Termo de Referência 19/2023

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
19/2023	410003-COORDENACAO GERAL DE RECURSOS LOGISTICOS	FERNANDA NACIF MARCAL	30/11/2023 15:51 (v 10.0)

Status

ASSINADO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Serviços de TIC		53115.031680/2022-04

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de Solução integrada de segurança cibernética, contando com gestão de vulnerabilidades, defesa cibernética, resposta incidentes de segurança, incluindo os serviços de segurança da informação especializados em sustentação e implementação de soluções de cibersegurança, nos termos da Tabela 1 abaixo, conforme condições e exigências estabelecidas neste instrumento.

Tabela 1 - Detalhamento do Objeto

Grupo	Item	Especificação	CATMAT/ CATSER	Unidade de medida	Quantidade	Valor Unitário	Valor Total
1	1	Solução de gerenciamento de vulnerabilidades de segurança	27502	Dispositivo	1500	R$ 340,98	R$ 511.470,00
	2	Solução de correlação de eventos de segurança e resposta a incidentes	27502	Eventos por segundo - EPS	1300	R$ 690,32	R$ 897.416,00
	3	Solução de micro segmentação de ambiente corporativo	27502	Dispositivo	300	R$ 1.395,40	R$ 418.620,00
	4	Solução de simulação de ataques em ambiente corporativo	27502	Usuários	1500	R$ 758,23	R$ 1.137.345,00
	5	Solução de proteção de usuários e controle de dados em nuvem	27502	Usuários	1500	R$ 1.309,87	R$ 1.964.805,00

	6	Serviços de segurança da informação e resposta a incidentes de segurança	27340	UND SERVIÇO TÉCNICO	12	R$ 93.681,58	R$ 1.124.178,96
Valor Global							**R$. 6.053.834,96**

1.2. Os serviços objetos desta contratação são caracterizados como como comuns, uma vez que o padrão de desempenho e qualidade pode ser objetivamente definido pelo edital, por meio de especificações usuais de mercado, nos termos do inc. XIII do art. 6º da Lei 14.133, de 2021;

1.3. O prazo de vigência da contratação será de 12 (doze) meses, contados da assinatura do contrato, prorrogável para até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

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

1.4. No caso de discrepância entre as especificações dos objetos presentes no Catálogo de Materiais e Serviços do ComprasGov.br, conforme os códigos CATSER, e as especificações estipuladas no Termo de Referência e no Edital, as últimas terão precedência.

2. DESCRIÇÃO DA SOLUÇÃO

2.1. A solução de TIC consiste no fornecimento de subscrições de tecnologias de defesa cibernética e serviços conforme especificação técnica pormenorizada no **Anexo A** deste Termo de Referência.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE

3.1. A presente contratação é motivada pela necessidade de implantação de uma solução integrada para o gerenciamento de vulnerabilidades e visibilidade de riscos de segurança da informação no âmbito do Ministério das Comunicações.

3.1.1. Tecnicamente, no cenário complexo atual relacionado à segurança cibernética e às diretrizes gerais do governo federal, surgem diariamente inúmeros artefatos maliciosos, vulnerabilidades conhecidas, técnicas comuns de ataque, entre outros desafios. À medida que os avanços tecnológicos proporcionam novos e incríveis meios de realizar ou facilitar atividades cotidianas, pessoas mal-intencionadas trabalham diligentemente para explorar e tirar proveito de brechas, muitas vezes causadas por serviços de tecnologia que passam despercebidos.

3.1.2. Abordar o tema da segurança cibernética há 5 ou 6 anos era, sem dúvida, extremamente relevante, mas sempre foi necessária uma análise profunda para entender as necessidades de proteção. Atualmente, pode-se afirmar que o mundo está literalmente envolvido em uma guerra cibernética, e muitos especialistas apontam que a ocorrência de um ataque cibernético em uma organização é apenas uma questão de tempo (conforme mencionado em https://tiinside.com.br/09/12/2021/ataques-ciberneticos-a-pergunta-nao-e-mais-se-serei-atacado-mas-quando-e-como/).
Essa afirmação é respaldada pelo aumento na dependência de meios digitais e tecnológicos em diversas funções e setores da cadeia corporativa, tanto no âmbito privado quanto e governamental, tornando os ataques cibernéticos altamente lucrativos para os agressores (conforme descrito em https://www.securityreport.com.br/overview/a-evolucao-dos-ataques-ciberneticos-ate-onde-os-hackers-podem-ir/).

3.1.3. Quando se analisa o ambiente de empresas privadas, é possível observar uma série de ataques cibernéticos recentes que obtiveram sucesso, resultando em prejuízos significativos. A seguir, são apresentados alguns exemplos:

3.1.3.1. Lojas Renner: https://www.cnnbrasil.com.br/business/site-da-renner-continua-fora-do-ar-apos-ataque-hacker/

3.1.3.2. JBS: https://g1.globo.com/economia/noticia/2021/06/09/jbs-diz-que-pagou-11-milhoes-em-resposta-a-ataque-hacker-em-operacoes-nos-eua.ghtml

3.1.3.3. Colonial Pipeline: https://thehack.com.br/ataque-a-colonial-pipeline-partiu-de-senha-de-vpn-vazada-na-dark-web/

3.1.3.4. Universidade Estácio de Sá: https://www.securityreport.com.br/destaques/universidade-estacio-de-sa-e-alvo-de-ataque-hacker/

3.1.3.5. CVC: https://veja.abril.com.br/coluna/radar-economico/cvc-segue-sequestrada-e-vendas-sao-afetadas/

3.1.4. Quando abordamos o cenário governamental, se torna possível observar um cenário semelhante, senão pior. Vide alguns exemplos:

3.1.4.1. 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

3.1.4.2. Ministério da Saúde 2020: https://www.poder360.com.br/governo/ministerio-da-saude-identifica-virus-na-rede-do-datasus/

3.1.4.3. Ministério da Saúde 2021: https://www.cnnbrasil.com.br/nacional/site-do-ministerio-da-saude-sofre-ataque-hacker-durante-madrugada-e-sai-do-ar/

3.1.4.4. CNJ - Conselho Nacional de Justiça: https://www.conjur.com.br/2019-abr-01/cnj-sofre-ataque-hacker-dados-milhares-pessoas-vazam

3.1.4.5. 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

3.1.4.6. 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

3.1.4.7. TRF1 - Tribunal Regional de Brasília: https://www.cisoadvisor.com.br/invasao-de-rede-tira-do-ar-tribunal-federal-regional-de-brasilia/

3.1.4.8. 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/

3.1.5. Ao observar todos estes casos, torna-se evidente como os incidentes cibernéticos afetam diretamente a vida dos cidadãos, frequentemente impedindo-os de realizar compras ou utilizar serviços de empresas privadas ou governamentais essenciais para o funcionamento da nação. Além dos impactos financeiros, também é notável um aumento significativo dos ataques cibernéticos de natureza política (conforme destacado em: https://www.uol.com.br/tilt/noticias/redacao/2022/01/20/ataques-ciberneticos-como-arma-politica.htm).

3.1.6. A título de exemplo desses ataques recentes, cita-se o ataque ao Oleoduto Colonial Pipeline (conforme relatado em 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.

3.1.7. Portanto, considerando os riscos e necessidades previamente mencionados, este estudo tem como objetivo explorar os cenários a serem definidos para encontrar a melhor alternativa que atenderá às necessidades do Ministério das Comunicações - MCom, com foco na vantajosidade financeira para administração pública.

3.1.8. Os detalhes da demanda para a contratação de uma solução integrada para gerenciamento de vulnerabilidades e visibilidade de riscos de segurança, incluindo visibilidade contínua de eventos de segurança e resposta a incidentes de segurança, estão especificados na Tabela 2:

Tabela 2 - Detalhamento da Demanda

Item	Descrição
Solução de gerenciamento de vulnerabilidades de segurança	Esta camada de proteção deve implementar visibilidade contínua de vulnerabilidades de segurança, permitindo o gerenciamento de todo o ciclo de vida delas, desde a descoberta até a remediação.
Solução de correlação de eventos de segurança e resposta a incidentes	Esta camada de proteção deverá atuar diretamente na ingestão de eventos de todas as tecnologias de proteção utilizadas no ambiente, além de priorizar e gerar alertas para consolidar a resposta a incidentes de segurança em uma única visão.
Solução de micro segmentação de ambiente corporativo	Esta camada de proteção estará diretamente relacionada à segmentação do ambiente corporativo, possibilitando que as aplicações e servidores comuniquem-se na rede apenas com os endereços e portas estritamente necessários.
Solução de simulação de ataques em ambiente corporativo	Deverá implementar a capacidade de realizar testes de segurança no ambiente, garantindo que esteja protegido contra os principais tipos de ameaças e técnicas de ataque. Além disso, deve estabelecer uma camada de evolução contínua para todas as soluções de defesa existentes no ambiente.
Solução de proteção de usuários e controle de dados em nuvem	Esta solução implementará uma camada de proteção para os usuários, tanto em relação ao acesso à internet quanto ao comportamento em aplicações de nuvem. Além disso, fornecerá meios para um acesso remoto seguro, eliminando a necessidade de conceitos inseguros, como as VPNs (Confiança zero).
Serviços de segurança da informação e resposta a incidentes de segurança	Serviços especializados em segurança da informação, focados na implementação, suporte e manutenção do ambiente, visando maximizar a utilização das ferramentas, suas integrações, bem como as proteções oferecidas por cada uma delas.

3.1.9. O quantitativo estimado para esta demanda, baseado nas necessidades elencadas pode ser encontrado na Tabela 3:

Tabela 3 - Quantitativo da Demanda

Item	Descrição	Unidade	Quantidade
1	Solução de gerenciamento de vulnerabilidades de segurança	Dispositivo	1500
2	Solução de correlação de eventos de segurança e resposta a incidentes	Eventos por segundo - EPS	1300
3	Solução de micro segmentação de ambiente corporativo	Dispositivo	300
4	Solução de simulação de ataques em ambiente corporativo	Usuários	1500
5	Solução de proteção de usuários e controle de dados em nuvem	Usuários	1500
6	Serviços especializados em segurança da informação	UND SERVIÇO TÉCNICO	12

3.2. O objeto da contratação está previsto no Plano de Contratações Anual 2023, conforme detalhamento a seguir:

I) ID PCA no PNCP: 37753638000103-0-000001/2023;

II) Data de publicação no PNCP: 20/05/2023;

III) Id do item no PCA:194;

IV) Classe/Grupo: 168 – Serviços Auxiliares de Tecnologia da Informação e Comunicação (TIC);

V) Identificador da Futura Contratação: 410003-303/2022.

3.3. O objeto da contratação também está alinhado com a Estratégia de Governo Digital 2020-2023, com o Plano Estratégico Institucional e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2023-2024 do Ministério das Comunicações, conforme demonstrado na Tabela 4 e Tabela 5:

Tabela 4 - Estratégia de Governo Digital e Plano Estratégico Institucional

ID	OBJETIVO ESTRATÉGICO	REFERÊNCIA

OE 8	Aprimorar a Governança, a integridade, a gestão estratégia e a gestão da informação	Planejamento Estratégico Institucional 2021-2023 (PEI 2021-2023) https://www.gov.br/mcom/pt-br/acesso-a-informacao/transparencia-e-prestacao-de-contas/CadernodoPEI20212023v2.pdf
OE 9	Garantir recursos materiais e infraestrutura de TIC necessários ao desempenho das atribuições institucionais	
Objetivo 11	Garantia da segurança das plataformas de governo digital e de missão crítica	Estratégia de Governo Digital – EGD 2020-2023 https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Decreto/D10332.htm
Objetivo 16	Otimização das infraestruturas de tecnologia da informação	

Tabela 5 - Plano Diretor de Tecnologia da Informação

Necessidade	Meta do PDTIC associada	Ação do PDTIC
N1. Implementação de processos de governança e gestão de TI	M1. Prover serviços de apoio à gestão e à fiscalização de contratos de TI	Implementar processo de gestão de vulnerabilidades de Segurança da Informação
N4. Provimento, manutenção e atualização do parque de equipamentos e infraestrutura de redes	M6 - Prover equipamentos e serviços de infraestrutura e manter alta disponibilidade do ambiente tecnológico do Ministério	Prover soluções e serviços de correio eletrônico, banco de dados, rede de comunicação, armazenamento e backup
N5. Aprimoramento dos processos de Segurança da Informação	M7 – Prover e prospectar soluções e conscientização para segurança da informação	Prover soluções de segurança da informação e comunicações

Fonte da informação: https://www.gov.br/mcom/pt-br/arquivos/comites/cgd/pdtic_mcom_23-24_v1.0

3.4. Ressalta-se que o objeto dessa contratação não tem por objetivo a oferta digital de serviços públicos.

4. REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio:

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

4.1.1. Manter a confidencialidade, integridade e disponibilidade do ambiente tecnológico;

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

4.1.3. Garantir a disponibilidade, continuidade e qualidade dos serviços para o cumprimento das atividades finalísticas do Ministério e, consequentemente, o alcance dos resultados desejados para a sociedade;

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

Requisitos de Capacitação

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

4.2.1. 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.

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

Requisitos Legais

4.3. 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), Lei n° 10.520, de 17 de julho de 2001, Decreto 10.024, de 20 de setembro de 2019, e a outras legislações aplicáveis;

4.4. A contratada deverá se submeter a Política de Segurança da Informação (POSIC) do Ministério das Comunicações, nos termos da Portaria MCOM nº 2.454 de 22 de abril de 2021.

Requisitos Temporais

4.5. Os serviços referentes aos Itens 01 e 05 devem ser iniciados no prazo máximo de 60 dias corridos, a contar do recebimento da Ordem de Serviço (OS), emitida pela Contratante. Em circunstâncias excepcionais e devidamente justificadas pelo CONTRATADO, esse prazo poderá ser prorrogado por um período equivalente, mediante autorização prévia da CONTRATANTE;

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

4.5.2. Os serviços serão prestados em Brasília/DF, na Esplanada dos Ministérios, Bloco “R” e Anexo, Térreo, Ministério das Comunicações.

4.6. Os serviços previstos no Item 06 devem ser iniciados no prazo máximo de 5 (cinco) dias corridos, a contar do recebimento da Ordem de Serviço (OS), emitida pela Contratante. Em circunstâncias

excepcionais e devidamente justificadas pelo CONTRATADO, esse prazo poderá ser prorrogado por um período equivalente, mediante autorização prévia da CONTRATANTE;

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

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

Requisitos de Sustentabilidade e Sociais, Ambientais e Culturais

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

4.9.1. Nesta contratação, não se aplicam critérios de sustentabilidade específicos listados no Guia Nacional de Contratações Sustentáveis, elaborado pela Câmara Nacional de Sustentabilidade da Controladoria Geral da União/Advocacia Geral da União, e suas atualizações. O escopo da contratação envolve o licenciamento de softwares e serviços, sem a inclusão de fornecimento de mão de obra. Portanto, não foram identificados elementos específicos de sustentabilidade aplicáveis ao objeto.

Requisitos da Arquitetura Tecnológica

4.10. Os serviços deverão observar integralmente os requisitos de arquitetura tecnológica descritos no subitem 2 deste Termo de Referência, bem como aqueles especificados no Anexo A;

4.10.1. 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.

Requisitos de Projeto e de Implementação

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

4.11.1. Todas as subscrições e licenciamentos previstos e necessários para a execução dos serviços devem ser entregues, instalados e configurados na Infraestrutura do MCom.

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

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

4.11.3.1. Definição do escopo;

4.11.3.2. Definição de quais tarefas deverão ser realizadas para implementação e configuração dos itens;

4.11.3.3. Cronograma de Implantação; e

4.11.3.4. Plano de arquitetura e desenho da solução.

4.11.4. O Plano de Projeto deverá ser aprovada pela CONTRATANTE.

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

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

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

Requisitos de Implantação

4.12. Os serviços deverão observar integralmente os requisitos de Projeto e Implementação previstos neste Termo de Referência. Deverá, ainda, observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

4.12.1. 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;

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

Requisitos de Garantia, Manutenção e Assistência Técnica

4.13. A garantia dos serviços devem ser compatíveis e respeitar o período de vigência contratual;

4.14. A garantia deverá abranger todas as atualizações de versões de software utilizados para o fornecimento dos serviços;

Requisitos de Experiência Profissional e Formação de Equipe

4.15. Os requisitos de experiência profissional e formação de equipe, quando aplicável, estão descritos no nas especificações contidas no Anexo A, apêndice deste Termo de Referência.

Requisitos de Metodologia de Trabalho

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

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

4.18. O Contratado deve fornecer meios para contato e registro de ocorrências com funcionamento 24 horas por dia e 7 dias por semana de maneira eletrônica.

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

Requisitos de Segurança da Informação e Privacidade

4.20. A solução deverá atender integralmente aos princípios e procedimentos elencados na Política de Segurança da Informação do Ministério das Comunicações.

Vistoria

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

Indicação de marcas ou modelos (Art. 41, inciso I, da Lei nº 14.133, de 2021):

4.22. Na presente contratação será admitida a indicação de marca, característica ou modelo, de acordo com os detalhamentos pormenorizados nos Estudos Técnicos Preliminares e no Anexo A deste Termo de Referência visando compatibilidades técnicas para o ambiente em que os serviços serão executados.

Subcontratação

4.23. Não é admitida a subcontratação do objeto contratual.

Garantia da Contratação

4.24. 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.

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

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

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

Informações relevantes para o dimensionamento da proposta

4.28. Em conformidade com os Estudos Técnicos Preliminares, que fazem parte integrante deste processo de contratação, esta demanda abrange aprimoramentos e expansões nos níveis de defesa cibernética do Ministério das Comunicações.

4.29. O ambiente em questão deverá suportar a quantidade de usuários e equipamentos já definidos em tópicos anteriores.

4.30. Será permitido a utilização do sistema de virtualização da CONTRATANTE para instalação de componentes que sejam pré-requisitos para funcionamento completo da solução.

4.31. Os itens que compõe a contratação se integram para atender às funcionalidades de defesa cibernética necessárias para o ambiente do MCom e, portanto, o parcelamento não é considerado viável do ponto de vista técnico.

> 4.31.1. Do ponto de vista da eficiência técnica, a contratação em um único grupo é mais vantajosa, pois permite a plena integração entre as ferramentas, com visibilidade das vulnerabilidades e correção automatizada dessas vulnerabilidades encontradas, incluindo simulações de ataques para verificar a eficácia das correções e dos ambientes de segurança que irão apontar falhas não relacionadas a vulnerabilidades conhecidas. Além disso, por se tratar de uma solução composta por múltiplos serviços integrados, cada um com características e resultados finais diferentes, mas interligados, é fundamental garantir a qualidade dos serviços prestados por um mesmo prestador, visando otimizar custos e facilitar a gestão em um único contrato, reduzindo o tempo de serviço quando surgem problemas. Não há prejuízo à ampla competividade, uma vez que existem várias empresas no mercado com capacidade de fornecer os serviços na forma em que estão agrupados.
>
> 4.31.2. Conforme deliberações do TCU sobre a matéria, como a decisão que afirma que "***A aquisição de itens diversos em lotes deve estar respaldada em critérios justificantes***", adotando o entendimento do Acórdão nº 5260/2011, de 06/07/2011, que decidiu que "***Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si***".
>
> 4.31.3. Justifica-se a necessidade de um lote único que agrupe todos os itens para adquirir uma solução de gestão do ciclo de vida de vulnerabilidades de segurança, atendendo às necessidades do Ministério conforme as especificações técnicas e quantidades descritas neste documento.

4.31.4. Fundamenta-se ainda na necessidade de integração entre os componentes geridos por uma única empresa contratada, reduzindo o tempo de resposta caso ocorram problemas e proporcionando maior efetividade e entrega de informações integradas que consolidem os resultados dos diversos componentes implantados.

4.31.5. Resta claro que o agrupamento dos itens não é opcional, mas sim, rigorosamente necessário para uma manutenção efetiva das licenças de software e serviços exclusivos ao software adquirido, não cabendo, assim, dividir o fornecimento do objeto por item.

4.32. Para calcular os custos unitários dos itens do Grupo/Lote 1, as licitantes devem incluir os custos relacionados aos serviços de instalação da solução.

4.33. A contratação resultará na celebração de uma Ata de Registro de Preço (ARP) por meio do Sistema de Registro de Preço (SRP). Durante a vigência da ARP, o Ministério das Comunicações terá a flexibilidade de requisitar qualquer quantidade dos itens registrados, seja em uma única Ordem de Fornecimento de Bens ou em ordens sucessivas, respeitando os limites das quantidades registradas.

4.34. A participação de consórcios no certame que se originará do presente Termo de Referência não será permitida. Isso se deve ao fato de que a complexidade e o vulto do objeto não restringem a participação de fornecedores aptos a executar o objeto.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

5.1.1. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

5.1.2. encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

5.1.3. receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.4. aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

5.1.5. liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

5.1.6. comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.1.7. definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do contratado, com base em pesquisas de mercado, quando aplicável;

5.1.8. prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer;

5.2. São obrigações do CONTRATADO

5.2.1. indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;

5.2.2. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

5.2.3. reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

5.2.4. propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

5.2.5. manter, durante toda a execução do contrato, as mesmas condições da habilitação;

5.2.6. quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

5.2.7. quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

5.2.8. ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

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

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

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

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

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

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

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

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

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

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

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

6. MODELO DE EXECUÇÃO DO CONTRATO

Condições de execução

6.1. A execução do objeto seguirá a seguinte dinâmica:

6.1.1. O gestor do contrato emitirá a Ordem de Serviço para a entrega dos bens especificados ou início da execução dos serviços.

6.1.2. O início da execução do objeto deverá ocorrer conforme os prazos previstos nos subitens **4.5** e **4.6** do Termo de Referência, a saber:

6.1.2.1. O prazo de entrega dos serviços especificados nos itens 1, 2, 3, 4 e 5 é de 60 dias corridos, contados do recebimento da Ordem de Serviço. O prazo de entrega poderá ser prorrogado, excepcionalmente, por até igual período, desde que justificado previamente pelo CONTRATADO e autorizado pela CONTRATANTE;

6.1.2.2. Os serviços previstos no Item 06 devem ser iniciados no prazo máximo de 5 (cinco) dias corridos, a contar do recebimento da Ordem de Serviço (OS), emitida pela Contratante. Em circunstâncias excepcionais e devidamente justificadas pelo CONTRATADO, esse prazo poderá ser prorrogado por um período equivalente, mediante autorização prévia da CONTRATANTE

6.1.2.3. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 10 (dez) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

Local e horário da prestação dos serviços

6.2. Os serviços serão prestados em Brasília/DF, na Esplanada dos Ministérios, Bloco “R” e Anexo, Térreo, Ministério das Comunicações.

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

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

6.4. O prazo de garantia contratual dos serviços é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

Formas de transferência de conhecimento

6.5. A transferência do conhecimento deverá ser realizada observando-se os requisitos de capacitação já definidos neste Termo de Referência.

Procedimentos de transição e finalização do contrato

6.6. Ao final do contrato, a CONTRATADA deverá fornecer todas as informações, documentações, processos e demais informações necessárias para finalização e transição do contrato;

6.7. Cada Ordem de Serviço conterá a quantidade a ser fornecida, incluindo a sua localização e o prazo, conforme definições deste Termo de Referência.

Quantidade mínima de serviços para comparação e controle

6.8. Cada OS conterá o volume de serviços demandados, incluindo a sua localização e o prazo, conforme modelo descrito no **Anexo F**.

Mecanismos formais de comunicação

6.9. S***ão definidos como mecanismos formais de comunicação, entre a Contratante e o Contratado, os seguintes:***

6.9.1. Ordem de Serviço;

6.9.2. Ata de Reunião;

6.9.3. Ofício;

6.9.4. Sistema de abertura de chamados;

6.9.5. E-mails e Cartas;

Formas de Pagamento

6.10. 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

6.11. 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.

6.12. 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 D e E deste Termo de Referência.

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. Considerando as características do objeto, não será necessário que a Contratada mantenha o preposto da empresa no local da execução do objeto.

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 10 (dez) 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;
Fiscalização

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

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.

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

8.1. A avaliação da qualidade dos itens 1, 2, 3, 4 e 5, quando entregues, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:

8.1.1. Todos os licenciamentos referentes aos softwares utilizados pelas soluções devem estar registrados para utilização da CONTRATANTE, em modo subscrição (assinatura), legalizado, não sendo admitidas versões “shareware” ou “trial”.

8.1.2. Só haverá o recebimento definitivo, após a finalização da implementação de todas as licenças necessárias, proporcionando a operacionalização de todas as características expostas neste Termo de Referência, assim como a entrega da documentação de projeto que comprove tais fatos.

8.2. Quanto a avaliação da qualidade do item 6, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:

8.2.1. Deverá ser aferido mensalmente, mediante a entrega de relatórios que comprovem a execução dos serviços expostos no termo de referência;

8.3. A avaliação da execução do objeto utilizará o Instrumento de Medição de Resultado (IMR), conforme previsto no Anexo I;

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

8.4.1. não produzir os resultados acordados;

8.4.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

8.4.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

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

Do recebimento

8.6. Os serviços serão recebidos provisoriamente, no prazo de 05 (cinco) dias, 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).

8.6.1. 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.

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

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

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

8.10. Para efeito de recebimento provisório, 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.

8.10.1. 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;

8.11. 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.

8.12. 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)

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

8.14. 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.

8.15. 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.

8.16. 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:

8.16.1. 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).

8.16.2. 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;

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

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

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

8.17. 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.

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

8.19. 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.

8.20. O pagamento para os itens 1, 2, 3, 4 e 5 será efetuado em parcela única, após a entrega dos serviços, conforme estipulado no Instrumento de Medição de Resultado (IMR);

8.21. O pagamento para o item 6 será realizado após as medições estabelecidas Instrumento de Medição de Resultado (IMR);

Procedimentos de Teste e Inspeção

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

8.22.1. O Instrumento de Medição de Resultados (IMR), contido no ANEXO I - Instrumento de Medição de Resultado (IMR) deste Termo de Referência, fixa os critérios de aceitação do serviço prestado, abrangendo as métricas, indicadores e níveis mínimos de serviço, bem como eventuais fixações de valores para retenção ou glosa no pagamento.

8.22.2. Além disso, será verificado se a entrega dos bens está de acordo com o Termo de Referência e a Proposta Comercial da Contratada.

Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

8.23. Comete infração administrativa a CONTRATADA que cometer quaisquer das infrações previstas no art. 155 da Lei nº 14.133, de 2021, quais sejam:

8.23.1. dar causa à inexecução parcial do contrato;

8.23.2. dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

8.23.3. dar causa à inexecução total do contrato;

8.23.4. deixar de entregar a documentação exigida para o certame;

8.23.5. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

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

8.23.7. ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

8.23.8. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

8.23.9. fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

8.23.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

8.23.11. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances;

8.23.12. praticar atos ilícitos com vistas a frustrar os objetivos deste certame;

8.23.13. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

8.24. A CONTRATADA que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

8.24.1. 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;

8.24.2. Multa de 5% (cinco por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta da CONTRATADA, por qualquer das infrações dos subitens 8.23.1 a 8.23.13;

8.25. Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, nos casos dos subitens 8.23.2 a 8.23.7, quando não se justificar a imposição de penalidade mais grave;

8.26. Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 8.23.8 a 8.23.13, bem como nos demais casos que justifiquem a imposição da penalidade mais grave;

8.27. Para a aplicação das sanções previstas serão considerados:

8.27.1. a natureza e a gravidade da infração cometida;

8.27.2. as peculiaridades do caso concreto;

8.27.3. as circunstâncias agravantes ou atenuantes;

8.27.4. os danos que dela provierem para a Administração Pública;

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

8.28. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

8.29. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

8.30. Se, durante o processo de aplicação de penalidade, 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.

8.30.1. 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.

