ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO

1.1. Formação de Registro de Preços para aquisição de solução de gerenciamento de vulnerabilidades de ativos de tecnologia da informação para atender as necessidades do Ministério Público do Estado do Pará, conforme condições, quantidades e exigências estabelecidas neste instrumento.

2. ESPECIFICAÇÕES TÉCNICAS MÍNIMAS DOS SERVIÇOS

CLASSIFICAÇÃO POR GRUPO

	Lote I ou Único – (identificação do agrupamento)				
Item	**Especificações Técnicas Mínimas**	**Apresentação**	**Quantidade Máxima (art. 82, I Lei 14133/21)**	**Preço Unitário Máximo**	**Valor Global Máximo do Item**
01	Solução de Gerenciamento de vulnerabilidades para ativos em tecnologia da informação, com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 36 meses. **Cód. Comprasnet/ CATSER: 27502**	Unidade	6000	885,06	5.310.360,00
02	Suporte técnico especializado. **Cód. Comprasnet/ CATSER: 26972**	Mês	36	27.356,17	984.822,12
	Valor Global Máximo do Grupo/Lote =				R$ 6.295.182,12

2.1. O agrupamento de itens diversos no mesmo grupo justifica-se pelos motivos expostos no tópico 10 deste Termo de Referência.

2.2 Não será possível o licitante oferecer proposta em quantitativo inferior ao máximo previsto no edital, obrigando-se nos limites dela (art.82, IV da Lei 14.133/21).

Obs: Os valores deverão ser calculados com duas casas decimais;

Obs: A proposta apresentada em desacordo com este Termo de Referência será desclassificada;

Obs: O valor estimado do certame é de R$ 6.295.182,12

Obs: Em caso de divergência entre a descrição e/ou descrição detalhada do item cadastrado no sistema de compras do governo federal e as consignadas no termo de referência, prevalecem as consignadas no termo de referência.

3. FUNDAMENTAÇÃO E JUSTIFICATIVA DA CONTRATAÇÃO (art. 6º, inciso XXIII, alínea 'b', da Lei nº 14.133/2021).

3.1. Esta demanda tem como objetivo priorizar o acompanhamento da execução do Plano de Segurança Institucional do MPPA, em consonância às diretrizes traçadas pelo Conselho Nacional do Ministério Público (CNMP), através da Política de Segurança Institucional e do Sistema Nacional de Segurança Institucional do Ministério Público, objetivando preservar a liberdade e a independência da atuação dos membros e servidores, bem como, controlar as vulnerabilidades das informações e sistemas utilizados pela instituição, através de uma robusta solução de gerenciamento de riscos e vulnerabilidades.

3.2. Para exercer seu papel institucional em todo o estado, o MPPA conta com uma grande rede integrada de dados, sistemas e informações, dada a sua vasta infraestrutura. Essa transformação digital é responsável por migrar grande parte de serviços e gestões para o meio digital, priorizando maior alcance, integração entre sistemas e bases, redes, ambientes tecnológicos e uma melhor experiência para cidadãos que procuram o MPPA.
3.3. O processo de digitalização de serviços públicos requer que o MPPA realize investimentos que permitam proteger perímetros, redes e ativos, promovendo a gestão de vulnerabilidades, com o intuito de monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a disponibilidade das aplicações de forma a minimizar o risco de paralisações e de se produzir impacto negativo sobre o desempenho do MPPA. Desta forma, temos a indispensável necessidade de se promover uma segurança em todo o ambiente tecnológico que sustenta a instituição.
3.4. Com o objetivo de garantir o controle eficaz e a detecção de possíveis vulnerabilidades nos sistemas e aplicações, visando ao tratamento adequado e à redução do risco de impactos na continuidade dos serviços oferecidos pelo MPPA, de forma segura e com o desempenho necessário, torna-se necessário analisar o cenário atual e identificar modelo de melhoria que atenda esse tipo de necessidade. O cerne do objeto a ser estudado é justamente atender à necessidade de cobrir todo o parque de servidores e ativos de rede com ferramenta capaz de executar o processo de gestão de vulnerabilidades.
3.5. A justificativa para a aquisição desta solução é fundamentada na necessidade de manter um entendimento atualizado do ambiente tecnológico e todo o seu espaço cibernético. Ao monitorar esse espaço em tempo real, ganha-se a capacidade de fornecer suporte estratégico de alto nível para a tomada de decisões que dependam desse ambiente. Dado que este ambiente influencia outros meios, é caracterizado por sua alta volatilidade e incerteza, é crucial contar com um monitoramento constante e eficaz, que é proporcionado pela solução em questão.
3.6. Assim, motivado pela necessidade da continuação e aprimoramento do monitoramento da segurança cibernética, bem como dos projetos que aumentem a capacidade de detecção e resposta a incidentes, considerou que é imprescindível que se avalie opções que atendam esse tipo de necessidade. Diante da gravidade dos incidentes de segurança que o MPPA tem enfrentado e da escassez de recursos humanos para lidar com o problema, a presente contratação é imprescindível para a continuidade dos serviços e para manter sob sigilo as informações classificadas.
3.7. Percebido o risco de vazamento de informações, cuja confidencialidade é fundamental para os objetivos estratégicos do MPPA e para os usuários dos serviços prestados, reconhecemos a necessidade de se contar com serviços especializados de gestão de vulnerabilidades. Em resumo, a ausência dessa solução deixa o MPPA em risco de ataques cibernéticos, perda de dados sensíveis, possíveis custos financeiros e danos à reputação. Portanto, é fundamental que o MPPA, responsável pelo gerenciamento de dados sensíveis, implemente práticas eficazes de segurança cibernética, incluindo a gestão proativa de vulnerabilidades.

4. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

4.1. Identificação de Vulnerabilidades: O sistema de gestão de vulnerabilidades deve escanear ativamente sistemas e redes em busca de vulnerabilidades de segurança, identificando potenciais brechas que possam comprometer a integridade e a confidencialidade dos dados pessoais. Esse processo de identificação é fundamental para garantir a segurança dos dados e o cumprimento dos padrões de proteção estabelecidos pela resolução.
4.2. Monitoramento Contínuo: O sistema de gestão de vulnerabilidades deve oferecer recursos para o monitoramento contínuo do ambiente de TI, permitindo a detecção precoce de novas vulnerabilidades e ameaças emergentes. Isso é essencial para garantir uma resposta rápida e eficaz a possíveis incidentes de segurança que possam afetar a proteção dos dados pessoais.
4.3. Priorização e Tratamento de Vulnerabilidades: O sistema de gestão de vulnerabilidades deve ser capaz de indicar prioridades com base na identificação e em métricas relevantes, incluindo a gravidade da vulnerabilidade, a probabilidade de sua exploração e o impacto potencial sobre os sistemas. Deve utilizar o sistema de pontuação Common Vulnerability Scoring System (CVSS) para atribuir uma pontuação numérica a cada vulnerabilidade detectada. Essa abordagem permite que as equipes de segurança concentrem seus esforços nas vulnerabilidades mais críticas primeiro, reduzindo assim os riscos imediatos para o ambiente. Ao estabelecer prioridades com base nessas métricas, as organizações podem alocar recursos de forma mais eficiente e direcionada, promovendo uma abordagem estratégica e proativa para a gestão da segurança da informação.

4.4. Relatórios e Auditorias: Um sistema de gestão de vulnerabilidades pode gerar relatórios detalhados sobre o estado da segurança da informação, incluindo informações sobre vulnerabilidades identificadas, medidas de mitigação implementadas e métricas de desempenho de segurança. Esses relatórios são essenciais para demonstrar conformidade com os requisitos da Resolução CNMP 281/2023 e para apoiar auditorias de segurança.
4.5. Integração com Outros Sistemas de Segurança: O sistema de gestão de vulnerabilidades deve ser integrado com outros sistemas de segurança, como sistemas de prevenção de intrusões (IPS), firewalls e sistemas de detecção de intrusões (IDS), para fornecer uma defesa em camadas abrangente contra ameaças cibernéticas. Essa integração ajuda a fortalecer a postura de segurança do Poder Judiciário e a proteger efetivamente os dados pessoais.
4.6. O sistema de gestão de vulnerabilidades deve desempenhar um papel crucial no atendimento aos requisitos da Resolução CNMP 281/2023, fornecendo os recursos necessários para identificar, monitorar e tratar vulnerabilidades de segurança que possam afetar a proteção dos dados pessoais tratados pelo Poder Judiciário brasileiro. Ao implementar um sistema de gestão de vulnerabilidades eficaz, o Poder Judiciário pode fortalecer sua postura de segurança cibernética e garantir a conformidade com as normas e regulamentações de proteção de dados.

5.NATUREZA, QUANTITATIVOS, DESCRIÇÃO DOS SERVIÇO E VIGÊNCIA DA CONTRATAÇÃO

5.1. Natureza do Serviço:
5.1.1. O objeto a ser contratado se enquadra como bem comum, pois os padrões de desempenho e qualidade podem ser objetivamente definidos, por meio de especificações usuais de mercado, nos termos do art. 6º, inciso XIII da Lei 14.133 de 2021.
5.1.2. O objeto desta contratação não se enquadra como sendo de serviço de grande vulto, conforme art.6º, XXII da Lei 14.133/2021.
5.2. Os quantitativos:
5.2.1. A quantidade a ser adquirida do(s) serviços(s) será de 6000 (seis mil) licenças de software de gerenciamento de vulnerabilidades em ativos de tecnologia e aplicações, junto com 36 meses de suporte técnico especializado em virtude da quantidade de ativos em tecnologia da informação, quantidade de usuários de nosso domínio do MPPA e quantidade de aplicações de nosso ambiente.
5.2.2. É vedado efetuar acréscimos nos quantitativos estabelecidos na ata de registro de preços, conforme estabelece o art. 19 do Decreto Estadual n.º 3.371/2023**.**
5.3. Da Utilização do Sistema de Registro de Preços:
5.3.1. A formação de registro de preços é devida a não ser possível definir previamente o quantitativo a ser demandado pela Administração. A complexidade e a constante evolução do ambiente de tecnologia da informação torna desafiador manter uma contagem exata de ativos, usuários e aplicações do MPPA. A dinâmica dos ativos de TI, com novas aquisições, substituições e desativações, dificulta a precisão na contagem. Da mesma forma, a base de usuários de domínio está sujeita a flutuações com a posse de novos servidores e membros. Além disso, as aplicações utilizadas podem variar ao longo do tempo, assim como o número de usuários que as acessam.
5.3.2. Diante dessa realidade, adotar uma solução de gestão de vulnerabilidades baseada em licenças para aquisição de quantidade variáveis se torna essencial. Esse modelo oferece a flexibilidade necessária para lidar com as mudanças constantes no ambiente de TI. Ao permitir que as licenças sejam adquiridas de acordo com a demanda e a evolução dos ativos, usuários e aplicações, essa abordagem garante uma adaptação mais fluida às necessidades da organização.
5.3.3. Além disso, a adoção do registro de preços reduz custos e complexidades administrativas. A organização paga apenas pelo que utiliza, otimizando os gastos com licenciamento. Isso também simplifica as tarefas administrativas nos processos de aquisição.
5.3.4. Em suma, utilizar o sistema de registro de preços para contratação de solução de gerenciamento de vulnerabilidades oferece uma abordagem mais eficaz para lidar com a complexidade e a dinâmica do ambiente de TI atual. Ela permite que o MPPA se adapte rapidamente às mudanças, garantindo ao mesmo tempo uma infraestrutura de segurança adequada e otimização de recursos.
5.3.5. Haverá o registro de mais de um fornecedor ou prestador de serviço, desde que aceitem cotar o objeto em preço igual ao do licitante vencedor, assegurada a preferência de contratação de acordo com a ordem de classificação; (art.82, VII da Lei 14.133/21);

