no horário de expediente normal da ENAP (2ª a 6ª feira, das 8h00min às 18h00min);

1.5.1.125. Qualquer atividade que possa colocar em risco o funcionamento normal das unidades da ENAP 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 a ENAP;

1.5.1.126. 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 da ENAP ou de forma remota.

1.5.1.127. PROCESSO DE MONITORAMENTO, DETECÇÃO E RESPOSTA

1.5.1.128. A CONTRATADA será responsável por implantar, operar e suportar toda a plataforma ofertada;

1.5.1.129. A fim de balizar todo o processo de

monitoramento de ataques cibernéticos da ENAP, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir *ipsis litteris*.

1.5.1.130. É sabido que para o sucesso de um monitoramento de ataques cibernético, a primeira definição se deve a que tipo de ocorrência de eventos de segurança, se deseja detectar e tomar algum tipo de ação, logo será de responsabilidade da CONTRATADA como primeiro passo deste processo, a definição de linha de base de eventos monitorados.

1.5.1.131. Tal definição de linha de base de eventos de segurança monitorados, não deve ser tomada de forma unilateral pela CONTRATADA. A ENAP deverá participar ativamente no processo de construção de forma consultiva. Porém, se ratifica que é de responsabilidade da CONTRATADA a definição, e colocar em operação tal linha de base.

1.5.1.132. Espera-se que a linha de base de eventos de segurança monitorados, seja revista de forma mensal, contudo, não se limitando a este tempo, pois todos os dias novos ataques são projetados no mundo, e se espera que a CONTRATADA tome ciência destes ataques, e por sua vez atualize a linha de base, para que em um cenário onde estes novos ataques sejam direcionados a ENAP, sejam detectados através dos serviços em questão.

1.5.1.133. O produto de um evento é a correlação dos logs gerados pelos itens de configuração do parque da ENAP. Uma vez definida a linha de base de eventos, será também de responsabilidade da CONTRATADA avaliar se todos os insumos para a correta geração do

evento, estão sendo enviados corretamente para a ferramenta.

1.5.1.134. Caso a CONTRATADA identifique a ausência dos insumos (eventos) a ser gerado por um item de configuração, será de responsabilidade da CONTRATADA a correção e/ou habilitação de tal insumo dos itens de configuração. Caso o item de configuração não pertencer ao objeto contratado, porém necessário para a correta geração do evento, deverá a CONTRATADA solicitar à ENAP a correção e/ou habilitação de tal insumo no item de configuração em questão.

1.5.1.135. Dar-se-á então o passo de classificação do evento, também de responsabilidade da CONTRATADA. O grupo de monitoramento de ataques da CONTRATADA deve focar as ações nos eventos que são significativos. Logo, tal grupo deve analisar todos os eventos apresentados, classificando-os nos seguintes grupos, a saber:

1.5.1.136. Eventos de Informação: Estes eventos não requerem qualquer ação. São usados para fazer verificação de funcionalidade dos itens de configuração de segurança. Ou seja, tem por objetivo puro e simples, identificar se as ferramentas e soluções estão funcionando dentro do esperado. Estes eventos são também úteis para gerar estatísticas como, por exemplo, porcentagem de hosts com a última vacina de antivírus do dia.

1.5.1.137. Eventos de Aviso: Este grupo de eventos deve ser utilizado quando existe algum comportamento anômalo, se comparado a linha de base de operação padrão do ambiente (serviço ou solução), porém, ainda não gerou algum tipo de impacto ao ambiente (serviço ou solução) do ENAP, como por exemplo fictício: É esperado que exista 1.000 (mil) ataques do tipo

port scan bloqueados pelo firewall, porém, na última hora, este número passou para 10.000 (dez mil) ataques, todavia, o firewall ainda continua bloqueando sem que haja degradação da performance do ambiente (serviço, tráfego e/ou solução).

1.5.1.138. Eventos de Exceção: Estes eventos são aqueles que sugere que os pilares de segurança da informação (confidencialidade, integridade e conformidade), foram impactados como, por exemplo: Uma infecção gerada por um malware do tipo ransomware, onde não tenha sido bloqueada pela solução de antivírus da ENAP. Este é o único tipo de evento que pode iniciar o processo de resposta a incidentes de segurança.