8.30.2. 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.

8.31. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao fornecedor/adjudicatário, observando-se o procedimento previsto na Lei nº 14.133, de 2021, e subsidiariamente na Lei nº 9.784, de 1999.

8.32. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, também será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada e prevista no Instrumento de Medição de Resultado (IMR), contido no ANEXO I deste Termo de Referência, sem prejuízo das sanções cabíveis, nos casos em que o contratado:

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

8.32.2. 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

8.33. 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.

8.34. 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.

8.35. 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:

8.35.1. o prazo de validade;

8.35.2. a data da emissão;

8.35.3. os dados do contrato e do órgão contratante;

8.35.4. o período respectivo de execução do contrato;

8.35.5. o valor a pagar; e

8.35.6. eventual destaque do valor de retenções tributárias cabíveis.

8.36. 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;

8.37. 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.

8.38. 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)

8.39. 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.

8.40. 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.

8.41. 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.

8.42. 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

8.43. 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.

8.44. 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 Custos da Tecnologia da Informação (ICTI) de correção monetária, calculado e divulgado pelo Instituto de Pesquisa Econômica Aplicada (IPEA).

Forma de pagamento

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

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

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

8.48. 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.

8.49. 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.

Cessão de crédito

8.50. 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.

8.50.1. As cessões de crédito não fiduciárias dependerão de prévia aprovação do contratante.

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

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

8.53. 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).

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

9. SELEÇÃO DO FORNECEDOR E REGIME EXECUÇÃO

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.

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 Municipal/Distrital 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 Municipal/Distrital 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 Municipal/Distrital 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 capital mínimo de 5% 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).

Qualificação Técnica

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

9.27.1. A declaração acima poderá ser substituída por declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação

9.28. 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.

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

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

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

9.29.3. Se referir a fornecimentos de soluções e serviços de cibersegurança compatíveis e similares com o objeto contido neste Termo de Referência.

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

9.31. 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.

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

9.32.1. 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;

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

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

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

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

9.32.6. 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;

9.32.7. 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.

10. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

10.1. O custo estimado total da contratação é de **R$ 6.053.834,96 (seis milhões, cinquenta e três mil, oitocentos e trinta e quatro reais e noventa e seis centavos)**, conforme custos unitários apostos na Tabela 1 do subitem 1 deste Termo de Referência.

10.2. A estimativa de preço foi realizada para a elaboração do orçamento detalhado, composta por preços unitários e fundamentada em pesquisa de preço realizada em conformidade com o art.20 da Instrução Normativa SGD/ME nº 94 /2022.

10.3. Em caso de licitação para Registro de Preços, os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

10.3.1. em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos do disposto na alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

10.3.2. em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

10.3.3. serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação; ou

10.3.4. poderão ser repactuados, a pedido do interessado, conforme critérios definidos para a contratação.

11. ADEQUAÇÃO ORÇAMENTÁRIA

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

11.2. **A contratação será atendida pela seguinte dotação: Programa de Trabalho 24.122.0032.2000.0001 Administração da Unidade, Plano Orçamentário 0001 - Sustentação e Modernização dos Serviços de Tecnologia de Informação e Comunicações, a ser custeado com dotação consignada na Lei Orçamentária Anual - LOA 2023, Lei nº 14.535, de 17 de janeiro de 2023.**

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

Cronograma Físico Financeiro

ITEM	ETAPA DA EXECUÇÃO DO OBJETO	MEDIÇÃO
1, 2, 3, 4 e 5	A Contratada deverá entregar todos os serviços relacionados na Ordem de Serviço no prazo máximo de 60 dias corridos, contados a partir do recebimento da OS.	Liquidação: O pagamento de 100% do valor da parcela relacionada aos itens mencionados na Ordem de Serviço deverá ser efetuado em até 10 dias após o recebimento pela Contratante da nota fiscal ou documento de cobrança equivalente, com possibilidade de prorrogação por igual período, de acordo com o art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022, e condicionado à emissão do Termo de Recebimento Definitivo (TRD)
6	A Contratada deverá iniciar a execução dos serviços no prazo máximo de 5 dias corridos, contados a partir do recebimento da OS.	Liquidação: O pagamento será computado mensalmente de acordo o previsto no Instrumento de Medição de Resultados (IMR).

12. INFORMAÇÕES COMPLEMENTARES

12.1. O conteúdo deste Termo de Referência compatibiliza-se com o modelo "Termo de Referência Serviços de TIC - LICITAÇÃO", elaborado pela Secretaria de Gestão, complementado e uniformizado pela Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União da AGU, atualizado em maio de 2023 e disponível em: https://www.gov.br/governodigital/pt-br/contratacoes/templates-e-listas-de-verificacao, acesso em 20/10/2023.

13. 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.

Despacho: Termo de Referência elaborado em conformidade com a Instrução Normativa SGD/ME nº 94/2022.

MICHEL GULARTE RECONDO

Integrante Requisitante

Assinou eletronicamente em 30/11/2023 às 15:32:45.

Despacho: Termo de Referência elaborado em conformidade com a Instrução Normativa SGD/ME nº 94/2022.

JOSE CARLOS DE ALBUQUERQUE

Integrante Técnico substituto

Despacho: Termo de Referência elaborado em conformidade com a Instrução Normativa SGD/ME nº 94/2022.

HENRIQUE ULISSES DE ABREU

Integrante Administrativo

Assinou eletronicamente em 30/11/2023 às 15:22:22.

Despacho: Aprovo o presente Termo de Referência e os seus anexos.

GUSTAVO HENRIQUE DE SOUTO SILVA

Autoridade Máxima de TIC e Autoridade Competente

 *Assinou eletronicamente em 30/11/2023 às 15:51:47.*

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 Referência - Anexo A.pdf (1.14 MB)
- Anexo II - Termo de Referência - Anexos B_ C_ D_ E_ F_ G_ H_ I.pdf (201.3 KB)

Anexo I - Termo de Referência - Anexo A.pdf

ANEXO A

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS

A solução de TIC consiste no fornecimento das seguintes plataformas, componentes e serviços conforme especificações técnicas detalhadas abaixo:

1. Item1 - Solução de gerenciamento de vulnerabilidades de segurança

1.1. Características gerais

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

1.1.2. Deve estar licenciada para no mínimo 1500 ativos.

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

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

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

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

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

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

1.1.8. A solução deve possuir integração via API no mínimo as seguintes linguagens: Python, Powershell, Ruby, javascript, Java, Swift e PHP;

1.1.9. A solução deve possuir métodos de consulta via api e envio, tais como: HTTP METHOD (POST, GET, PUT AND DELETE);

1.1.10. A solução deve incluir a opção para agentes instalados e licenciados em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

1.1.10.1. Tais agentes devem ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades;

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

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

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

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

1.1.14. O acesso a console de gerenciamento deve ser fornecida para pelo menos 10 usuários simultâneos;

1.1.15. A solução deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM);
1.1.16. A solução deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção;
1.1.17. A solução deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (outputs);
1.1.18. A solução deve fornecer controle de acesso baseado em função (*RBAC- Role Based Access Control*) para controlar o acesso do usuário a conjuntos de dados e funcionalidades;
1.1.19. A solução deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e dashboards;
1.1.20. A solução deve ter a capacidade de excluir determinados endereços IP do escopo de qualquer varredura ou scan;
1.1.21. A solução deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito;
1.1.22. A solução deve suportar métodos de autenticação usando bases de autenticação local, como Active Directory, e SAML (Security Assertion Markup Language) para uso de SSO (Single Sign-On);
1.1.23. A solução deve ser capaz de orquestrar scanners ilimitados dentro da infraestrutura;
1.1.24. A solução não deve impor nenhum limite de quantidade de scanners implementados dentro da infraestrutura;
1.1.25. A solução deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de email;
1.1.26. A solução deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características:
1.1.26.1. Sistema Operacional, Endereço IP, DNS, NetBIOS Host, MAC, AWS Instance Type, AWS EC2 Name, Software instalado, Azure VM ID, AWS Region, Google Cloud Instance ID, Azure Resource ID, Ativos avaliados;

1.2. Dos requisitos e relatórios e painéis gerenciais

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

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

1.3. Das varreduras

1.3.1. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como appliances virtuais;
1.3.2. A solução deve suportar varredura com e sem agente, de maneira ativa e passiva, distribuídas em diferentes localidades e regiões e gerenciar todos por uma console central;
1.3.3. A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de vulnerabilidades;
1.3.4. Tais agentes devem realizar conexões para o sistema gerenciamento através de protocolo seguro;
1.3.5. A solução deve ser configurável para permitir a otimização das configurações de varredura;
1.3.6. A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;
1.3.7. A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
1.3.8. A solução deve se integrar com solução de gerenciamento de acessos privilegiados para autenticação nos dispositivos, no mínimo, os seguintes:
    1.3.8.1. CyberArk;
    1.3.8.2. BeyondTrust;
    1.3.8.3. Thicotic
    1.3.8.4. Centrify;
1.3.9. A solução deve suportar o agendamento de scans personalizados, incluindo a capacidade de executar varreduras em tempos designados, com frequência pré-determinada;
1.3.10. A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de scan;
1.3.11. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
1.3.12. A solução deve ser capaz de realizar em tempo real a descoberta de vulnerabilidades nas seguintes tecnologias:
    1.3.12.1. Cloud Services;
    1.3.12.2. Data Leakage;
    1.3.12.3. Database;
    1.3.12.4. IoT;
    1.3.12.5. Mobile Devices;

1.3.12.6. Operating System;
1.3.12.7. Peer-To-Peer;
1.3.12.8. SCADA;
1.3.12.9. Web Servers;
1.3.12.10. Web Clients;

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

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

1.4. Da análise e priorização de vulnerabilidades

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

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

1.4.2.1. CVSS Impact Score;
1.4.2.2. Idade da Vulnerabilidade;
1.4.2.3. Maturidade de códigos de exploração da vulnerabilidade encontrada;
1.4.2.4. Frequência de uso da vulnerabilidade em ataques e campanhas atuais;
1.4.2.5. Disponibilidade do código de exploração da vulnerabilidade;
1.4.2.6. Presença de módulos de exploração de vulnerabilidade em frameworks automatizados de exploração de vulnerabilidades como CANVAS, Metasploit e Core Impact;
1.4.2.7. Popularidade da vulnerabilidade em fóruns e comunicações na Darkweb;

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

1.5. Da Análise de Risco do Ambiente

1.5.1. A solução deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;

1.5.2. O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;

1.5.3. Deve ser capaz de calcular a criticidade dos ativos da organização;

1.5.4. A solução deve ser capaz de realizar um benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor;

1.5.5. A solução deve prover visão sobre quais ações de remediação reduzem o maior nível de risco do ambiente;

1.5.6. A solução deve também permitir a visualização de ações de remediação agregadas para visão consolidada de redução de risco;

1.5.7. Deve permitir modificar a qualquer momento o tipo de indústria para comparação. Ex: Mudar de Setor Público para Mercado Financeiro;

1.5.8. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;

1.5.9. A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo);
1.5.10. A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos;
1.5.11. A solução deve oferecer uma capacidade de comparação (benchmarking) da pontuação referente a exposição cibernética com outros players da mesma indústria assim como outras empresas do mercado;
1.5.12. A solução deve permitir um acompanhamento histórico do nível de exposição da organização;
1.5.13. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução;
1.5.14. A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade;
1.5.15. A solução deve permitir a segregação lógica entre áreas distintas da empresa afim de obter a pontuação referente exposição cibernética por área;

1.6. Da descoberta de ativos

1.6.1. A solução deve ser capaz de realizar escaneamento de descoberta de rede utilizando os seguintes critérios como alvo: IP, CIRD e Range;
1.6.2. A solução deve disponibilizar modelos de escaneamento de descoberta, ajustável, com os seguintes tipos de scan:
    1.6.2.1. Enumeração de Hosts;
    1.6.2.2. Identificação de Sistema Operacional (SO);
    1.6.2.3. Port Scan (Portas comuns);
    1.6.2.4. Port Scan (Todas as portas);
    1.6.2.5. Customizado;
1.6.3. A solução deve permitir realizar escaneamento de descoberta customizado podendo ser parametrizado de acordo com a necessidade;
1.6.4. A parametrização do escaneamento de descoberta deve, no mínimo, conter os seguintes requisitos:
    1.6.4.1. Descoberta de Host;
    1.6.4.2. Ping o host remoto;
    1.6.4.3. Usar descoberta rápida;
    1.6.4.4. Métodos de ping;
        1.6.4.4.1. ARP;
        1.6.4.4.2. TCP;
        1.6.4.4.3. ICMP;
        1.6.4.4.4. UDP;
    1.6.4.5. Escaneamento de descoberta de dispositivos de OT/SCADA;
    1.6.4.6. Escaneamento de descoberta em redes de impressora;
1.6.5. Port Scanning:
    1.6.5.1. Portas;

1.6.5.1.1. Considerar portas não escaneadas como fechadas;
1.6.5.1.2. Range de portas a serem escaneadas;
1.6.5.2. Enumerar Portas locais:
1.6.5.2.1. SSH;
1.6.5.2.2. WMI;
1.6.5.2.3. SNMP;
1.6.6. Descoberta de Serviços:
1.6.6.1. Sondar todas as portas para encontrar serviços;
1.6.6.2. Procurar por serviços baseado em SSL/TLS;
1.6.6.3. Enumerar todas as cifras SSL/TLS;
1.6.7. A solução deve realizar descoberta de ativo de forma passiva e adicionado automaticamente na console de gerenciamento;
1.6.8. A solução deve descobrir passivamente quando um host é adicionado na rede;

1.7. Da avaliação de vulnerabilidade

1.7.1. A solução deve ser capaz de realizar testes sem a necessidade de agentes instalados no dispositivo destino para detecção de vulnerabilidades;
1.7.2. A solução deve detectar e classificar através de severidades, riscos e vulnerabilidades;
1.7.3. A solução deve também fornecer informações detalhadas sobre a natureza da vulnerabilidade, evidências da existência da vulnerabilidade e recomendações para mitigá-los;
1.7.4. A solução deve incluir uma saída detalhada das vulnerabilidades descobertas como versões de DLL esperadas e encontradas;
1.7.5. A solução deve ser compatível com CVE e fornecer pelo menos 10 anos de cobertura CVE;
1.7.6. A solução deve identificar vulnerabilidades especificas para o Active Directory com os seguintes padrões de verificação;
1.7.6.1. Contas administrativas vulneráveis a Kerberoasting attack;
1.7.6.2. Ultilização de criptografia vulnerável com autenticação Kerberos;
1.7.6.3. Contas com pré-autenticação do Kerberos desabilitada;
1.7.6.4. Verificação de usuários com a opção de nunca expirar a senha com a opção habilitada;
1.7.6.5. Verificar validação de fragilidades do tipo “Unconstrained Delegation”;
1.7.6.6. Verificação de “Pre-Windows 2000 Compatible Access”;
1.7.6.7. Verificação de validade de chaves mestras "Kerberos KRBTGT”;
1.7.6.8. Verificação de “SID History Injection”;
1.7.6.9. Verificação de “Printer Bug Exploit”;
1.7.6.10. Verificação de “Primary Group ID”;
1.7.6.11. Verificação de usuários com Passwords em branco;
1.7.7. A solução deve suportar o uso de SMB e WMI para verificação de sistemas Microsoft Windows;
1.7.8. A solução deve ser capaz de iniciar automaticamente serviços de registro remoto em sistemas Windows ao executar uma varredura credenciada;
1.7.9. A solução deve ser capaz de parar automaticamente o serviço de registro remoto em sistemas Windows novamente assim que a varredura estiver completa;

1.7.10. O scanner deve oferecer suporte a shell seguro (SSH) com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix;
1.7.11. A solução deve fornecer auditoria de patch (MS Bulletins) para as principais versões de Windows;
1.7.12. A solução deve fornecer varredura para aplicativos comerciais diversos e proprietários, incluindo, mas não limitando-se a: Java, Adobe, Oracle, Apple, Microsoft, Check Point, Palo Alto Networks, Cisco, Fortinet, Fireeye, McAfee, etc;
1.7.13. A solução deve incluir classificação de severidades de acordo com o padrão Sistema Comum de Pontuação de Vulnerabilidade Versão (CVSS2 e CSVSS 3);
1.7.14. A solução deve fornecer informações acerca da disponibilidade de códigos de exploração das vulnerabilidades encontradas em frameworks de exploração para as plataformas mais populares: Core, Metasploit e Canvas;
1.7.15. A solução deve informar se a vulnerabilidade pode e está sendo ativamente explorada por código malicioso (malware);
1.7.16. A solução deve possuir importação de arquivos .YARA;
1.7.17. Deve ser capaz de identificar e classificar vulnerabilidades de máquinas virtuais em nuvem pública em infraestruturas como serviço nas plataformas AWS, Microsoft Azure e Google Cloud;

1.8. Da auditoria de Configuração

1.8.1. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;
1.8.2. A solução deve fornecer benchmarks de auditoria de segurança e configuração para conformidade regulatória e outros padrões de práticas recomendadas pela área ou fabricantes;
1.8.3. A solução deve realizar verificações de auditoria contendo as de segurança, com indicação de sucesso ou falha, baseado nos principais frameworks reconhecidos pela indústria, pelo menos os seguintes:
1.8.3.1. Center for Internet Security Benchmarks (CIS);
1.8.3.2. Defense Information Systems Agency (DISA) STIGs;
1.8.3.3. Health Insurance Portability and Accountability Act (HIPAA);
1.8.3.4. Payment Card Industry Data Security Standards (PCI DSS);
1.8.4. A solução deve fornecer auditoria de programas antivírus para determinação de presença e status de inicialização;
1.8.5. A solução deve fornecer auditorias de configuração com base benchmarks em CIS (Center for Internet Security) L1 e L2, para ambos os sistemas operacionais Microsoft Windows e Linux;
1.8.6. A solução deve permitir auditoria de conformidade em servidores Windows, Linux, Bancos de Dados SQL Server, a fim de determinar se estão configurados de acordo com os principais Framework de segurança como, por exemplo, CIS e DISA;
1.8.7. A solução deve oferecer validação e suporte a SCAP (Security Content Automation Protocol);

1.9. Análise dinâmica de vulnerabilidades para aplicações Web

1.9.1. A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;
1.9.2. A solução deve ser capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);
1.9.3. Deve estar licenciado para no mínimo 5 FQDNs simultâneos;
1.9.4. A solução deve avaliar no mínimo os padrões de segurança OWASP Top 10;
1.9.5. A solução deve possuir templates prontos de varreduras entre simples e extensos;
1.9.6. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:
    1.9.6.1. Cookies, Headers, Formulários e Links;
    1.9.6.2. Nomes e valores de parâmetros da aplicação;
    1.9.6.3. Elementos JSON e XML;
    1.9.6.4. Elementos DOM;
1.9.7. A solução deve permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;
1.9.8. A solução deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;
1.9.9. A solução deve excluir determinadas URLs da varredura através de expressões regulares;
1.9.10. A solução deve excluir determinados tipos de arquivos através de suas extensões;
1.9.11. A solução deve instituir no mínimo os seguintes limites:
    1.9.11.1. Número máximo de URLs para crawl e navegação;
    1.9.11.2. Número máximo de diretórios para varreduras;
    1.9.11.3. Número máximo de elementos DOM;
    1.9.11.4. Tamanho máximo de respostas;
    1.9.11.5. Limite de requisições de redirecionamentos;
    1.9.11.6. Tempo máximo para a varredura;
    1.9.11.7. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;
    1.9.11.8. Número máximo de requisições HTTP por segundo;
1.9.12. A solução deve detectar congestionamento de rede e limitar os seguintes aspectos da varredura:
    1.9.12.1. Limite em segundos para timeout de requisições de rede;
    1.9.12.2. Número máximo de timeouts antes que a varredura seja abortada;
1.9.13. A solução deve agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
1.9.14. A solução deve enviar notificações através de no mínimo E-mail;
1.9.15. A solução deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques;
1.9.16. A solução deve avaliar sistemas web utilizando protocolos HTTP e HTTPs;
1.9.17. A solução deve possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizado a ser enviada durante os testes;
1.9.18. A solução deve ser compatível com avaliação de web services REST e SOAP;
1.9.19. Deverá suportar no mínimo os seguintes esquemas de autenticação:
    1.9.19.1. Autenticação básica (digest);
    1.9.19.2. NTLM;
    1.9.19.3. Form de login;
    1.9.19.4. Autentiçação de Cookies;

1.9.19.5. Autenticação através de Selenium;
1.9.19.6. Autenticação através de Bearer;
1.9.20. A solução deve importar scripts de autenticação selenium previamente configurados pelo usuário;
1.9.21. A solução deve customizar parâmetros Selenium como delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos;
1.9.22. A solução deve exibir os resultados das varreduras em tendência temporal para acompanhamento de correções e introdução de novas vulnerabilidades;
1.9.23. A solução deve exibir os resultados agregados de acordo com as categorias do OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project);
1.9.24. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
1.9.25. Para cada vulnerabilidade encontrada, devem ser exibidas as evidências dela em seus detalhes;
1.9.26. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc), deve evidenciar nos detalhes do evento encontrado:
1.9.26.1. Payload injetado;
1.9.26.2. Evidência em forma de resposta da aplicação;
1.9.26.3. Detalhes da requisição HTTP;
1.9.26.4. Detalhes da resposta HTTP;
1.9.27. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;
1.9.28. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;
1.9.29. A solução deve possuir suporte a varreduras de componentes como as linguagens de programação, os frameworks (AngularJS), servidores Web (Nginx e Apache Tomcat) e os CMS (Wordpress, Joomla, Drupal, Magento.

1.10. Análise em ambiente Microsoft Active Directory

1.10.1. A solução deve ser capaz de identificar vulnerabilidades ocultas em configurações dedicadas ao Active Directory;
1.10.2. A solução deve oferecer medidas preventivas de hardening para o Active Directory;
1.10.3. A solução deve ter a capacidade de identificar ataques específicos direcionados à estrutura do Active Directory (AD);
1.10.4. A solução deve fornecer análises detalhadas de cada configuração incorreta que represente riscos de segurança, apresentando informações de forma acessível e contextualizada para as equipes envolvidas;
1.10.5. A solução deve incluir recomendações de correção para cada configuração incorreta identificada no Active Directory;
1.10.6. A solução deve ter a capacidade de avaliar relações de confiança perigosas entre florestas e domínios;
1.10.7. A solução deve capturar as mudanças que ocorrem no AD e demostrar na console de administração;
1.10.8. A solução deve possuir dashboard com os principais ataques e vulnerabilidades por domínio;

1.10.9. A solução deve permitir a correlação de mudanças no Active Directory e desvios de segurança;
1.10.10. A solução deve analisar em detalhes um ataque explorando as descrições através do framework MITRE ATT&CK;
1.10.11. A solução deve prover interface web para gerenciamento de todas as funcionalidades;
1.10.12. A solução deve possuir capacidade nativa de criação de dashboards customizados;
1.10.13. A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;
1.10.14. A solução deve ter a capacidade de realizar alterações no Active Directory, seus objetos e atributos;
1.10.15. A solução não deve armazenar ou sincronizar nenhuma credencial de objetos do Active Directory;
1.10.16. A solução deve suportar ambientes com múltiplas florestas e domínios;
1.10.17. A solução deve suportar monitoramento contínuo de ambientes com Active Directory com o nível funcional de floresta e domínio a partir do 2003;
1.10.18. A solução deve suportar reter os eventos coletados por no mínimo um ano;
1.10.19. A solução deve descobrir e mapear a superfície de ataque do Active Directory e seus domínios monitorados com os seguintes padrões:
    1.10.19.1. Não depender de agentes ou sensores para coleta de informações do AD;
    1.10.19.2. A solução deve seguir as boas práticas de *menor privilégio,* a conta de serviço utilizada para conexão com o Active Directory, sendo o menor nível de acesso esperado para a conta de serviço como parte do grupo *Domain User*;
    1.10.19.3. Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles;
1.10.20. A solução deve analisar continuamente a postura de segurança do AD, minimamente avaliando:
    1.10.20.1. Validação de GPOs desvinculadas, desabilitadas ou órfãs;
    1.10.20.2. Validação de contas desativadas em grupos privilegiados;
    1.10.20.3. Domínio usando uma configuração perigosa de compatibilidade com versões anteriores por meio de alterações no atributo *dSHeuristics*;
    1.10.20.4. Validação de atributos relacionados a roaming de credenciais vulneráveis (*ms-PKI-DPAPIMasterKeys*) gerenciados por um usuário sem privilégios;
    1.10.20.5. Validação de domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como *NTLMv1;*
    1.10.20.6. Validação de contas com senhas que nunca expiram;
    1.10.20.7. Validação de senhas reversíveis em GPOs;
    1.10.20.8. Validação de uso de senhas reversíveis em contas de usuário;
    1.10.20.9. Validação de utilização de protocolo criptográfico fraco (Ex. DES) em contas de usuário;
    1.10.20.10. Validação de uso do LAPS (Solução de senha de administrador local) para gerenciar senhas de contas locais com privilégios;
    1.10.20.11. Validação se o domínio possui um nível funcional desatualizado;
    1.10.20.12. Validação de contas de usuário utilizando senha antiga;
    1.10.20.13. Validação se o atributo *AdminCount* está definido em usuários padrão;
    1.10.20.14. Validação do uso recente da conta de administrador padrão;

1.10.20.15. Validação de usuários com permissão para ingressar computadores no domínio;
1.10.20.16. Validação de contas dormentes;
1.10.20.17. Validação de computadores executando um sistema operacional obsoleto;
1.10.20.18. Validação de restrições de *logon* para usuários privilegiados em ambiente com múltiplos tiers (1, 2 e 3) de segregação de ativos;
1.10.20.19. Validação de direitos perigosos configurados no *Schema* do AD;
1.10.20.20. Validação de relação de confiança perigosa com outras *Florestas* e *Domínios*;
1.10.20.21. Validação de contas que possuem um atributo perigoso de histórico SID (*SID History*);
1.10.20.22. Validação de contas utilizando controle de acesso compatível com versões anteriores ao Windows 2000;
1.10.20.23. Validação da última alteração de senha do KDC;
1.10.20.24. Validação da última alteração da senha da conta SSO do *Azure AD*;
1.10.20.25. Validação de contas que podem ter senha em branco/vazia;
1.10.20.26. Validação de utilização do grupo nativo *Protected Users*;
1.10.20.27. Validação de privilégios sensíveis (Ex. *Debug a program, Replace a process level token, etc.)* perigosos atribuídos aos usuários;
1.10.20.28. Validação de possível senha em *clear-text*;
1.10.20.29. Validação de sanidade das GPOs e componentes CSEs (*Client-Side Extension*);
1.10.20.30. Validação de uso de algoritmos de criptografia fracos na PKI do Active Directory;
1.10.20.31. Validação de contas de serviço com SPN (*Service Principal Name*) que fazem parte de grupos privilegiados;
1.10.20.32. Validação de contas anormais nos grupos administrativos padrão do AD;
1.10.20.33. Validação de consistência no *container adminSDHolder*;
1.10.20.34. Validação de delegação *Kerberos* perigosa;
1.10.20.35. Validação em permissões de objetos raiz que permitem ataques do tipo DCSync;
1.10.20.36. Validação de políticas de senha fracas aplicadas aos usuários;
1.10.20.37. Validação das permissões relacionadas às contas do *Azure AD Connect*;
1.10.20.38. Validação do ID do grupo primário do usuário (*Primary Group ID*);
1.10.20.39. Validação de permissões em GPOs sensíveis associadas aos *Containers Configuration, Sites, Root Partition* e *OUs* sensíveis como *Domain Controllers;*
1.10.20.40. Controladores de domínio gerenciados por usuários ilegítimos;
1.10.20.41. Validação de certificado mapeado através de atributo *altSecurityIdentities* em contas privilegiadas;
1.10.20.42. Validação de uso de protocolo *Netlogon* inseguro (Zerologon/CVE-2020-1472);

1.10.21. A solução deve identificar vulnerabilidades e configurações incorretas do AD à medida que são introduzidas sendo:
1.10.21.1. Identificar todas as vulnerabilidades e configurações incorretas no AD;
1.10.21.2. Monitorar relações de confiança perigosas em toda a estrutura AD;

1.10.21.3. Apresentar ameaças e alterações sem a necessidade de scans estáticos e programados no Active Directory e sua infraestrutura;
1.10.21.4. Apresentar as ameaças e alterações em tempo real ou em menos de cinco minutos;

1.10.22. Detecção e resposta a ataques:

1.10.22.1. Monitorar continuamente os indicadores de possíveis ataque como DCSync, DCShadow, Password Spraying, Password Guessing/Brute Force, Lsaas Injecton nos controladores de domínio, Golden Ticket, NTLM Relay, entre outros;
1.10.22.2. Detecção de ataques ao AD em tempo real ou em menos de um minuto;
1.10.22.3. Análise detalhada do ataque, apresentando ativo de origem, vetor de ataque, controlador de domínio afetado, técnica aplicada;
1.10.22.4. Apresentação de ataques em uma linha do tempo;
1.10.22.5. Investigar ameaças, reproduzir ataques e procurar por backdoors;
1.10.22.6. Permitir busca ágil de eventos específicos na base da solução através de queries customizadas;
1.10.23. A solução deve ser capaz de enviar alertas por e-mail;
1.10.24. A solução nativamente deve ser capaz de se integrar com SIEM através de protocolo SYSLOG;
1.10.25. A solução deve ser capaz de filtrar e enriquecer os eventos que serão enviados para o SIEM;
1.10.26. A solução deve produzir regras YARA na detecção de ataques (Ex. DCSync, Golden Ticket) identificados pela ferramenta;
1.10.27. A solução deve possuir conjunto de APIs REST, todas as chamadas disponíveis devem estar contidas na documentação;
1.10.28. A solução deve permitir a criação de listas de exclusões, suportando minimamente Exclusão por domínios do AD monitorados e por itens analisados;

1.11. Correção automatizada de vulnerabilidades de segurança

1.11.1. A plataforma deverá ser ofertada em modelo SaaS (Software as a Service), ou seja, não deve requerer recursos computacionais on-premises para ser implementada.