5.3.6. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará o Ministério Público do Estado do Pará a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente motivada.
5.3.7. Fica vedado efetuar acréscimos nos quantitativos fixados na Ata de Registro de Preços (ARP) (art.19 do Decreto Estadual n.º 3.371 de 2023).
5.3.8. Fica vedado a contratação, no mesmo órgão ou na mesma entidade, de mais de uma empresa para a execução do mesmo serviço, a fim de assegurar a responsabilidade contratual e o princípio da padronização, ressalvado o disposto no art. 49 da Lei nº 14.133, de 2021;
5.3.9. Poderá ser admitida adesão à presente Ata de Registro de Preços, desde que sejam observados os requisitos do art. 86, §§ 2º, 4º e 5º da Lei 14.133/2021 e procedimentos estabelecidos no art. 31 do Decreto Estadual nº 3.371/2023.
5.4. **Regras para o controle de Adesão à Ata de Registro de Preços:**
5.4.1. As aquisições ou as contratações adicionais através de adesão à Ata de Registro de Preços por órgãos ou entidades não participantes não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o órgão ou entidade gerenciadora e para os órgãos ou entidades participantes.
5.4.2. O quantitativo decorrente das adesões à ata de registro de preços por órgãos ou entidades não participantes não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão ou entidades gerenciadoras e órgãos ou entidades participantes, independentemente do número de órgãos ou entidades não participantes que aderirem. (art. 86, § 5º da Lei nº 14.133/2021)
5.4.3. É vedado a adesão de órgãos e/ou entidades da Administração Pública Federal à ata de registro de preços gerenciadas por órgão ou entidades estadual, distrital ou municipal.
5.5. Da validade, formalização da Ata de Registro de Preços e Cadastro de Reserva:
5.5.1. O prazo de vigência da ata de registro de preços será de 1 (um) ano, contado do primeiro dia útil subsequente à divulgação no Portal Nacional de Compras Públicas, podendo ser prorrogado por igual período, mediante a anuência do fornecedor, desde que comprovado que as condições e o preço permanecem vantajosos.
5.5.2. No ato de prorrogação da vigência da ata de registro de preços poderá haver a renovação dos quantitativos registrados, até o limite do quantitativo original.
5.5.3. O ato de prorrogação da vigência da ata deverá indicar expressamente o prazo de prorrogação e o quantitativo renovado.
5.5.4. O contrato decorrente da ata de registro de preços terá sua vigência estabelecida no próprio instrumento contratual e observará no momento da contratação e a cada exercício financeiro a disponibilidade de créditos orçamentários, bem como a previsão no plano plurianual, quando ultrapassar 1 (um) exercício financeiro (art. 36 do Decreto Estadual 3.371/2023).
5.5.5. Na formalização do contrato ou do instrumento substituto deverá haver a indicação da disponibilidade dos créditos orçamentários respectivos.
5.5.6. A contratação com os fornecedores registrados na ata será formalizada pelo órgão ou pela entidade interessada por intermédio de instrumento contratual, emissão de nota de empenho, conforme o art. 95 da Lei nº 14.133, de 2021.
5.5.7. O instrumento contratual de que trata o item 5.5.6 deverá ser assinado no prazo de validade da ata de registro de preços.
5.5.8. Os contratos decorrentes do sistema de registro de preços poderão ser alterados, observado o art. 124 da Lei nº 14.133/21 (art. 35 do Decreto Estadual 3.371/2023).
5.5.9. Após a homologação da licitação deverão ser observadas as seguintes condições para formalização da Ata de Registro de Preços (ARP) (art. 14 do Decreto Estadual 3.371/2023):
5.5.10. Serão registrados na ata os preços e os quantitativos do adjudicatário;
5.5.11. Será incluído na ata, na forma de anexo, o registro:
5.5.11.1. Dos licitantes ou dos fornecedores que aceitarem cotar os bens, as obras ou os serviços com preços iguais aos do adjudicatário, observada a classificação na licitação;
5.5.11.2. Dos licitantes ou dos fornecedores que mantiverem sua proposta original.
5.5.12. Será respeitada, nas contratações, a ordem de classificação dos licitantes ou dos fornecedores registrados na ata.
5.5.13. O registro a que se refere o item 5.5.11 tem por objetivo a formação de cadastro de reserva, para o caso de impossibilidade de atendimento pelo signatário da ata.

5.5.14. Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem reduzir suas propostas para o preço do adjudicatário antecederão aqueles que mantiverem sua proposta original.
5.5.15. A habilitação dos licitantes que comporão o cadastro de reserva a que se refere o item 5.5.13 somente será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:
5.5.15.1. Quando o licitante vencedor não assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital ou no aviso de contratação direta; e
5.5.15.2. Quando houver o cancelamento do registro do licitante ou do registro de preços nas hipóteses previstas sobre o Remanejamento das Quantidades Registradas na Ata de Registro de Preços.
5.5.16. O preço registrado com indicação dos licitantes e fornecedores será divulgado no PNCP e ficará disponibilizado durante a vigência da ata de registro de preços.
5.5.17. Após a homologação da licitação ou da contratação direta, o licitante mais bem classificado ou o fornecedor, no caso da contratação direta, será convocado para assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital de licitação ou no aviso de contratação direta, sob pena de decair o direito, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.
5.5.18. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação do licitante ou fornecedor convocado, desde que apresentada dentro do prazo, devidamente justificada, e que a justificativa seja aceita pela Administração.
5.5.19. A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no sistema de compras do governo federal.
5.5.20. Quando o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital ou no aviso de contratação, e observado o disposto no item 5.5.12. e subitens, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.
5.5.21. Na hipótese de nenhum dos licitantes que trata o item 5.5.11.1, aceitar a contratação nos termos do item anterior, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital ou do aviso de contratação direta, poderá:
5.5.22. Convocar para negociação os demais licitantes ou fornecedores remanescentes cujos preços foram registrados sem redução, observada a ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou
5.5.23. Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes ou fornecedores remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.
5.5.24. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada.
5.6. A especificação dos serviços:
5.6.16. ITEM01 - Solução de Gerenciamento de vulnerabilidades para ativos em tecnologia da informação, com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 36 meses.
5.6.16.1. Características gerais
5.6.16.1.1. A solução deve ser licenciada pelo número de ativos de tecnologia da informação, no mínimo ativos de rede, IPs, endpoints, aplicações web, containers e usuários de Active Directory;
5.6.16.1.2. O licenciamento deverá ser flexível, ou seja, não limitado por módulo;
5.6.16.1.3. A solução deve ser licenciada pelo número de ativos de TI;
5.6.16.1.4. A solução deve fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externo ou de terceiros;
5.6.16.1.5. Caso a solução dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela CONTRATADA.
5.6.16.1.6. A solução deverá suportar API baseada em REST para automação de processos e integração com aplicações terceiras;
5.6.16.1.7. A documentação de API da solução deverá ter acesso público através de website ou documentação do próprio fabricante;

5.6.16.1.8. A solução deve suportar reter os eventos coletados por no mínimo um ano;
5.6.16.1.9. A solução deve prover integração no mínimo com as seguintes plataformas abaixo:
5.6.16.1.9.1. Jira;
5.6.16.1.9.2. Slack;
5.6.16.1.9.3. AWS SNS;
5.6.16.1.9.4. Jenkins;
5.6.16.1.9.5. Terraform Cloud;
5.6.16.1.9.6. CircleCI;
5.6.16.1.9.7. Splunk;
5.6.16.1.9.8. AWS CloudTrail;
5.6.16.1.10. A solução deve possuir integração com os seguintes Repositórios:
5.6.16.1.10.1. Docker;
5.6.16.1.10.2. Docker EE;
5.6.16.1.10.3. AWS ECR;
5.6.16.1.10.4. JFrog Artifactory;
5.6.16.1.11. A solução deve possuir integração com Microsoft Azure Container, Vmware Harbor e Sonatype Nexus para importar e analisar imagens;
5.6.16.1.12. O acesso à console de gerenciamento deve ser fornecida para pelo menos 10 usuários simultâneos;
5.6.16.1.13. A console de administração deverá possuir controle de acesso no mínimo permitindo usuários com capacidade de somente visualizar as informações e usuários com capacidade para efetuar análise das imagens;
5.6.16.1.14. A solução deve prover interface web para gerenciamento de todas as funcionalidades;
5.6.16.1.15. A solução deve possuir capacidade nativa de criação de dashboards customizados;
5.6.16.1.16. A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;
5.6.16.1.17. A solução deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito;
5.6.16.1.18. A solução deve agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
5.6.16.1.19. A solução deve capturar as mudanças que ocorrem no AD e demostrar na console de administração;
5.6.16.1.20. A solução deve nativamente ser capaz de se integrar com SIEM através de protocolo SYSLOG;
5.6.16.1.21. A solução deve possuir conjunto de APIs REST, todas as chamadas disponíveis devem estar contidas na documentação;
5.6.16.1.22. A solução deve permitir a criação de listas de exclusões, suportando minimamente Exclusão por domínios do AD monitorados e por itens analisados;
5.6.16.1.23. A solução deve descobrir e mapear a superfície de ataque do Active Directory e seus domínios monitorados com os seguintes padrões:
5.6.16.1.23.1. Não depender de agentes ou sensores para coleta de informações do AD;
5.6.16.1.23.2. 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;
5.6.16.1.23.3. Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles;
5.6.16.1.24. A solução deve suportar ambientes com múltiplas florestas e domínios;
5.6.16.1.25. A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de vulnerabilidades;
5.6.16.1.26. Tais agentes devem realizar conexões para o sistema gerenciamento através de protocolo seguro;

5.6.16.2. Dos requisitos e relatórios e painéis gerenciais

5.6.16.2.1. A solução deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção;
5.6.16.2.2. A solução deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (outputs);

5.6.16.2.3. A solução deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de email;
5.6.16.2.4. A solução deve enviar notificações através de no mínimo E-mail e SMS;
5.6.16.2.5. A solução deve exibir os resultados das varreduras em tendência temporal para acompanhamento de correções e introdução de novas vulnerabilidades;
5.6.16.2.6. A solução deve exibir os resultados agregados de acordo com as categorias do OWASP Top 10;
5.6.16.2.7. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
5.6.16.2.8. Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes;
5.6.16.2.9. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc), deve evidenciar nos detalhes do evento encontrado:
5.6.16.2.9.1. Payload injetado;
5.6.16.2.9.2. Evidência em forma de resposta da aplicação;
5.6.16.2.9.3. Detalhes da requisição HTTP;
5.6.16.2.9.4. Detalhes da resposta HTTP;
5.6.16.2.10. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;
5.6.16.2.11. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;
5.6.16.2.12. A solução deve fornecer sugestões de correção automaticamente;
5.6.16.2.13. A solução deverá possuir painéis gerenciais (dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados;
5.6.16.2.14. Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento;
5.6.16.2.15. Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução;
5.6.16.2.16. Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um exploit disponível e informações do ativo;
5.6.16.2.17. A solução deve permitir a customização de relatórios;
5.6.16.2.18. A solução deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas;
5.6.16.2.19. A solução deve ser capaz de produzir relatórios, pelo menos, nos seguintes formatos: HTML, PDF e CSV;
5.6.16.2.20. A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e alvos específicos;
5.6.16.2.21. A solução deve suportar o envio automático de relatórios para destinatários específicos;
5.6.16.2.22. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: diário, semanal, mensal e anual;
5.6.16.2.23. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
5.6.16.2.24. A solução deve ser configurável para permitir a otimização das configurações de varredura;
5.6.16.2.25. 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;
5.6.16.2.26. A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
5.6.16.2.27. A solução deve se integrar com solução de gerenciamento de acessos privilegiados para autenticação nos dispositivos, no mínimo, os seguintes:
5.6.16.2.27.1. CyberArk;
5.6.16.2.27.2. BeyondTrust;
5.6.16.2.27.3. Delinea;
5.6.16.2.28. A solução deve também permitir a visualização de ações de remediação agregadas para visão consolidada de redução de risco;
5.6.16.2.29. A solução deve permitir um acompanhamento histórico do nível de exposição da organização;

5.6.16.2.30. 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;
5.6.16.2.31. Deve apresentar os resultados em forma ilustrativa (Dashboard);
5.6.16.2.32. O Dashboard deve oferecer uma visão dos seus ativos vulneráveis considerando:
5.6.16.2.32.1. Número de ativos críticos vulneráveis;
5.6.16.2.32.2. Número de caminhos de ataque que levam a esses ativos críticos;
5.6.16.2.32.3. Número de descobertas abertas e sua gravidade;
5.6.16.2.32.4. Matriz para visualizar caminhos com diferentes combinações de valores alvo;
5.6.16.2.32.5. Lista de tendências de caminhos de ataque.
5.6.16.2.33. Deve apresentar o número total alcançado de ativos críticos;
5.6.16.2.34. Deve apresentar uma tendência dos caminhos de ataque, listando os caminhos de ataques mais populares;
5.6.16.2.35. Deve ser possível exportar uma descoberta como CSV;
5.6.16.2.36. Deve ser possível arquivar uma descoberta;
5.6.16.2.37. Deve ser possível ver o histórico do log da descoberta;
5.6.16.2.38. A solução deve possuir análise por benchmarks e compliance para os seguintes padrões em formato de Dashboard:
5.6.16.2.38.1. CIS;
5.6.16.2.38.2. NIST;
5.6.16.2.38.3. ISO-27001;
5.6.16.2.38.4. HIPAA;
5.6.16.2.38.5. PCI-DSS;
5.6.16.2.38.6. CCM;
5.6.16.2.38.7. GDPR;
5.6.16.2.39. A solução deve integrar a esteira DevOps através de API, invocando o envio da imagem para análise em repositório próprio da solução ou utilizando scanner implementado em infraestrutura proprietária do órgão com a finalidade de evitar o envio de imagens e propriedade intelectual da contratante;