1.5.1.139. Uma vez classificado o evento, se inicia o passo de resposta ao mesmo, que também é de responsabilidade da CONTRATADA. As respostas são baseadas nos grupos de classificação de eventos, a saber:

1.5.1.140. Para eventos do tipo informação, não é requerido qualquer tipo de ação, porém, como já mencionado no presente documento, tais eventos são utilizados para verificação do perfeito funcionamento das soluções de segurança. Portanto, a CONTRATADA deverá utilizá-los para tal fim.

1.5.1.141. Para eventos do tipo Aviso, a CONTRATADA deverá garantir que uma interface humana, ou seja, uma analista que pertence ao GRUPO DE MONITORAMENTO DE ATAQUES, esteja validando se tal evento pode se transformar em um evento do tipo exceção, e obviamente tomar as ações cabíveis para identificar a causa raiz da mudança de comportamento do ambiente.

1.5.1.142. Para eventos do tipo Exceção, a CONTRATADA deverá transformar tal evento em um incidente de segurança, realizando, portanto,

a abertura na ferramenta de incidente de segurança da informação definida no PROCESSO DE MONITORAMENTO, DETECÇÃO E RESPOSTA, descrito no presente documento. Após a abertura do incidente de segurança, obedecendo os critérios estabelecidos para tal, se encerra a participação do grupo de monitoramento de ataques.

1.5.1.143. Como último passo do processo, a CONTRATADA deve encerrar os eventos após as devidas ações tomadas, conforme definido no parágrafo acima. Eventos podem ter apenas dois tipos de status “aberto” ou “encerrado”, ou seja, após o correto tratamento, o evento deverá ter seu status alterado na ferramenta de “aberto” para “encerrado”.

1.5.1.144. Importante ressaltar que todo o processo de tratamento do evento, independente de qual fase e/ou status, deve ser registrado no módulo de tratamento de eventos da ferramenta. Também é responsabilidade da CONTRATADA a segurança dos eventos, e fica expressamente proibido a remoção de qualquer evento, independentemente de sua classificação e fase de tratamento.

1.5.1.145. PROCESSO DE CAÇADA CONTÍNUA A AMEAÇAS

1.5.1.146. Com o aumento do volume e complexidade das ameaças será exigido que a empresa CONTRATADA execute processos proativos e manuais de caçada de ameaças (Threat Hunting) no ambiente da ENAP. A fim de balizar todo o processo de caçada de ameaças, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir *ipsis litteris*.

1.5.1.147. A CONTRATADA deverá inclusive nos finais de semana e feriados, a:

1.5.1.148. Definir uma hipótese e uma declaração de uma possibilidade de ameaça, tal hipótese deve ser elaborada utilizando como referência novos vetores de ameaças e novas tendências baseadas em inteligência de ameaças e fontes de riscos digitais, informações relevantes coletadas por processos de aprendizagem de máquina e inteligência artificial e investigações de táticas, técnicas e procedimentos criando desta forma uma hipótese de como ameaças podem existir dentro do ambiente e de como encontrá-las;

1.5.1.149. Uma vez que a hipótese tenha sido definida a CONTRATADA deverá realizar um plano de coleta dos eventos dentro das plataformas relevantes de acordo com a hipótese definida;

1.5.1.150. Uma vez que os eventos relevantes estejam disponíveis, a CONTRATADA deverá avaliar a massa de eventos para buscar anomalias associadas a hipótese definida;

1.5.1.151. Caso sejam encontrados eventos maliciosos, estes entram no processo de resposta a incidentes de segurança da informação, conforme descrito neste documento;

1.5.1.152. Caso não sejam encontrados eventos maliciosos, o processo de caçada é finalizado, sendo repetido no dia seguinte com uma nova hipótese;

1.5.1.153. Todo processo deve ser documentado através da plataforma de ITMS da CONTRATADA, incluindo qual hipótese foi utilizada, quais dados foram analisados e o resultado da análise;

1.5.1.154. GRUPO TÉCNICO DE MONITORAMENTO DE ATAQUES

CIBERNÉTICOS

1.5.1.155. Através dos seus 02 (dois) centros de operação de segurança, a CONTRATADA deverá manter uma torre de operação denominada GRUPO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS, com objetivo e foco de trabalhar no processo de monitoramento de ataques cibernéticos.