1.11.2. A plataforma deve prover visibilidade e cobertura em tempo real para os sistemas operacionais e aplicações utilizadas nos ativos da organização, ou seja, qualquer alteração no inventário (instalação / desinstalação / alteração de aplicativos deve ser refletida instantaneamente na solução).

1.11.3. A plataforma deve fornecer uma solução integrada para gerenciamento de vulnerabilidade, priorização de risco e remediação em uma única plataforma.
1.11.4. A plataforma deve prover pelo menos dois métodos de autenticação (Ex: usuário e senha, e-mail de verificação, SAML2).
1.11.5. A plataforma deve ter a possibilidade de instalar um componente na rede interna para fazer o caching de patches, atendendo requisitos de ativos que não podem realizar download das atualizações diretamente da internet, bem como este componente não

deve ocasionar custo adicional. Tal componente deve ser executado em pelo menos um dos seguintes sistemas operacionais: Ubuntu ou Red Hat Linux.

1.11.6. Deve prover atualização de patches para servidores sem interrupção do serviço principal, sem forçar a reinicialização do mesmo.

1.11.7. A plataforma deve atualizar não apenas o Sistema operacional, mas também as aplicações instaladas nos ativos.

1.11.8. Deve trabalhar com reconhecimento automático de aplicações instaladas nos hosts, mantendo também o fluxo de atualizações disponível.

1.11.9. Deve fornecer gerenciamento de patches fim a fim para o sistema operacional Windows;

1.11.10. Deve fornecer gerenciamento de patches para aplicações de terceiros no Windows;

1.11.11. Deve fornecer gerenciamento de patch para o sistema operacional Linux;

1.11.12. Deve fornecer gerenciamento de patches para aplicativos de terceiros no Linux e não apenas na camada de SO.

1.11.13. Deve fornecer gerenciamento de patches para o sistema operacional Mac.

1.11.14. Para o sistema operacional Windows, minimamente, as seguintes aplicações devem poder ser atualizadas:

1.11.14.1. 7-zip;

1.11.14.2. Adobe Reader;

1.11.14.3. Adobe Acrobat Reader;

1.11.14.4. Adobe Photoshop;

1.11.14.5. Adobe Creative Cloud;

1.11.14.6. Adobe Flash Player;

1.11.14.7. Autocad;

1.11.14.8. Bizagi Modeler Free

1.11.14.9. Keepass;

1.11.14.10. Openssl;

1.11.14.11. Opera;

1.11.14.12. Python;

1.11.14.13. Google Chrome;

1.11.14.14. Google Earth;

1.11.14.15. Google Drive;

1.11.14.16. Mozilla Firefox;

1.11.14.17. Mozilla Thunderbird;

1.11.14.18. Sun Java;

1.11.14.19. Microsoft Office;

1.11.14.20. Microsoft Visual Studio;

1.11.14.21. Microsoft System Center;

1.11.14.22. Microsoft SQL Server;

1.11.14.23. Microsoft Exchange;

1.11.14.24. Microsoft Edge;

1.11.14.25. Microsoft Teams;

1.11.14.26. Microsoft OneDrive;

1.11.14.27. Microsoft Internet Explorer;
1.11.14.28. Microsoft Outlook;
1.11.14.29. Microsoft Visio;
1.11.14.30. Microsoft Windows Defender;
1.11.14.31. Notepad++;
1.11.14.32. PowerBI;
1.11.14.33. Microsoft IIS;
1.11.14.34. Tomcat;
1.11.14.35. PDF Reader;
1.11.14.36. Zoom;
1.11.14.37. Vmware Workstation;
1.11.14.38. Webex;
1.11.14.39. Whatsapp;
1.11.14.40. VLC

1.11.15. Para os sistemas operacionais Linux, minimamente, as seguintes aplicações devem poder ser atualizadas:

1.11.15.1. Abrt;
1.11.15.2. Adduser;
1.11.15.3. Alsa-Lib
1.11.15.4. Alsa-Tools-Firmware;
1.11.15.5. Apparmor;
1.11.15.6. Apport;
1.11.15.7. Apt;
1.11.15.8. Apt-Utils;
1.11.15.9. Base-Files;
1.11.15.10. Bash;
1.11.15.11. Binutils;
1.11.15.12. BZIP2;
1.11.15.13. Chrony;
1.11.15.14. Coreutils;
1.11.15.15. Crontabs;
1.11.15.16. Curl;
1.11.15.17. Dash;
1.11.15.18. Debianutils;
1.11.15.19. Device-Mapper;
1.11.15.20. Diffstat;
1.11.15.21. Diffutils;
1.11.15.22. Dirmngr;
1.11.15.23. Distro-Info;
1.11.15.24. Dnsutils;
1.11.15.25. Dpkg;
1.11.15.26. Elfutils;
1.11.15.27. Fdisk;
1.11.15.28. Findutils;

1.11.15.29. Firewalld;
1.11.15.30. FTP;
1.11.15.31. Gdisk;
1.11.15.32. Git;
1.11.15.33. GLIB2;
1.11.15.34. Glibc;
1.11.15.35. Glibc-Common;
1.11.15.36. GNUPG2;
1.11.15.37. Gnupg-Utils;
1.11.15.38. Grep;
1.11.15.39. Grub2-Tools;
1.11.15.40. Grub-Common;
1.11.15.41. Gzip;
1.11.15.42. Iproute;
1.11.15.43. Iprutils;
1.11.15.44. Iptables;
1.11.15.45. Iputils;
1.11.15.46. Kernel-Tools;
1.11.15.47. Kmod;
1.11.15.48. Libcap;
1.11.15.49. Mount;
1.11.15.50. Net-Tools;
1.11.15.51. Openssh;
1.11.15.52. Openssl;
1.11.15.53. Open-Vm-Tools;
1.11.15.54. PAM;
1.11.15.55. Passwd;
1.11.15.56. Patchutils;
1.11.15.57. Perl;
1.11.15.58. Postfix;
1.11.15.59. Python;
1.11.15.60. RPM;
1.11.15.61. Rsyslog;
1.11.15.62. Shadow-Utils;
1.11.15.63. Sqlite;
1.11.15.64. Sudo;
1.11.15.65. Tar;
1.11.15.66. Tcpdump;
1.11.15.67. Telnet;
1.11.15.68. Time;
1.11.15.69. Unzip;
1.11.15.70. Vim;
1.11.15.71. Wget;
1.11.15.72. Yum;

1.11.15.73. Zerofree;
1.11.15.74. Zip.

1.11.16. Para os sistemas operacionais MAC, minimamente, as seguintes aplicações devem poder ser atualizadas:
1.11.16.1. Microsoft Office;
1.11.16.2. Zoom;
1.11.16.3. Adobe Acrobat Reader;
1.11.16.4. Mongodb;
1.11.16.5. Google Chrome;
1.11.16.6. Whatsapp
1.11.16.7. Safari;
1.11.16.8. Microsoft Teams;
1.11.16.9. Microsoft OneDrive;
1.11.16.10. Mozilla Firefox.

1.11.17. Deve prover avaliação contínua de vulnerabilidades para identificação de quais atualizações devem ser instaladas em cada host.

1.11.18. Deve fornecer painel com priorização de ameaças com base nos ativos, aplicações ou sistemas operacionais.

1.11.19. A priorização de vulnerabilidade e correções a serem realizadas deve ser combinada com um motor inteligência interna a própria solução.

1.11.20. O processo de priorização e remediação de vulnerabilidades deve acompanhar todo o seu ciclo de vida, ou seja, descoberta/identificação, correção manual ou automatizada e contabilização nas visões para acompanhamento das ações que foram tomadas.

1.11.21. A própria ferramenta deve conter um processo de classificação de risco para priorizar a correção de vulnerabilidades descobertas, trazendo contexto de risco daquilo que precisa de atenção imediata.

1.11.22. Deve prover uma visão de classificação de risco baseada em ativos.

1.11.23. Deve prover classificação de risco por aplicação.

1.11.24. Deve apresentar a classificação de risco e priorizar as vulnerabilidades a serem corrigidas em ordem de criticidade não só do CVE, mas também em relação à um contexto de performance, situação do ambiente e tipos de ativo.

1.11.25. Deve fornecer detecção de vulnerabilidades a serem corrigidas em tempo real.

1.11.26. Deve prover meios para conter a exploração de softwares em tempo real;

1.11.27. Deve ter a funcionalidade de proteção contra exploração de vulnerabilidades, sem necessariamente instalar um patch de correção ("patch virtual"), utilizando o mesmo agente de patch management.

1.11.28. Deve possuir informações de CVE tanto recentes quanto legados, tal capacidade deve ser comprovada por documentações oficiais.

1.11.29. Deve manter a base de dados atualizada constantemente, no tocante a novas vulnerabilidades e patches de correção a serem instalados nos ativos.

1.11.30. Deve permitir a execução de comandos de forma remota em todos os dispositivos que possuem os agentes instalados.

1.11.31. Deve permitir o agendamento de instalação das atualizações (Patches) ou execução de script de forma remota.

1.11.32. Deve possibilitar a execução de ações automáticas pré-configuradas e personalizadas (Ações Automáticas).

1.11.33. As ações automáticas devem possibilitar a instalação automática de patches baseado em critérios personalizáveis, como:

1.11.34. Atualizações de sistema operacional;

1.11.35. Atualizações de aplicações específicas;

1.11.36. Por severidade/criticidade do patch de correção;

1.12. Toda instalação de patch deve permitir a opção de reinicialização automática da estação/servidor, dando também a opção para que o usuário cancele o restart, se necessário.

1.13. Deve ser possível enviar “pop-ups” para os usuários, quando os mesmos estiverem pendentes de reinicialização.

1.14. Deve possibilitar a geração de scripts para Windows, Linux e Mac.

1.15. Deve possuir proteção contra vulnerabilidades de dia 0 (zero day).

1.16. Deve possuir mecanismos de "Ações recomendadas", de forma a guiar as correções a serem realizadas.

1.17. Deve suportar segregação de função por usuário, ou seja, permitir que usuários da mesma empresa tenham permissões diferentes dentro da plataforma.

1.18. Deve ser capaz de segregar diferentes ativos entre diferentes grupos de usuários com diferentes níveis de permissão.

1.19. A segregação de ativos por grupos, deve respeitar características dinâmicas, de forma a movimentar os ativos entre os grupos de forma automática. Tal característica deve suportar a configuração, minimamente, dos seguintes atributos (Para movimentação automática dos ativos):

1.19.1. Nome do ativo;

1.19.2. Tipo do ativo;

1.19.3. Nível de risco do ativo;

1.19.4. Status do ativo;

1.19.5. CVE's específicos detectados no mesmo;

1.19.6. Aplicações específicas instaladas nos ativos, assim como a versão detectada do mesmo;

1.19.7. Sistema operacional e versão do mesmo.

1.19.8. Deve permitir a instalação do agente por linha de comando (Powershell, cmd, bash, etc).

1.19.9. Permitir a instalação de agente por meio de GPO ou qualquer outra plataforma de software deployment utilizada.

1.19.10. Os agentes devem ser capazes de scanear as plataformas Windows, Linux e Mac.

1.19.11. Para o sistema operacional Windows, as seguintes versões, minimamente, devem ser suportadas:

1.19.11.1. Windows 7, 8, 8.1, 10 e 11.

1.19.11.2. Windows server 2008, 2012, 2016, 2019 e 2022.

1.19.12. Para o sistema operacional Linux, as seguintes distribuições, minimamente, devem ser suportadas:
1.19.12.1. Centos;
1.19.12.2. Redhat;
1.19.12.3. Fedora;
1.19.12.4. Ubuntu;
1.19.12.5. Debian
1.19.12.6. Kali Linux;
1.19.12.7. Amazon Linux;
1.19.12.8. Oracle Linux.
1.19.13. Para o sistema operacional Mac, as seguintes distribuições, minimamente, devem ser suportadas:
1.19.13.1. MAC OS;
1.19.13.2. MAC OS X.
1.19.14. O agente não deve depender de nenhum componente externo, não fornecido, para seu pleno funcionamento.
1.19.15. O agente pode fornecer proteção de virtual Patching para aplicações terceiras.
1.19.16. O agente deve funcionar de forma oculta no sistema operacional, não apresentando interface para o usuário final.

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

2.1. Arquitetura

2.1.1. Deve ser baseada em nuvem (Cloud), de forma a manter todos os eventos armazenados na nuvem do fabricante da solução.
2.1.2. Não serão aceitos serviços entregues por meio de software livre ou open-source.
2.1.3. A solução deve fornecer componentes já licenciados para coleta e envio de logs/tráfego até a plataforma central.
2.1.4. O componente para coleta de logs/tráfego deve fornecer a possibilidade de instalação em servidores Windows, Linux ou imagens prontas previamente fornecidas.
2.1.5. Deverá estar licenciada, em nome do Ministério 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.
2.1.6. Deve possuir capacidade de recebimento e armazenamento, mínimo, de todos os logs de ativos de segurança, alertas de segurança, tráfego de pacotes, dentre outras informações relacionadas, em formado bruto (raw) e/ou metadados, necessárias para fins de correlacionamento e forense, conforme especificação abaixo:

	Tráfego de Pacotes	Logs, Eventos, Alertas, dentre outras informações
Metadados	Armazenar por no mínimo 365 dias	Armazenar por no mínimo 365 dias

Dados brutos (raw)	Armazenar por no mínimo 365 dias	Armazenar por no mínimo 365 dias

2.1.7. Deve ter a capacidade de manter os itens coletados indexados para buscas rápidas por pelo menos 7 dias. Itens a serem buscados em datas superiores ao período de indexação devem respeitar o período de retenção do tópico anterior.

2.2. Requerimentos Gerais

2.2.1. Deverá ser capaz de gerenciar de forma eficiente incidentes de segurança. O software de gerenciamento de incidentes de segurança deve permitir a definição de um processo abrangente desde o registro e triagem inicial de um incidente até sua resolução e prevenção.
2.2.2. Deve permitir a automação de fluxos de forma gráfica, incluindo estágios, tarefas paralelas ou sequenciais, regras de decisão e aprovação, sem a necessidade de programação ou alteração de código fonte para as integrações já existentes.
2.2.3. Deve permitir automatização e orquestração de fluxos relacionados a resposta de incidentes de segurança, integrando e simplificando as operações.
2.2.4. Deve fornecer visibilidade, rastreabilidade e indexação dos eventos detectados, integrando as várias ferramentas de segurança que a entidade possui, aumentando a capacidade de detecção e maturidade da segurança cibernética.
2.2.5. Deve permitir acelerar a resposta às lacunas de segurança cibernética por meio de análise contextual, automação de processos e capacidade de articulação para investigação, utilizando fluxos de análise e inteligência associada às metodologias de ataque de grupos de cibercrime.
2.2.6. Deve identificar, registrar e indexar incidentes de segurança rapidamente, registrando os eventos relatados pelas soluções que a CONTRATADA atualmente possui.
2.2.7. Deve permitir integração e interoperabilidade com o ecossistema de segurança da entidade, independentemente da marca dos produtos de segurança utilizados.
2.2.8. Deve permitir a integração baseada em fluxos de trabalho através do cruzamento de dados das soluções de segurança como Firewalls, IPSs e sistemas de chamados.
2.2.9. Deve possuir controle granular de níveis de acesso a plataforma.
2.2.10. Deve funcionar, obrigatoriamente, com autenticação de dois fatores nativa, sendo no mínimo eles: OTP, SMS ou voz.
2.2.11. Deve permitir que se configure políticas restritas de senha como período de redefinição, bloqueio por tentativas sem sucesso, histórico de senha e desativação de usuários por tempo de inatividade.
2.2.12. Deve registrar e listar todos os alertas ativos, permitindo filtros e pesquisas sob demanda em uma linguagem de queries.
2.2.13. Deve permitir a criação de listas a serem utilizadas durantes as pesquisas, com objetivo de poder facilmente utilizá-las para inclusão ou remoção de recursos na busca, evitando a repetição de comandos, tornando as ações de caça a ameaças (hunting) mais ágeis.
2.2.14. Deve possuir alertas indicando a gravidade do incidente, permitindo a detecção, validação e investigação, a fim de reconstruir toda a cadeia do ataque.
2.2.15. Deve suportar uma linha do tempo visual em relação aos eventos registrados.

2.2.16. Deve oferecer suporte à integração com soluções de segurança de terceiros. A integração deve ser baseada em syslog, ingestão/absorção de alertas e/ou análise de tráfego de rede.
2.2.17. Deve permitir a criação de painéis e dashboards com gráficos de gestão, de forma ágil e intuitiva, sem a necessidade de programação e alteração do código-fonte.
2.2.18. Deve permitir aos atendentes e solucionadores de incidentes a possibilidade de criação de seus próprios painéis e gráficos dentro da solução, compartilhando sempre que necessário com grupos ou usuários específicos, permitindo gerenciamento das permissões de compartilhamento de acordo com os perfis de cada usuário.
2.2.19. Deve permitir a criação de gráficos, utilizando como origem de dados, as informações de diferentes soluções de segurança da organização.
2.2.20. Deve permitir configurar o envio automático e agendado de relatórios e gráficos gerenciais para grupos de usuários ou usuários específicos.
2.2.21. Deve incluir painéis unificados, buscas e relatórios, para facilitar a transição da detecção para a investigação e a resposta subsequente ao incidente relatado.
2.2.22. O coletor da solução deverá ser capaz de coletar, aplicar parsing, normalizar e categorizar os eventos dos dispositivos monitorados em tempo próximo ao real.
2.2.23. Deve possuir parsing, para interpretação automática de logs, para pelo menos as seguintes marcas/soluções:
    2.2.23.1. Aerohive;
    2.2.23.2. Akamai;
    2.2.23.3. AWS;
    2.2.23.4. Apache;
    2.2.23.5. Arbor;
    2.2.23.6. ArcSight;
    2.2.23.7. Aruba;
    2.2.23.8. Barracuda;
    2.2.23.9. BeyondTrust;
    2.2.23.10. BlueCoat;
    2.2.23.11. Broadcom;
    2.2.23.12. Brocade;
    2.2.23.13. Carbom Black;
    2.2.23.14. CheckPoint;
    2.2.23.15. Cisco;
    2.2.23.16. Citrix;
    2.2.23.17. Crowdstrike;
    2.2.23.18. CyberArk.
    2.2.23.19. Cylance;
    2.2.23.20. Docker;
    2.2.23.21. Eset;
    2.2.23.22. F5;
    2.2.23.23. FireEye;
    2.2.23.24. Forcepoint;
    2.2.23.25. Forescout;
    2.2.23.26. Fortinet;
    2.2.23.27. Graylog;
    2.2.23.28. Huawei

2.2.23.29. HP;
2.2.23.30. IBM;
2.2.23.31. Imperva;
2.2.23.32. Juniper;
2.2.23.33. Mandiant;
2.2.23.34. McAfee;
2.2.23.35. Microsoft;
2.2.23.36. Nagios;
2.2.23.37. Nginx;
2.2.23.38. Oracle;
2.2.23.39. Palo Alto;
2.2.23.40. Proofpoint;
2.2.23.41. Pulse Secure;
2.2.23.42. Riverbad;
2.2.23.43. RSA;
2.2.23.44. SonicWall;
2.2.23.45. Sophos;
2.2.23.46. Splunk;
2.2.23.47. Symantec;
2.2.23.48. Tenable;
2.2.23.49. Trend Micro;
2.2.23.50. Varonis;
2.2.23.51. Digital Guardian;
2.2.23.52. Veritas
2.2.23.53. Vmware;
2.2.23.54. WatchGuard;
2.2.23.55. Zscaler.

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

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

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

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

2.2.27.1. AWS;
2.2.27.2. Carbon Black;
2.2.27.3. Checkpoint;
2.2.27.4. Cisco;
2.2.27.5. Crowdstrike;

2.2.27.6. Druva;
2.2.27.7. FireEye;
2.2.27.8. Fortinet
2.2.27.9. Google Cloud Plataform;
2.2.27.10. Huawei
2.2.27.11. Imperva;
2.2.27.12. McAfee;
2.2.27.13. Microsoft;
2.2.27.14. Microsoft Azure;
2.2.27.15. Okta;
2.2.27.16. Palo Alto;
2.2.27.17. Proofpoint;
2.2.27.18. Sophos;
2.2.27.19. Symantec;
2.2.27.20. Veritas
2.2.27.21. VMware

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

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

2.2.30. Deve possuir nativamente integrações para serviços de nuvem, considerando minimamente:

2.2.30.1. AWS CloudTrail;
2.2.30.2. AWS CloudWatch;
2.2.30.3. AWS GuardDuty;
2.2.30.4. AWS S3;
2.2.30.5. AWS Security Hub;
2.2.30.6. AWS VPC Flow Logs;
2.2.30.7. Azure;
2.2.30.8. Azure Active Directory (Para UEBA);
2.2.30.9. Bitglass;
2.2.30.10. Box.com;
2.2.30.11. Canary;
2.2.30.12. CipherCloud CASB+;
2.2.30.13. Cisco Umbrella;
2.2.30.14. Cisco Umbrella S3;
2.2.30.15. Corelight;
2.2.30.16. Crowdstrike Falcon;
2.2.30.17. CSC Global Domain Manager;
2.2.30.18. Digital Guardian;
2.2.30.19. Druva;
2.2.30.20. Duo Auth;
2.2.30.21. Entrust Intellitrust;
2.2.30.22. FireEye Detection on Demand for AWS S3;
2.2.30.23. FireEye Email Threat Prevention;
2.2.30.24. FireEye Message Security for Slack;
2.2.30.25. FireEye Messaging Security for Microsoft 365;

2.2.30.26. FireEye Network Security;
2.2.30.27. Google Cloud;
2.2.30.28. Google Cloud Audit Events;
2.2.30.29. Kentik;
2.2.30.30. McAfee MVision Mobile;
2.2.30.31. Microsoft CASB;
2.2.30.32. Microsoft Graph;
2.2.30.33. Microsoft Office 365;
2.2.30.34. Mimecast;
2.2.30.35. Netskope;
2.2.30.36. Okta;
2.2.30.37. Proofpoint CASB Integration;
2.2.30.38. Proofpoint SIEM Integration;
2.2.30.39. Qualys File Integrity Monitoring;
2.2.30.40. Security Onion;
2.2.30.41. Signal Sciences WAF;
2.2.30.42. Sophos Antivirus SIEM Integration;
2.2.30.43. Symantec Mobile Protection;
2.2.30.44. Symantec Web Security Service;
2.2.30.45. Windows Defender ATP;
2.2.30.46. Zimperium.

2.3. Inteligência de Ameaças

2.3.1. Deve incluir regras de correlação e inteligência de ameaças.
2.3.2. Deve incluir um pacote de regras para detecção. Elas devem ser alimentadas automaticamente, sem gerar impacto ou solicitar intervenção de um analista. Por sua vez, ela deve permitir a criação de regras personalizadas pela CONTRATADA, incluído a entrada manual de novos indicadores de comprometimento.
2.3.3. Deve fornecer uma boa variedade de regras de inteligência já criadas e disponíveis para detecção de ameaças e também permitir customização de novas para atender necessidades específicas.
2.3.4. Deve incluir inteligência de ameaças que revise, valide e compare as fontes que estão sendo utilizadas para detecção de ameaças.
2.3.5. Deve incluir a descrição das famílias de malware.
2.3.6. Deve fornecer atribuição automática de alertas a grupos de APTs.
2.3.7. O fabricante deve possuir especialistas em segurança que estejam monitorando as ameaças atuais ao redor do mundo, gerando a partir disso, novos pacotes de regras para aprimorar a solução em seu nível de detecção. Tal serviço não deve ocasionar custo adicional para a CONTRATANTE.
2.3.8. O fabricante deve rastrear grupos de crimes cibernéticos, a fim de aprimorar regras de detecção a partir de incidentes globais.
2.3.9. Deve utilizar uma rede de inteligência que processa diversas amostras de malware exclusivas por dia.
2.3.10. Deve injetar inteligência nos dados de log registrados.