5.6.16.3. Das Varreduras

5.6.16.3.1. A solução deve realizar varreduras de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance);
5.6.16.3.2. 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;
5.6.16.3.3. A solução deve possuir recurso de varredura ativa, comunicando-se com os alvos através da rede.
5.6.16.3.4. A solução deve ser capaz de executar varreduras em sistemas web através de endereços IP ou FQDN (DNS);
5.6.16.3.5. A solução deve incluir agentes instalados e licenciados em estações de trabalho e servidores para varreduras diretamente no sistema operacional;
5.6.16.3.6. Os agentes devem ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades;
5.6.16.3.7. A solução deve ter a capacidade de excluir determinados endereços IP do escopo de qualquer varredura ou scan;
5.6.16.3.8. A solução deve realizar varredura em dispositivos na rede interna, dispositivos expostos a outras redes externas, e em nuvens públicas como Azure, AWS ou GCP.
5.6.16.3.9. A solução deve possuir templates prontos de varreduras simples e extensas;
5.6.16.3.10. A solução deve permitir a exclusão de URLs específicas da varredura;
5.6.16.3.11. A solução deve permitir a exclusão de tipos de arquivos através de suas extensões;
5.6.16.3.12. A solução deve instituir os seguintes limites mínimos:
5.6.16.3.12.1. Número máximo de URLs para crawl e navegação;
5.6.16.3.12.2. Número máximo de diretórios para varreduras;
5.6.16.3.12.3. Número máximo de elementos DOM;
5.6.16.3.12.4. Tamanho máximo de respostas;
5.6.16.3.12.5. Limite de requisições de redirecionamentos;
5.6.16.3.12.6. Tempo máximo para a varredura;

5.6.16.3.12.7. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;
5.6.16.3.12.8. Número máximo de requisições HTTP por segundo.
5.6.16.3.13. A solução deve detectar congestionamento de rede e limitar os seguintes aspectos da varredura:
5.6.16.3.13.1. Limite em segundos para timeout de requisições de rede;
5.6.16.3.13.2. Número máximo de timeouts antes que a varredura seja abortada;
5.6.16.3.14. A solução deve permitir a seleção granular de testes através da seleção de testes, plug-ins ou ataques;
5.6.16.3.15. A solução deve avaliar sistemas web utilizando protocolos HTTP e HTTPS;
5.6.16.3.16. A solução deve possibilitar a definição personalizada de atributos no HEADER da requisição HTTP durante os testes;
5.6.16.3.17. A solução deve ser compatível com avaliação de web services REST e SOAP;
5.6.16.3.18. A solução deve suportar os seguintes esquemas de autenticação mínimos:
5.6.16.3.18.1. Autenticação básica (digest);
5.6.16.3.18.2. NTLM;
5.6.16.3.18.3. Form de login;
5.6.16.3.18.4. Autenticação de Cookies;
5.6.16.3.18.5. Autenticação através de Selenium;
5.6.16.3.18.6. Autenticação através de Bearer.
5.6.16.3.19. A solução deve importar scripts de autenticação Selenium configurados pelo usuário.
5.6.16.3.20. A solução deve permitir a customização de parâmetros Selenium, como delay de exibição da página, delay de execução de comandos e delay de recepção de novos comandos.
5.6.16.3.21. A solução deve suportar varreduras de componentes mínimos para: Wordpress, Blog Designer Plugin for Wordpress, Event Calendar Plugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat, Apache Tomcat JK connecto, Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI;
5.6.16.3.22. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo pelo menos Windows, Linux, Mac OS e appliances virtuais.
5.6.16.3.23. A solução deve ser capaz de realizar escaneamento de descoberta de rede utilizando como alvo IP, CIRD e Range;
5.6.16.3.24. A solução deve disponibilizar modelos de escaneamento de descoberta ajustáveis com os seguintes tipos de scan:
5.6.16.3.24.1. Enumeração de Hosts;
5.6.16.3.24.2. Identificação de Sistema Operacional (SO);
5.6.16.3.24.3. Port Scan (Todas as portas);
5.6.16.3.24.4. Customizado.
5.6.16.3.25. A solução deve permitir escaneamento de descoberta customizado parametrizado conforme a necessidade;
5.6.16.3.26. A parametrização do escaneamento de descoberta deve conter pelo menos:
5.6.16.3.26.1. Descoberta de Host;
5.6.16.3.26.2. Ping do host remoto;
5.6.16.3.26.3. Uso de descoberta rápida;
5.6.16.3.26.4. Escaneamento de redes de impressora.
5.6.16.3.27. Port Scanning:
5.6.16.3.27.1. Portas.
5.6.16.3.27.1.1. Considerar portas não escaneadas como fechadas.
5.6.16.3.27.1.2. Range de portas a serem escaneadas.
5.6.16.3.27.2. Enumerar Portas locais, no mínimo:
5.6.16.3.27.2.1. SSH (netstat);
5.6.16.3.27.2.2. WMI (netstat);
5.6.16.3.27.2.3. SNMP.
5.6.16.3.28. Descoberta de Serviços:
5.6.16.3.28.1. Sondar todas as portas para encontrar serviços.
5.6.16.3.28.2. Procurar por serviços baseados em SSL/TLS.
5.6.16.3.28.3. Enumerar todas as cifras SSL/TLS.

5.6.16.3.29. A solução deve ser capaz de iniciar automaticamente serviços de registro remoto em sistemas Windows ao executar uma varredura credenciada.
5.6.16.3.30. A solução deve ser capaz de parar automaticamente o serviço de registro remoto em sistemas Windows assim que a varredura estiver completa.
5.6.16.3.31. O scanner deve oferecer suporte a SSH com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix.
5.6.16.3.32. A solução deve fornecer varredura para aplicativos comerciais e proprietários, incluindo pelo menos: Java, Adobe, Oracle, Apple, Microsoft, Check Point, Palo Alto Networks, Cisco, Fortinet;
5.6.16.3.33. A solução deve analisar, testar e reportar falhas de segurança em aplicações em Containers Docker como parte dos ativos a serem inspecionados;
5.6.16.3.34. A solução deve identificar containers que não foram analisados antes de sua implementação em produção;
5.6.16.3.35. A solução deve analisar as camadas de um container;
5.6.16.3.36. A solução deve ter a capacidade de testar automaticamente todas as imagens armazenadas ou previamente testadas sempre que uma nova vulnerabilidade for publicada e atualizada no banco de dados de vulnerabilidade da solução, sem intervenção manual;

5.6.16.4. Da Análise e Priorização de Vulnerabilidades

5.6.16.4.1. A solução deve avaliar, no mínimo, os padrões de segurança OWASP Top 10;
5.6.16.4.2. A solução deve suportar as diretivas PCI ASV para definição de escopo de análise da aplicação;
5.6.16.4.3. A solução deve ser capaz de exibir severidade e pontuação com base em CVSS (Common Vulnerability Scoring System) e inteligência de ameaças;
5.6.16.4.4. A solução deve utilizar sistema de pontuação e priorização das vulnerabilidades que inclua no mínimo:
5.6.16.4.4.1. CVSS Impact Score;
5.6.16.4.4.2. Idade da Vulnerabilidade;
5.6.16.4.4.3. Maturidade de códigos de exploração da vulnerabilidade encontrada;
5.6.16.4.4.4. Frequência de uso da vulnerabilidade em ataques e campanhas atuais;
5.6.16.4.4.5. Disponibilidade do código de exploração da vulnerabilidade.
5.6.16.4.5. O mecanismo de priorização deve ser atualizado diariamente com base em inteligência de ameaças e observação de tendências na Internet;
5.6.16.4.6. A solução deve fornecer visão sobre quais ações de remediação reduzem o maior nível de risco do ambiente;
5.6.16.4.7. A solução deve incluir classificação de severidades de acordo com o padrão Sistema Comum de Pontuação de Vulnerabilidade, versão no mínimo CVSS;
5.6.16.4.8. A solução deve informar os CVEs para cada vulnerabilidade encontrada nos pacotes e bibliotecas residentes na imagem;
5.6.16.4.9. A solução deve possuir funcionalidade para analisar detalhadamente cada configuração incorreta que acarreta riscos de segurança, contextualizando tal risco para os times envolvidos;
5.6.16.4.10. A solução deve oferecer recomendações de correção para cada configuração incorreta no Active Directory;

5.6.16.5. Da Análise de Risco do Ambiente

5.6.16.5.1. A solução deve gerar um score combinando dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;
5.6.16.5.2. O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e calcular a probabilidade de exploração de uma determinada vulnerabilidade;
5.6.16.5.3. A solução deve suportar as diretivas PCI ASV para definição de balanceadores de carga das aplicações, bem como suas configurações para inclusão no relatório de resultados.
5.6.16.5.4. Deve ser capaz de calcular a criticidade dos ativos da organização;
5.6.16.5.5. A solução deve gerar uma pontuação para cada um dos ativos, levando em conta as vulnerabilidades presentes e a classificação do ativo na rede (peso do ativo);
5.6.16.5.6. Deve gerar uma pontuação global referente à exposição cibernética da organização, baseado nas pontuações de cada um dos ativos;
5.6.16.5.7. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes), podendo sobrescrever a classificação atribuída automaticamente pela solução;

5.6.16.5.8. A solução deve contextualizar riscos compreendendo as vulnerabilidades de aplicativos no contexto de suas configurações de infraestrutura para obter uma imagem real do risco que eles apresentam;
5.6.16.5.9. Deve possuir políticas de análise em ambiente de nuvem para, no mínimo, as seguintes plataformas:
5.6.16.5.9.1. AWS;
5.6.16.5.10. Azure;
5.6.16.5.11. Google Cloud Provider.
5.6.16.5.12. A solução deve permitir a correlação de mudanças no Active Directory e desvios de segurança;
5.6.16.5.13. Deve suportar monitoramento contínuo de ambientes com Active Directory, a partir do nível funcional de floresta e domínio de 2003;
5.6.16.6. Do Gerenciamento da Análise de Ataques Exploráveis
5.6.16.6.1. Deve identificar a criticidade do ataque, pelo menos como baixo, médio e alto;
5.6.16.6.2. Deve prover evidências relacionadas à descoberta do ataque;
5.6.16.6.3. Deve mostrar o objeto de origem e destino relacionado ao ataque;
5.6.16.6.4. Deve apresentar informações detalhadas relacionadas à mitigação para o ataque em análise;
5.6.16.6.5. Deve fornecer quais ferramentas e possíveis malwares associados ao ataque;
5.6.16.6.6. Deve disponibilizar graficamente, via console de gerenciamento, as conexões entre os objetos do ataque;
5.6.16.6.7. Deve disponibilizar uma biblioteca com 'Queries' para busca de objetos nos seguintes segmentos, no mínimo:
5.6.16.6.7.1. Rede;
5.6.16.6.7.2. Endpoint;
5.6.16.6.7.3. Active Directory;
5.6.16.6.7.4. Permissão;
5.6.16.6.7.5. Ransomware;
5.6.16.6.7.6. Vetores;
5.6.16.6.7.7. Credenciamento.
5.6.16.6.8. Deve permitir analisar, pelo menos, os seguintes caminhos das superfícies de ataques:
5.6.16.6.8.1. Aplicações WEB (DAST);
5.6.16.6.8.2. Nuvem;
5.6.16.6.8.3. Active Directory;
5.6.16.6.8.4. Infraestrutura (Desktops, Servidores).
5.6.16.6.9. Deve informar se o caminho de ataque leva a um ativo crítico;
5.6.16.6.10. Deve ser possível identificar o host suspeito;
5.6.16.6.11. Deve ser possível identificar o usuário suspeito;
5.6.16.6.12. Deve ser possível identificar o IP suspeito;
5.6.16.6.13. Deve permitir visualização ilustrativa do caminho de ataque;
5.6.16.6.14. Deve ser possível identificar a técnica utilizada pelo atacante, no mínimo:
5.6.16.6.14.1. Network Sniffing;
5.6.16.6.14.2. LSASS Memory;
5.6.16.6.14.3. Remote Desktop Protocol;
5.6.16.6.14.4. Exploração de serviços remotos;
5.6.16.6.14.5. System Services Discovery;
5.6.16.6.14.6. Modificação da Política de Grupo;
5.6.16.6.14.7. Mecanismo de Controle de Elevação de Abuso.
5.6.16.6.15. A solução deve fornecer informações sobre a disponibilidade de códigos de exploração das vulnerabilidades encontradas em frameworks;
5.6.16.6.16. Deve informar se a vulnerabilidade pode e está sendo ativamente explorada por código malicioso (malware);
5.6.16.6.17. Deve ser capaz de analisar imagens preparadas pelos desenvolvedores na esteira DevOps em busca de imagens com vulnerabilidades identificadas e malware residente no sistema de arquivos;
5.6.16.6.18. Deve identificar containers que tiveram mudanças de arquivos entre a análise e sua implementação em produção;