1.5.1.156. Este grupo deverá ser exclusivo para trabalhar no serviço em questão, não podem os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem, com os demais serviços descritos no objeto do presente documento.

1.5.1.157. Todos os profissionais que integram GRUPO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS, devem obrigatoriamente compor o quadro de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho), sendo proibida a terceirização ou subcontratação de tal serviço.

1.5.1.158. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no tópico CATÁLOGO DE SERVIÇO e NMS – NÍVEIS MÍNIMOS DE SERVIÇOS do presente documento.

1.5.1.159. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para executar o processo de monitoramento de ataques cibernéticos da ENAP, a CONTRATADA deverá, obrigatoriamente, compor o GRUPO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS, com 02 (dois) profissionais para cada perfil que segue descrito abaixo:

Perfis	Certificações	Descrição
• Analista de Segurança I	• Certified in Cybersecurity – CC (ISC)	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.
• Analista de Segurança II	• Certified Ethical Hacker	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM. Experiência comprovada de no mínimo 36 (trinta e seis) meses em segurança da informação.
• Analista III	• Certificação da solução a ser utilizada no serviço	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.

Tabela - Certificações Grupo de Monitoramento de ataques

1.5.1.160. Todos os profissionais deverão possuir diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

1.5.1.161. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS, porém, conforme já foi mencionado neste documento, este(s) deve(m) compor única e exclusivamente o time denominado GRUPO DE MONITORAMENTO

DE ATAQUES CIBERNÉTICOS.

1.5.1.162. No momento da assinatura do contrato, será exigido da CONTRATADA, as seguintes documentações do(s) profissionais que participarão do GRUPO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS, os quais devem comprovar as exigências e obrigações descritas neste documento: carteira de trabalho devidamente assinada pela CONTRATADA, para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento

1.5.1.163. ENTREGAS A SEREM REALIZADAS

1.5.1.164. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a ENAP definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma online e em tempo de execução, através do portal de indicadores descrito no tópico de condições gerais para prestação do serviço deste documento, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de eventos correlacionados	Soma de eventos correlacionados	Eventos correlacionados	Eventos correlacionados	Número total de eventos correlacionados
Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	Incidentes	Número total de incidentes abertos
Quantitativo de solicitações por grupo de tecnologia	Soma de solicitações relacionadas aos grupos de tecnologia	Solicitações relacionadas aos grupos de tecnologia	Solicitações	Número total de solicitações relacionadas por grupo de tecnologia
Quantitativo de regras de correlacionamento	Soma do número de regras de correlacionamento	Regras de correlacionamento	Regras de correlacionamento	Número total de regras de correlacionamento
TOP 10 – Regras de correlacionamento	Soma do número de eventos	Eventos	Regra de correlacionamento	TOP 10 do número de

	correlacionados por regra de correlacionamento	correlacionados		eventos correlacionados por regra de correlacionamento
TOP 10 – IP de destino de regras de correlacionamento	Soma do número de eventos correlacionados por IP de destino	Eventos correlacionados por IP de destino	IP de destino	TOP do número de eventos correlacionados por IP de destino
TOP 10 – Regras de correlacionamento por país de origem	Soma do número de eventos correlacionados por país de origem	Eventos correlacionados por país de origem	País de origem	TOP do número de eventos correlacionados por país de origem
TOP 10 – Tipos de ataques	Soma do número de ataques correlacionados por tipo de ataque	Eventos correlacionados por ataque	Ataques	TOP 10 por tipo de ataque

1.5.1.165. Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com a presença de profissional que conheça todos os serviços prestados, e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler).

1.5.1.166. Neste contexto, o profissional deve apresentá-lo de forma presencial nas dependências da ENAP, ou de forma virtual, por meio de solução de videoconferência.