2.3.11. Deve oferecer análises sobre "beaconing", permitindo no mínimo, a detecção de malwares que tentam estabelecer contato com “Command and Control”.
2.3.12. Deve incluir como fonte de inteligência as ameaças, plataformas de segurança contratadas e permitir identificar a telemetria e o perfil de proliferação de um ataque, além de ter informações sobre vítimas e táticas, técnicas e procedimentos geralmente utilizados pelo invasor.
2.3.13. Deve possibilitar consultas de segurança específicas (Buscando referências a malwares ou ataques conhecidos), incluindo análise, para no mínimo:
    2.3.13.1. URLs;
    2.3.13.2. Domínios;
    2.3.13.3. Hashes MD5;
    2.3.13.4. Endereços IP.

2.3.14. Deve permitir a criação de listas a serem utilizadas com escopo de inteligência, facilitando assim o uso das mesmas em regras ou mesmo para customizar detecções especificas do negócio.
2.3.15. Deve fornecer a possibilidade de análise de malwares, executando o mesmo de maneira controlada (sandbox), a fim de receber um relatório sobre os comportamentos encontrados com a execução.
2.3.16. Depois que uma ameaça for detectada, ela deve relacionar as informações registradas na plataforma central e as vincular fornecendo detalhes de inteligência.
2.3.17. Deve oferecer análises mínimas em:
    2.3.17.1. Beaconing;
    2.3.17.2. Beaconing Diferencial;
    2.3.17.3. Geo-feasibility;
    2.3.17.4. Uso indevido de credenciais;
    2.3.17.5. Detecção de conexão não reconhecida;
    2.3.17.6. Detecção de Fast-Flux DNS;
    2.3.17.7. Entropia DNS;
    2.3.17.8. Detecção de ataques via PowerShell;
    2.3.17.9. Detecção de Exfiltração de Dados;
    2.3.17.10. Detecção de conexões de entrada SSH, Telnet, SMB e RDP que sejam anômalas;
    2.3.17.11. Detecção de contas comprometidas com VPN;
    2.3.17.12. Detecção de movimento lateral.
2.3.18. Deve permitir que sejam realizadas pesquisas em seu ambiente para atividades de "caça" a malwares e atividades maliciosas.
2.3.19. Deve possuir capacidade analítica de eventos/tráfego, independente das regras, para detecção de no mínimo os seguintes comportamentos:
    2.3.19.1. Uso suspeito de chave da API Amazon Web Services (AWS);
    2.3.19.2. Login de autenticação multifator anormal do Duo com base no histórico de login anterior deste usuário;
    2.3.19.3. Atividade anormal do Google Cloud Platform (GCP) por um usuário;
    2.3.19.4. Logon anormal no Microsoft Office 365 com base no histórico de logon anterior deste usuário;
    2.3.19.5. Login anormal do Okta com base no histórico de login anterior deste usuário;
    2.3.19.6. Login anormal do protocolo RDP (Remote Desktop Protocol) com base no histórico de login anterior deste usuário;

2.3.19.7. Download ou upload anormal de arquivo do SharePoint com base no histórico anterior deste usuário;
2.3.19.8. Detecção de força bruta do Citrix NetScaler, realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.
2.3.19.9. Detecção de força bruta no Druva, realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.
2.3.19.10. Tráfego de rede para domínios semelhantes a (permutações) do domínio da organização descoberto. Isso pode indicar um ataque de phishing ou alguma outra atividade suspeita.
2.3.19.11. Detecção de força bruta no Linux, realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.
2.3.19.12. Detecção de força bruta do Office 365, realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.
2.3.19.13. Okta detecção de força bruta. Isso realiza verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.
2.3.19.14. Vários logins de RDP pelo mesmo usuário.
2.3.19.15. Vários logins de RDP no mesmo host.
2.3.19.16. Login de VPN anormal com base no histórico de login de VPN anterior do usuário.
2.3.19.17. Uma conta de usuário foi excluída dentro de 24 horas após sua criação.
2.3.19.18. Detecção de força bruta do Windows NT LAN Manager (NTLM), realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.
2.3.19.19. Vários erros de "usuários únicos não encontrados" de uma fonte. Isso pode indicar uma tentativa de enumeração do usuário.
2.3.19.20. Vários processos exclusivos de um usuário ou host dentro de um curto período de tempo. Isso pode indicar atividade de reconhecimento.

2.4. Capacidades de Investigação

2.4.1. Deve incluir recursos de workflow para resposta a incidentes de segurança.
2.4.2. Deve ser capaz de coordenar os processos de segurança atuais no nível de alertas de rede e alertas de outras soluções de segurança.
2.4.3. Deve fornecer recursos de busca e pesquisa nas estações de trabalho, de acordo com os seguintes exemplos:
2.4.3.1. Ampla pesquisa por comportamentos maliciosos conhecidos;
2.4.3.2. Caça proativa de atividades suspeitas;
2.4.3.3. Investigação completa nos endpoints comprometidos;
2.4.3.4. Procurar evidências de intrusões avançadas como ameaças sem arquivo (fileless).
2.4.4. Deve fornecer recursos de resposta em tempo real, para no mínimo:
2.4.4.1. Investigar todos as atividades em terminais suspeitos;
2.4.4.2. Reproduzir a linha do tempo completa de um ataque avançado;
2.4.4.3. Capturar detalhes da atividade que ocorreu durante intrusões;
2.4.4.4. Executar uma análise aprofundada no nível de: Acesso ao disco, análise de memória e detecção de rootkit.

2.4.5. Depois que a solução detectar um alerta, a mesma deve fornecer pelo menos as seguintes informações:
  2.4.5.1. A inteligência em torno do alerta detectado;
  2.4.5.2. Métodos de detecção da ameaça em questão;
  2.4.5.3. Mostrar graficamente uma linha do tempo de eventos relacionados ao alerta detectado;
  2.4.5.4. Dicas de pesquisa para orientar os analistas em todo o processo de resposta a incidentes. Essas dicas devem estar associadas à experiência que o fabricante tem em responder a incidentes críticos de segurança em empresas em todo o mundo;
  2.4.5.5. Mostrar os eventos brutos (raw data) que geraram o alerta;
  2.4.5.6. Histórico de eventos associados.
2.4.6. A visualização de um caso deve permitir pelo menos, as seguintes ações:
  2.4.6.1. Controle do Nome, Status, Prioridade, Classificação e Descrição do caso;
  2.4.6.2. Permitir que o caso seja assinado para algum usuário;
  2.4.6.3. Permitir que qualquer log/evento relacionado possa ser adicionado e visualizado no mesmo;
  2.4.6.4. Permitir a visualização de todos os alertas/incidentes envolvidos no caso;
  2.4.6.5. Permitir que o caso seja exportado em formatos CSV e JSON;
  2.4.6.6. Permitir a adição e visualização de comentários no caso.
2.4.7. Deve incluir dicas intuitivas de investigação, trazendo automaticamente no mínimo, os seguintes dados para consulta no alerta:
  2.4.7.1. Existem outras regras alertadas para esse IP de origem?
  2.4.7.2. Existem regras acionadas que foram baseadas em sensores de inteligência, relacionadas a algum desses índices de comprometimento?
  2.4.7.3. Quais logs estão disponíveis para este dispositivo?
  2.4.7.4. Quais logs estão disponíveis para este IP?
  2.4.7.5. Em quais outros hosts esse malware foi encontrado?
  2.4.7.6. Existem outros logs com esse hash?
  2.4.7.7. Existem alertas relacionados usando o IP do agente?
  2.4.7.8. Existem alertas relacionados usando o este dispositivo?
  2.4.7.9. Existem alertas relacionados usando o hash envolvido no incidente?
2.4.8. No nível analista/operador, Deve fornecer:
  2.4.8.1. Um painel de pesquisa, onde são registrados alertas e casos atribuídos aos analistas;
  2.4.8.2. Detalhe de alertas como: nível de risco, nome do alerta, tipo de alerta, origem, data da primeira ocorrência, data da última ocorrência, número de eventos, resumo, fontes e destino, status do alerta e opções de: exportação do alerta nos formatos CSV e JSON para excluir e\ou fechá-lo;
  2.4.8.3. Cada alerta deve poder ser atribuído a um analista específico, para iniciar o processo de investigação, contenção, caça, etc.;
  2.4.8.4. Deve haver um painel de casos, que permita a criação, gerenciamento e alocação de casos, a fim de rastrear as atividades e o tempo de resposta de cada analista;
  2.4.8.5. Cada caso pode conter vários alertas, várias anotações, para validar o estado evolutivo na resposta a um incidente;
  2.4.8.6. A ferramenta deve poder atribuir a cada caso níveis de: prioridade, gravidade e, como opção, outro tipo de classificação;

2.4.8.7. Cada caso deve ter: Descrição, Eventos, Alertas, Revisões e Notas, bem como o registro do qual o analista foi designado ou modificou o caso.

2.4.9. Deve ter a capacidade de realizar pesquisas para o processo de busca proativa e reativa nos eventos e metadados coletados de maneira automática.

2.4.10. Deve ter um módulo de pesquisa avançada ou indexação de pesquisa que contenha:

2.4.10.1. Um módulo de ajuda de sintaxe;

2.4.10.2. Um módulo de histórico de pesquisas;

2.4.10.3. Um módulo de pesquisa salva como favorita;

2.4.10.4. Capacidade de salvar a pesquisa.

2.4.11. As pesquisas devem ter uma sintaxe completa baseada em Query Language contemplando documentação completa e atualizada.

2.4.12. Deve incluir opções de pesquisa, com base em cada um dos campos de metadados, como: Domínio, porta de destino, método HTTP, metaclasses, porta de origem, useragent, IP de Origem, IP de destino, etc.

2.4.13. Deve possuir um módulo de UEBA ao qual poderá ser utilizado para melhor compreensão dos eventos, identificando possíveis entidades (equipamentos ou usuários) envolvidos anteriormente em outros eventos maliciosos ou suspeitos.

2.4.14. A visualização de um alerta/incidente deve permitir pelo menos, as seguintes ações:

2.4.14.1. Assinar o incidente para um analista;

2.4.14.2. Marcar como falso positivo;

2.4.14.3. Adicionar o alerta em um caso para um trabalho aprofundado envolvendo mais pessoas e artefatos de investigação;

2.4.14.4. Fechar ou suprimir o alerta;

2.4.14.5. Exportar o alerta para CSV ou JSON;

2.4.14.6. Fazer pesquisas de Índices de comprometimento diretamente em bases externas como VirusTotal e DomainTools;

2.4.14.7. Adicionar através de um clique, artefatos em listas para facilitar o trabalho de investigação e melhorar a assertividade das regras de detecção;

2.4.14.8. Visualizar a correlação de índices de comprometimento em outros incidentes abertos ou fechados;

2.4.14.9. Consultar análises realizadas automaticamente em bases de inteligência cibernética;

2.4.14.10. Analisar o histórico de modificações no incidente;

2.4.14.11. Adicionar comentários no incidente;

2.4.14.12. Quando realiza análise em sandbox para artefatos envolvidos em incidentes, permitir a visualização das modificações que o binário realizou.

2.4.15. Ao visualizar um tipo de evento, a plataforma deve permitir, a partir de cliques com o mouse (Sem necessidade de escrita de query), incrementar as buscas, para pelo menos as seguintes ações:

2.4.15.1. Realizar uma busca por qualquer campo daquela classe. Exemplo: Ip de origem/destino, hash md5, destinatário/remetente, ações aplicadas, etc;

2.4.15.2. No caso de uma busca já estar sendo realizada, deve ser possível adicionar qualquer campo listado na busca atual para seguimento das atividades de hunting;

2.4.15.3. Deve ser possível também realizar exclusões na busca a partir do valor de qualquer campo listado;

2.4.15.4. Dever ser possível realizar um agrupamento de qualquer valor listado, formando automaticamente um dashboard, estabelecendo as contagens e classificações de acordo com os valores dos campos;

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

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

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

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

2.5. Orquestração e Automatização

2.5.1. A arquitetura da plataforma de orquestração deve ser moderna e granular ao ponto de ao menos possuir as seguintes segmentações de seus serviços:

2.5.1.1. Serviço para orquestração;

2.5.1.2. Serviço Web para acesso a interface de gerência;

2.5.1.3. Ambiente virtual para execução de playbooks;

2.5.1.4. Ambiente isolado para interpretações do OS;

2.5.1.5. Serviço de banco de dados para gestão e armazenamento de dados o orquestrador;

2.5.1.6. Serviço de filas;

2.5.1.7. Database para armazenamento de informações do serviço de filas;

2.5.1.8. Serviço para tratativas de I/O do sistema web;

2.5.1.9. Serviço para tratativas de execução do serviço de fila;

2.5.1.10. Serviço de agendamento de comandos.

2.5.2. Deve possuir uma interface gráfica que contemple ao menos os itens abaixo para melhor organização, gerência e ação durante possíveis investigações ou automatizações de atividades internas.

2.5.2.1. Dashboard;

2.5.2.2. Guia de chamados;

2.5.2.3. Playbooks;

2.5.2.4. Dispositivos;

2.5.2.5. Adaptadores;

2.5.2.6. Tabelas;

2.5.2.7. Tags;

2.5.2.8. Formulários;

2.5.2.9. Scripts;

2.5.2.10. Tipos;

2.5.2.11. Biblioteca.

2.5.3. Deve possuir plugins predefinidos e compatíveis com as diferentes tecnologias que a entidade possui no nível de segurança cibernética.

2.5.4. Deve fornecer uma biblioteca de plug-ins que permita integrar fluxos de trabalho e automação com vários tipos de tecnologias, para no mínimo:

2.5.4.1. TIPs - plataformas de inteligência;

2.5.4.2. Ferramentas de análise de malware;

2.5.4.3. EDR - Detecção e resposta do terminal;
2.5.4.4. SIEM;
2.5.4.5. Armazenamento - baseado em nuvem;
2.5.4.6. Sistemas de chamados;
2.5.4.7. Soluções de endpoint;
2.5.4.8. Firewalls;
2.5.4.9. Switches;
2.5.4.10. Ferramentas de sandbox;
2.5.4.11. Servidores de email;
2.5.4.12. Ferramentas de chat;
2.5.4.13. Dispositivos móveis etc.

2.5.5. A solução deve ter um ambiente gráfico que permita a criação dos fluxos para interação com as diferentes tecnologias.

2.5.6. A solução deve permitir a automação das atividades de resposta a incidentes com base nas necessidades e processos da entidade.

2.5.7. A solução deve poder registrar as métricas de desempenho e tempo economizado nas tarefas usando a orquestração.

2.5.8. Deve permitir etapas para escalação e aprovação em fluxos de trabalho.

2.5.9. Deve suportar a definição de tarefas ou ações assíncronas.

2.5.10. A solução deve suportar SMTP para envio de e-mails.

2.5.11. Deve permitir nível de acesso a console e componentes de forma granular.

2.5.12. No nível de gerenciamento de caso/ticket a solução deve ser capaz de alterar dinamicamente a prioridade dos casos, alterar a atribuição e o status de acordo com o fluxo definido.

2.5.13. Deve permitir a criação de novos plugins, além de fornecer a habilidade de customização de playbooks através de linguagens de programaçãopara criação de templates.

2.5.14. Deve fornecer um serviço HTTP server para receber informações através de um método POST e então converter o conteúdo recebido para JSON a fim de obter melhores integrações e expandir as capacidades com integrações web.

2.5.15. Deve suportar operações básicas no processamento de fluxo, como:

2.5.15.1. Realizar operações matemáticas básicas (+, -, *, /,%, **), suportando retornar o resultado com decimais ou números exatos (arredondados);
2.5.15.2. Suporte à pesquisa de arquivos, tipo de documento de conteúdo que corresponda a uma expressão regular. Deve suportar documentos do tipo: csv, doc, docx, eml, epub, gif, jpg, json, html, msg, odt, ogg, pdf, png, pptx, ps, rtf, tiff, txt, wav, xlsx, zip;
2.5.15.3. Programar a ocorrência de eventos no futuro semelhante para Windows ou Unix;
2.5.15.4. Conectar-se a um servidor IMAP e\ou POP3;
2.5.15.5. Executar localmente os seguintes comandos: Ping, Telnet para uma porta, traceroute, whois e\ou aguardar alguns segundos;
2.5.15.6. Exibir hora local;
2.5.15.7. Operar arquivos locais através das seguintes operações: criar arquivos, adicionar a um arquivo (anexar), excluir arquivos, mover arquivos, ler arquivos, listar diretórios etc.;
2.5.15.8. Ler um feed RSS;

2.5.15.9. Realizar uma captura de tela de uma página do site. Deve suportar o uso de proxy e permitir armazenar a imagem em um arquivo;
2.5.15.10. Enviar dados através de uma porta TCP;
2.5.15.11. Oferecer suporte ao SFTP, através das seguintes operações: Listar diretório, ver se existe um arquivo, ver se existe um diretório, buscar um arquivo, buscar um diretório e seu conteúdo recursivamente, fazer upload de um arquivo;
2.5.15.12. Enviar uma mensagem via SMTP;
2.5.15.13. Executar comandos remotamente via SSH e coletar a saída de execução assim como seus erros de execução;
2.5.15.14. Criar um elemento STIX a partir de um indicador de consolidação do índice de comprometimento (Hash, IP, URL, HostName, Domínio);
2.5.15.15. Gerar uma solicitação HTTP para uma API Web;
2.5.15.16. Oferecer suporte ao uso de cabeçalhos HTTP personalizados;
2.5.15.17. Importar arquivos a serem utilizados em ações do playbook;
2.5.15.18. Adicionar tags para fácil identificação de ativos envolvidos em um playbook;
2.5.15.19. Possuir a capacidade de executar sequências condicionais que mudem a direção ou fluxo de um playbook em execução.

2.5.16. Deve suportar a interpretação de dados como:
2.5.16.1. Extrair o domínio de uma URL;
2.5.16.2. Extrair o domínio de um email;
2.5.16.3. Extrair um ou mais URLs de um texto;
2.5.16.4. Codifique um texto em base64;
2.5.16.5. Decodifique base64 em texto;
2.5.16.6. Decodifique um texto JSON usando uma expressão jsonpath;
2.5.16.7. Extrair um subtexto do XML usando um filtro xpath;
2.5.16.8. Codifique uma string usando urlEncode;
2.5.16.9. Decodifique um URL usando urlDecode;
2.5.16.10. Resolver do IP para o domínio;
2.5.16.11. Resolver do domínio para o IP;
2.5.16.12. Converter de texto em campo Hash MD5;
2.5.16.13. Filtrar de uma lista de textos aqueles que contêm um determinado subtexto;
2.5.16.14. Aplicar uma substituição em expressão regular;
2.5.16.15. Verificar se um texto corresponde a uma determinada expressão regular;
2.5.16.16. Contar os itens em uma lista.

2.5.17. Deve possuir conectores nativos para ao menos os seguintes serviços, visando ampliar a capacidade de resposta automatizada:
2.5.17.1. AbuseIPDB;
2.5.17.2. AlienVault OTX;
2.5.17.3. AlienVault ThreatCrowd;
2.5.17.4. Amazon Alexa;
2.5.17.5. Amazon Athena;
2.5.17.6. Amazon CloudTrail;
2.5.17.7. Amazon EC2;
2.5.17.8. Amazon IAM;
2.5.17.9. Amazon S3;
2.5.17.10. Amazon SNS;
2.5.17.11. Amazon VPC;

2.5.17.12. Amazon WAF;
2.5.17.13. Anomali ThreatStream;
2.5.17.14. AOL Moloch;
2.5.17.15. Apache Kafka;
2.5.17.16. Apility.io;
2.5.17.17. Atlassian Jira;
2.5.17.18. Best Practical Request Tracker;
2.5.17.19. BlacklistMaster;
2.5.17.20. Censys;
2.5.17.21. Cherwell;
2.5.17.22. Cisco AMP;
2.5.17.23. Cisco Firepower;
2.5.17.24. Cisco IOS;
2.5.17.25. Cisco Threat Grid;
2.5.17.26. Cisco Umbrella;
2.5.17.27. Citrix;
2.5.17.28. Claroty CTD;
2.5.17.29. Cofence PhishMe;
2.5.17.30. Cofense Intelligence;
2.5.17.31. Cuckoo Sandbox;
2.5.17.32. Cylance Protect;
2.5.17.33. DomainTools;
2.5.17.34. Elasticsearch;
2.5.17.35. Farsight DNSDB;
2.5.17.36. Forcepoint Web Security;
2.5.17.37. GitHub;
2.5.17.38. Google Chrome;
2.5.17.39. Google Geolocation;
2.5.17.40. Google Safe Browsing;
2.5.17.41. HackerTarget;
2.5.17.42. Have I Been Pwned?;
2.5.17.43. IBM Domino;
2.5.17.44. IBM Qradar;
2.5.17.45. IBM X-Force;
2.5.17.46. IDA Pro;
2.5.17.47. IFTTT;
2.5.17.48. Infoblox;
2.5.17.49. Internet Archive Wayback Machine;
2.5.17.50. IntSights;
2.5.17.51. IPHub;
2.5.17.52. Juniper Cyphort;
2.5.17.53. MAC Vendors Lookup;
2.5.17.54. MailboxLayer;
2.5.17.55. Malshare;
2.5.17.56. Malwares;
2.5.17.57. ManageEngine ServiceDesk;
2.5.17.58. McAfee ePolicy Orchestrator (ePO);

2.5.17.59. Micro Focus ArcSight CEF;
2.5.17.60. Micro Focus ArcSight ESM;
2.5.17.61. MicroFocus ArcSight Logger;
2.5.17.62. Microsoft Active Directory;
2.5.17.63. Microsoft Exchange;
2.5.17.64. Microsoft NetBIOS;
2.5.17.65. Microsoft SCCM;
2.5.17.66. Microsoft SharePoint;
2.5.17.67. Microsoft SMB;
2.5.17.68. Microsoft Windows;
2.5.17.69. MISP;
2.5.17.70. Mozilla Firefox;
2.5.17.71. MxToolbox;
2.5.17.72. My IP Address;
2.5.17.73. Neutrino API;
2.5.17.74. Nmap;
2.5.17.75. Palo Alto Networks Panorama;
2.5.17.76. Pastebin;
2.5.17.77. PhishTank;
2.5.17.78. Proofpoint URL Defense;
2.5.17.79. ProxyCheck;
2.5.17.80. Recorded Future;
2.5.17.81. RestPack.io;
2.5.17.82. ReversingLabs TitaniumCloud;
2.5.17.83. RiskIQ PassiveTotal;
2.5.17.84. RSA NetWitness;
2.5.17.85. ServiceNow;
2.5.17.86. Shodan;
2.5.17.87. Slack;
2.5.17.88. Solarwinds Log Manager;
2.5.17.89. Splunk;
2.5.17.90. SSH;
2.5.17.91. Symantec Blue Coat ProxySG;
2.5.17.92. Symantec Endpoint Protection;
2.5.17.93. syslog-ng;
2.5.17.94. Telegram;
2.5.17.95. Tenable Nessus;
2.5.17.96. Tenable SecurityCenter;
2.5.17.97. TheHive;
2.5.17.98. ThreatConnect;
2.5.17.99. Twitter;
2.5.17.100. Unshorten.me;
2.5.17.101. URLScan.io;
2.5.17.102. URLVoid APIVoid;
2.5.17.103. Vade Secure IsItPhishing;
2.5.17.104. VirusTotal;
2.5.17.105. Vulners;

2.5.17.106. WhoAPI;
2.5.17.107. Whois XML API;
2.5.17.108. Wireshark.

2.5.18. Deve possuir um guia de API bem documentado com diversas possibilidades de consumo não limitando-se há:
2.5.18.1. Listar requisições dos usuários;
2.5.18.2. Criar novas requisições;
2.5.18.3. Atualizar informações sobre requisições e chamados;
2.5.18.4. Enviar solicitação de troca de senha para usuário;
2.5.18.5. Deletar requisição;
2.5.18.6. Gerenciar e executar playbooks.

3. Item 3 - Solução de micro segmentação de ambiente corporativo

3.1.1. Deve suportar a micro segmentação tanto em dispositivos físicos quanto em dispositivos virtualizados (independente da tecnologia utilizada para virtualização);

3.1.2. Deve possibilitar a criação de ilhas no ambiente, onde os ativos tenham sua comunicação restrita apenas ao que for previamente identificado e liberado, principalmente no contexto de aplicações que devem ter sua comunicação liberada apenas no contexto estritamente necessário.

3.1.3. Deverá suportar, minimamente, a instalação de agentes nos seguintes sistemas operacionais:
3.1.3.1. Amazon Linux;
3.1.3.2. CentOS 5 ou superior;
3.1.3.3. Oracle Linux 5 ou superior;
3.1.3.4. Redhat 5 ou superior;
3.1.3.5. Debian 7 ou superior;
3.1.3.6. Ubuntu 14.04 ou superior;
3.1.3.7. Windows Server 2008 R2 SP1 ou superior;
3.1.3.8. Windows 7 ou superior;
3.1.3.9. MacOS 11 ou superior.

3.1.4. No caso de dispositivos que não possam receber os agentes, a solução deve disponibilizar um mecanismo que permita cadastrar os mesmos e criar regras para ditar como estes recursos podem interagir com a rede protegida.

3.1.5. Deve suportar a instalação dos agentes em nuvens públicas ou privadas, independente do provedor, baseando-se apenas na compatibilidade de sistemas operacionais já citada.

3.1.6. Deverá suportar a segmentação de ambientes em contêineres, atendendo minimamente as seguintes plataformas e tecnologias relacionadas:

3.1.7. Orchestration Platforms

3.1.7.1. AWS Elastic Kubernetes Service (EKS);
3.1.7.2. Azure Kubernetes Service (AKS);
3.1.7.3. Google Kubernetes Engine (GKE);
3.1.7.4. K3s;
3.1.7.5. Kubernetes;
3.1.7.6. OpenShift;

3.1.7.7. Rancher Kubernetes Engine (RKE).

3.1.8. Container Runtime

3.1.8.1. Containerd;
3.1.8.2. Docker;
3.1.8.3. CRI-O.

3.1.9. Network Plugins

3.1.9.1. AWS VPN CNI;
3.1.9.2. Kubenet;
3.1.9.3. Azure CNI;
3.1.9.4. Calico;
3.1.9.5. Flannel;
3.1.9.6. OpenShift SDN (OVS);
3.1.9.7. OVN-Kubernetes (OVN);
3.1.9.8. Canal.

3.1.10. Deverá ser independente de hardware, ou seja, funcionar em qualquer infraestrutura de rede composta pela compatibilidade requirida já especificada.