5.6.16.6.19. Deve identificar ataques específicos para a estrutura do Active Directory;
5.6.16.6.20. Deve identificar vulnerabilidades e configurações incorretas do AD à medida que são introduzidas, sendo capaz de:
5.6.16.6.20.1. Identificar todas as vulnerabilidades e configurações incorretas no AD;
5.6.16.6.20.2. Monitorar relações de confiança perigosas em toda a estrutura do AD;
5.6.16.6.20.3. Apresentar ameaças e alterações sem a necessidade de scans estáticos e programados no Active Directory e sua infraestrutura;
5.6.16.6.20.4. Apresentar as ameaças e alterações em tempo real ou em menos de cinco minutos.
5.6.16.6.21. Detecção e resposta a ataques:
5.6.16.6.21.1. Monitorar continuamente os indicadores de possíveis ataques como DCSync, DCShadow, Password Spraying, Password Guessing/Brute Force, Lsaas Injection nos controladores de domínio, Golden Ticket, NTLM Relay, entre outros;
5.6.16.6.21.2. Detectar ataques ao AD em tempo real ou em menos de um minuto;
5.6.16.6.21.3. Realizar análise detalhada do ataque, apresentando ativo de origem, vetor de ataque, controlador de domínio afetado, técnica aplicada;
5.6.16.6.21.4. Apresentar ataques em uma linha do tempo;
5.6.16.6.21.5. Investigar ameaças, reproduzir ataques e procurar por backdoors;
5.6.16.6.21.6. Permitir busca ágil de eventos específicos na base da solução através de queries customizadas.

5.6.16.7. Da Descoberta de Ativos

5.6.16.7.1. A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de scan;
5.6.16.7.2. Para varreduras extensas e detalhadas, a solução deve varrer e auditar no mínimo os seguintes elementos:
5.6.16.7.2.1. Cookies, headers, formulários e links;
5.6.16.7.2.2. Nomes e valores de parâmetros da aplicação;
5.6.16.7.2.3. Elementos JSON e XML;
5.6.16.7.2.4. Elementos DOM.
5.6.16.7.3. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
5.6.16.7.4. A solução deve realizar descoberta de ativo de forma passiva e adicioná-lo automaticamente na console de gerenciamento;
5.6.16.7.5. A solução deve descobrir passivamente quando um host é adicionado na rede;
5.6.16.7.6. A solução deve suportar o uso do netstat (Linux) e WMI (Windows) para uma enumeração rápida e precisa de portas em um sistema quando as credenciais são fornecidas;
5.6.16.7.7. A solução deve possibilitar a verificação remota de portas, além da enumeração local de portas, para ajudar a determinar se algum mecanismo de controle de acesso está sendo utilizado;
5.6.16.7.8. 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;
5.6.16.7.9. A solução deve inventariar o sistema operacional de cada imagem analisada e suas vulnerabilidades encontradas;
5.6.16.7.10. A solução deve inventariar os pacotes e bibliotecas e suas respectivas versões, listando-as dentro do relatório de resultados de análise de cada imagem;
5.6.16.7.11. A solução deve fornecer scanner em formato Docker para implementação local e análise de imagens sem a necessidade de envio destas para repositório remoto, fora do ambiente da contratante;

5.6.16.8. Da Avaliação de Vulnerabilidade

5.6.16.8.1. A solução deve ser capaz de realizar em tempo real a descoberta de vulnerabilidades nas seguintes tecnologias:
5.6.16.8.1.1. Serviços em nuvem;
5.6.16.8.1.2. Vazamento de dados;
5.6.16.8.1.3. Banco de dados;
5.6.16.8.1.4. Internet das coisas;
5.6.16.8.1.5. Dispositivos móveis;
5.6.16.8.1.6. Sistemas operacionais;
5.6.16.8.1.7. Servidores web;

5.6.16.8.1.8. Clientes web.
5.6.16.8.2. A solução deve ser capaz de realizar testes sem a necessidade de agentes instalados no dispositivo destino para detecção de vulnerabilidades;
5.6.16.8.3. A solução deve detectar e classificar através de severidades, riscos e vulnerabilidades;
5.6.16.8.4. A solução deve também fornecer informações detalhadas sobre a natureza da vulnerabilidade, evidências da existência da vulnerabilidade e recomendações para mitigá-las;
5.6.16.8.5. A solução deve incluir uma saída detalhada das vulnerabilidades descobertas como versões de DLL esperadas e encontradas;
5.6.16.8.6. A solução deve ser compatível com CVE (Common Vunerability and Exposures);
5.6.16.8.7. A solução deve identificar vulnerabilidades específicas para o Active Directory com os seguintes padrões de verificação:
5.6.16.8.7.1. Contas administrativas vulneráveis a Kerberoasting attack;
5.6.16.8.7.2. Utilização de criptografia vulnerável com autenticação Kerberos;
5.6.16.8.7.3. Contas com pré-autenticação do Kerberos desabilitada;
5.6.16.8.7.4. Verificação de usuários com a opção de nunca expirar a senha com a opção habilitada;
5.6.16.8.7.5. Verificação de validação de fragilidades do tipo “Unconstrained Delegation”;
5.6.16.8.7.6. Verificação de “Pre-Windows 2000 Compatible Access”;
5.6.16.8.7.7. Verificação de validade de chaves mestras "Kerberos KRBTGT”;
5.6.16.8.7.8. Verificação de “SID History Injection”;
5.6.16.8.7.9. Verificação de “Printer Bug Exploit”;
5.6.16.8.7.10. Verificação de “Primary Group ID”;
5.6.16.8.7.11. Verificação de usuários com Passwords em branco.
5.6.16.8.8. A solução deve suportar o uso de SMB e WMI para verificação de sistemas Microsoft Windows;
5.6.16.8.9. A solução deve identificar fraquezas ocultas em configurações dedicadas ao Active Directory;
5.6.16.8.10. A solução deve possuir ações preventivas de hardening para o Active Directory;
5.6.16.8.11. A solução deve avaliar relações de confiança perigosas entre florestas e domínios;
5.6.16.8.12. A solução deve analisar continuamente a postura de segurança do Active Directory, minimamente avaliando:
5.6.16.8.12.1. Validação de GPOs desvinculadas, desabilitadas ou órfãs;
5.6.16.8.12.2. Validação de contas desativadas em grupos privilegiados;
5.6.16.8.12.3. Domínio usando uma configuração perigosa de compatibilidade com versões anteriores por meio de alterações no atributo dSHeuristics;
5.6.16.8.12.4. Validação de atributos relacionados a roaming de credenciais vulneráveis (ms-PKI-DPAPIMasterKeys) gerenciados por um usuário sem privilégios;
5.6.16.8.12.5. Validação de domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como NTLMv1;
5.6.16.8.12.6. Validação de contas com senhas que nunca expiram;
5.6.16.8.12.7. Validação de senhas reversíveis em GPOs;
5.6.16.8.12.8. Validação de uso de senhas reversíveis em contas de usuário;
5.6.16.8.12.9. Validação de utilização de protocolo criptográfico fraco (Ex. DES) em contas de usuário;
5.6.16.8.12.10. Validação de uso do LAPS (Solução de senha de administrador local) para gerenciar senhas de contas locais com privilégios;
5.6.16.8.12.11. Validação se o domínio possui um nível funcional desatualizado;
5.6.16.8.12.12. Validação de contas de usuário utilizando senha antiga;
5.6.16.8.12.13. Validação se o atributo AdminCount está definido em usuários padrão;
5.6.16.8.12.14. Validação do uso recente da conta de administrador padrão;
5.6.16.8.12.15. Validação de usuários com permissão para ingressar computadores no domínio;
5.6.16.8.12.16. Validação de contas dormentes;
5.6.16.8.12.17. Validação de computadores executando um sistema operacional obsoleto;
5.6.16.8.12.18. Validação de restrições de logon para usuários privilegiados em ambiente com múltiplos tiers (1, e 3) de segregação de ativos;
5.6.16.8.12.19. Validação de direitos perigosos configurados no Schema do AD;
5.6.16.8.12.20. Validação de relação de confiança perigosa com outras Florestas e Domínios;

5.6.16.8.12.21. Validação de contas que possuem um atributo perigoso de histórico SID (SID History);
5.6.16.8.12.22. Validação de contas utilizando controle de acesso compatível com versões anteriores ao Windows 2000;
5.6.16.8.12.23. Validação da última alteração de senha do KDC;
5.6.16.8.12.24. Validação de contas que podem ter senha em branco/vazia;
5.6.16.8.12.25. Validação de utilização do grupo nativo Protected Users;
5.6.16.8.12.26. Validação de privilégios sensíveis (Ex. Debug a program, Replace a process level token, etc.) perigosos atribuídos aos usuários;
5.6.16.8.12.27. Validação de possível senha em clear-text;
5.6.16.8.12.28. Validação de sanidade das GPOs e componentes CSEs (Client-Side Extension);
5.6.16.8.12.29. Validação de uso de algoritmos de criptografia fracos na PKI do Active Directory;
5.6.16.8.12.30. Validação de contas de serviço com SPN (Service Principal Name) que fazem parte de grupos privilegiados;
5.6.16.8.12.31. Validação de contas anormais nos grupos administrativos padrão do AD;
5.6.16.8.12.32. Validação de consistência no container adminSDHolder;
5.6.16.8.12.33. Validação de delegação Kerberos perigosa;
5.6.16.8.12.34. Validação em permissões de objetos raiz que permitem ataques do tipo DCSync;
5.6.16.8.12.35. Validação de políticas de senha fracas aplicadas aos usuários;
5.6.16.8.12.36. Validação das permissões relacionadas às contas do Azure AD Connect;
5.6.16.8.12.37. Validação do ID do grupo primário do usuário (Primary Group ID);
5.6.16.8.12.38. Validação de permissões em GPOs sensíveis associadas aos Containers Configuration, Sites, Root Partition e OUs sensíveis como Domain Controllers;
5.6.16.8.12.39. Controladores de domínio gerenciados por usuários ilegítimos;
5.6.16.8.12.40. Validação de certificado mapeado através de atributo altSecurityIdentities em contas privilegiadas;
5.6.16.8.12.41. Validação de uso de protocolo Netlogon inseguro (Zerologon/CVE-2020-1472);

5.6.16.9. Da Auditoria de Configuração

5.6.16.9.1. A solução deve fornecer auditoria de patch (MS Bulletins) para as principais versões de Windows;
5.6.16.9.2. A solução deve fornecer auditoria de patch para todos os principais sistemas operacionais Unix incluindo Mac OS, Linux, Solaris e IBM AIX;
5.6.16.9.3. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;
5.6.16.9.4. A solução deve fornecer benchmarks de auditoria de segurança e configuração para conformidade regulatória e outros padrões de práticas recomendadas pela área ou fabricantes;
5.6.16.9.5. 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:
5.6.16.9.5.1. Center for Internet Security Benchmarks (CIS);
5.6.16.9.5.2. Defense Information Systems Agency (DISA) STIGs;
5.6.16.9.5.3. Health Insurance Portability and Accountability Act (HIPAA);
5.6.16.9.5.4. Payment Card Industry Data Security Standards (PCI DSS);
5.6.16.9.6. A solução deve fornecer auditoria de programas antivírus para determinação de presença e status de inicialização para no mínimo os seguintes produtos: TrendMicro Office Scan, ESET, McAfee VirusScan, Microsoft Endpoint Protection e Kaspersky.
5.6.16.9.7. A solução deve oferecer validação e suporte a SCAP (Security Content Automation Protocol).
5.6.16.9.8. A solução deve ser possível avaliar modelos de infraestrutura como código (IaC), com integrações nativas em no mínimo:
5.6.16.9.8.1. Terraform;
5.6.16.9.8.2. AWS CloudFormation;
5.6.16.9.8.3. Azure Resource Manager;
5.6.16.9.8.4. Kubernetes.
5.6.16.9.9. A solução deve possuir funcionalidade de monitoramento dos repositórios sempre que houver alteração de código uma verificação automática via IaC deve apresentar a diferença.