Anexo III - Minuta de Termo de Contrato.pdf

Contrato 14/2024

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
14/2024	114702-ENAP-ESCOLA NACIONAL DE ADM. PUBLICA/DF	INGRID MELO POL FERREIRA	17/06/2024 14:21 (v 6.0)

Status

CONCLUIDO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
V - prestação de serviços, inclusive os técnico-profissionais especializados/Serviço continuado sem dedicação exclusiva de mão de obra		04600002376/2023-45

1. Cláusula primeira - do objeto

ANEXO III - MINUTA DE TERMO DE CONTRATO
Lei nº 14.133, de 1º de abril de 2021
SERVIÇOS – LICITAÇÃO

Fundação Escola Nacional de Administração Pública- Enap

(Processo Administrativo n° 04600.002376/2023-45)

CONTRATO ADMINISTRATIVO Nº ...../2024, QUE FAZEM ENTRE SI A FUNDAÇÃO ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA - ENAP E A EMPRESA .....

A **FUNDAÇÃO ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA - Enap**, instituída por força da Lei nº 6.871, de 03 de dezembro de 1980, e alterada pelo Decreto nº 11.345, de 1º de janeiro de 2023, vinculada ao Ministério da Gestão e Inovação em Serviços Públicos, com sede no Setor de Áreas Isoladas Sudoeste nº 02-A, nesta capital, CNPJ sob o nº 00.627.612/0001-09, neste ato representada pela Presidenta, a Senhora Betânia Lemos, nomeada pela Portaria da Casa Civil da Presidência da República nº 1.818, de 27 de fevereiro de 2023, publicada no Diário Oficial da União, em 28 de fevereiro de 2023, portadora da matrícula funcional nº xx043xx, com competência delegada pela Portaria MGI nº 572, de 08 de março de 2023, e atribuições conferidas pelo Estatuto aprovado pelo Decreto nº 10.369, de 22 de maio de 2020, doravante denominado CONTRATANTE, e o(a) ....., inscrito(a) no CNPJ/MF sob o nº ....., sediado(a) na ....., em ..... 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 04600.002376/2023-45, 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 Pregão Eletrônico n. .../2024, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – OBJETO (art. 92, I e II)

1.1. O objeto do presente instrumento é a contratação de solução de tecnologia da informação e comunicação de empresas especializadas no fornecimento de serviços gerenciados de segurança para a ENAP, nas condições estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

ITEM	ESPECIFICAÇÃO	MÉTRICA OU UNIDADE DE MEDIDA MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR 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

CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 12 (doze) meses contados da assinatura do contrato, prorrogável para até 05 (cinco) anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

2.1.1. 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;

2.1.2. O contratado não tem direito subjetivo à prorrogação contratual;

2.1.3. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo;

2.1.4. 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.

3. Cláusula terceira - modelos de execução e gestão contratuais

CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS (art. 92, IV, VII e XVIII)

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

CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. Não será admitida a subcontratação do objeto contratual.

5. Cláusula quinta - preço

CLÁUSULA QUINTA – PREÇO (art. 92, V)

5.1. O valor mensal da contratação é de R$ ..... (.....), perfazendo o valor total de R$ ..... (....).

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

6. Cláusula sexta - pagamento

CLÁUSULA SEXTA - PAGAMENTO (art. 92, V e VI)

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

CLÁUSULA SÉTIMA - REAJUSTE (art. 92, V)

7.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em __/__/____.

7.2. 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 Custo da 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.

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

7.4. 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).

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

7.6. 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.

7.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

7.8. O reajuste será realizado por apostilamento.

8. Cláusula oitava - obrigações do contratante

CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE (art. 92, X, XI e XIV)

8.1. São obrigações do Contratante, além das previstas no termo de referência:

8.2. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

8.3. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.4. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

8.5. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

8.6. Comunicar a empresa para emissão de Nota Fiscal em relação 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;

8.7.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;

8.8. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

8.9. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

8.10. 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.

8.11. 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.

8.12. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 (trinta) dias.

8.13. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

8.14. 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.