3.2. Características de visibilidade

3.2.1. A solução deverá, a partir da instalação dos agentes, fornecer um mapa de dependência de aplicativos em tempo real de como a comunicação de rede está acontecendo, de forma a proporcionar o completo entendimento dos administradores para uma melhor tomada de decisão.

3.2.2. Além do mapa visual de comunicações, a solução ainda deverá fornecer meios para filtragem específica de comunicações em modo de log na console, contendo todos os detalhes de origem, destino, portas, protocolos e aplicações internas que realizaram a comunicação.

3.2.3. A visão detalhada dos logs deve permitir a criação de regras para fluxos detectados como bloqueados a partir de interação com os logs, apenas selecionando as comunicações desejadas.

3.2.4. A solução deve realizar sugestões inteligentes de como a regra deverá ser criada, de forma a facilitar a ação do administrador da ferramenta.

3.2.5. A visão detalhada do tráfego de rede deverá mostrar quais os processos do sistema operacional foram responsáveis por aquela comunicação, permitindo ainda que as regras possam controlar essa comunicação apenas quando esse mesmo processo iniciar a comunicação, garantindo que aquela comunicação de fato corresponde a aplicação de origem para a plataforma do sistema operacional.

3.2.6. Os agentes da solução deverão alimentar continuamente a console central, de forma que o administrador de rede sempre tenha contexto atualizado sobre as comunicações que estão ocorrendo.

3.2.7. A visibilidade gerada pela solução deverá suportar conceitos de RBAC, ou seja, segmentar a possibilidade de controle e visibilidade na console baseado no nível de permissão atribuído ao administrador autenticado na plataforma.

3.2.8. Os dados de visibilidade deverão estar disponíveis para consulta na console por pelo menos 90 dias.

3.3. Regras de segmentação e visibilidade

3.3.1. A solução deverá permitir a criação de rótulos a serem aplicados nas cargas de trabalho, de maneira que a identificação dos servidores e aplicações do ambiente sejam facilmente reconhecidos.
3.3.2. Os rótulos deverão suportar o conceito de escopo da rede, ou seja, produção, homologação e desenvolvimento, assim como a qual ambiente e localização o ativo está incluso.
3.3.3. As regras deverão ser criadas baseadas em dois critérios principais, sendo eles: Escopo interno, ou seja, apenas entre serviços pertencentes a mesma aplicação identificada ou também no contexto de escopo externo, no caso de aplicações diferentes que precisam de comunicação de rede entre si.
3.3.4. Todos os rótulos e atributos definidos nos tópicos anteriores deverão estar disponíveis amplamente para criação de políticas, seja pelo papel que o ativo executa, ou aplicação representada, ambiente ou localização.
3.3.5. As regras deverão possibilitar a criação granular, baseado nos rótulos e atributos solicitados, baseados em origem, destino, porta, protocolo, aplicação e processos do sistema operacional para os sistemas operacionais Windows e Linux.
3.3.6. As regras também deverão conseguir utilizar listas de IPs, sub redes, FQDNs, range de portas e portas customizadas para controles específicos.
3.3.7. Deverá suportar a utilização de portas dinâmicas, ou seja, baseado no processo do sistema operacional e não em um range específico.
3.3.8. A solução deverá permitir a duplicação de políticas por parte do administrador, de forma a facilitar o processo de criação de regras.
3.3.9. A solução deverá possuir, de forma nativa, um templates de política para serviços como Microsoft Active Directory, SQL Server, SharePoint, Exchange, Microsoft System Center, SharePoint e Windows Server Update Service, já contendo todas as portas, protocolos e processos catalogados e com regras criadas, de forma a facilitar a implementação inicial sem impactos na rede corporativa.
3.3.10. A solução deverá suportar a importação e exportação de políticas pela console administrativa.
3.3.11. A solução deverá permitir a atribuição de políticas em grupos específicos de hosts ou em hosts específicos.
3.3.12. No caso de remoção do agente da solução, todas as regras criadas deverão ser imediatamente removidas.
3.3.13. A solução deverá possuir integração nativa com scanners de vulnerabilidade para controle contextual de ativos com base nas vulnerabilidades que ele possui.
3.3.14. Essa integração deverá permitir a ingestão de dados de, pelo menos, os seguintes fabricantes: Qualys, Tenable e Rapid7.
3.3.15. A solução deverá permitir integração com Active Directory para controle de regras de acesso baseado em grupos do Active Directory.
3.3.16. A solução deverá suportar meios para visualização de impacto das políticas antes de aplicação de modificações das mesmas.
3.3.17. A visibilidade da solução deverá permitir facilmente a identificação de quais tráfegos estão ocorrendo por qual política de definida e até mesmo se não existe uma política para o tráfego identificado.
3.3.18. A aplicação de políticas não deverá impor a criação de nenhuma camada de firewall nos hosts protegidos, ou seja, visando não gerar sobrecarga nos mesmos, o agente da

solução deverá apenas orquestrar o firewall nativo dos sistemas operacionais para aplicação de todas as regras definidas na console.

3.3.19. No caso de dispositivos Windows, a aplicação das políticas (enforcement) deverá ser realizada por meio da orquestração do Microsoft Windows Filtering Platform nativo do sistema operacional, sem a necessidade sobrecarregar o mesmo com camadas de software adicionais.

3.3.20. No caso de dispositivos Linux, o enforcement das políticas deverá ser realizado através da orquestração do Linux IP Tables nativo do sistema operacional, sem a necessidade sobrecarregar o mesmo com camadas de software adicionais.

3.3.21. O enforcement de políticas e instalação do agente não deverá requerer nenhum tipo de modificação no kernel do sistema operacional.

3.3.22. A solução deverá suportar o controle de políticas para regras de inbound e outbound no firewall dos ativos protegidos.

3.3.23. Deverá ser possível a criação de regras para "isolamento" de ativos na rede, de forma que a comunicação dos mesmos seja restrita apenas ao que tenha sido previamente definido, impedindo, por exemplo, que ativos contaminados por ameaças possam se comunicar na rede com os demais servidores do datacenter.

3.3.24. Deve possibilitar a integração com recursos IPSEC nativos do sistema operacional para criptografar o tráfico entre componentes protegidos pela solução.

3.3.25. As políticas da solução devem possibilitar a coexistência com políticas de firewall que já existam em determinados hosts protegidos.

3.3.26. Deve permitir a identificação e proteção do ambiente a partir de componentes que não tenham o agente instalado.

3.3.27. O agente da solução deve se automonitorar quanto a falhas de processo ou eventos de adulteração e reiniciar, se necessário, para garantir a funcionalidade contínua.

3.3.28. O agente da solução deve monitorar continuamente as regras aplicadas evitando assim que as mesmas sejam modificadas ou mesmo eliminadas ("anti tampering").

3.3.29. O agente deve ser protegido por uma senha adicional prevenindo a remoção acidental ou proposital do mesmo.

3.3.30. Deverá reter ao menos as 1.000 versões da política para rollback em caso de necessidade e remoção automática das versões mais antigas para melhorar o desempenho.

3.4. Gestão de vulnerabilidades

3.4.1. A solução deverá possuir integração nativa com scanners de vulnerabilidade para realizar o controle contextual de ativos com base nas vulnerabilidades identificadas nos mesmos.

3.4.2. Essa integração deverá permitir a ingestão de dados de, pelo menos, os seguintes fabricantes: Qualys, Tenable e Rapid7.

3.4.3. A solução deverá gerar visões específicas, a partir da ingestão de dados de vulnerabilidades, sobre como as portas e aplicações vulneráveis estão se comunicando na rede corporativa.

3.4.4. A partir desta integração, deverá ser possível visualizar o nível de risco do ativo durante a análise de tráfego da rede corporativo.

3.4.5. O risco de exposição deverá ser calculado para cada carga de trabalho, fornecendo uma medição numérica com base no número e na gravidade das vulnerabilidades em

uma carga de trabalho combinada com todos os caminhos que conectam uma porta vulnerável.

3.4.6. Quando não existir a possibilidade de correção da vulnerabilidade do ativo, a solução deverá fornecer sugestões de ajustes para regras de micros segmentação daquele ativo, de forma a mitigar o maior número possível de brechas do mesmo.

3.5. Arquitetura e implementação

3.5.1. A solução deverá ser compatível com o modelo SaaS – Software as a Service, ou seja, não deve requerer nenhum tipo de instalação de componentes ou máquinas virtuais no ambiente para funcionamento de seus componentes administrativos.

3.5.2. A plataforma SaaS do fornecedor deve possuir certificação SOC 2 Tipo 2 emitido por auditor independente.

3.5.3. Os agentes devem se comunicar diretamente com a plataforma SaaS sem a necessidade de agregadores caracterizando-se assim uma aplicação de duas camadas.

3.5.4. O agente deverá suportar a utilização de servidores proxies caso o seguimento de rede não possua comunicação direta com a internet.

3.5.5. Os componentes administrativos da solução não deverão possuir dependência de nenhum outro componente de rede ou infraestrutura para o seu perfeito funcionamento.

3.5.6. A implementação do agente deverá ser compatível com ferramentas de deployment de software de uso geral como SCCM, Chef, Ansible, Puppet ou outra que seja passível de execução de um script shell ou PowerShell.

3.5.7. Deve proporcionar a instalação do agente de forma manual, através de msi e scripts já elaborados e disponibilizados pelo fabricante da solução.

3.5.8. O processo de remoção e atualização de versão dos agentes deverá seguir os mesmos modelos já definidos de instalação.

3.5.9. Deve ser possível a implementação dos agentes em modo apenas de monitoramento, fornecendo visibilidade do tráfego para que o administrador da solução criar regras e planejar a mudança para modo bloqueio com visibilidade e contexto de todo o tráfego de rede.

3.5.10. A solução deverá permitir a criação de políticas, fornecendo apenas a visibilidade e impacto das mesmas, para posterior provisionamento da mesma e enforcement das regras.

3.5.11. Deve permitir integração via SAML 2.0 com IDPs externos, como no mínimo o Microsoft Azure AD\Entra, possibilitando autenticação na console administrativa a partir de um usuário gerenciado internamente pela CONTRATANTE.

3.5.12. Deve possuir auditoria para rastreamento de todas as modificações realizadas na console administrativa.

3.5.13. Deve possibilitar a capacidade de filtragem de tráfego com base em aplicações, rótulos, ambientes, período de tempo, status da política, etc. Permitindo ainda exportação dos logs para consumo externo a ferramenta.

3.5.14. Não deve haver limitação de número de regras e quantidade de tráfego a ser analisado pela ferramenta.

3.5.15. A comunicação entre o agente e a console central deve ser criptografada.

3.6. API e integrações

3.6.1. A solução deve possuir uma API forte e bem documentada.
3.6.2. Via API dever ser possível realizar operações em políticas e controlar os ativos da solução.
3.6.3. Deve ser baseada em HTTP e ser compatível com métodos GET, PUT, POST e DELETE.
3.6.4. Dever ser autenticada via chave a ser gerada no portal da solução.
3.6.5. Deve possibilitar integração com ferramentas DevOps como Chef, Puppet, Ansible e SCCM.
3.6.6. Deve possuir integração com ferramentas de SIEM, sendo no mínimo suportado as soluções QRadar, Splunk ou Arcsight.
3.6.7. Os logs podem ser transmitidos para outros SIEMs ou Syslog Servers nos formatos JSON, CEF ou LEEF.

4. Item 4 - Solução de simulação de ataques em ambiente corporativo

4.1. Requerimentos Gerais

4.1.1. A solução deve proporcionar a simulação, avaliação e gestão estendida da postura de segurança da organização, possibilitando a medição da efetividade através de testes e avaliações do nível de proteção tanto do perímetro quanto em ambientes internos. Isso deve proporcionar uma compreensão completa da eficácia dos controles de segurança.
4.1.2. A solução deve permitir que os profissionais de segurança possam identificar, diagnosticar, gerenciar, controlar e validar sua postura de segurança cibernética de ponta a ponta.
4.1.3. A plataforma deve fornecer capacidades diferentes que permitam escalabilidade sem troca futura, atendendo minimamente conceitos como validação de brechas e simulações de ataques (BAS), automatização de Red e Purple Teaming (CART), gerenciamento da superfície de ataques (ASM) e priorização e contextualização de vulnerabilidade.
4.1.4. A plataforma deve se alinhar ao programa de gerenciamento contínuo de ameaças - CTEM do Gartner, atendendo minimamente 4 das etapas deste programa: escopo, descoberta, priorização, validação e mobilização.
4.1.5. A solução deve permitir recriar cenários reais de ataques à infraestrutura de segurança da organização sem gerar impactos ao ambiente.
4.1.6. A solução deve fornecer a possibilidade de executar os ataques baseados em táticas, técnicas e procedimentos que os atacantes e grupos de criminosos cibernéticos utilizam, sendo eles utilizados em pelo menos os seguintes cenários:
    4.1.6.1. Reconhecimento externo (EASM) – Validação de domínios e subdomínios a fim de identificar fraquezas e vulnerabilidades expostas na internet referente a organização. Nesta fase, a solução deverá utilizar de fontes de inteligência aberta (OSINT) para descoberta de credencias e outras informações as quais possam beneficiar um atacante.

4.1.6.2. Reconhecimento interno (IASM) – A solução deve fornecer um caminho para correlação dos dados de reconhecimento externo e apresentar um mapa de ataque contendo o caminho de ataque interno ao qual um atacante poderia percorrer, levando em consideração cenários de avaliação do serviço de diretórios (AD) local ou nuvem assim como provedores de nuvem sendo minimamente suportado AWS, Azure e GCP.

4.1.6.3. Base Inicial – Ataques relacionados a fase de acesso inicial, execução, persistência e escalação de privilégio.

4.1.6.4. Execução & C2C – Técnicas de evasão de defesa, acesso de credenciais e descoberta do ambiente.

4.1.6.5. Propagação na rede – Movimentação lateral, coleção e comunicação externa C2C, permitindo que o atacante mova para seus objetivos finais.

4.1.6.6. Ações com objetivos – Comunicação externa para exfiltração de dados e geração de impacto.

4.1.7. A solução deve permitir simulações automáticas, orientadas a avaliar os ajustes e configurações de distintos controles de segurança.

4.1.8. A solução deve permitir a simulação de táticas, técnicas e procedimentos maliciosos de forma individual, assim como permitir a simulação de forma secundária respeitando o ciclo de vida de um ataque.

4.1.9. A solução deve identificar quais testes foram executados com êxito e quais falharam durante o processo de prevenção. Para os resultados, deve haver a possibilidade de criação de evidência da detecção e/ou bloqueio através de uma integração com um SIEM, e/ou no próprio dispositivo que detectou e/ou bloqueou a simulação.

4.1.10. As simulações serão executadas a partir de componentes da solução ou equipamento reservado exclusivamente para ela.

4.1.11. A solução deve ser implementada em modelo de nuvem SaaS, podendo ela permitir a implementação em regiões de nuvem disponíveis para o território brasileiro quando necessário.

4.1.12. A solução deve possuir suporte e licenciamento realização de avaliações em diferentes vetores de ataque tais como, endpoint, rede, web e cloud.

4.1.13. A solução deve possuir um módulo capaz de fornecer através de sua rede de inteligência ameaças emergentes e relevantes para a plataforma, fornecendo informações detalhadas sobre tais ameaças e quais medidas de remediação recomendadas.

4.1.14. A solução deve permitir integração com soluções de gestão de vulnerabilidades, fornecendo apoio para priorização de riscos encontrados na organização, através do consumo dos relatórios fornecidos pela ferramenta de gestão de vulnerabilidades, deve ser possível apresentar de forma clara quais CVEs estão disponíveis na plataforma de ataques para simulação.

4.2. Requerimentos funcionais e arquitetura

4.2.1. A solução deve permitir integração com diferentes serviços de SSO, tais como: ADFS, Azure AD\Entra, OKTA, JumpCloud entre outros.

4.2.2. A solução deve permitir a integração com diferentes plataformas de segurança via API.

4.2.3. Todos os componentes da solução devem poder ser gerenciados por uma console central, permitindo a configuração, monitoração e atualização dos agentes de forma automática.

4.2.4. Toda a comunicação entre os componentes deve ser feita através de protocolos seguros como HTTPS com TLS 1.2 ou superior.

4.2.5. A solução deve suportar a comunicação dos componentes instalados por meio de um proxy web.

4.2.6. O processo de instalação dos agentes deve ser feito de forma manual, automatizada ou em lote.

4.2.7. A solução não deve possuir limitações em seus agentes, simuladores ou atores de ataque.

4.2.8. A solução deve fornecer em cada um de seus vetores o nível de risco encontrado após cada simulação, devendo a plataforma comparar o resultado atual com o anterior para fornecer uma visão de avanço ou regresso dos testes, estes dados poderão ser utilizados para definição de baseline do ambiente.

4.2.9. A solução deve suportar regras SIGMA e fornecer para alguns cenários a opção de convertê-las em buscas (queries) as quais poderão ser utilizadas para buscas em plataformas de SIEM ou até mesmo criação de regras de correlação.

4.2.10. A solução deve ser capaz de poder trocar informações com outras tecnologias de segurança do ambiente para fornecer, melhor visibilidade na detecção, gestão de vulnerabilidades, automação de playbooks e validação de processos internos. Permitindo no mínimo as seguintes integrações:

4.2.10.1. Azure Sentinel;
4.2.10.2. BlackBerry Cylance OPTICS;
4.2.10.3. BlackBerry Cylance PROTECT;
4.2.10.4. Carbon Black;
4.2.10.5. Checkpoint Harmony Endpoint Protection
4.2.10.6. CrowdStrike Falcon;
4.2.10.7. CrowdStrike Falcon LogScale;
4.2.10.8. Cynet;
4.2.10.9. Fortinet FortiGate Firewall
4.2.10.10. Fortinet FortiAnalyzer
4.2.10.11. IBM Qradar;
4.2.10.12. InsightVM;
4.2.10.13. LogRhythm;
4.2.10.14. McAfee ESM SIEM;
4.2.10.15. MicroFocus ArcSight;
4.2.10.16. Microsoft Defender ATP;
4.2.10.17. Microsoft Defender TVM;
4.2.10.18. Palo Alto Cortex XDR;
4.2.10.19. Palo Alto Cortex XSOAR;
4.2.10.20. Palo Alto Firewall;
4.2.10.21. Qualys VM;
4.2.10.22. RSA Archer;
4.2.10.23. RSA Netwitness;
4.2.10.24. SentinelOne;
4.2.10.25. Service Now;

4.2.10.26. Securonix;
4.2.10.27. Splunk;
4.2.10.28. Sumo logic SIEM;
4.2.10.29. Tenable IO;
4.2.10.30. Tenable SC;
4.2.10.31. Trellix EDR;
4.2.10.32. Trellix HX;
4.2.10.33. Trend Micro Vision One;

4.2.11. Todos os produtos de segurança que não possuírem integração direta, devem poder ser integrados por meio soluções de correlacionamento de eventos (SIEM), permitindo a integração com produtos não homologados.
4.2.12. A solução deve fornecer suporte a regras SIGMA e suportar através de uma interface amigável capacidade de conversão das regras para padrões que possam ser utilizados em diferentes plataformas através da geração de scripts ou queries, suportando conversão para minimamente as seguintes tecnologias:
4.2.12.1. Arcsight;
4.2.12.2. Azure Sentinel;
4.2.12.3. ElastAlert;
4.2.12.4. Elastic Search;
4.2.12.5. Humio;
4.2.12.6. IBM Qradar;
4.2.12.7. Kibana;
4.2.12.8. Logpoint;
4.2.12.9. Splunk;
4.2.12.10. Sumologic.
4.2.13. A solução deve permitir a visualização do status de conexão e versão de software dos agentes, permitindo através da console realizar operações como reinicialização, deleção ou mesmo desinstalação do componente.
4.2.14. A solução deve permitir avaliar as capacidades de defesa da organização contra táticas, técnicas e procedimentos utilizados por grupos criminosos conhecidos.
4.2.15. A solução deve possuir uma biblioteca de ataques associada a criminosos cibernéticos e deve atualizá-la de forma automática quando novas ameaças emergentes surgirem.
4.2.16. O portfólio de ataques da solução deve ser baseado em frameworks e padrões de segurança cibernética, tais como MITRE ATTACK, OWASP, CVSS e NIST.
4.2.17. As simulações de ataque devem corresponder, sempre que possível, a uma técnica descrita pelo MITRE e apresentar detalhes sobre os respectivos TTPs.
4.2.18. A solução deve incluir diversas simulações de ataque predefinidas, que incluem minimamente os seguintes tipos de ataques:
4.2.18.1. Para validação do vetor de endpoint a plataforma deve oferecer simulações de ataque para:
4.2.18.1.1. Ransomware: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de ransomwares, devendo estes buscar arquivos sensíveis no host e utilizar chaves geradas de forma segura e controlada para criptografia de arquivos.
4.2.18.1.2. Worm: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de worms, devendo

estes realizar a descoberta de hosts vulneráveis e simular a proliferação para eles através de técnicas utilizando protocolos tais como SMB ou NFS.

4.2.18.1.3. Trojan: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de trojans, estes deverão coletar informações gerais do host como nome de usuário, e-mail e outras. Podendo também estabelecer comunicação utilizando diferentes métodos de reverse shell.

4.2.18.1.4. Antivírus: Validação da efetividade de inspeção e proteção de ameaças contra arquivos maliciosos, os malwares escritos em disco devem ser atualizados diariamente através de diversos feeds de segurança.

4.2.18.1.5. MITRE ATT&CK: Validação da efetividade dos recursos de anti-malware através da execução de comandos customizados que devem simular o comportamento de adversários mapeados no framework ATT&CK.

4.2.18.2. Para validação do vetor de web gateway a plataforma deve oferecer simulações de ataque para:

4.2.18.2.1. Phishing: Validação da efetividade dos recursos de filtragem dinâmica de URL e proteção de ataques de phishing, acessando IPs e URLs reais associados a ataques de phishing identificados recentemente.

4.2.18.2.2. Ransomware: Validação da efetividade dos recursos de filtragem dinâmica de URL e proteção contra ransomware, acessando IPs e URLs reais associados ao Ransomware, como servidores Botnet, C&C, sites de distribuição e pagamento.

4.2.18.2.3. C&C: Validação da efetividade dos recursos de filtragem dinâmica de URL e proteção contra malwares, acessando IPs e URLs reais associados a atividades de C&C como Botnet.

4.2.18.2.4. Política: Validação da efetividade da proteção de filtro de categorias do gateway da web. A validação é feita através do acesso a diferentes sites divididos por categorias, como pornografia, jogos de azar etc.

4.2.18.2.5. Arquivos: Validação da efetividade dos recursos de inspeção de tráfego de entrada e eficácia da proteção contra arquivos maliciosos. A validação é realizada através da tentativa de baixar por HTTPS uma variedade de malwares simulados que imitam o comportamento de worms, trojans e ransomware.

4.2.18.2.6. Exploits: Validação da efetividade dos recursos de inspeção de tráfego de entrada e eficácia da proteção contra arquivos maliciosos. A validação é realizada através da tentativa de baixar por HTTPS uma variedade de malwares que simulam o comportamento de worms, trojans e ransomware.

4.2.18.3. Para validação do vetor de email gateway a plataforma deve oferecer simulações de ataque para:

4.2.18.3.1. Ransomware: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por ransomwares, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

4.2.18.3.2. Worm: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por worms, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

4.2.18.3.3. Malware: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por diferentes códigos maliciosos (malwares), estas validações devem poder simular cenários interativos envolvendo técnicas de exploração de controles como UAC, roubo de credenciais e C&C. Toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente

4.2.18.3.4. Payload: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos em payloads, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

4.2.18.3.5. Exploits: Validação da efetividade dos recursos de proteção de e-mail através da execução de diversos arquivos que exploram diferentes vulnerabilidades em programas, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

4.2.18.3.6. Dummy: Validação da efetividade dos recursos de proteção de e-mail através da execução de diferentes técnicas de execução de códigos, isto deve incluir uso de recursos conhecidos como payloads do metasploit como exemplo MessageBox. Toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

4.2.18.3.7. True File Type Detection: Validação da efetividade dos recursos de proteção de e-mail através do envio de arquivos com diferentes extensões não pertencentes ao seu formato de arquivo original, este teste deve apoiar na identificação de possíveis brechas que podem ser utilizadas para comprometer o ambiente através da falsificação de formatos originais de arquivos.

4.2.18.4. Para validação do vetor de web application firewall (WAF) a plataforma deve oferecer simulações de ataque para minimamente:

4.2.18.4.1. SQL injection;

4.2.18.4.2. Cross-site scripting (XSS);

4.2.18.4.3. NoSQL Injection;

4.2.18.4.4. XML Injection;

4.2.18.4.5. Path Traversal;

4.2.18.4.6. File inclusion for remote code execution;

4.2.18.4.7. Command injection;

4.2.18.4.8. WAF Bypass.

4.2.18.5. Para validação de movimentação lateral a plataforma deve oferecer simulações de ataque que permitam validação dos seguintes métodos:

4.2.18.5.1. Pass-the-Password;

4.2.18.5.2. Pass-the-Ticket;

4.2.18.5.3. Pass-the-Hash;

4.2.18.5.4. Brute Force;

4.2.18.5.5. LLMNR/NBT-NS Poisoning and Relay;

4.2.18.5.6. Kerberoast;

4.2.18.5.7. Password Spraying;

4.2.18.5.8. Steal LAPS passwords.

4.2.19. A solução deve fornecer a possibilidade de criar modelos customizados nos vetores de ataque sem causar impactos ao ambiente.

4.2.20. Para o cenário de movimentação lateral, o agente da solução deve poder atuar exatamente como um atacante no ambiente, não devendo este depender da implementação de outros agentes para validação dos diferentes métodos. A plataforma deve possuir capacidade de realizar um "pivoting" na rede e fornecer um mapa de toda trilha percorrida e alvos alcançados, podendo os alvos serem considerados ou não joias da coroa (Crown Jewels).

4.2.21. A solução deve fornecer um caminho para validação completa da cadeia de ataque (Full Kill-chain), permitindo assim que seja avaliadas fases tais como pré-exploração, exploração e pós-exploração.

4.2.22. A solução deve permitir a criação de campanhas de phishing customizadas para avaliação da conscientização dos colaboradores em cenários reais, as campanhas devem minimamente permitir que sejam criados conteúdos através da plataforma em português.

4.2.23. Cada um dos testes ou ações hospedadas na base de conhecimento da solução, deve ter uma descrição e o código da técnica ou das táticas de acordo com a nomenclatura do MITRE.

4.2.24. A solução deve ter a capacidade de repetir periodicamente os testes que o usuário deseja e comparar os resultados de cada execução com um resultado esperado, permitindo definir se o ataque foi detectado, bloqueado e que tipo de registro foi detectado no SIEM ou nas tecnologias de segurança testadas.

4.2.25. Os componentes de ataque devem poder ser instalados, minimamente, nos seguintes ambientes:

- 4.2.25.1. Windows 11 build 22000+, 10 build 1067, 8.1, 7 SP1;
- 4.2.25.2. Server 2012 ou superior;
- 4.2.25.3. Linux Alpine 3.12, Ubuntu 16.04, Debian 10, CentOS 7, RHEL 7, Fedora 33, openSUSE 15 e SUSE Enterprise 12 SP2 ou versões superiores
- 4.2.25.4. MacOS 10.15x ou superior.