5.6.17. ITEM02 - Suporte Técnico Especializado

5.6.17.1. A CONTRATADA deverá fornecer serviços de manutenção e suporte técnico pelo período de 36 (trinta e seis) meses, contados da data da assinatura do contrato de suporte técnico especializado, contemplando o suporte técnico para os sistemas e/ou *appliances* que compõem a Solução de Gerenciamento de Vulnerabilidades;
5.6.17.2. A CONTRATADA deverá prestar suporte técnico especializado para a solução de gerenciamento de vulnerabilidade independentemente da quantidade de ativos de tecnologia da informação licenciados para a solução;
5.6.17.3. A CONTRATADA deverá prestar serviço de manutenção e suporte técnico destinado a:
5.6.17.3.1.1. Restabelecimento de serviços interrompidos ou degradados;
5.6.17.3.1.2. Solução de problemas de configuração e falhas técnicas nos serviços;
5.6.17.3.1.3. Esclarecimentos de dúvidas sobre configurações e utilização dos serviços;
5.6.17.3.1.4. Implementação de novas funcionalidades;
5.6.17.3.1.5. Entre outras situações correlatas as acima exemplificadas.
5.6.17.4. A CONTRATADA deverá atender as seguintes premissas:
5.6.17.4.1. Os serviços serão solicitados mediante a abertura de chamados a serem efetuados por técnicos do departamento de informática do MPPA, via chamada telefônica, e-mail ou website, sem custos para a CONTRATANTE;
5.6.17.4.2. Nao haverá limitação de quantidade de abertura de chamados para suporte;
5.6.17.4.3. O suporte deve estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, nos 365 (trezentos e sessenta e cinco dias) do ano, sendo o português Brasileiro o idioma de suporte técnico obrigatório;
5.6.17.4.4. Os serviços de suporte deverão ser prestados por técnicos devidamente capacitados nos respectivos componentes da solução. Caberá a CONTRATADA fornecer aos seus técnicos todas as ferramentas e os instrumentos necessários a execução dos serviços;
5.6.17.4.5. Todas as solicitações feitas pelo CONTRATANTE deverão ser registradas pela CONTRATADA em sistema informatizado para acompanhamento e controle da execução dos serviços;
5.6.17.4.6. O acompanhamento da prestação de serviço deverá ser através de um número de protocolo fornecido pela CONTRATADA, no momento da abertura da solicitação;
5.6.17.4.7. Requisitos de Atendimento:
5.6.17.4.7.1. A CONTRATADA deverá realizar, mensalmente, procedimento de *health check* (check up) das configurações da(s) ferramenta(s) que façam parte da solução, propondo as melhorias necessárias através de relatórios, baseando-se nas boas práticas recomendadas pelo fabricante;
5.6.17.4.7.2. A CONTRATADA deve emitir, mensalmente, relatórios de vulnerabilidades e proposições de melhorias, no contexto da solução contratada, para avaliação do CONTRATANTE:
5.6.17.4.7.2.1. Procedimentos de correção e/ou contramedidas recomendadas pela equipe especializada da Contratada;
5.6.17.4.7.2.2. Orientações para o *System Hardening* dos serviços, servidores, elementos ativos e aplicações avaliados;
5.6.17.4.7.2.3. Sugestão para incremento da segurança e proteção do ambiente;
5.6.17.4.7.2.4. Os relatórios devem ser entregues em português, podendo os anexos técnicos possuírem dados em língua inglesa.
5.6.17.4.7.3. A CONTRATADA deve comunicar formalmente o CONTRATANTE sempre que identificar algum serviço com falhas de implementação e que tornem o ambiente vulnerável a indisponibilidade, bem como a realização permanente de ações proativas voltadas ao incremento da segurança do parque computacional do MPPA, a fim de mantê-lo estável, disponível e íntegro;
5.6.17.4.7.4. A CONTRATADA deverá apoiar o CONTRATANTE em caso de mudanças requeridas por conta de atualizações ou remanejamentos de infraestrutura, quando tais alterações envolver a solução ora contratada;
5.6.17.4.7.5. A CONTRATADA deverá realizar, no contexto da solução contratada, sob autorização e supervisão da CONTRATADA: instalação de softwares, acompanhamento de migrações de regras e políticas, elaboração e execução de scripts, análise de performance, resolução de problemas e implementação de segurança;
5.6.17.4.7.6. Os relatórios produzidos devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços. Nesse contexto, o profissional deve

apresentá-lo de forma presencial nas dependências do CONTRATANTE ou de forma virtual, por meio de solução de videoconferência de preferência do CONTRATANTE;
5.6.17.4.7.7. Não serão aceitos relatórios obtidos diretamente de ferramentas automatizadas utilizadas, sem a devida transcrição e contextualização adequada com o ambiente do MPPA.
5.6.17.4.8. Dos prazos de atendimento:
5.6.17.4.8.1. A tabela abaixo descreve os prazos de atendimento que deverão ser cumpridos pela CONTRATADA, de acordo com a severidade de cada chamado aberto:

Tabela de Solução dos chamados			
Severidade	**Descrição**	**Tempo para primeiro contato após abertura do chamado**	**Tempo de resolução do chamado**
Urgente	Serviço crítico parado em produção.	30 minutos	até 01 (uma) hora
Alta	Erros e problemas que estão impactando no ambiente de produção.	60 minutos	até 04 (quatro) hora
Média	Problemas ou erros contornáveis que afetam o ambiente em produção, mas não possuem alto impacto.	90 minutos	até 06 (seis) horas
Baixa	Problemas ou erros contornáveis que não impactam significativamente no ambiente em produção.	120 minutos	até 08 (oito) horas
Informações	Consulta Técnica, dúvidas em geral, monitoramento.	150 minutos	até 24 (vinte e quatro) horas

5.6.17.4.8.2. O prazo de atendimento deve começar a ser contabilizado a partir do momento de efetivação da abertura do chamado, através de telefone, e-mail ou website;
5.6.17.4.9. A CONTRATADA deve apresentar relatório de visita para cada solicitação de suporte on-site, contendo a data e hora da solicitação de suporte técnico, o início e o término do atendimento, identificação do problema, providencias adotadas e demais informações pertinentes;
5.6.17.4.10. O nível de severidade será informado no momento da abertura de cada chamado pelo técnico responsável do CONTRATANTE;
5.6.17.4.11. Todas as solicitações de suporte técnico devem ser registradas pela CONTRATADA para acompanhar e controlar a execução dos chamados;
5.6.17.4.12. O descumprimento dos prazos de atendimento implicara na aplicação de glosas conforme tabela abaixo:

Tabela de aplicação de Glosas		
Severidade	**Fórmula de cálculo da glosa**	**Limite da glosa**
Urgente	HS x 0,5% * VFM	20% da VFM
Alta	HS x 0,4% * VFM	15% da VFM
Média	HS x 0,3% * VFM	10% da VFM
Baixa	HS x 0,2% * VFM	10% da VFM
Informações	HS x 0,1% * VFM	10% da VFM

HS = Horas totais que extrapolaram o limite de resolução dos chamados, no caso de hora quebrada, será apurado o percentual da hora descumprida.
VFM = Valor da Fatura Mensal para pagamento do serviço de suporte.
Em caso de descumprimento contumaz pela CONTRATADA nos prazos para atendimento do suporte técnico a fiscalização poderá adotar a aplicação de sanções: advertência, multa, impedimento de licitar e contratar, e declaração de inidoneidade para licitar ou contratar, na forma da Lei nº 14.133/2021.

5.6.17.4.13. A CONTRATADA deve emitir relatório mensal em arquivo eletrônico ou em sistema de consulta online, com informações dos chamados abertos e efetivamente atendidos no período;
5.6.17.4.14. O relatório deve possuir os seguintes parâmetros:
5.6.17.4.14.1. Quantidade de ocorrências (chamados) registradas no período;
5.6.17.4.14.2. Número do chamado registrado e nível de severidade;
5.6.17.4.14.3. Data e hora de abertura;
5.6.17.4.14.4. Data e hora de início e conclusão do atendimento;
5.6.17.4.14.5. Identificação do técnico do MPPA que fez o registro do chamado;
5.6.17.4.14.6. Descrição do problema;
5.6.17.4.14.7. Descrição da solução;
5.6.17.4.15. Problemas cuja solução dependa de correção de falhas (*bugs*) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução, não necessitarão observar os prazos estabelecidos acima;
5.6.17.4.16. A CONTRATADA deverá, de acordo com o nível de severidade, prover solução paliativa para atender os problemas de falhas (bugs), atualizações ou patches de correção que ainda nao foram disponibilizadas pela fabricante, no prazo de 24 (vinte e quatro) horas, para restabelecer o ambiente do CONTRATANTE;
5.6.17.4.17. A solução do chamado definitiva deverá ser disponibilizada no prazo máximo de 60 (sessenta) dias, sendo a CONTRATADA responsável pelos tramites juntamente a fabricante da liberação das correções;
5.6.17.4.18. Nas manutenções que necessitem de intervenção para parada física ou reinicialização do equipamento, o CONTRATANTE deverá ser notificado previamente para que faça o agendamento da manutenção e aprovação;
5.6.17.4.19. As paradas de manutenção deverão acontecer fora do horário de expediente, de preferência após a 20 (vinte) horas devendo ser restabelecida antes das 8 (oito) horas da manhã do dia seguinte. Poderá ocorrer durante o dia da semana ou aos finais de semana, sem ônus para o CONTRATANTE;
5.6.17.4.19.1. Todo o procedimento de manutenção deverá ser documentado, explicando o passo a passo completo e fazendo registro das ocorrências incoerentes para subsidiar novas paradas que possam acontecer;
5.6.17.4.19.2. O relatório deverá ser assinado pelo fiscal técnico do contrato ou responsável pelo acompanhamento do serviço por parte do CONTRATANTE.
5.7. O prazo de duração e prorrogação do contrato:
5.7.1. O prazo de vigência da contratação é de 36 meses, contados do primeiro dia útil seguinte ao da sua divulgação no Portal Nacional de Contratações Pública - PNCP, na forma do artigo 183 da Lei n° 14.133, de 2021, com exclusão do dia do começo e inclusão do dia do vencimento, prorrogável por até 5 anos, na forma do artigo 106, §2º (aluguel de equipamentos ou utilização de programas de informática) da Lei n° 14.133, de 2021.
5.7.2. A prorrogação de que trata este item estará condicionada à demonstração de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado, bem como à verificação de que trata o art. 91, § 4º da Lei nº 14.133/2021.

6. REQUISITOS DA CONTRATAÇÃO

6.1. A contratação deverá obedecer aos seguintes requisitos:
6.1.1. O serviço prestado e sua disponibilização são caracterizados como de natureza contínua. Isso porque o serviço é essencial para a garantia de segurança cibernética dos nossos ativos de tecnologia, usuários e aplicações. Sendo que o sucesso de agentes externos na exploração de vulnerabilidades pode ter impactos significativos nas atividades ministeriais causando

indisponibilidade das ferramentas tecnológicas utilizados como ferramenta de trabalho pelos servidores do MPPA.

6.2. Sustentabilidade:

6.2.1. A CONTRATADA, como prática de sustentabilidade na execução dos serviços, deverá fornecer bens que não contenham substâncias perigosas em concentração acima da recomendada, bem como ficar encarregada de promover o descarte adequado dos equipamentos e demais materiais recolhidos, seja quando do encerramento do contrato, por ocasião da substituição por outros, ou quando forem danificados irreversivelmente, seguindo os preceitos da Lei nº 12.305/10, que trata da Política Nacional de Resíduos Sólidos (PNRS).

6.3. Da Vistoria

6.3.1. Não se aplica

6.4. Da exigência de Carta de Solidariedade:

6.4.1. Não se aplica.

6.5. Da subcontratação

6.5.1. Não será permitida a subcontratação na presente contratação.

6.6. Garantia Contratual:

6.6.1. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133/21, no percentual de 5% do valor contratual, conforme regras previstas no contrato.

6.6.2. A garantia nas modalidades caução e fiança bancária deverá ser prestada em até 10 (dez) dias após a assinatura do contrato.