8.15. 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

CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO (art. 92, XIV, XVI e XVII)

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, além das previstas no termo de referência:

9.2. Manter preposto aceito pela Administração no local do serviço para representá-lo na execução do contrato.

9.3. 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.

9.4. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II) e prestar todo esclarecimento ou informação por eles solicitados;

9.5. Alocar os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

9.6. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

9.7, Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado 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 no edital, o valor correspondente aos danos sofridos;

9.8. 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 do fiscal ou gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

9.9. 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: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

9.10. 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 e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante;

9.11.Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

9.12. 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 empreendimento.

9.13. 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.

9.14. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.

9.15. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

9.16. 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.

9.17. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

9.18. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

9.19 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 (art. 116);

9.20. 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 (art. 116, parágrafo único);

9.21. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

9.22.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;

9.23. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante;

9.24. Realizar os serviços de manutenção e assistência técnica no seguinte local sendo o ponto de contato com a equipe de Tecnologia da Informação da Enap, no seguinte endereço: SAIS - nº 02-A - Setor Policial Sul - Brasília/DF;

9.24.1. O técnico deverá se deslocar ao local da repartição do local demandado**.**

9.25. Realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução dos serviços;

9.26. Ceder ao Contratante todos os direitos patrimoniais relativos ao objeto contratado, o qual poderá ser livremente utilizado e/ou alterado em outras ocasiões, sem necessidade de nova autorização do Contratado.

9.26.1. Considerando que o projeto contratado se refere a obra imaterial de caráter tecnológico, insuscetível de privilégio, a cessão dos direitos a que se refere o subitem acima inclui o fornecimento de todos os dados, documentos e elementos de informação pertinentes à tecnologia de concepção, desenvolvimento, fixação em suporte físico de qualquer natureza e aplicação da obra.

10. Cláusula décima - obrigações pertinentes a LGPD

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.

10.11. 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.

10.12. 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.

10.13. 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

CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO (art. 92, XII)

11.1. A contratação conta com garantia de execução, nos moldes do art. 96 da Lei nº 14.133, de 2021, na modalidade seguro-garantia, em valor correspondente a 5% (cinco por cento) do valor anual do contrato.

O item acima será escolhido, caso o adjudicatário opte pela oferta de seguro-garantia, que deverá ser apresentada antes da assinatura do contrato, conforme item 2.1 da Nota Explicativa da AGU e previsão do art. 96, § 3º, da Lei n.º 14.133/2021.

11.1. O contratado apresentará, 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, podendo optar por caução em dinheiro ou títulos da dívida pública ou, ainda, pela fiança bancária, em valor correspondente a 5% (cinco por cento) do valor anual do contrato**.**

O item acima será escolhido, caso o adjudicatário opte por outras modalidades de seguro, conforme item 3 da Nota Explicativa da AGU e previsão do incisos I, III e IV art. 96, da Lei n.º 14.133/2021.

11.2. Caso utilizada a modalidade de seguro-garantia, a apólice permanecerá e vigor mesmo que o contratado não pague o prêmio nas datas convencionadas.

11.3. Caso utilizada a modalidade de seguro-garantia, a apólice deverá ter validade durante a vigência do contrato e por mais 90 (noventa) dias após término da vigência contratual, permanecendo em vigor mesmo que o contratado não pague o prêmio nas datas convencionadas.

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

11.5. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no item 11.9 deste contrato.

11.6. 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.

11.7. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

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

11.7.2 multas moratórias e punitivas aplicadas pela Administração à contratada; e

11.7.3 obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo contratado, quando couber.

11.8. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item 11.7, observada a legislação que rege a matéria.

11.9. A garantia em dinheiro deverá ser efetuada em favor do contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

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

11.11. 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.

11.12. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

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

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

11.14.1. 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 (art. 137, § 4º, da Lei n.º 14.133, de 2021).

11.14.2. 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 n° 662, de 11 de abril de 2022.

11.15. Extinguir-se-á a garantia com a restituição da apólice, carta fiança ou autorização para a liberação de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do contratante, mediante termo circunstanciado, de que o contratado cumpriu todas as cláusulas do contrato;

11.16. 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.

11.17. 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.