4.2.26. A solução deve realizar as simulações de ataque através de um agente único ao qual deverá ser capaz de executar ataques em diferentes vetores de forma individual ou simultânea.

4.2.27. A solução deve permitir através de um framework aberto a customização de diferentes cenários e cadeias de execução que sejam compatíveis minimamente com as seguintes plataformas:

- 4.2.27.1. Powershell;
- 4.2.27.2. Python;
- 4.2.27.3. Bash;
- 4.2.27.4. Sh;
- 4.2.27.5. CMD.

4.3. Requerimentos de gestão e relatório

4.3.1. A solução deve possuir uma console em nuvem a qual deverá ser utilizada para orquestração e envio dos ataques.

4.3.2. O painel principal (dashboard) deve apresentar de forma clara os vetores licenciados assim também como informações sobre controles de segurança, ameaças emergentes,

integrações e outros detalhes importantes que possam ser utilizados para melhor compreensão dos testes realizados.

4.3.3. A console de gerenciamento deve permitir a criação de painéis dinâmicos aos quais permitam a customização e manipulação de dados a serem apresentados no novo painel (dashboard).

4.3.4. A console de gerenciamento deve possuir um dashboard que exiba todas as informações de vulnerabilidades baseadas em ataques, incluindo proteção geral de controles de segurança, principais vulnerabilidades encontradas em ativos de rede, principais ativos vulneráveis, principais CVEs e muito mais.

4.3.5. A console deve possuir em seu painel principal a opção de rastreabilidade em tempo de execução dos testes.

4.3.6. A console deve fornecer uma visão global dos itens que foram identificados.

4.3.7. A console deve fornecer uma visão detalhada após integração com plataformas de gestão

4.3.8. A solução deve possuir uma interface amigável em seu agente para facilitar o gerenciamento de ataques em andamento, visualização de logs e configurações pertinentes aos recursos envolvidos no ataque, proxy, e-mail etc.

4.3.9. Após conclusão dos ataques envolvendo de forma individual ou conjunta os vetores de ataque deverá ser fornecido um score de risco, este score deve prover uma clara visão sobre a maturidade atual e histórica do ambiente.

4.3.10. A solução deve permitir a geração de relatórios técnicos ou gerenciais aos quais devem conter minimamente:

4.3.11. Informações sobre o score de risco atual;

4.3.12. Descrição e recomendação para correção dos problemas encontrados;

4.3.13. A solução deve permitir em sua guia de relatórios a extração de dados completos contendo informações gerais de todos os ataques realizados em um determinado vetor, assim também como oferecer opções para download de relatórios em formato PDF, CSV ou TXT.

4.3.14. A solução deve permitir a geração de relatórios e download dos mesmos através de sua interface assim como permitir o envio dos mesmos através de e-mail.

4.3.15. A solução deve permitir a geração de relatórios e visão detalhada por ambientes.

4.3.16. A solução deverá prover uma visão clara do desempenho individual de cada vetor de ataque assim como também possuir um gráfico de comparação para benchmark.

4.3.17. A solução deve fornecer um caminho simples para minimamente:

4.3.18. Realizar a abertura de chamados;

4.3.19. Gerenciar usuários da plataforma;

4.3.20. Acessar documentações do produto;

4.3.21. Gerenciar logs e atividades em execução.

4.3.22. A console deve fornecer uma guia para download e gestão dos agentes implementados.

5. Item 5 - Solução de proteção de usuários e controle de dados em nuvem

5.1. Características Gerais

5.1.1. Todas as funcionalidades deverão ser ofertadas na nuvem como um serviço, utilizando um único agente instalado na máquina do usuário. A nuvem deverá ser distribuída globalmente , incluindo o Brasil e deverá ser licenciada para pelo menos 1500 usuários;

5.1.2. A plataforma de segurança deverá ter ponto de presença no Brasil, onde todos os usuários em território nacional terão suas transações processadas, incluindo todas as inspeções e aplicação de políticas de controle de acesso e segurança em tempo real;

5.1.3. O Data Center localizado no Brasil deverá ter rede independente com Sistema Autônomo e conectividade, redundante, em PTT (Ponto de Troca de Tráfego) no Brasil com peering com provedores de serviços, empresas de telecomunicações, CDNs (Content Delivery Network) e provedores de nuvem pública tais como (AWS, Microsoft e Google). Desta forma garantindo a melhor experiência e baixa latência aos usuários;

5.1.4. Não serão aceitos sistemas baseados em hardware ou software projetados para uso genérico, ou de código aberto ("open source").

5.1.5. A solução deverá suportar as seguintes opções de arquitetura de conectividade à plataforma de segurança, com suporte a todas as funcionalidades descritas neste certame no que tange controle de acesso e segurança à Internet e aplicações SaaS:

5.1.5.1. Com Agentes instalados nas máquinas;

5.1.5.2. Com túneis GRE (Generic Routing Encapsulation) ou IPSec, sem a necessidade de uso de agentes nas máquinas dos usuários, possibilitando saídas locais à Internet de filiais, sede e data center;

5.1.5.3. Utilização de proxy explícito via arquivos PAC (Proxy Auto-Configuration), neste caso com funcionalidades limitadas a acesso Web HTTP, HTTPS e FTP;

5.1.6. A solução de segurança, proteção de dados, controle de acesso à Internet e aplicações deverá fornecer SLA de disponibilidade de 99.999% e de latência da inspeção completa de todos os componentes.

5.1.7. Toda a plataforma de segurança deverá suportar geração de logs detalhados de acesso dos usuários Web, Aplicações Cloud, Bloqueios de Segurança e acessos;

5.1.8. Todas as inspeções e aplicações de políticas deverão ser realizadas na nuvem. Com exceção da verificação de postura, nenhuma inspeção de controle de acesso ou segurança deverá ser realizada na máquina do usuário.

5.1.9. A solução de segurança, proteção de dados e controle de acesso à Internet deverá oferecer suporte à criação de múltiplos administradores com privilégios distintos e segmentados. Por exemplo, políticas criadas por um administrador global não poderão ser excluídas ou alteradas por um administrador regional ou de um departamento específico;

5.1.10. Deve oferecer suporte a uma hierarquia entre as contas administrativas que garanta que as políticas e as configurações definidas por administradores com hierarquia mais alta não possam ser substituídas por administradores com hierarquia menor;

5.1.11. No caso da utilização de agentes, a gestão de como o tráfego será encaminhado a plataforma, incluindo eventuais exclusões específicas (bypass), deverá ser gerenciada de maneira centralizada em uma console Web com o contexto de usuário e grupos de usuários. Não serão aceitas soluções que requeiram alteração ou customizações diretamente na máquina do usuário;

5.1.12. O usuário deve ser capaz de reportar um problema diretamente do agente instalado no dispositivo;
5.1.13. O usuário deve ser capaz de iniciar uma captura de pacotes diretamente do agente instalado no dispositivo;
5.1.14. O agente único deve ser compatível com no mínimo os seguintes sistemas operacionais:
    5.1.14.1. Windows 11, 10 e 8;
    5.1.14.2. Fedora;
    5.1.14.3. Ubuntu;
    5.1.14.4. Debian
    5.1.14.5. CentOS;
    5.1.14.6. MacOS 10.10 e superiores;
    5.1.14.7. IOS 9 e superiores;
    5.1.14.8. Android 8 e superiores;
5.1.15. Toda a solução proposta deverá ser implementada com autenticação dos usuários integrada e suportar aplicações de políticas granulares com base em nome do usuário, departamento e grupos, integrados com a plataforma Microsoft Azure AD\Entra da CONTRATANTE utilizando protocolo SAML 2.0 (Security Assertion Markup Language).
5.1.16. A solução de segurança deverá realizar, em uma única plataforma, sem passar por inspeção em múltiplos componentes de rede dentro da nuvem do fabricante ou de terceiros, os controles de acesso e proteção de segurança para acesso à Internet e aplicações SaaS, consolidando capacidades de soluções de SWG e FWaaS.
5.1.17. Os mecanismos de inspeção da plataforma (URL filtering, Antivirus, etc) devem verificar todo o conteúdo dos pacotes de forma simultânea e em uma única abertura;
5.1.18. A solução deverá integrar-se nativamente e enviar em tempo real logs para plataformas de SIEM (Security Information and Event Management) como Splunk, IBM Qradar e MS Sentinel;
5.1.19. A solução deve ser capaz de fornecer a visualização de logs em tempo real;
5.1.20. A solução deverá armazenar os logs de auditoria por no mínimo 4 meses;
5.1.21. Os logs de auditoria devem conter no mínimo:
    5.1.21.1. Ação: Importação, relatório, atualização, Patch, Login e Logout, Criação, Deleção;
    5.1.21.2. IP do Cliente;
    5.1.21.3. Interface utilizada: API, Console Administrativa;
    5.1.21.4. Categoria: Alerta, Backup/Restore, Gerenciamento, Controle de Acesso, Configurações de ICAP, Gerenciamento de funções, Segurança de Mobile, Controle de acesso Web, Segurança Web e configurações avançadas;
5.1.22. A cada alteração de configuração, a solução deve ser capaz de apresentar visualmente o que foi modificado;
5.1.23. A solução deve mostrar de forma visual o que foi adicionado ou excluído em uma mudança de configuração;
5.1.24. Os logs apresentados tanto no console de administração quanto os enviados as plataformas de SIEM devem conter todos os campos das transações, sem aplicar agregação ou sumarização dos eventos;

5.2. Características para funcionalidades de SWG (Secure Web Gateway)

5.2.1. Suportar inspeção de SSL/TLS em 100% do tráfego Web, sem limites de volume de transações ou percentual inspecionado, em protocolos TLS 1.0, 1.1, 1.2 e 1.3;

5.2.2. Possibilidade de criar regras granulares de exceção a inspeção SSL/TLS, com base categorias de URL, host e domínios de destino, usuário, grupo, departamento ou tipo de browsers;

5.2.3. A solução deverá identificar automaticamente tráfegos Web em portas não padrão (80 e 443) e realizar a inspeção Web completa, incluindo inspeção SSL e todas as funcionalidades de controle de acesso e segurança, mesmo em uma arquitetura de proxy transparente;

5.2.4. Capacidade de criar filtros de URLs com base em categorias e subcategorias, que deverão ser atualizadas constantemente pelo fabricante;

5.2.5. Suportar a criação de categorias customizadas;

5.2.6. Suportar a criação e manutenção de categorias, políticas de filtros de URL, regras de Firewall via API;

5.2.7. A solução deve fornecer mecanismo para bloquear o acesso Web a destinos hospedados em determinados países. Este bloqueio deverá ser configurado de maneira simples, apenas selecionando os países que deseja bloquear;

5.2.8. A solução deve suportar nativamente o idioma Português do Brasil em páginas de erro e bloqueio apresentadas aos usuários, além de permitir customização;

5.2.9. A solução deverá ter capacidade de criar políticas Web, granulares, com critérios utilizando nome do usuário, grupos, departamento, categorias de URL, localidades para liberação ou bloqueio de upload e/ou download de arquivos de acordo com o seu tipo. Exemplo: EXE, RAR, PKG, XLS, PDF.

5.2.10. A solução deverá prover proteção de antivírus e antimalware com base em assinatura de arquivos. Esta proteção deverá ser realizada para download e upload, e a base de dados de assinatura ser atualizada constantemente pelo fabricante;

5.2.11. A solução deverá fornecer proteção contra ameaças avançadas, utilizando análise estática com base em reputação do domínio, origem, idade do domínio entre outras variáveis, além de uma análise dinâmica do conteúdo Web de 100% das requisições realizada a fim de detectar potenciais riscos aos usuários, tais como injeção de JavaScript malicioso, assinaturas de roubo de cookies XSS, conteúdo ativos maliciosos, conteúdos vulneráveis de ActiveX, Phishing dentre outras;

5.2.12. A solução deverá ter atualizações constantes, minimamente diárias, de base de dados utilizada para bloqueio de segurança com base em reputação, prevenção a fraudes como Phishing, botnets, Command and Control, malware, spyware ou qualquer outro tipo de conteúdo malicioso;

5.2.13. A solução deverá detectar e bloquear assinaturas de ataques XSS (Cross Site Scripting) e de roubo de cookies dos usuários;

5.3. Características para funcionalidades de FWaaS (Firewall as a Service)

5.3.1. A solução deverá suportar capacidades de Firewall como serviço para os métodos de implantação com agentes instalados nas máquinas dos usuários, em todas as plataformas, e também sem o uso de agentes no caso de implantação com túneis GRE ou IPSec;
5.3.2. No caso da implantação com túneis GRE ou IPSec, a solução de FWaaS deverá funcionar de forma independente se o usuário estiver ou não utilizando agentes na máquina;
5.3.3. A solução deve suportar no mínimo 350Mbps por túnel IPSEC;
5.3.4. Toda a inspeção e aplicação de política de Firewall, independentemente do método de implantação, deverá ser realizada na nuvem;
5.3.5. A solução deverá suportar a criação de Localidades (exemplo: Escritório A) a partir de um túnel, GRE ou IPSec, e ter a capacidade de criar regras de firewall utilizando o critério localidade;
5.3.6. A solução deverá suportar a criação de sub-localidades, ou objetos de Firewall que entreguem o mesmo caso de uso, utilizando um IP ou uma Subnet CIRD (exemplo: 10.20.0.0/24), e estas sub-localidades poderão ser utilizadas como critérios das regras de Firewall;
5.3.7. A solução deverá suportar a criação de regras de Firewall utilizando Destino, Protocolo udp/tcp e porta;
5.3.8. A solução deverá suportar como destino IP, Subnets ou endereços completos (FQDN);
5.3.9. A solução deverá suportar a criação de políticas de Firewall bloqueando o acesso a destinos em países específicos, para todos os protocolos, não apenas o Web;
5.3.10. A solução deverá suportar criar regras, nos dois métodos de implementação com túneis ou agentes, com base em metadados do IdP como nome do usuário, grupos e departamento;
5.3.11. O FWaaS deverá ter capacidade de inspeção na camada 7, fazendo uso de tecnologia de DPI (Deep Packet Inspection), ou similar que entregue o mesmo caso de uso, para identificar nos primeiros pacotes a aplicação que está sendo utilizada;
5.3.12. A solução de FWaaS deverá possuir a capacidade de criar políticas específicas granulares para proteção de DNS;
5.3.13. A solução deverá suportar políticas de proteção de DNS granulares contendo metadados do IdP (usuário, grupos e departamento), Localidades, Origem, Domínios Destino e tipos das requisições de DNS como A, A6, AAAA, TXT, MX, etc;
5.3.14. Para a proteção de DNS a solução deverá permitir ações como bloqueio ou redirecionar para um IP específico;
5.3.15. A solução deverá ter proteção nativa contra-ataques de DNS Tunneling, permitindo bloqueio de destinos conhecidos maliciosos e mecanismo de detecção de assinaturas de ataques utilizando ferramentas conhecidas de DNS Tunneling como dnscat e iodine, independente do domínio utilizado;
5.3.16. A proteção de DNS deverá permitir bloqueio via DNS, independente do protocolo da aplicação, de domínios com baixa reputação ou com histórico de ser malicioso para Phishing, Conteúdo Malicioso e utilizados para Botnets;

5.3.17. A solução deverá ter mecanismos para bloquear requisições de DNS utilizando DOT (DNS over TLS);
5.3.18. A solução deverá detectar e redirecionar requisições de DNS utilizando DOH (DNS over HTTPS), de forma transparente, para aplicação de políticas de DNS, detalhadas nos itens acima;
5.3.19. Assim como todo o escopo do FWaaS a solução de proteção de DNS deverá suportar a implementação com o uso de agentes nas máquinas dos usuários e de túneis GRE ou IPSec da sede, filiais e data center;

5.4. Características para funcionalidades de visibilidade e controle de aplicações

5.4.1. A solução deverá identificar automaticamente uso de aplicações Cloud pelos usuários, criando visibilidade em Dashboards e relatórios de Shadow IT.
5.4.2. O relatório de Shadow IT deverá permitir identificar uso de aplicações não sancionadas e com risco elevado, além de visualizar pela própria interface Web da solução quais usuários estão utilizando estas aplicações;
5.4.3. A solução deverá suportar a identificação e permitir a classificação entre aplicações sancionadas e não sancionadas pela CONTRATANTE de no mínimo 7500 aplicações distintas. Esta base de dados deverá ser mantida e constantemente atualizada pelo fabricante e deverá conter as seguintes informações:
    5.4.3.1. Categoria da aplicação;
    5.4.3.2. Índice que indique o risco da aplicação;
    5.4.3.3. Marcador se teve vazamento de dados nos últimos 3 anos;
    5.4.3.4. Se tem suporte a Fator Duplo de Autenticação;
    5.4.3.5. Se possui mecanismos de criptografia forte;
    5.4.3.6. Se mantém logs de auditoria;
    5.4.3.7. Certificações (ISO 27001, SOC 2, PCI, etc);
5.4.4. A solução deverá permitir a criação de políticas de acesso com base na classificação da aplicação SaaS realizada pela CONTRATANTE entre sancionadas e não sancionadas, índice de risco da aplicação, além de utilizar como critério adicional na política qualquer informação detalhada no item anterior;
5.4.5. A solução deverá suportar criar políticas granulares com critérios utilizando usuário, grupo, departamento, localidade e ações específicas nas aplicações SaaS. Como por exemplo, aplicações de compartilhamento de arquivos ter as opções de Upload e Download como critério, em aplicações como Webmail, ter as opções de Leitura e Envia de e-mails como critério;

5.5. Características para funcionalidades de Monitoramento da Experiência do Usuário

5.5.1. A solução deverá realizar monitoramento sintético, a partir da máquina do usuário final, com testes de página Web e de Rede;
5.5.2. A console de gerenciamento deverá ser Web, e ter toda a configuração de forma centralizada;

5.5.3. A execução dos testes não deverá impactar o usuário final e deverá ser realizada em segundo plano, sendo transparente e imperceptível;

5.5.4. A solução deverá suportar a criação de até 6 (seis) testes Web ou de Rede;

5.5.5. Quando executado testes de Web e Rede da mesma aplicação, por exemplo Microsoft Teams, a solução deverá consolidar as métricas e apresentar uma única visão da experiência do usuário ao utilizar a aplicação SaaS;

5.5.6. A solução deverá apresentar Dashboards com o status das aplicações, bem como um mapa desta experiência distribuída em diferentes regiões do Brasil e do mundo;

5.5.7. A Geolocalização deverá ser feita de maneira automática e transparente, sem nenhuma entrada de dados manual;

5.5.8. Caso o usuário esteja dentro de localizações conhecidas da solução de SWG e FWaaS, como Localidades criadas através de túneis GRE, a solução deverá identificar que se trata de uma localidade conhecida;

5.5.9. Os testes e coleta de dados deverão acontecer no máximo a cada 15 (quinze) minutos;

5.5.10. A solução deverá coletar no mínimo as seguintes métricas de experiência:

5.5.10.1. Métricas Web:

5.5.10.1.1. Tempo total de carregamento da página;

5.5.10.1.2. Tempo de resposta do Servidor;

5.5.10.1.3. Tempo de resolução de DNS;

5.5.10.2. Métricas de Rede:

5.5.10.2.1. Latência total;

5.5.10.2.2. Latência de rede até o destino final e em todos os nós no caminho;

5.5.10.2.3. Perda de pacote total;

5.5.10.2.4. Perda de pacote até o destino final e em todos os nós no caminho;

5.5.10.2.5. Caminho completo com métricas de latência e perda de pacotes. Incluindo: computador do usuário, rede wi-fi local, roteador local, saída para Internet, Fornecedora da solução SASE, empresas de telecomunicações / ISP e destino;

5.5.11. Métricas do dispositivo do usuário:

5.5.11.1. Consumo de CPU;

5.5.11.2. Qualidade do sinal Wi-Fi;

5.5.11.3. Memória;

5.5.11.4. Nível de bateria;

5.5.11.5. Estatísticas de I/O de discos;

5.5.11.6. Sistema Operacional, Descrição do hardware, DNS utilizado, IP público e IP externo utilizado;

5.5.11.7. Histórico de eventos no sistema operacional, como troca de rede wi-fi, troca de IP, etc;

5.5.12. Utilizando as métricas do dispositivo do usuário, testes Web e de Rede, a solução deverá ter um mecanismo simples de identificar a experiência do usuário em uma aplicação, atribuindo um índice que indica se a experiência está Boa, Razoável ou Ruim;

5.5.13. A solução deverá suportar o monitoramento de Websites na Internet, aplicações SaaS e aplicações privadas fornecidas pela solução de ZTNA;

5.5.14. A solução deverá suportar a criação de alertas customizáveis com notificação por e-mail;
5.5.15. A solução deverá manter o histórico da experiência de todos os usuários, por no mínimo 48 (quarenta e oito) horas.

5.6. ACESSO A APLICAÇÕES PRIVADAS

5.6.1. A solução deverá fornecer acesso remoto a aplicações e recursos internos da CONTRATANTE, com segurança, validação de identidade, tunelamento encriptado, segregação de aplicações, verificação de postura e conexão direta com privilégio mínimo;
5.6.2. Deve permitir a conexão de até 500 usuários remotos de forma simultânea;
5.6.3. A solução deve habilitar uma arquitetura de privilégio mínimo, Zero Trust, definindo uma política de acesso granular para fornecer às pessoas certas no contexto certo, o acesso menos privilegiado aos aplicativos ou recursos e reduzir a superfície de ataque;
5.6.4. A solução deverá ser na nuvem e ter apenas o componente que irá viabilizar a conexão (conector ou publicador) instalado dentro do Data Center da CONTRATANTE em uma, ou mais, máquinas virtuais. Este componente deverá:
5.6.5. Ter arquitetura de alta disponibilidade e realizar o balanceamento de carga automaticamente, sem depender de nenhum componente de rede da infraestrutura da CONTRATANTE;
5.6.6. Não ter uma superfície de ataque exposta na Internet, não tendo nenhum IP público ou nenhuma necessidade de conexões de entrada da Internet para o componente
5.6.7. Toda a conexão deverá ser apenas de saída, do componente com destino a nuvem do fabricante;
5.6.8. Cada instância de conector ou publicador deverá suportar no mínimo 500mb de banda passante para acesso às aplicações internas;
5.6.9. Os conectores ou publicadores deverão atualizar suas versões de forma automática e realizar suas atualizações em janelas pré-definidas pela CONTRATANTE (ex: Domingo às 4 AM) de forma 100% automatizada, sem causar interrupção dos serviços e sem intervenção do administrador;
5.6.10. Permitir ser instalado de forma flexível em qualquer ponto da rede da CONTRATANTE, como por exemplo atrás de uma NAT (Network Address Translation);
5.6.11. Não criar um ponto único de conexão à rede da CONTRATANTE, sendo possível a implementação de múltiplos conectores ou publicadores em pontos da rede, data centers ou nuvem distintas, fornecendo ao usuário o acesso direto aos recursos com menor latência possível de forma dinâmica;
5.6.12. Permitir o usuário a conectar em aplicações distintas simultaneamente utilizando conectores ou publicadores em pontos da rede distintos, priorizando sempre a melhor experiência do usuário;
5.6.13. Os conectores ou publicadores deverão ser independentes, não exigindo conectividade interna completa a todos os recursos privados. Sendo possível, por exemplo, fornece acesso a aplicações ou recursos simultaneamente aos usuários em

múltiplos Data Centers ou Nuvem, mesmo que estes Data Centers ou Nuvem não tenham conexão entre eles;

5.6.14. A solução deverá autenticar o usuário em um provedor de identidade (IdP) e com base em identidade, políticas granulares, segmentação de aplicações e posturas específicas fornecer acesso a aplicações Web, ou qualquer outra com protocolo TCP e UDP, tais como (SSH, RDP, SQL, Aplicações Client-to-Server, Compartilhamento de Arquivos, etc) de forma transparente, sem a necessidade de alteração do cliente original da aplicação, criando um túnel encriptado que conectará o usuário até a aplicação e não a rede da CONTRATANTE.

5.6.15. A solução não deve operar como uma VPN fornecendo um IP da rede local, e sim conectar o usuário direto, após validação de política de identidade, postura e políticas de acesso, aos recursos e aplicações com túneis encriptados específicos;

5.6.16. Os usuários remotos não devem possuir visibilidade de aplicativos não autorizados. Os recursos não autorizados não devem apenas ser inacessíveis, mas também completamente invisíveis;

5.6.17. A definição de aplicações ou segmentos de aplicações deverá ter a flexibilidade de suportar hostname (FQDN), IP ou domínio com wildcard, como por exemplo (*.rede.local)

5.6.18. A solução deve fazer com que cada solicitação do usuário flua por meio de políticas contextual para autenticação e autorização consistentes, além de fornecer um ponto de monitoramento e registro unificado;

5.6.19. A solução deverá utilizar túneis encriptados TLS ou DTLS, versão 1.2 ou 1.3;

5.6.20. Todas as comunicações entre os componentes da solução e a infraestrutura em nuvem do fabricante devem mutualmente utilizar certificados pinados;

5.6.21. A solução deve ser blindada contra-ataques de “Man-in-the-middle” (MITM);

5.6.22. A plataforma deverá suportar múltiplos provedores de identidade (IdP - Identity Provider) e múltiplos domínios, na mesma instância e console de gestão, que suporte autenticação utilizando protocolo SAML 2.0. Viabilizando desta forma, acesso seguro a outras unidades de negócio e terceiros a recursos privados da CONTRATANTE, além de possibilitar a simplificação e modernização da conectividade e integrações futuras;

5.6.23. A solução deverá suportar controle granular de timeout de autenticação baseado em políticas específicas de acordo com o recurso ou aplicação acessada. Como por exemplo, para acesso ao ERP o usuário deverá ter se autenticado na última 1 hora pelo menos, caso negativo, solicitar autenticação novamente, para as demais aplicações o usuário deverá ter se autenticado nos últimos 3 dias;

5.6.24. A solução deve permitir o acesso a quais recursos por meio de uma estrutura de política simples que leva em consideração qualquer atributo do usuário fornecido pelo IdP, inclusive customizados, e o estado do dispositivo;

5.6.25. A plataforma deverá permitir a descoberta automatizada de novas aplicações que não foram previamente provisionadas aos usuários explicitamente;

5.6.26. A solução deve trazer o monitoramento da atividade dos usuários, dando às equipes de TI uma maneira de monitorar e gerenciar facilmente todas as atividades de forma granular, entendendo qual usuário, quando, qual aplicação, qual política autorizou ou negou o acesso, status da postura e localização do usuário;

5.6.27. A solução deverá suportar envio, em tempo real, das informações do item anterior para uma plataforma de SIEM;
5.6.28. A solução deve usar o painel Web para criar e editar políticas com facilidade. O portal de gestão central deve trazer:
5.6.28.1. Controle de acesso centralizado;
5.6.28.2. Gestão de políticas;
5.6.28.3. Configuração de postura;
5.6.28.4. Registro de atividades detalhados e seus metadados como usuário, localidade, postura, IP de origem, aplicação destino, política de acesso que concedeu ou negou o acesso;
5.6.28.5. Status da estrutura que suporte a solução como conectores ou publicadores;
5.6.28.6. Status do processo de atualização automatizada dos conectores e publicadores;
5.6.28.7. Status das aplicações que deverão ser monitoradas se estão disponíveis ou não
5.6.28.8. Gerenciar a segmentação do acesso ou recursos;
5.6.28.9. Suportar a configuração de qualquer aplicação TCP ou UDP com tráfego originado pelo usuário de forma transparente, sem nenhuma alteração ou customização no seu cliente original;
5.6.28.10. Permitir o agrupamento de aplicações ou recursos para facilitar a criação de políticas (ex: Aplicações Administrativas);
5.6.29. A solução deverá suportar a gestão de políticas de acesso via API;
5.6.30. A solução deverá suportar diferentes tipos de validação de postura. O suporte a cada tipo pode variar dependendo da plataforma (Windows, Mac, Linux, iOS e Android), sendo requerido que no mínimo deverá suportar 2 dos tipos abaixo por plataforma:
5.6.31. Validação da presença de um Antivírus;
5.6.32. Validação de Certificado Cliente (chave privada e pública) assinada por um CA específico;
5.6.33. Validação de Certificado confiável no dispositivo;
5.6.34. Validação de qualquer processo executando na máquina, incluindo a validação da assinatura do seu fabricante;
5.6.35. Validação de máquina no domínio;
5.6.36. Validação de disco encriptado;
5.6.37. Validação de Registro de chave no Windows;
5.6.38. Validação de presença de um arquivo;
5.6.39. Exigência de uma versão mínima do Sistema Operacional;
5.6.40. Detectar alterações não autorizadas em dispositivos móveis.
5.6.41. A solução deverá ter mecanismos de proteção e políticas granulares de postura para cada acesso à aplicação. Desta maneira permitindo criar maiores restrições a aplicações mais críticas ao negócio e menos restritas a aplicações de suporte a TI.