6.6.3. No caso de seguro-garantia, sua apresentação deverá ocorrer, no máximo, até a data de assinatura do contrato.

6.7. **Dos direitos e obrigações da CONTRATANTE:**

6.7.1. Sem que a isto limite seus direitos, terá o Ministério Público as seguintes garantias:

6.7.1.1. Receber o objeto de acordo com o que consta neste instrumento, no edital e nos seus anexos;

6.7.1.2. Devolver o objeto em desacordo com as especificações exigidas neste instrumento, no edital e nos seus anexos.

6.7.2. Sem que a isto limite sua responsabilidade, será o Órgão responsável pelos seguintes itens:

6.7.2.1. Cumprir todos os compromissos financeiros assumidos com a CONTRATADA no prazo estipulado;

6.7.2.2. Emitir Nota de Empenho a crédito do fornecedor no valor correspondente à quantidade solicitada;

6.7.2.3. Proporcionar todas as facilidades, inclusive esclarecimentos atinentes ao objeto, para que a empresa possa cumprir as obrigações dentro das normas e condições da aquisição.

6.7.2.4. Os objetos licitados serão recebidos e conferidos pela FISCALIZAÇÃO designada pela Autoridade competente no âmbito do Ministério Público com competência necessária para proceder o recebimento dos objetos licitados e atestar as Notas Fiscais após a verificação das especificações técnicas, da qualidade, da quantidade e preços pactuados;

6.7.2.5. Promover, através de seu representante, o acompanhamento e a fiscalização do objeto contratado, sob os aspectos qualitativos e quantitativos, prazos de vigência e entregas, anotando em registro próprio as falhas detectadas e comunicando ao Órgão por escrito as advertências e as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte desta;

6.7.2.6. Cumprir e fazer cumprir o disposto neste instrumento, no edital e nos seus anexos.

6.7.3. Caberá ao MPPA, enquanto entidade gerenciadora da Ata, a prática de todos os atos de controle e administração do SRP, em especial:

6.7.3.1. Realizar pesquisa de mercado para identificação do valor estimado da licitação ou contratação direta e consolidar os dados das pesquisas de mercado realizadas pelos órgãos e entidades participantes, inclusive no caso de compra centralizada;

6.7.3.2. Promover, no caso de compra nacional, a divulgação da ação, a pesquisa de mercado e a consolidação da demanda dos órgãos e entidades da administração direta e indireta da União, dos Estados, do Distrito Federal e dos Municípios, conforme o caso;

6.7.3.3. Remanejar os quantitativos da ata;

6.7.3.4. Promover atos necessários à instrução processual para a realização do procedimento licitatório ou da contratação direta;

6.7.3.5. Confirmar junto aos órgãos ou entidades participantes a sua concordância com o objeto a ser contratado, inclusive quanto aos quantitativos e termo de referência ou projeto básico;

6.7.3.6. Promover os atos necessários à instrução processual para a realização do procedimento licitatório ou da contratação direta, bem como todos os atos decorrentes, tais como a assinatura da ata e a sua disponibilização aos órgãos ou entidades participantes;
6.7.3.7. Gerenciar a ata de registro de preços;
6.7.3.8. Conduzir as alterações ou as atualizações dos preços registrados;
6.7.3.9. Deliberar quanto à adesão posterior de órgãos e entidades que não manifestaram interesse durante o período de divulgação da intenção para registro de preços;
6.7.3.10. Verificar se os pedidos de realização de registro de preços, formulados pelos órgãos e entidades da Administração Pública, efetivamente se enquadram nas hipóteses previstas, podendo indeferir os pedidos que não estejam de acordo com as referidas hipóteses.
6.7.3.11. Aplicar, garantida a ampla defesa e o contraditório, as penalidades decorrentes de infrações no procedimento licitatório ou na contratação direta;
6.7.3.12. Aplicar, garantida a ampla defesa e o contraditório, as penalidades decorrentes do descumprimento do pactuado na ata de registro de preços, em relação à sua demanda registrada, ou do descumprimento das obrigações contratuais, em relação às suas próprias contratações, e registrar no Sicaf.
6.8. **Dos direitos e obrigações da CONTRATADA:**
6.8.1. Sem que a isto limite suas garantias, a CONTRATADA terá os seguintes direitos:
6.8.1.1. Receber informações e esclarecimentos necessários ao cumprimento das condições estabelecidas;
6.8.1.2. Receber o Atesto do recebimento do objeto contratado após verificação das especificações;
6.8.1.3. Receber formalmente a notificação de ocorrência de irregularidades que a fiscalização identificar na execução do objeto licitado, até para que possa a empresa proceder correções;
6.8.1.4. Receber o pagamento nas condições estabelecidas neste instrumento.
6.8.2. Sem que a isto limite sua responsabilidade, será a CONTRATADA responsável pelos seguintes itens:
6.8.2.1. Cumprir fielmente as obrigações assumidas, conforme as especificações exigidas, utilizando-se de todos os recursos materiais e humanos necessários para entregar os produtos licitados no prazo, no local e horário indicados, observando rigorosamente as exigências estabelecidas nas especificações e na proposta de preços apresentada pela empresa;
6.8.2.2. Arcar com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas, responsabilizando-se pelos danos causados diretamente à administração ou a terceiros, decorrentes de sua culpa ou dolo, por ocasião da entrega dos objetos licitados no local indicado, incluindo os possíveis danos causados por transportadoras, sem qualquer ônus ao contratante, ressarcindo os eventuais prejuízos causados ao Órgão e/ou terceiros, provocados por irregularidades cometidas na execução das obrigações assumidas;
6.8.2.3. Ser responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução. A inadimplência da CONTRATADA, com referência aos encargos estabelecidos neste subitem não transfere a responsabilidade por seu pagamento à Administração do Ministério Público, nem poderá onerar o objeto desta licitação, razão pela qual a CONTRATADA renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com o Ministério Público;
6.8.2.4. Prestar todos os esclarecimentos que forem solicitados pelo Ministério Público, credenciando junto ao Órgão, um representante para prestar os devidos esclarecimentos e atender as reclamações que porventura surgirem durante a execução do objeto;
6.8.2.5. Manter, durante toda a execução, todas as condições de habilitação e qualificação exigidas no Pregão que sejam compatíveis com as obrigações a ser assumidas, cumprindo durante a vigência do contrato todas as leis e posturas federais, estaduais e municipais vigentes, a regularidade com o fisco, com o sistema de seguridade social, com a legislação trabalhista, normas e padrões de proteção ao meio ambiente e cumprimento dos direitos da mulher, inclusive os que protegem a maternidade, sob pena da rescisão contratual, sem direito a indenização conforme preceitua o art. 28 §4° da Constituição do Estado do Pará, sendo a única responsável por prejuízos decorrentes de infrações a que houver dado causa, em especial a:
6.8.2.5.1. **Regularidade Fiscal** com a Fazenda Nacional, o Sistema de Seguridade Social e o Fundo de Garantia do Tempo de Serviço – FGTS;
6.8.2.5.2. **Regularidade Fiscal** perante as Fazendas Estaduais e Municipais da sede da licitante;
6.8.2.5.3. **Regularidade Trabalhista;**

6.8.2.5.4. Cumprimento do disposto no art. 7º, XXXIII, da Constituição Federal/88 (trabalho de menores de idade, observada a Lei nº 9.854/1999);
6.8.2.6. Não transferir a outrem, no todo ou em parte, o objeto do presente, sem prévia e expressa anuência do Ministério Público; não sendo aceita, sob nenhum pretexto, a transferência de responsabilidade da CONTRATADA para outras entidades, sejam fabricantes, técnicos ou quaisquer outros.
6.8.2.7. A CONTRATADA é obrigada a reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, sem ônus para a Contratante.
6.8.2.8. Informar o Órgão de qualquer alteração necessária à consolidação dos ajustes decorrentes da execução do objeto, tais como: mudança de endereço, razão social, telefone, e-mail, dissolução da sociedade, falência e outros;
6.8.2.9. Disponibilizar uma conta de e-mail para fins de comunicação entre as partes, que integrará o preambulo do instrumento de contratação, mantendo-o permanentemente atualizado.
6.8.2.10. Comunicar imediatamente à Administração, bem como ao responsável pela fiscalização, qualquer anormalidade verificada, inclusive de ordem funcional, para que sejam adotadas as providências de regularização necessárias, em qualquer tempo até o final da garantia.
6.8.2.11. Manter sigilo, sob pena de responsabilidade civil, criminal e administrativa, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do Contrato, devendo orientar seus empregados nesse sentido;
6.8.2.12. Responsabilizar-se por quaisquer consequências oriundas de acidentes que possam vitimar seus empregados, quando do cumprimento do objeto desta contratação;
6.8.2.13. Ressarcir os eventuais prejuízos causados ao Órgão e/ou terceiros, provocados por irregularidades cometidas na execução das obrigações assumidas.
6.8.2.14. Observar a Resolução nº 172/2017-CNMP que altera o artigo 3º, caput, da Resolução CNMP nº 37/2009 que VEDA ao Ministério Público a contratação das pessoas jurídicas que tenham em seu quadro societário cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive, dos membros ocupantes de cargos de direção ou no exercício de funções administrativas, assim como de servidores ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação;
6.8.2.14.1. A vedação do item 6.8.2.14 não se aplica às hipóteses nas quais a contratação seja realizada por ramo do Ministério Público diverso daquele ao qual pertence o membro ou servidor gerador da incompatibilidade.
6.8.2.14.2. A vedação do item 6.8.2.14 se estende às contratações cujo procedimento licitatório tenha sido deflagrado quando os membros e servidores geradores de incompatibilidade estavam no exercício dos respectivos cargos e funções, assim como às licitações iniciadas até 6 (seis) meses após a desincompatibilização.
6.8.2.14.3. A contratação de empresa pertencente a parente de membro ou servidor não abrangido pelas hipóteses expressas de nepotismo poderá ser vedada pelo órgão do Ministério Público competente, quando, no caso concreto, identificar risco potencial de contaminação do processo licitatório;
6.8.2.15. Observar a VEDAÇÃO de contratação de Empresa que tenha entre seus empregados colocados à disposição do Ministério Público para o exercício de funções de chefia, pessoas que incidam na vedação dos arts. 1º e 2º da Resolução nº 177/2017-CNMP:
6.8.2.15.1. Pessoa que tenha sido condenada em decisão com trânsito em julgado ou proferida por órgão jurisdicional colegiado, nos seguintes casos:

I – Atos de improbidade administrativa;
II – Crimes:
a) contra a administração pública;
b) contra a incolumidade pública;
c) contra a fé pública;
d) contra o patrimônio;
e) de abuso de autoridade, nos casos em que houver condenação à perda do cargo ou à inabilitação para o exercício de função pública;
f) de tráfico de entorpecentes e drogas afins, racismo, tortura, terrorismo e hediondos;
g) contra a vida e a dignidade sexual;

h) praticados por organização ou associação criminosa;
i) de redução de pessoa à condição análoga à de escravo;
j) eleitorais, para os quais a lei comine pena privativa de liberdade;
k) de lavagem ou ocultação de bens, direitos e valores.

6.8.2.15.2. Aqueles que tenham:

I – Praticado atos causadores da perda do cargo ou emprego público, reconhecidos por decisão transitada em julgado ou proferida por órgão judicial colegiado;

II – Sido excluídos do exercício da profissão, por decisão definitiva sancionatória judicial ou administrativa do órgão profissional competente, salvo se o ato houver sido anulado ou suspenso pelo Poder Judiciário;

III – tido suas contas relativas ao exercício de cargos ou funções públicas rejeitadas por irregularidade insanável que configure ato doloso de improbidade administrativa, por decisão irrecorrível do órgão competente, salvo se esta houver sido suspensa ou anulada pelo Poder Judiciário, devendo tal condição constar expressamente dos editais de licitação.

6.9. **Dos preços dos itens:**

6.9.1. A ausência de diferenciação de preços entre as licenças para o sistema de gerenciamento de vulnerabilidades e no serviço de suporte técnico especializado justifica-se pelo fato de que o sistema opera com licenças baseadas em ativos de tecnologia da informação, e não há variação significativa nas condições de uso desses ativos. Todos os ativos são geridos dentro da mesma infraestrutura, garantindo uniformidade na instalação e operação do sistema. O suporte técnico é prestado de maneira consistente para todos os ativos, não havendo necessidade de adaptações específicas ou variações no acondicionamento. Portanto, a padronização dos preços é apropriada, refletindo a uniformidade das condições de uso e suporte técnico para todas as licenças e serviços contratados.

6.9.2. A atualização ou alteração dos preços registrados será realizada 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: (art. 21 do Decreto Estadual nº 3371/2023)

6.9.2.1. 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 Federal nº 14.133, de 2021;

6.9.2.2. 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;

6.9.2.3. Na hipótese de previsão no edital de cláusula de reajustamento ou repactuação sobre os preços registrados, nos termos do disposto na Lei Federal nº 14.133, de 2021.