11.18. O contratado autoriza o contratante a reter, a qualquer tempo, a garantia, na forma prevista neste Contrato.

11.19. A garantia de execução é independente de eventual garantia do produto ou serviço prevista especificamente no Termo de Referência.

12. Cláusula décima segunda - infrações e sanções administrativas

CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS (art. 92, XIV)

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

a) der causa à inexecução parcial do contrato;

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

c) der causa à inexecução total do contrato;

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

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

f) praticar ato fraudulento na execução do contrato;

g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

12.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

I. Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

II. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

III. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima deste Contrato, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 202

IV. Multa:

(1) Moratória de 1% (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

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

(a) O atraso superior a 30 (trinta) dias 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.

(3) Compensatória, para as infrações descritas nas alíneas “e” a “h” do subitem 12.1, de 15% a 30% do valor do Contrato.

(4) Compensatória, para a inexecução total do contrato prevista na alínea “c” do subitem 12.1, de 5% a 15% do valor do Contrato.

(5) Para infração descrita na alínea “b” do subitem 12.1, a multa será de 10% a 20% do valor do Contrato.

(6) Para infrações descritas na alínea “d” do subitem 12.1, a multa será de 0,5% a 2% do valor do Contrato.

(7) Para a infração descrita na alínea “a” do subitem 12.1, a multa será de 1% a 5% do valor do Contrato, ressalvadas as disposições constantes nos itens 8.20. e 8.21. do Termo de Referência.

12.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021)

12.4. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

12.5. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021)

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

12.7. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

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

12.9. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

a) a natureza e a gravidade da infração cometida;

b) as peculiaridades do caso concreto;

c) as circunstâncias agravantes ou atenuantes;

d) os danos que dela provierem para o Contratante;

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

12.10. 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 (art. 159).

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

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

12.13. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

12.14. 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.

13. Cláusula décima terceira - da extinção contratual

CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL (art. 92, XIX)

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 su 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 artigo 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 artigos 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:

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 (art. 131, *caput,* da Lei n.º 14.133, de 2021).

13.8. 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 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 - dotação orçamentária

CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA (art. 92, VIII)

14.1 As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União deste exercício, na dotação abaixo discriminada:

14.1.1. Gestão/Unidade: 110788

14.1.2. Fonte de Recursos: -

14.1.3. Programa de Trabalho: 04.122.0032.2000.0001

14.1.4. Elemento de Despesa: 3.3.90.40

14.1.5. Plano Interno: II1WN

14.1.6. Nota de Empenho: 2024NExxxxx

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

15. Cláusula décima quinta - dos casos omissos

CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS (art. 92, III)

15.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

16. Cláusula décima sexta - alterações

CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

16.2. 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.

16.3. 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 (art. 132 da Lei nº 14.133, de 2021).

16.4. 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.

17. Cláusula décima sétima - publicação

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

CLÁUSULA DÉCIMA OITAVA– FORO (art. 92, §1º)

18.1. Fica eleito o Foro da Justiça Federal em Brasília-DF, Seção Judiciária do Distrito Federal, 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.

18.2. Para firmeza e validade do pactuado, o presente termo de contrato, perante duas testemunhas a tudo presentes, vai eletronicamente assinado pelos contraentes, conforme Resolução nº 09, publicada no Boletim Interno da Escola Nacional de Administração Pública nº 33, de 04 de agosto de 2015, depois de lido e achado em ordem.

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.

EVERALDO MELO DO NASCIMENTO

Equipe de apoio

Anexo IV - Valores Maximos Admissiveis.pdf

ANEXO IV
VALORES MÁXIMOS ADMISSÍVEIS

ITEM	ESPECIFICAÇÃO	CATSER	UNID.	QUANT.	VALOR UNITÁRIO	VALOR TOTAL
1	**Serviço de monitoramento e visibilidade de ataques cibernéticos**	27359	Mês	12	R$ 28.965,70	R$ 347.588,40
2	**Serviço de monitoramento, detecção e resposta a incidentes**	27359	Mês	12	R$ 77.714,82	R$ 932.577,84
VALOR TOTAL ESTIMADO						R$ 1.280.166,24