6. Item 6 - Serviços de segurança da informação e resposta a incidentes de segurança

Os serviços especializados listados deverão conter as seguintes frentes de atuação:

I. Serviços de operação e sustentação de segurança;
II. Serviço de Gestão de Incidentes de Segurança;
III. Serviço de descoberta e gestão de vulnerabilidades de segurança;
IV. Serviço de validação de segurança;
V. Serviços de micro segmentação de datacenter;
VI. Serviços de proteção de acesso seguro a rede e proteção de usuários.

6.1. Requisitos Gerais

6.1.1. Serviço de Gestão de Incidentes de Segurança deverá ser prestado em período integral (24x7) para o tratamento e investigação de incidentes de segurança da informação;
6.1.2. 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;
6.1.3. 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;
6.1.4. 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;
6.1.5. Entende-se por administração diária a administração de todos os passos técnicos e processos que envolvem os serviços contratados, de forma que os mesmos sejam 100% integrados ao ambiente da CONTRATANTE, porém utilizando a mão de obra da CONTRATADA;
6.1.6. Entende-se por sustentação a responsabilidade 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;
6.1.7. 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;
6.1.8. A CONTRATADA deverá seguir o processo de mudança estabelecido pelo CONTRATANTE;
6.1.9. A CONTRATADA deverá implementar conceitos de Threat Hunting, monitorando de forma contínua todos os eventos correlacionados;
6.1.10. 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;
6.1.11. 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;
6.1.12. Todos os serviços de manutenção corretiva e preventiva são considerados de natureza contínua e deverão minimizar a necessidade de parada do ambiente em produção;

6.1.13. 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.

6.1.14. 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 do presente certame.

6.1.15. Os serviços devem ser executados de acordo com normas, procedimentos e técnicas adotadas pela CONTRATANTE;

6.1.16. Deverá ser fornecido ao CONTRATANTE acesso à console dos serviços fornecidos para que seja possível o acompanhamento, auditoria e direcionamento de ações no ambiente;

6.1.17. A CONTRATADA deverá comunicar a CONTRATANTE quanto ocorrência de qualquer incidente de segurança, seguido de todas as ações de remediação realizadas;

6.1.18. Os contatos para notificação de incidentes críticos ou fluxos para aprovação de ações serão documentados durante o período de implementação;

6.1.19. 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;

6.1.20. 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;

6.1.21. 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;

6.1.22. Qualquer atividade realizada fora do horário comercial não deverá atribuir nenhum custo adicional para a CONTRATANTE;

6.1.23. Qualquer atualização de plataformas envolvidas na contratação não deverá ter nenhum custo adicional para a CONTRATANTE;

6.1.24. 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;

6.1.25. 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;

6.1.26. 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;

6.1.27. A CONTRATADA deverá ter fluxos de resposta a incidentes bem definidos para os mais variados tipos de incidentes existentes;

A CONTRATADA deverá criar relatórios gerenciais a serem apresentados e entregues para a CONTRATANTE mensalmente, em dia a ser definido no período de implementação. Os dados deste relatório poderão ser customizados a pedido da CONTRATANTE, de modo a atender necessidades específicas de negócio. Adicionalmente, os relatórios devem conter índices de resposta a incidentes, indicadores e efetividade de todas os serviços contratados;

6.1.28. Todas as ações de resposta a incidentes executadas pela CONTRATADA deverão ser armazenadas em procedimentos operacionais, para consultas sempre que necessário;

6.1.29. A contratada deverá detectar e reportar qualquer tipo de incidentes que tenham características de reincidência;

6.1.30. Serão considerados incidentes de segurança, minimamente, as seguintes ações:

6.1.30.1. Aplicações maliciosas detectadas em estações de trabalho e servidores;

6.1.30.2. Exploração de vulnerabilidades;

6.1.30.3. Uso indevido de credenciais;

6.1.30.4. Phishing ou spam;

6.1.30.5. Ataques de Força Bruta;

6.1.30.6. Execução de códigos ou scripts maliciosos;

6.1.30.7. Ataques de saturação;

6.1.30.8. Comunicações com IPs ou domínios maliciosos;

6.1.30.9. Atividades que tenham o intuito de comprometer a integridade de ativos e entidades da CONTRATANTE;

6.1.30.10. Atividades que tenham o intuito de comprometer a confidencialidade de informações da CONTRATANTE;

6.1.30.11. Atividades que tenham o intuito de comprometer a disponibilidade dos serviços tecnológicos oferecidos pela CONTRATANTE.

6.1.31. 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;

6.1.32. A CONTRATADA deverá operar todas as plataformas contidas nesta contratação, de forma a realizar todas as atividades pertinentes as 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;

6.1.33. 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;

6.1.34. Apresenta-se abaixo tabela que contêm, mas não se limita, as atividades que irão compor a rotina deste serviço:

ITEM	ATIVIDADE	CAMADA DE PROTEÇÃO
1	Deploy de sensores/Agentes	Identificação e correção de vulnerabilidades
2	Criação de scan de vulnerabilidade	Identificação e correção de vulnerabilidades
3	Manutenção de scan de vulnerabilidade	Identificação e correção de vulnerabilidades
4	Organização de tags e ativos	Identificação e correção de vulnerabilidades
5	Priorização de visualização de vulnerabilidades mais críticas	Identificação e correção de vulnerabilidades
6	Identificação de vulnerabilidades em sistemas operacionais	Identificação e correção de vulnerabilidades
7	Identificação de vulnerabilidades em aplicações utilizadas por usuários	Identificação e correção de vulnerabilidades
8	Identificação de vulnerabilidades em ativos de rede	Identificação e correção de vulnerabilidades

9	Correção contínua de vulnerabilidades em sistemas operacionais	Identificação e correção de vulnerabilidades
10	Correção contínua de vulnerabilidades em aplicações utilizadas por usuários	Identificação e correção de vulnerabilidades
11	Correção de vulnerabilidades em ativos críticos	Identificação e correção de vulnerabilidades
12	Emissão de nota técnica para ativos que não possam ser atualizados/corrigidos	Identificação e correção de vulnerabilidades
13	Emissão de relatórios de ativos vulneráveis	Identificação e correção de vulnerabilidades
14	Emissão de relatórios de CVEs aplicáveis a ativos scaneados	Identificação e correção de vulnerabilidades
15	Emissão de relatórios de CVEs corrigidos em determinado período	Identificação e correção de vulnerabilidades
16	Deploys de sensores para coleta de eventos	Correlacionamento e resposta de eventos de segurança
17	Manutenção de sensores para coleta de eventos	Correlacionamento e resposta de eventos de segurança
18	Apois em integrações com fontes para envio de logs	Correlacionamento e resposta de eventos de segurança
19	Normalização/Parser de logs quando necessário	Correlacionamento e resposta de eventos de segurança
20	Triagem de incidentes de segurança	Correlacionamento e resposta de eventos de segurança
21	Registro de incidentes de segurança	Correlacionamento e resposta de eventos de segurança
22	Resposta a incidentes de segurança	Correlacionamento e resposta de eventos de segurança
23	Criação de regras de detecção	Correlacionamento e resposta de eventos de segurança
24	Manutenção de regras de detecção	Correlacionamento e resposta de eventos de segurança
25	Realização de comunicados provenientes de incidentes de segurança	Correlacionamento e resposta de eventos de segurança
26	Emissão de relatórios e dashboards	Correlacionamento e resposta de eventos de segurança
27	Deploys de agentes/conectores	Simulação de ataques
28	Realizar testes de segurança/ataques para soluções de endpoint/EDR	Simulação de ataques
29	Realizar testes de segurança/ataques para soluções de proteção para email	Simulação de ataques
30	Realizar testes de segurança/ataques para técnicas de movimentação lateral	Simulação de ataques

31	Realizar testes de segurança/ataques para soluções de DLP	Simulação de ataques
32	Realizar testes de segurança/ataques para soluções de Web application firewall	Simulação de ataques
33	Realizar testes de segurança/ataques de ameaças recentes	Simulação de ataques
34	Criar e efetuar simulações de phishing para o ambiente	Simulação de ataques
35	Apoiar em todas as demandas de melhorias do ambiente	Simulação de ataques
36	Emitir relatórios executivos	Simulação de ataques
37	Liberação de acesso a páginas web	Proteção em nuvem de usuários
38	Criação de exceções de ssl inspection	Proteção em nuvem de usuários
39	Emissão de relatórios	Proteção em nuvem de usuários
40	Publicação de aplicações para acesso remoto seguro	Proteção em nuvem de usuários
41	Liberação de comunicação de rede entre componentes micro segmentados	Micro segmentação de rede

6.1.35. Para o faturamento mensal, a contratada deverá emitir e apresentar o "Relatório Mensal de Acompanhamento do Contrato", que deverá conter, minimamente:

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

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

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

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

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

6.1.35.6. Sumário de toda as vulnerabilidades de segurança encontradas no período do relatório;

6.1.35.7. Sumário de todos os e-mails retidos, organizando por camada de proteção;

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

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

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

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

6.1.35.12. Resultados dos testes de campanhas de phishing realizadas com os usuários;

6.1.35.13. Resultados completos de testes de segurança direcionados a solução de WAF em uso;

6.1.35.14. Resultados completos referentes ao nível de maturidade de segurança do ambiente baseado nos testes de segurança realizados;

6.1.35.15. Indicadores de utilização de serviços web.

6.2. Serviços de Operação e sustentação de segurança

6.2.1. 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.

6.2.1.1. As ferramentas já existentes serão monitoradas, sendo os relatórios apresentados para o Ministério, contendo os problemas e riscos identificados e a proposta de solução.

6.2.2. Principais atividades a serem executadas de forma contínua pela CONTRATADA:

6.2.2.1. Acompanhar a execução dos serviços para o cumprimento dos níveis de serviço estabelecidos;

6.2.2.2. Priorizar os atendimentos críticos, conforme definição do CONTRATANTE;

6.2.2.3. Monitorar de forma permanente e realizar avaliações críticas sobre os produtos e serviços de segurança do CONTRATANTE;

6.2.2.4. 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;

6.2.2.5. Atuar proativamente na antecipação e identificação de incidentes de segurança, antes mesmo do impacto nos serviços;

6.2.2.6. Reagir aos eventos de Segurança da Informação que possam afetar a disponibilidade, integridade ou confidencialidade das informações existentes nos sistemas ou serviços de TI do CONTRATANTE;

6.2.2.7. 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;

6.2.2.8. Prover os fiscais do contrato com os relatórios técnicos e gerenciais suficientes para a comprovação dos serviços realizados;

6.2.2.9. Supervisionar sua equipe na execução dos serviços executados;

6.2.2.10. Orientar a atuação da equipe técnica em situações críticas de trabalho, bem como interagir com os usuários quando a situação requerer;

6.2.2.11. 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;

6.2.2.12. Consolidar em manuais de procedimentos e em base de conhecimento todas as soluções adotadas na execução das atividades;

6.2.2.13. Implantar as melhorias solicitadas pelos servidores do CONTRATANTE através das aberturas de chamados no sistema de gestão de serviços de TI;

6.2.2.14. Sugerir novas tecnologias para modernizar o ambiente tecnológico, buscando subsidiar a equipe do CONTRATANTE na gestão de segurança da informação;

6.2.2.15. Administrar todas as soluções envolvidas na contratação em questão;

6.2.2.16. Abrir chamados técnicos para os serviços de suporte técnico remoto das soluções de hardware e software relacionados à Segurança da Informação no ambiente tecnológico do CONTRATANTE;

6.2.2.17. Realizar as atividades em estrita observância na Política de Segurança da Informação (PSI) e demais normas estipuladas pelo CONTRATANTE;

6.2.2.18. Implantar as melhorias solicitadas pelos servidores do CONTRATANTE;

6.2.2.19. 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;

6.2.2.20. 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;

6.2.2.21. 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;

6.2.2.22. 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.

6.2.3. Execução de mudanças de configuração nos ativos sob sua administração;

6.2.4. Execução das atividades relativas aos normativos e governança do CONTRATANTE naquilo que for relativo à sua área de atuação;

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

6.2.5.1. Implementação, sustentação e administração da solução de SIEM;

6.2.5.2. Configuração de repositórios e processamento de logs/eventos;

6.2.5.3. Criação/envio de procedimentos para envio de logs para soluções administradas por equipes terceiras;

6.2.5.4. Customização da interpretação dos logs sempre que necessário;

6.2.5.5. Criação/configuração de alertas para cada tipo de log processado;

6.2.5.6. Monitoramento de saúde de recebimento de logs de todas as fontes configuradas para envio;

6.2.5.7. Configuração e disponibilização dos agentes de privilégios;

6.2.5.8. Criação/Manutenção de regras de detecção;

6.2.5.9. Implementação, sustentação e administração da solução de gestão de vulnerabilidades;

6.2.5.10. Implementação, sustentação e administração da solução de controle de proteção de usuários e controle de dados em nuvem;

6.2.5.11. Configurar políticas para análise e correção de posturas indesejadas;

6.2.5.12. Apontar vulnerabilidades por ordem de criticidade e acompanhar o processo de remediação das mesmas.

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

6.2.7. Qualquer atividade técnica relacionada aos serviços contratados neste certame, mesmo que não tenha sido explicitamente listada, será de responsabilidade da CONTRATADA;

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

6.3. Serviço de descoberta e gestão de vulnerabilidades de Segurança

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

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

6.3.3. 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.

6.3.4. 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.

6.3.5. Para as 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.

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

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

6.3.8. 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.

6.3.9. 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.

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

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

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

6.3.13. 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.

6.4. Serviço de Gestão de Incidentes de Segurança

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

6.4.2. 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.

6.4.3. 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.

6.4.4. 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.

6.4.5. Uma vez realizadas 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.

6.4.6. 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.

6.4.7. 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.

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

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

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

6.4.11. 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 todas e quaisquer evidências, e identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo, para execução de análise forense do caso.

6.4.12. 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 incidente de segurança. Tal análise deve ser realizada com o objetivo de identificar pessoas, locais

e/ou eventos, correlacionando todas as informações reunidas e gerando como um produto final um laudo sobre o incidente de segurança em questão.

6.4.13. 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.

6.4.14. 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);

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

6.4.16. 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:

6.4.16.1. 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;

6.4.16.2. Criar, em colaboração com a CONTRATANTE, casos de uso (regras) que devem ser implementados no SIEM fornecido;

6.4.16.3. Revisar periodicamente as regras do SIEM, realizando as adaptações e evoluções necessárias;

6.4.16.4. 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;

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

6.4.17.1. Relatórios de ameaças e segurança;

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

6.4.17.3. Identificação de exploit kits;

6.4.17.4. Indicadores de ataques “ZeroDays” ;

6.4.17.5. Indicadores de comprometimento, suspeitas e avisos informativos;

6.4.17.6. Inteligência de tendências;

6.4.17.7. Proxies anônimos;

6.4.17.8. Classificação de sites;

6.4.17.9. Endereços de rede TOR.

6.5. Serviço de validação de segurança.

6.5.1. 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;

6.5.2. 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;

6.5.3. Tais testes devem ser contínuos a fim de criar um baseline de possíveis modificações nos resultados durante o período contratual.

6.5.4. Os ativos de segurança a serem validados contemplam, no mínimo, IDS/IPS, Firewall, Endpoint Security e WAF;
6.5.5. Deve avaliar o nível de segurança fornecido por um grupo de endpoints e ativos de segurança de rede independentemente de fabricante e tecnologia;
6.5.6. 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;
6.5.7. 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;
6.5.8. Para a execução de exploração de vulnerabilidades, Malwares e ataques às aplicações web, devem ser usados "payloads" reais de ataques maliciosos;
6.5.9. 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;
6.5.10. Deverão ser realizados testes contínuos de movimentação lateral, de modo a identificar e prevenir possibilidades para atacantes navegarem pela rede corporativa;
6.5.11. 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;
6.5.12. Deve executar ataques em aplicações Web sobre os protocolos HTTP e HTTPS;
6.5.13. Deve executar ataques de URLs usando protocolo HTTP e HTTPS a partir da Internet ou internamente;
6.5.14. Deverão ser executados testes de acessos a URLs por categorização, de forma a validar a política de acesso web já em implementada pela CONTRATANTE;
6.5.15. Deve realizar testes de SMTP, tanto a partir da Internet para o domínio corporativo quanto entre contas de domínios corporativos;
6.5.16. Os testes via SMTP deverão compor campanhas de phishing, de forma a testar a capacidade de resposta dos usuários a ameaças deste gênero;
6.5.17. Deve utilizar técnicas, táticas e procedimentos contidos no MITRE ATT&CK;
6.5.18. 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.

6.6. Serviços de micro segmentação de datacenter.

6.6.1. Deverá apoiar na instalação dos agentes nos servidores do ambiente;
6.6.2. Deverá realizar a criação de rótulos e identificadores para cada servidor com o apoio da CONTRATANTE;
6.6.3. Deverá fornecer continuamente informações de visibilidade que apoiem na compreensão de como as comunicações de rede ocorrem no datacenter.
6.6.4. Deverá realizar a escrita das regras de micro segmentação em conjunto com a equipe da CONTRATANTE;
6.6.5. Deverá realizar atualizações periódicas das regras sempre que for necessário para o funcionamento correto das comunicações entre os componentes segmentados.

6.7. Serviços de proteção de acesso seguro a rede e proteção de usuários.

6.7.1. Deverá apoiar na política de criação de acesso à internet de forma segura;
6.7.2. Deverá realizar a liberação de URLs sempre que necessário;
6.7.3. Deverá apoiar na instalação de agentes e criação de métodos de acesso remoto;
6.7.4. Deverá realizar troubleshooting de acesso a aplicações e páginas sempre que ocorrerem problemas;
6.7.5. Deverá apoiar na implementação do conceito de ZTNA (acesso de confiança zero à rede) nos acessos remotos, ou seja, confiança zero;
6.7.6. Deverá apoiar na publicação de aplicações, assim como na criação de políticas de acesso para grupos e usuários específicos, de forma que o acesso remoto ao ambiente seja seguro.

6.8. Qualidade dos serviços profissionais a serem prestados

6.8.1. Para a execução do objeto deste certame, faz-se necessário que a contratada possua equipe especializada, devidamente qualificada, e detentora de conhecimento e habilidades adequadas para solucionar as questões relacionadas à segurança cibernética do Ministério.
6.8.2. Portanto, em razão da complexidade dos serviços a serem prestados, é obrigatório que a Contratada os execute com profissionais certificados pelos fabricantes das ferramentas que venha a fornecer, devendo ser observada a devida experiência profissional, de modo a reduzir o risco de baixa qualidade na prestação dos serviços;
6.8.3. A Contratada é obrigada a manter todas as competências exigidas para cada serviço, durante o período de execução contratual.
6.8.4. Serviços especificados para a plataforma de segurança cibernética:
6.8.4.1. Serviços de operação e sustentação de segurança/Serviço de Gestão de incidentes de segurança.
6.8.4.1.1. A CONTRATADA deverá manter uma torre de operação de forma a sustentar estes dois pilares de serviço, com objetivo e foco de trabalhar no processo de Sustentação, Monitoramento, Detecção, Investigação e Triagem de Alertas de Segurança.
6.8.4.1.2. Os serviços e ferramentas pertencentes a esta torre, são:
6.8.4.1.2.1. Serviço de micro segmentação de ambiente corporativo;
6.8.4.1.2.2. Serviço de proteção de usuários e controle de dados em nuvem;
6.8.4.1.2.3. Serviço de gerenciamento, monitoramento, visibilidade, detecção e correlacionamento de eventos de segurança.

Características dos serviços	
Descrição	Monitoramento de ataques cibernéticos utilizando ferramentas e soluções indicadas, e sustentação dessas ferramentas.
Atividades mínimas	• Detecta ameaças relacionadas à segurança cibernética; • Monitora alertas de segurança cibernética; • Recebe e analisa os alertas de equipes de tratamento de incidentes de segurança de outros órgãos ou entidades da Administração Pública;

	• Revisa os alertas mais recentes para determinar a relevância e a urgência; • Realiza a investigação preliminar para garantir que um incidente de segurança genuíno esteja ocorrendo; • Cria novos tickets de problemas para alertas que sinalizam um incidente de segurança e exigem uma revisão e resposta da equipe de nível 2; • Supervisiona e configura as ferramentas de monitoramento de segurança; • Administra o as soluções de proteção indicadas de forma a manter as melhores práticas de segurança sempre aplicadas; • Atende demandas diárias referente as proteções indicadas de forma a não apenas manter o ambiente operacional, mas também sustentar todos os outputs que se façam necessários.

6.8.4.2. Serviços de gestão de vulnerabilidades/validação de segurança:

6.8.4.2.1. A CONTRATADA deverá manter uma torre de operação com foco no monitoramento e descoberta de vulnerabilidades, realizando também testes de segurança contínuos.

6.8.4.2.2. Os serviços e ferramentas pertencentes a esta torre, são:

6.8.4.2.2.1. Serviço de descoberta e gestão de vulnerabilidades de segurança;

6.8.4.2.2.2. Serviço de validação de segurança, emulando ataques cibernéticos, medindo a efetividade dos controles de segurança ativos, através da execução real dos ataques, sem que haja interrupção dos serviços tecnológicos do ambiente.

Características dos serviços	
Descrição	Execução de scans de vulnerabilidades e testes de segurança em todo o parque tecnológico, gerando relatórios com nível de risco para que as vulnerabilidades mais críticas sejam tratadas com priorização.
Atividades mínimas	• Trabalha de forma proativa para rastrear vulnerabilidades de segurança; • Revê dados de descoberta de ativos e avaliação de vulnerabilidades; • Realiza avaliação de efetividade de plataformas de segurança, afim de comprovar o funcionamento das camadas ativas de proteção, promovendo ações de melhoria contínuas nos controles de segurança. • Analisa alertas, informações sobre ameaças e dados de segurança;

	• Recomenda otimização de ferramentas de monitoramento de segurança; • Conduz testes que possam medir a efetividades de segurança do ambiente periodicamente ou a cada mudança que se faça necessário; • Monitora continuamente eventos (logs) e tratamento de incidentes.

7. NÍVEL MINIMOS DE SERVIÇOS – NMS

7.1. Sempre que houver uma entrega de produto ou serviço, deve ser realizada medição com base nos parâmetros apresentados neste item.

7.2. Não havendo falhas ou erros nos produtos, estes serão recebidos e encaminhados para pagamento.

7.3. Havendo falhas ou erro nos produtos que resultem em alguma das não conformidades abaixo, poderão, a critério do Ministério das Comunicações, ser aplicado o Fator de Qualidade dos Produtos que resultará em descontos nos valores a serem pagos.

7.4. Para os serviços mensais, serão mensalmente avaliados os parâmetros apresentados a seguir:

7.5. Para os serviços de resposta à incidentes:

7.5.1. Incidentes de prioridade Crítica

7.5.1.1. Caso o início do atendimento não ocorra nos prazos estabelecidos, poderá aplicado desconto de 0,5% do valor mensal dos serviços, por atendimento em atraso, até um total 2,5%.

7.5.1.2. Caso as informações e recomendações relacionadas ao incidente não sejam repassadas nos prazos estabelecidos, poderá ser aplicado desconto de 0,5% (meio por cento) do valor mensal dos serviços, por repasse em atraso, até um total 2,5%.

7.5.2. Incidentes de prioridade Alta

7.5.2.1. Caso o início do atendimento não ocorra nos prazos estabelecidos, poderá ser aplicado desconto de 0,25% do valor mensal dos serviços, por atendimento em atraso, até um total 2%.

7.5.2.2. Caso as informações e recomendações relacionadas ao incidente não sejam repassadas nos prazos estabelecidos, poderá ser aplicado desconto de 0,25% do valor mensal dos serviços, por repasse em atraso, até um total 2%.

7.5.3. Incidentes de prioridade Média

7.5.3.1. Caso o início do atendimento não ocorra nos prazos estabelecidos, poderá ser aplicado desconto de 0,2% do valor mensal dos serviços, por atendimento em atraso, até um total 1%.

7.5.3.2. Caso as informações e recomendações relacionadas ao incidente não sejam repassadas nos prazos estabelecidos, poderá ser aplicado desconto de 0,2% do valor mensal dos serviços, por repasse em atraso, até um total 1%.

7.5.4. Incidentes de prioridade Baixa

7.5.4.1. Caso o início do atendimento não ocorra nos prazos estabelecidos, poderá ser aplicado desconto de 0,1% do valor mensal dos serviços, por atendimento em atraso, até um total 1%.

7.6. Para os serviços de apoio técnico especializados:

7.6.1. Caso o(s) produto(s) não esteja(m) adequado(s) ao(s) requisito(s) da Ordem de Serviço, poderá ser aplicado desconto de 5% (cinco por cento) do valor mensal dos serviços.

7.6.2. Para cada 5 (CINCO) dias de atraso, poderá ser somada desconto de 1% do valor mensal dos serviços relacionados ao produto impactado até um total de 10%, a partir do qual passa-se à apuração de sanções contratuais.