6.9.3. **Da Negociação dos preços registrados:**

6.9.3.1. Na hipótese de o preço registrado tornar-se superior ao preço praticado no mercado, por motivo superveniente, o órgão ou a entidade gerenciadora convocará o fornecedor para negociar a redução do preço registrado

6.9.3.1.1. Caso o fornecedor não aceite reduzir seu preço aos valores praticados pelo mercado, o fornecedor será liberado do compromisso assumido quanto ao item registrado, sem aplicação de penalidades administrativas

6.9.3.1.2. Na hipótese acima mencionada, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado.

6.9.3.1.3. Se não obtiver êxito nas negociações, o órgão ou a entidade gerenciadora procederá ao cancelamento do preço registrado na Ata de Registro de Preços (ARP), nos termos do disposto no art. 25 do Decreto Estadual nº 3.371/2023 e adotará as medidas cabíveis para a obtenção de contratação mais vantajosa.

6.9.3.1.4. Na hipótese de redução do preço registrado, órgão ou entidade gerenciadora comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da Ata de Registro de Preços (ARP), para que avaliem a conveniência e a oportunidade de diligenciarem negociação com vistas a alteração contratual.

6.9.3.2. Na hipótese de o preço de mercado tornar-se superior ao preço registrado e o fornecedor não poder cumprir as obrigações estabelecidas na ata, será facultado ao fornecedor requerer ao gerenciador a alteração do preço registrado, mediante comprovação de fato superveniente que o impossibilite de cumprir o compromisso.

6.9.3.2.1. Para fins do disposto no item 6.9.3.1 o fornecedor encaminhará, juntamente com o pedido de alteração, a documentação comprobatória ou a planilha de custos que demonstre a inviabilidade do preço registrado em relação às condições inicialmente pactuadas.
6.9.3.2.2. Na hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado, o pedido será indeferido pelo órgão ou pela entidade gerenciadora e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do seu registro, sem prejuízo da aplicação das sanções previstas na Lei nº 14.133, de 2021, e na legislação aplicável.
6.9.3.2.3. Na hipótese de cancelamento do registro do fornecedor, em virtude do fornecedor não aceitar alterar o preço, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam manter seus preços registrados.
6.9.3.2.4. Se não obtiver êxito nas negociações, o órgão ou a entidade gerenciadora procederá ao cancelamento da ata de registro de preços, e adotará as medidas cabíveis para a obtenção da contratação mais vantajosa.
6.9.3.2.5. Na hipótese de comprovação do disposto no item 6.9.3.1 e 6.9.3.1.1, o órgão ou a entidade gerenciadora atualizará o preço registrado, de acordo com a realidade dos valores praticados pelo mercado.
6.9.3.2.6. O órgão ou a entidade gerenciadora comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços sobre a efetiva alteração do preço registrado, para que avaliem a necessidade de alteração contratual.
6.9.4. **Do cancelamento do registro do fornecedor**
6.9.4.1. O registro do fornecedor será cancelado, quando o fornecedor (art. 24 do Decreto Estadual 3371/2023):
6.9.4.1.1. Descumprir as condições da ata de registro de preços sem motivo justificado;
6.9.4.1.2. Não retirar a nota de empenho, ou instrumento equivalente, no prazo estabelecido pela Administração sem justificativa razoável;
6.9.4.1.3. Não aceitar manter seu preço registrado, na hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado, o pedido será indeferido pelo órgão e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do seu registro, sem prejuízo da aplicação das sanções previstas na Lei nº 14.133, de 2021, e na legislação aplicável;
6.9.4.1.4. Sofrer sanção de impedimento de licitar e contratar ou de declaração de inidoneidade para licitar ou contratar.
6.9.5. **Do cancelamento dos preços registrados (art. 25 do Decreto Estadual 3371/2023):**
6.9.5.1. O cancelamento dos preços registrados poderá ser realizado pelo MPPA, em determinada ata de registro de preços, total ou parcialmente, nas seguintes hipóteses, desde que devidamente comprovadas e justificadas:
6.9.5.1.1. Por razão de interesse público;
6.9.5.1.2. A pedido do fornecedor, decorrente de caso fortuito ou força maior;
6.9.5.1.3. Se não houver êxito nas negociações, o MPPA procederá ao cancelamento da ata de registro de preços e adotará as medidas cabíveis para a obtenção de contratação mais vantajosa, nos termos do art. 25 do Decreto Estadual 3.371/2023.
6.10. Da participação de consórcio:
6.10.1. Será admitida a participação de consórcio, nos termos dos art.15 da Lei 14.133/2021, havendo acréscimo de 10%, sobre o valor exigido de licitante individual para a habilitação econômico-financeira, salvo justificação;
6.10.1.1. O acréscimo previsto no item 6.10.1 não se aplica aos consórcios compostos, em sua totalidade, de microempresas e pequenas empresas, assim definidas em lei.

7. MODO DE EXECUÇÃO: PRAZOS, CONDIÇÕES DE ENTREGA, RECEBIMENTO DO SERVIÇO E GARANTIA (art.6º, XXIII, alínea "e" da Lei 14.133/2021.)

7.1. MINISTÉRIO PÚBLICO formalizará, através de contrato ou nota de empenho (no caso desta substituir o contrato) e de acordo com a demanda Institucional, a quantidade necessária ao seu consumo regular, não havendo impedimento que a quantidade e período regular de fornecimento sejam modificados em razão da necessidade do órgão, devidamente justificada;
7.1.1. O detentor da Ata de Registro de Preços terá o prazo de **06 (seis) dias úteis** a contar da comunicação para assinar o contrato ou retirar a Nota de Empenho.

7.1.2. O detentor da Ata de Registro de Preços fica obrigado a atender todos os pedidos de fornecimento efetuados pelo ÓRGÃO durante a vigência da Ata, mesmo que a entrega deles decorrentes esteja prevista para data posterior ao seu vencimento.

7.2. Caso os serviços envolvam **demolição, conserto, instalação, montagem, operação, conservação, reparação, adaptação e manutenção a ser realizada nos prédios deste Ministério Público do Estado do Pará,** serão demandados mediante emissão previa de Ordem de Serviço pelo gestor da Unidade Responsável pela atividade nos termos do modelo constante no Anexo da Portaria n.º 3296/2022-MP/PGJ, publicada no DOE de 22/06/2022.

7.3. A CONTRATADA se compromete a efetuar a entrega dos serviços solicitados no prazo não superior a **30 (trinta) dias corridos**, em remessa única, a contar do pedido formal de fornecimento;

7.4. Os serviços serão executados no Departamento de Informática, no edifício sede do MPPA, situado na Rua João Diogo, 100 – Cidade Velha, Belém, Pará, no horário das 08h00min às 17h00min, de segunda a sexta-feira, exceto nos feriados e dias facultativos, correndo por conta da CONTRATADA todas as despesas, inclusive de e/ou dos materiais utilizados nos serviços, seguros, transporte, tributos, encargos trabalhistas e previdenciários, decorrentes do fornecimento, devendo o início da execução ser agendada, com até 24h de antecedência, via e-mail: informatica@mppa.mp.br;

7.5. Na hipótese de ocorrência de caso fortuito ou de força maior que tenha o condão de motivar o atraso na execução do objeto no prazo previsto, deve a CONTRATADA submeter os fatos, por escrito, à FISCALIZAÇÃO do Contrato do MPE/PA, com as justificativas correspondentes, acompanhadas da comprovação devida, para análise e decisão, desde que dentro do prazo estabelecido para o início da execução dos serviços;

7.6. A justificativa, por escrito, deverá ser enviada, no prazo máximo de 72 (setenta e duas) horas contados da assinatura do contrato ou recebimento da nota de empenho, pelo e-mail informatica@mppa.mp.br ou protocolizada no Protocolo do Ministério Público do Estado do Pará, localizado no Ed. Sede do Órgão, Rua João Diogo nº. 100 – Cidade Velha, no horário de 8h às 17:00h de segunda a sexta-feira, ficando a critério da Fiscalização do Contrato a sua aceitação;

7.7. O recebimento do objeto pela FISCALIZAÇÃO, ou COMISSÃO DE DESIGNADA dar-se-á em duas etapas:

a) Em **caráter provisório**, de forma sumária, em até **5 (cinco) dias úteis** da entrega, acompanhada da assinatura de servidor designado para esse fim, em canhoto de fatura/nota fiscal, e representada pela conferência da quantidade de volumes e da qualidade do material entregue (esta em sentido da aparência e da embalagem) para posterior conferência de sua conformidade com as especificações.

b) **Definitivamente**, em a**té 15 (quinze) dias úteis** a contar do recebimento provisório, ocasião em que será feita a conferência da quantidade, avaliação da qualidade e verificação da adequação dos objetos licitados entregues pelo servidor ou comissão de fiscalização designada para esse fim;

c) O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

d) Na hipótese de ser verificada a impropriedade do material no ato da entrega, será imediatamente rejeitado, no todo ou em parte, a critério da FISCALIZAÇÃO responsável pelo seu recebimento, sendo o fornecedor notificado a proceder à substituição no prazo máximo de **15 (quinze) dias úteis** após a verificação, sendo-lhe, ainda, concedido igual prazo para retirada do material ou parte do que foi rejeitado, da data da comunicação;

e) Os objetos licitados serão recebidos e conferidos pela Fiscalização/comissão designada por esta Instituição.

7.8. O recebimento do serviço não exclui a responsabilidade administrativa, civil, penal e ético profissional da empresa por problemas causados durante o uso dos itens adquiridos, nem exclui a responsabilidade da CONTRATADA pelo perfeito desempenho dos serviços contratados, sendo responsável ainda pela solidez e segurança de tais serviços, cabendo-lhe sanar quaisquer irregularidades detectadas quando de sua utilização;

7.9. A não substituição do objeto ou a não retirada do material rejeitado, sujeitará a CONTRATADA em mora, cujo atraso computar-se-á desde o primeiro dia do vencimento do prazo;

7.10. A CONTRATADA deverá promover, às suas expensas, a substituição total ou parcial do objeto que apresentar qualquer irregularidade;

7.11. O prazo de garantia será de 36 (trinta e seis) meses, contra defeito de execução dos serviços, contados a partir da data da entrega da solução, com suporte técnico on-line ou on-site, situado no edifício sede do MPPA, situado na Rua João Diogo, 100 – Cidade Velha, Belém, Pará. A garantia no prazo mínimo aqui estipulado consiste na prestação pela Contratada, de todas as obrigações estabelecidas no Código de Defesa do Consumidor (e suas alterações), bem como dos encargos previstos à Contratada no Edital. Durante este período, os reparos e substituições porventura necessários deverão ser realizados pela Contratada, sem ônus para a Contratante.
7.11.1. Durante o período de garantia, a CONTRATADA, independentemente de ser ou não fabricante da solução implantada, obriga-se a substituir ou reparar o objeto que apresentar indícios de irregularidades, defeitos ou incorreções resultantes da fabricação no prazo máximo de 5 (quinze) dias úteis a contar da comunicação escrita da autoridade competente, sem acarretar ônus para a Contratante;
7.12. Relativamente, ao disposto nesta cláusula, aplicam-se também, subsidiariamente, no que couber, as disposições da Lei nº 8.078 de 11/09/90 – Código de Defesa do Consumidor;

8. MODELO DE GESTÃO E FISCALIZAÇÃO DO CONTRATO

8.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei 14.133/2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial (Lei 14.133/2021, art.115, caput)
8.2. 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. (Lei 14.133/2021, art.115, §5º)
8.3. A execução do contrato deverá ser acompanhada e fiscalizada por 1 (um) ou mais fiscais do contrato, representantes da Administração especialmente designados conforme requisitos estabelecidos no art. 7ºda Lei 14.133/2021, ou pelos respectivos substitutos, permitida a contratação de terceiros para assisti-los e subsidiá-los com informações pertinentes a essa atribuição.
8.4. O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas à execução do contrato, determinando o que for necessário para a regularização das faltas ou dos defeitos observados. (Lei 14.133/2021, art.117, §1º)
8.5. O fiscal do contrato informará a seus superiores, em tempo hábil para a adoção das medidas convenientes, a situação que demandar decisão ou providência que ultrapasse sua competência. (Lei 14.133/2021, art.117, §2º)
8.6. O fiscal do contrato será auxiliado pelos órgãos de assessoramento jurídico e de controle interno da Administração, que deverão dirimir dúvidas e subsidiá-lo com informações relevantes para prevenir riscos na execução contratual.
8.7. O contratado será obrigado a reparar, corrigir, remover, reconstruir ou substituir, a suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes de sua execução ou de materiais nela empregados. (Lei nº14.133/2021. Art.119)
8.8. O contratado será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pelo contratante. (Lei n.º 14.133/2021, art.121)
8.9. Somente o contratado será responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato (Lei nº 14.133/2021, art. 121, caput).
8.10. A inadimplência do contratado em relação aos encargos trabalhistas, fiscais e comerciais não transferirá à Administração a responsabilidade pelo seu pagamento e não poderá onerar o objeto do contrato (Lei nº 14.133/2021, art. 121, §1º).
8.11. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se, excepcionalmente, o uso de mensagem eletrônica para esse fim. (IN SEGES nº 98/2022).
8.12. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato. (IN SEGES nº 98/2022).