Anexo II - Termo de Referência - Anexos B_ C_ D_ E_ F_ G_ H_ I.pdf

ANEXO B – MODELO DE PROPOSTA DE PREÇO

PROCESSO:	
UASG:	
OBJETO	

LOTE	ITEM	Descrição	Unidade	Quantidade	Valor unitário (RS)	Valor total (R$)
1	1	Solução de gerenciamento de vulnerabilidades de segurança	Dispositivo	1500		
	2	Solução de correlação de eventos de segurança e resposta a incidentes	Eventos por segundo – EPS	1300		
	3	Solução de micro segmentação de ambiente corporativo	Dispositivo	300		
	4	Solução de simulação de ataques em ambiente corporativo	Usuários	1500		
	5	Solução de proteção de usuários e controle de dados em nuvem	Usuários	1500		
	6	Serviços de segurança da informação e resposta a incidentes de segurança	UND SERVIÇO TÉCNICO	12		
TOTAL						

IDENTIFICAÇÃO DA EMPRESA CONTRATADA:		
Razão Social:		
CNPJ:		
Endereço Completo		
CEP:	Fone/Fax:	E-mail:

DADOS BANCÁRIOS:		
Agência:	Conta Corrente:	Banco:
IDENTIFICAÇÃO DO RESPONSÁVEL PELA ASSINATURA DO CONTRATO:		
Nome Completo (sem abreviaturas):		
CPF:	IDENTIDADE / ÓRGÃO EXPEDITOR:	
Cargo / Função:		
Endereço Completo:		
Cidade / UF:	CEP:	

Demais condições:

1. Ao efetuar essa proposta, esta empresa proponente declara ter tomado pleno conhecimento do Termo de Referência e dos demais documentos integrantes da presente Inexigibilidade de Licitação, estando ciente das obrigações das partes e das condições de prestação dos serviços.

2. Esta empresa proponente declara atender aos requisitos de capacidade técnica adequada para execução do objeto.

3. Esta empresa proponente declara que todas as despesas diretas e indiretas envolvidas no provimento dos serviços estão incluídas nos valores desta proposta de preços e que esses preços são exequíveis.

Local e data: _____, _____ de _____de 2023.

_____

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. 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 subitem "FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR" do 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. A proposta deve ter validade de, no mínimo, 90 (noventa) dias.

ANEXO C – DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL

Declaração de Sustentabilidade	
PROPONENTE:	
CNPJ/RFB:	
ENDEREÇO:	

Declaro, sob as penas da Lei nº 6.938/1981, na qualidade de proponente do procedimento de inexigibilidade de licitação, instaurado pelo Processo de nº _____, que atendemos aos critérios de qualidade ambiental e sustentabilidade socioambiental, respeitando as normas de proteção do meio ambiente.

Estou ciente de que todos os resíduos sólidos gerados pelos produtos fornecidos que necessitam de destinação ambientalmente adequada (incluindo embalagens vazias) deverão ter seu descarte adequado, obedecendo aos procedimentos de logística reversa, em atendimento à LEI Nº 12.305/2010, que institui a Política Nacional de Resíduos Sólidos, em especial a responsabilidade compartilhada pelo ciclo de vida do produto, me comprometendo a aplicar o disposto nos artigos de 31 a 33 da Lei nº 12.305/2010 e nos artigos 13 a 18 do Decreto nº 7.404/2010, principalmente, no que diz respeito à LOGÍSTICA REVERSA.

Estou ciente da obrigatoriedade da apresentação das declarações e certidões pertinentes dos órgãos competentes quando solicitadas como requisito para habilitação e da obrigatoriedade do cumprimento integral ao que estabelece o art. 6º e seus incisos, da Instrução Normativa nº 01, de 19 de janeiro de 2010, do Ministério do Planejamento, Orçamento e Gestão – MPOG e Decreto nº 7746 de 5 de junho de 2012, que estabelece critérios, práticas e diretrizes para a promoção do desenvolvimento nacional sustentável.

Estou ciente da obrigatoriedade da apresentação do registro no Cadastro Técnico Federal de Atividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais caso minha empresa exerça uma das atividades constantes no Anexo II da Instrução Normativa nº 31, de 03 de dezembro de 2009, do IBAMA.

Por ser a expressão da verdade, firmamos a presente DECLARAÇÃO.

_____ de _____ de 2023.

_____

Nome:

RG/CPF:

Cargo:

ANEXO D – TERMO DE COMPROMISSO DE MANUTENÇÃO DO SIGILO

Este TERMO DE COMPROMISSO ("TERMO") é celebrado entre:

1. CONTRATANTE Ministério das Comunicações, Endereço: bloco R, Esplanada dos Ministérios, CEP 70.044, Brasília/DF, inscrito no CNPJ/MF 37.753.638/0001-03, neste ato representado pelo Gestor do Contrato xx/xxxx, e

2. CONTRATADA xxxxxxxx, Endereço xxxxxxxx, inscrita no CNPJ/MF xxxxxx, personificação xxxxxx, neste ato representada por seus respectivos procuradores abaixo assinados, na forma de seus respectivos Contratos Sociais.

A CONTRATANTE e a CONTRATADA podem ser referidas individualmente como PARTE e coletivamente como PARTES, onde o contexto assim o exigir.

CONSIDERANDO QUE as PARTES estabeleceram ou estão considerando estabelecer uma relação de negócio que inclui o XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX;

CONSIDERANDO QUE as PARTES podem divulgar entre si INFORMAÇÕES CONFIDENCIAIS, conforme definido abaixo neste instrumento, sobre aspectos de seus respectivos negócios, e em consideração da divulgação destas INFORMAÇÕES CONFIDENCIAIS;

CONSIDERANDO QUE as PARTES desejam ajustar as condições de revelação das INFORMAÇÕES CONFIDENCIAIS, bem como definir as regras relativas ao seu uso e proteção;

RESOLVEM as PARTES celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, o qual se regerá pelas considerações acima, bem como pelas cláusulas e condições a seguir:

1. Para a finalidade deste Termo, "INFORMAÇÕES CONFIDENCIAIS" significarão todas e quaisquer informações divulgadas por uma PARTE (de acordo com este instrumento, a "Parte Divulgadora") à outra PARTE (de acordo com este instrumento, a "Parte Recebedora"), em forma escrita ou verbal, tangível ou intangível, patenteada ou não, de natureza técnica, operacional, comercial, jurídica, a qual esteja claramente marcada como CONFIDENCIAL, incluindo, entre outras, mas não se limitando a, segredos comerciais, know-how, patentes, pesquisas, planos de negócio, informações de marketing, informações de usuários, situação financeira, métodos de contabilidade, técnicas e experiências acumuladas, e qualquer outra informação técnica, comercial e/ou financeira, seja expressa em notas, cartas, fax, memorandos, acordos, termos, análises, relatórios, atas, documentos, manuais, compilações, código de software, e-mail, estudos, especificações, desenhos, cópias, diagramas, modelos, amostras, fluxogramas, programas de computador, discos, disquetes, fitas, pareceres e pesquisas, ou divulgadas verbalmente e identificadas como confidenciais por ocasião da divulgação.

2. Não serão incluídas nas INFORMAÇÕES CONFIDENCIAIS quaisquer informações que: (i) sejam geralmente conhecidas, ou subsequentemente se tornem disponíveis ao comércio ou ao público; (ii) estejam na posse legal da Parte Recebedora antes da divulgação pela Parte Divulgadora; ou (iii) sejam legalmente recebidas pela Parte Recebedora de um terceiro, desde que essas informações não tenham chegado ao conhecimento da Parte Recebedora através

do referido terceiro, direta ou indiretamente, a partir da Parte Divulgadora numa base confidencial.

3. Quando a divulgação de INFORMAÇÕES CONFIDENCIAIS for necessária para estrito atendimento de ordem judicial ou agência governamental, o mesmo se procederá da seguinte maneira: (i) a Parte Recebedora fica obrigada a comunicar o teor da determinação judicial à Parte Divulgadora no prazo de 2 (dois) dias úteis a contar do recebimento da ordem, no caso de se tratar de determinação para cumprimento em prazo máximo de 5 (cinco) dias; ou no prazo de uma hora a contar do recebimento, no caso de se tratar de ordem judicial para cumprimento no prazo máxima de até 48 (quarenta e oito) horas; e (ii) fica a Parte Recebedora obrigada também a enviar à Parte Divulgadora cópia da resposta dada à determinação judicial ou administrativa concomitantemente ao atendimento da mesma. A Parte Recebedora cooperará com a Parte Divulgadora para possibilitar que a Parte Divulgadora procure uma liminar ou outra medida de proteção para impedir ou limitar a divulgação dessas Informações Confidenciais.

4. A Parte Recebedora não divulgará nenhuma INFORMAÇÃO CONFIDENCIAL da Parte Divulgadora a nenhum terceiro, exceto para a finalidade do cumprimento deste Termo e com o consentimento prévio por escrito da Parte Divulgadora. Além disso:

1. A Parte Recebedora, (i) não usará as INFORMAÇÕES CONFIDENCIAIS para interferir, direta ou indiretamente, com nenhum negócio real ou potencial da Parte Divulgadora, e (ii) não usará as Informações Confidenciais para nenhuma finalidade, exceto avaliar uma possível relação estratégica entre as Partes.

2. As Partes deverão proteger as INFORMAÇÕES CONFIDENCIAIS que lhe forem divulgadas, usando o mesmo grau de cuidado utilizado para proteger suas próprias INFORMAÇÕES CONFIDENCIAIS.

3. A Parte Recebedora não revelará, divulgará, transferirá, cederá, licenciará ou concederá acesso a essas INFORMAÇÕES CONFIDENCIAIS, direta ou indiretamente, a nenhum terceiro, sem o prévio consentimento por escrito da Parte Divulgadora, estando este terceiro, condicionado à assinatura de um Termo de Compromisso de Manutenção de Sigilo prevendo as mesmas condições e obrigações estipuladas neste Termo.

4. A Parte Recebedora informará imediatamente à Parte Divulgadora de qualquer divulgação ou uso não autorizado das Informações Confidenciais da Parte Divulgadora por qualquer pessoa, e tomará todas as medidas necessárias e apropriadas para aplicar o cumprimento das obrigações com a não divulgação e uso limitado das obrigações das empreiteiras e agentes da Parte Recebedora.

5. A Parte Recebedora deverá manter procedimentos administrativos adequados à prevenção de extravio ou perda de quaisquer documentos ou INFORMAÇÕES CONFIDENCIAIS, devendo comunicar à Parte Divulgadora, imediatamente, a ocorrência de incidentes desta natureza, o que não excluirá sua responsabilidade.

6. A Parte Recebedora obrigará seu pessoal que possa ter acesso às INFORMAÇÕES CONFIDENCIAIS que cumpram tais obrigações de sigilo, assinando o TERMO DE CIÊNCIA.

5. As Partes se comprometem e se obrigam a tomar todas as medidas necessárias à proteção da informação confidencial da outra Parte, bem como para evitar e prevenir revelação a terceiros, exceto se devidamente autorizado por escrito pela Parte Divulgadora. De qualquer

forma, a revelação é permitida para empresas coligadas, assim consideradas as empresas que direta ou indiretamente controlem ou sejam controladas pela Parte neste Termo. Além disso, cada Parte terá direito de revelar a informação a seus funcionários que precisem conhecê-la, para os fins deste Termo; tais funcionários deverão estar devidamente avisados acerca da natureza confidencial de tal informação, e estarão vinculados aos termos e condições do presente Termo de Compromisso de Manutenção de Sigilo independentemente de terem sido avisados do caráter confidencial da informação, ficando a Parte Recebedora responsável perante a Parte Divulgadora por eventual descumprimento do Termo.

6. O intercâmbio de informações nos termos deste instrumento não será interpretado de maneira a constituir uma obrigação de uma das Partes para celebrar qualquer Termo ou acordo de negócio, nem obrigarão a comprar quaisquer produtos ou serviços da outra ou oferecer para a venda quaisquer produtos ou serviços usando ou incorporando as Informações Confidenciais.

7. Cada Parte reconhece que em nenhuma hipótese este Termo será interpretado como forma de transferência de propriedade ou qualquer tipo de direito subsistido nas Informações Confidenciais da parte Divulgadora para a parte Recebedora, exceto o direito limitado para utilizar as Informações Confidenciais conforme estipulado neste Termo.

8. Este TERMO entrará em vigor por ocasião da assinatura pelas Partes. Os compromissos deste instrumento também serão obrigatórios às coligadas, subsidiárias ou sucessoras das Partes e continuará a ser obrigatório a elas até a ocasião em que a substância das Informações Confidenciais tenha caído no domínio público sem nenhum descumprimento ou negligência por parte da Parte Recebedora, ou até que a permissão para liberar essas Informações seja especificamente concedida por escrito pela Parte Divulgadora.

9. A omissão ou atraso em aplicar qualquer disposição deste Termo não constituirá uma renúncia de qualquer aplicação futura dessa disposição ou de quaisquer de seus termos. Se qualquer disposição deste Termo, ou sua aplicação, por qualquer razão e em qualquer medida for considerada inválida ou inexequível, o restante deste Termo e a aplicação de tal disposição a outras pessoas e/ou circunstâncias serão interpretados da melhor maneira possível para atingir a intenção das Partes signatárias.

10. As PARTES concordam que a violação do presente Termo, pelo uso de qualquer Informação Confidencial pertencente à Parte Divulgadora, sem sua devida autorização, causar-lhe-á danos e prejuízos irreparáveis, para os quais não existe remédio na lei. Desta forma, a Parte Divulgadora poderá, imediatamente, tomar todas as medidas extrajudiciais e judiciais, inclusive de caráter cautelar, como antecipação de tutela jurisdicional, que julgar cabíveis à defesa de seus direitos.

11. A Parte Recebedora deverá devolver, íntegros e integralmente, todos os documentos a ela fornecidos, inclusive as cópias porventura necessárias, na data estipulada pela Parte Reveladora para entrega, ou quando não mais for necessária a manutenção das Informações Confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias, sob pena de incorrer nas penalidades previstas neste Termo.

12. A Parte Recebedora deverá destruir quaisquer documentos por ela produzidos que contenham Informações Confidenciais da Parte Divulgadora, quando não mais for necessária a manutenção dessas Informações Confidenciais, comprometendo-se a não reter quaisquer

reproduções (incluindo reproduções magnéticas), cópias ou segundas vias, sob pena de incorrer nas penalidades previstas neste Termo.

13. A inobservância de quaisquer das disposições de confidencialidade estabelecidas neste Termo sujeitará a Parte infratora, como também o agente causador ou facilitador, por ação ou omissão ou qualquer daqueles relacionados neste TERMO, ao pagamento, recomposição, de todas as perdas e danos, comprovadamente suportados ou demonstrados pela outra Parte, bem como as de responsabilidade civil e criminal respectivas, as quais serão apuradas em regular processo.

14. As obrigações de confidencialidade decorrentes do presente Termo, tanto quanto as responsabilidades e obrigações outras derivadas do presente Termo, vigorarão durante o período de 5 (cinco) anos após a divulgação de cada Informação Confidencial à Parte Recebedora.

15. O não exercício por qualquer uma das Partes de direitos assegurados neste instrumento não importará em renúncia aos mesmos, sendo tal ato considerado como mera tolerância para todos os efeitos de direito.

16. Alterações do número, natureza e quantidade das Informações Confidenciais disponibilizadas para a Parte Recebedora não descaracterizarão ou reduzirão o compromisso ou as obrigações pactuadas neste Termo de Compromisso de Manutenção de Sigilo, que permanecerá válido e com todos os efeitos legais em qualquer das situações especificadas neste Termo.

17. O acréscimo, complementação, substituição ou esclarecimento de qualquer das Informações Confidenciais disponibilizadas para a Parte Recebedora, em razão do presente objeto, serão incorporadas 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, não sendo necessário, nessas hipóteses, assinatura ou formalização de Termo Aditivo.

18. Este instrumento não deve ser interpretado como criação ou envolvimento das Partes, ou suas Afiliadas, nem em obrigação de divulgar informações confidenciais para a outra Parte.

19. O fornecimento de INFORMAÇÕES CONFIDENCIAIS pela Parte Divulgadora ou por uma de suas Afiliadas não implica em renúncia, cessão a qualquer título, autorização de uso, alienação ou transferência de nenhum direito, já obtido ou potencial, associado a tais informações, que permanecem como propriedade da Parte Divulgadora ou de suas Afiliadas, para os fins que lhe aprouver.

20. Nenhum direito, licença, direito de exploração de marcas, invenções, direitos autorais, patentes ou direito de propriedade intelectual estão aqui implícitos, incluídos ou concedidos por meio do presente Termo, ou ainda, pela transmissão de Informações Confidenciais entre as Partes.

21. A CONTRATADA declara conhecer todas as Normas, Políticas e Procedimentos de Segurança estabelecidos pela Contratante para execução do CONTRATO, tanto nas dependências da Contratante como externamente.

22. A CONTRATADA responsabilizar-se-á integralmente e solidariamente, pelos atos de seus empregados praticados nas dependências da Contratante, ou mesmo fora dele, que venham a causar danos ou colocar em risco o patrimônio da CONTRATANTE.

23. Este TERMO contém o acordo integral de confidencialidade entre as PARTES com relação ao seu objeto. Quaisquer outros acordos, declarações, garantias anteriores ou contemporâneos com relação à proteção das Informações Confidenciais, verbais ou por escrito, serão substituídos por este Termo. Este Termo será aditado somente firmado pelos representantes autorizados de ambas as Partes.

24. Quaisquer controvérsias em decorrência deste Termo serão solucionadas de modo amistoso através do representante legal das PARTES, baseando-se nas leis da República Federativa do Brasil. E por estarem assim justas e contratadas, as Partes firmam o presente Instrumento em 03 (três) vias de igual teor e forma, na presença das testemunhas abaixo indicadas.

Brasília, ___ de _____ de _____.

DE ACORDO

CONTRATANTE	CONTRATADA	TESTEMUNHA	TESTEMUNHA

ANEXO E – TERMO DE CIÊNCIA

TERMO DE CIÊNCIA INDIVIDUAL – 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:
Observação: Este termo deve ser impresso em papel timbrado da empresa CONTRATADA.	

ANEXO F – MODELO DE ORDEM DE SERVIÇO

(*) Modelo meramente exemplificativo

ORDEM DE SERVIÇO Art. 32 da Instrução Normativa SGD/ME nº 94/2022					
1. IDENTIFICAÇÃO					
N° IDENTIFICADOR DA OSFB					
N° CONTRATO					
EMPRESA CONTRATADA / CNPJ:					
OBJETO DO CONTRATO:					
GESTOR DO CONTRATO: [*caput* art. 32 da IN 01/2019/SGD]	NOME:				
	E-MAIL:	TELFONE:	MATRÍCULA:		
REQUISITANTE: [Inc. IV do art. 32 da IN 01/2019/SGD]	NOME:				
	E-MAIL:	TELFONE:	MATRÍCULA:		
2. ESPECIFICAÇÃO DOS SERVIÇOS (Inc. I e II do art. 32 da IN 94/2022/SGD)					
ITEM	DESCRIÇÃO	UND	QTDE	VL UNITÁRIO	VL TOTAL ITEM
01					
VALOR TOTAL ESTIMADO:					
3. CRONOGRAMA (Inc. III do art. 32 da IN 94/202022/SGD)					
ITEM	PRAZO (EM DIAS)	DATA INÍCIO	DATA ENTREGA		
01					
4. INFORMAÇÃOES COMPLEMENTARES					
5. CIÊNCIA DA CONTRATADA					

<table>
<tr><td colspan="4">ORDEM DE SERVIÇO
Art. 32 da Instrução Normativa SGD/ME nº 94/2022</td></tr>
<tr><td colspan="4">1. IDENTIFICAÇÃO</td></tr>
<tr><td rowspan="2">PREPOSTO DA CONTRATADA:
[art. 32 da IN 01/2019/SGD]</td><td colspan="3">NOME:</td></tr>
<tr><td>E-MAIL:</td><td>TELFONE:</td><td>CPF:</td></tr>
<tr><td colspan="4">Brasília/DF, xx de xxxx de xxxx.</td></tr>
</table>

ANEXO G – MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO

(*) Modelo meramente exemplificativo

TERMO DE RECEBIMENTO PROVISÓRIO

Identificação

Contrato:		N° da OS / OFB:	
Objeto:			
Contratante:			
Contratada:			

Por este instrumento, atestamos que os serviços (ou bens), relacionados na O.S. acima identificada, foram recebidos nesta data e serão objeto de avaliação quanto à conformidade de qualidade, de acordo com os Critérios de Aceitação previamente definidos pela Contratante.

Ressaltamos que o recebimento definitivo destes serviços (ou bens) ocorrerá em até 10 dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Termo de Referência correspondente ao Contrato supracitado.

De Acordo

CONTRATANTE	CONTRATADA
Fiscal Técnico do Contrato	Preposto
_____ *<Nome>* Matrícula: *<Matr.>*	_____ *<Nome>* *<Qualificação>*

_____, _____ de _____ de 20_____.

ANEXO H – MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

(*) Modelo meramente exemplificativo

TERMO DE RECEBIMENTO DEFINITIVO

Identificação

Contrato Número:		N° da OS / OFB:	
Objeto:			
Gestor do Contrato:			
Fiscal Requisitante do Contrato:			

Por este instrumento, os servidores acima identificados atestam que o(s) serviço(s) ou bem(ns) integrantes da Ordem de Serviço ou de Fornecimento de Bens acima identificada possui(em) qualidade compatível com a especificada no Termo de Referência / Projeto Básico do Contrato supracitado.

De Acordo

Gestor do Contrato	Fiscal Requisitante do Contrato
_____ *<Nome>* Matrícula: *<Matr.>*	_____ *<Nome>* *<Qualificação>*

_____, _____ de _____ de 20_____.

ANEXO I – INSTRUMENTO DE MEDIÇÃO DE RESULTADO

1. INFORMAÇÕES GERAIS

1.1. O Instrumento de Medição de Resultado – IMR é o ajuste escrito anexo ao contrato entre o provedor de serviços e o órgão contratante, que define, em bases compreensíveis, tangíveis, objetivamente observáveis e comprováveis, os níveis esperados de qualidade da prestação do serviço e respectivas adequações de pagamento.

1.2. Objetivo a atingir: Prestação do serviço em elevados níveis de qualidade.

1.3. Forma de avaliação: Definição de situações que caracterizem o não atingimento do objetivo, e atribuição de descontos no valor de pagamento devido.

1.4. Sanções: embora a aplicação de índices de desconto seja instrumento de gestão contratual, não configurando sanção, a Contratante poderá, pela qualidade insuficiente, aplicar as penalidades previstas em contrato.

2. CONDIÇÕES GERAIS

2.1. Para o acompanhamento e avaliação dos serviços da Contratada será estabelecido e utilizado o Instrumento de Medição de Resultado – IMR entre as partes, baseando-se em indicadores e metas definidos neste documento.

2.2. A análise dos resultados destas avaliações pela Contratante poderá resultar em penalidades, conforme prevê o Processo de Aferição, caso a Contratada não cumpra com os seus compromissos de apresentação, pontualidade, disponibilidade e de prestação do objeto contratual, conforme estabelecido pelos indicadores.

2.3. O IMR deve ser considerado e entendido pela Contratada como um compromisso de qualidade que assumirá junto à Contratante. O IMR é um instrumento ágil e objetivo de avaliação da qualidade da execução contratual, associando o pagamento à qualidade efetivamente obtida.

2.4. Para o recebimento integral do valor contratado, a empresa contratada deverá cumprir com suas obrigações contratuais, em especial as dispostas nos indicadores de desempenho.

2.5. O IMR será implementado a partir da primeira medição da data de assinatura do contrato, cabendo ao Fiscal Técnico do contrato avaliar a execução dos serviços prestados.

2.6. Para consecução destes objetivos deverá ser adotado as regras e metodologias de medição de resultado descritas nos itens abaixo.

3. ITENS AVALIADOS

3.1.1. INDICADOR 1: ATRASO NO FORNECIMENTO DO SERVIÇO.

Tópico	Descrição	
Finalidade	Medir o atraso na entrega dos itens especificados na Ordem de Serviço, relacionados aos itens 01, 02, 03, 04 e/ou 05 do Termo de Referência.	
Meta a cumprir	IAE < = 0	A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Serviços dentro do prazo previsto.
Instrumento de medição	OS, Termo de Recebimento Provisório (TRP)	
Forma de acompanhamento	Será subtraída a data de entrega do serviço da OS (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OS.	
Periodicidade	Para cada OS encerrada e com Termo de Recebimento Definitivo.	
Mecanismo de Cálculo (métrica)	IAE = TEX – TEST Onde: IAE – Indicador de Atraso de Entrega da OS; TEX – Tempo de Execução – corresponde ao período de execução da OS, da sua data de início até a data de entrega dos produtos da OS. A data de início será aquela constante na OS; caso não esteja explícita, será o primeiro dia útil após a emissão da OS. A data de entrega da OS deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OS continua a correr, findando-se apenas quanto o Contratado entrega os produtos da OS e haja aceitação por parte do fiscal técnico. TEST – Tempo Estimado para a execução da OS – constante na OS, conforme estipulado no Termo 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. Obs3: Em caso de prorrogação do prazo de entrega, conforme disposto no Termo de Referência, o Tempo Estimado para execução da OS será recalculado considerando o período prorrogado autorizado pelo Ministério das Comunicações.	
Início de Vigência	A partir da emissão da OS.	
Faixas de ajuste no pagamento e Sanções	Para valores do indicador IAE: Menor ou igual a 0: Pagamento integral da OS; Sanções em conformidade com o subitem 8.24 deste Termo de Referência.	

3.1.2. INDICADOR 2: TEMPO DE RESPOSTA À INCIDENTES.

Tópico	Descrição	
Finalidade	Medir mensalmente o atendimento aos prazos estabelecidos para resposta à incidentes, de acordo com o nível de criticidade. Este indicador aplica-se ao Item 06 do Termo de Referência.	
Meta a cumprir	IAE < = 0	A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Serviços dentro do prazo previsto.
Instrumento de medição	Relatório Mensal de Acompanhamento do Contrato, apresentado pela CONTRADATA À CONTRATANTE.	
Forma de acompanhamento	Mensalmente, o Ministério das Comunicações avaliará o cumprimento, pela CONTRATADA, dos Níveis Mínimos de Serviços exigidos para o tempo de resposta aos incidentes	
Periodicidade	Mensal.	
Mecanismo de Cálculo (métrica)	**Verificação da quantidade de ocorrências registradas com tempo de resposta superior à meta.**	
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. Obs3: Em caso de prorrogação do prazo de entrega, conforme disposto no Termo de Referência, o Tempo Estimado para execução da OS será recalculado considerando o período prorrogado autorizado pelo Ministério das Comunicações.	
Início de Vigência	A partir do início da prestação do serviço.	
Faixas de ajuste no pagamento e Sanções	Sem atrasos: Para valores do indicador IAE: Menor ou igual a 0: Pagamento integral da OS; Descontos em conformidade com o item 7 – Níveis Mínimos de Serviço – NMS, do Anexo A deste Termo de Referência. Sanções em conformidade com o subitem 8.24 deste Termo de Referência.	

4. DISPOSIÇÕES FINAIS

4.1. Este instrumento define expectativas de serviços e responsabilidades entre o Ministério das Comunicações e a empresa.

Brasília/DF, de de 2023