9. DO PAGAMENTO E CRITÉRIOS DE MEDIÇÃO

9.1. Para o **item 01**, o pagamento será efetuado em parcela única pelo Departamento Financeiro do Ministério Público no prazo máximo de **20 (vinte) dias corridos**, no Banco: **XXXX**, Agência n° **XXXX**, Conta Corrente n° **XXXX**, após o recebimento definitivo do objeto contratado e efetivamente

entregue, mediante a apresentação da Nota Fiscal devidamente atestada pelo FISCAL, os quais observarão as especificações exigidas no Edital e no Termo de Referência;

9.2. Para o **item 02**, o pagamento será feito mensalmente pelo Departamento Financeiro do Ministério Público no prazo máximo de **20 (vinte) dias corridos**, no Banco: XXXX, Agência n° XXXX, Conta Corrente n° XXXX, após o recebimento definitivo do objeto contratado e efetivamente entregue, mediante a apresentação da Nota Fiscal devidamente atestada pelo FISCAL, os quais observarão as especificações exigidas no Edital e no Termo de Referência;

9.2.1. O atesto da nota fiscal será efetuado no prazo máximo de **7 (sete) dias úteis** contados do recebimento definitivo do material pelo responsável pela FISCALIZAÇÃO;

9.3. O pagamento dos fornecedores de bens e prestadores de serviços dos órgãos da Administração Direta e Indireta do Estado do Pará será efetuado mediante crédito em conta corrente aberta no Banco do Estado do Pará S/A – BANPARÁ, conforme Decreto Estadual nº 877, de 31/03/2008.

9.3.1. Caso o prestador não possua conta no banco BANPARÁ, será cobrada pelo banco taxa referente ao DOC/TED, sendo o valor desta taxa automaticamente descontado no valor depositado para pagamento da prestação do serviço**.**

9.4. O pagamento será efetuado no prazo previsto no item 9.1 salvo atraso na liberação de recursos pela Secretaria de Estado da Fazenda – SEFA.

9.5. A Contratada deverá encaminhar, junto com a nota fiscal, os seguintes documentos:

9.5.1. Certidão conjunta negativa de débitos relativos aos tributos federais e a dívida ativa da União;

9.5.2. Certidão negativa de débitos relativos às Contribuições Previdenciárias;

9.5.3. Certificado de regularidade do FGTS – CRF;

9.5.4. Certidão negativa de débitos inadimplidos perante a Justiça do Trabalho;

9.5.5. Certidão negativa de débitos com Fazenda Estadual;

9.5.6. Certidão negativa de débitos com a Fazenda Municipal;

9.5.7. As certidões constantes dos subitens 9.4.1 até 9.4.6 podem ser substituídas por consulta ao SICAF.

9.6. Ocorrendo erro nos documentos da cobrança (inclusive nota fiscal), este será devolvido e o pagamento será sustado para que a CONTRATADA tome medidas necessárias, passando o prazo para o pagamento a ser contado a partir da data da reapresentação do mesmo;

9.7. Não efetuado o pagamento pelo CONTRATANTE no prazo estabelecido na sub-cláusula 9.1.1,1 e desde que não haja culpa da CONTRATADA, os valores correspondentes à fatura serão atualizados financeiramente com base no critério abaixo especificado:

EM=I x N x VP

Onde:

EM=Encargos Monetários

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

VP=Valor da parcela a ser paga

I=Índice de atualização financeira = 0, 0001644, assim apurado:

$I = \frac{(TX/100)}{365}$ $I = \frac{(6/100)}{365}$ I=0,0001644

TX=Percentual da taxa anual=6%

10. FORMAS E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

10.1. Modalidade de licitação:

10.1.1. A presente aquisição dar-se-á por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, considerando que o objeto da aquisição ser considerado comum.

10.1.2. O critério de julgamento das propostas apresentadas pelos licitantes será menor preço, nos termos no art.82, inciso V, da Lei 14.133/2021, proporcionando ao Órgão uma contratação mais econômica.

10.1.3. O critério de julgamento das propostas apresentadas pelos licitantes será a de menor preço global por grupo, em virtude de tratar-se de uma solução integrada, onde o fornecedor que presta o serviço ora contratado será responsável por sua instalação no local de funcionamento, reduzindo os riscos de eventual incompatibilidade de equipamento ou configurações de sistemas.

10.1.4. Habilitação econômico-financeira

10.1.4.1. Não se aplica na presente licitação.
10.1.5. Os critérios de habilitação técnica a serem atendidos pelo fornecedor são:
10.1.5.1. Certidão(ões) ou Atestado(s) que comprovem aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, emitidos por pessoas jurídicas de direito público ou privado.
10.1.5.2. Exemplificativamente, será considerado compatível (equivalente ou superior) com objeto desta licitação soluções entregues com formato de licenças e suporte técnico para atender demandas voltadas para cibersegurança.
10.1.5.3. A aceitação ou recusa de atestados que apresentem objeto(s) diverso(s) do(s)previsto(s) no item anterior ficará condicionada ao exame e manifestação da unidade técnica designada como equipe de apoio do certame;
10.1.5.4. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:
10.1.5.5. Mínimo de 20% (o máximo permitido pela lei é 50%) da(s) parcela(s) de maior relevância, qual(is) seja(m): item 01.
10.1.5.5.1. O atestado de capacidade técnico-operacional referido no item anterior, deverá conter os seguintes elementos:
10.1.5.5.1.1. Nome do órgão ou empresa responsável pela emissão do atestado, com o CNPJ, inscrição estadual, endereço completo, o período de execução dos serviços e o número do contrato;
10.1.5.5.1.2. Manifestação acerca do conteúdo e da qualidade dos serviços prestados, atestando que os serviços foram cumpridos satisfatoriamente e que não consta dos arquivos da contratante nenhum registro desabonador de aspectos comerciais ou técnicos da Licitante Vencedora;
10.1.5.5.1.3. Identificação do responsável pela emissão do atestado, com nome, função e telefone para solicitação de informações adicionais.
10.1.6. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.
10.1.7. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

11. ADEQUAÇÃO ORÇAMENTÁRIA

11.1. A disponibilidade de créditos orçamentários será indicada por ocasião da formalização do contrato ou de outro instrumento hábil, conforme estabelece o art.13 do Decreto Estadual n.º 3.371/2023.

12. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

12.1. No caso do fornecedor deixar de cumprir total ou parcialmente as obrigações assumidas ou usar de má-fé ficaria sujeita as sanções previstas no item 13.3 assegurado seu direito do contraditório e ampla defesa.
12.1.1. A entrega do ofício de comunicação de abertura de Procedimento de Apuração de Responsabilidade, a partir do qual se iniciará a contagem do prazo para a defesa prévia, será realizada no e-mail da CONTRATADA constante do preâmbulo do contrato ou na sua proposta;
12.1.2. A divulgação da Portaria de Aplicação de Penalidade, a partir do qual se iniciará a contagem do prazo para recurso, será realizada no e-mail da CONTRATADA constante do preâmbulo do contrato ou na sua proposta e em publicação no Diário Oficial do Estado do Pará;
12.1.3. Caberá única e exclusivamente à empresa CONTRATADA o acompanhamento do seu e-mail com vistas ao recebimento da comunicação de abertura de Procedimento de Apuração de Responsabilidade e da Portaria de Aplicação de Penalidade, assim como mantê-lo devidamente atualizado através de comunicação formal ao Ministério Público do Estado do Pará.
12.1.4. Com a notificação acima, estará franqueada aos interessados vista integral ao processo no e-mail protocolo@mppa.mp.br ou no MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ, situado na Rua João Diogo, 100, 4º andar, Cidade Velha, Belém-Pará, CEP: 66015-165.
12.2. Comete infração administrativa, o licitante ou contratado que cometer alguma das infrações descrias no art.155 da Lei n.º 14.133/2021:
12.2.1. der causa à inexecução parcial do contrato;

12.2.2. der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
12.2.3. der causa à inexecução total do contrato;
12.2.4. ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
12.2.5. apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
12.2.6. praticar ato fraudulento na execução do contrato;
12.2.7. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
12.2.8. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.
12.3. Serão aplicadas ao licitante ou contratado que incorrer nas infrações acima descritas as seguintes sanções, as seguintes sanções:
12.3.1. **Advertência**, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);
12.3.2. **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nos incisos II, III e VII do art. 155 da Lei nº 14.133 de 2021, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);
12.3.3. **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas nos incisos VIII, IX, X e XII do art. 155 da Lei nº 14.133 de 2021, bem como nos incisos II, III e VII do mesmo artigo, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).
12.3.4. Multa:
12.3.4.1. moratória de1,5% (um e meio por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 20 (vinte) dias;
12.3.4.1.1. O atraso superior a 20 (vinte) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.
12.3.4.2. Compensatória, para as infrações descritas nas alíneas “e” a “h” do subitem 13.2, de 15% a 30% do valor do Contrato
12.3.4.3. Compensatória, para a inexecução total do contrato prevista na alínea “c” do subitem 13.2 de 15% a 30% do valor do Contrato.
12.3.4.4. Para infração descrita na alínea “b” do subitem 13.2, a multa será de 15% a 30% do valor do Contrato
12.3.4.5. Para infrações descritas na alínea “d” do subitem 13.2, a multa será de 0,5% a 15% do valor do Contrato.
12.3.4.6. Para a infração descrita na alínea “a” do subitem 13.2, a multa será de 0,5% a 15% do valor do Contrato.
12.4. A aplicação das sanções previstas no Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021).
12.5. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).
12.5.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021).
12.5.2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).
12.5.3. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 15 (quinze) dias úteis, a contar da data do recebimento da comunicação enviada pela autoridade competente.
12.6. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.
12.7. Os parâmetros para a aplicação das sanções estão descritos nos incisos do art. 156, §1º, da Lei nº 14.133, de 2021).
12.8. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos

lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

12.9. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos no Contrato ou para provocar confusão patrimonial, conforme observa o art. 160, da Lei nº 14.133, de 2021.

12.10. O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133, de 2021)

12.11. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

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

13.DISPOSIÇÕES GERAIS/INFORMAÇÕES COMPLEMENTARES

13.1. O Contratado deverá estar regularizado quanto à emissão de nota fiscal de acordo com a sua legislação estadual.

13.2. Além do preço ofertado na proposta comercial, nada mais poderá ser cobrado do Ministério Público, a qualquer título e a qualquer momento, para a perfeita execução do objeto contratado.

13.3. As empresas licitantes, antes de apresentarem suas propostas, deverão analisar toda a documentação referente a presente licitação, dirimindo oportunamente todas as dúvidas, de modo a não incorrerem em omissões que jamais poderão ser alegadas em favor de eventuais pretensões de acréscimo dos preços propostos, sendo de responsabilidade da CONTRATADA o fornecimento de todo o material empenhado, bem como os encargos, transportes, carga, descarga, taxas, impostos e outras despesas necessárias ao fornecimento do objeto.

13.4. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente motivada.

Belém, 13 de agosto de 2024.

VANNER FERNANDES VASCONCELLOS:42680557204

Assinado de forma digital por VANNER FERNANDES VASCONCELLOS:42680557204
Dados: 2024.08.14 12:51:00 -03'00'

VANNER FERNANDES VASCONCELLOS
Integrante requisitante

IGOR DE ANDRADE MONTEIRO:87205173272

Assinado de forma digital por IGOR DE ANDRADE MONTEIRO:87205173272
Dados: 2024.08.13 13:44:40 -03'00'

IGOR DE ANDRADE MONTEIRO
Integrante técnico

gov.br
Documento assinado digitalmente
LILIA REGINA DE ARAUJO
Data: 16/08/2024 09:59:25-0300
Verifique em https://validar.iti.gov.br

LILIA DE ARAUJO HADDAD
Integrante administrativo