



Tribunal Regional Eleitoral da Paraíba  
Avenida Princesa Isabel, 201 - Bairro Centro - CEP 58013-251 - João Pessoa - PB

## **CONTRATAÇÃO - TERMO DE REFERÊNCIA - SERVIÇOS Nº 6/2022 - TRE-PB/PTRE/DG/STIC/COGSC/SESEC**

### **1 – OBJETO**

A presente licitação tem como objetivo a formação de Ata de Registro de Preços para Solução unificada de Auditoria de Segurança no Active Directory, compreendendo aquisição de serviços de software e suporte técnico, de acordo com as quantidades, especificações e condições descritas neste Termo de Referência.

### **2 – JUSTIFICATIVA**

O registro de preços objetiva a dotar o corpo técnico do nosso tribunal e de outros tribunais eleitorais partícipes de ferramenta que auxilia encontrar e corrigir os pontos fracos do Active Directory antes que os ataques aconteçam além de detectar ataques ao Active Directory em tempo real.

### **3 – DA PADRONIZAÇÃO DOS SOFTWARES E LICENÇAS**

3.1. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (*I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas*), todos os softwares e licenças das soluções ofertadas deverão ser fornecidos por um único fabricante, o qual será responsável também pelo suporte e garantia da plataforma como um todo.

### **4 – COMPOSIÇÃO DO LOTE**

| <b>Lote 01 - Solução de Auditoria de Segurança no Active Directory com armazenamento e gerenciamento em Local (On Premise)</b> |                        |  |
|--|------------------------|--|
| <b>ITEM</b>  | <b>CATMAT / CATSER</b> | <b>DESCRIÇÃO</b>   |
| 1  | 27502                  | Licença de subscrição de solução de auditoria de segurança no Active Directory por usuário ativo do AD, durante 60 meses de uso e suporte do fabricante. |
| 2  | 26972                  | Instalação e configuração da solução.  |
| 3  | 26972                  | Repasse tecnológico, com período mínimo de 20 horas para no mínimo 10 alunos.  |

|   |       |   |
|---|-------|---|
| 4 | 26972 | Suporte Técnico Especializado durante 60 meses. |
|---|-------|---|

## QUANTIDADES REGISTRADAS PELOS TREs PARTICÍPES E TRE-PB

| TRIBUNAL         | ITEM 1 | ITEM 2 | ITEM 3 | ITEM 4 |
|------------------|--------|--------|--------|--------|
| TRE-AC           | 400    | 1      | 1      | 1      |
| TRE-AL           | 1100   | 1      | 1      | 1      |
| TRE-AM           | 1500   | 1      | 1      | 1      |
| TRE-AP           | 500    | 1      | 1      | 1      |
| TRE-BA           | 3000   | 1      | 1      | 1      |
| TRE-CE           | 1900   | 1      | 1      | 1      |
| TRE-DF           | 1105   | 1      | 1      | 1      |
| TRE-ES           | 1300   | 1      | 1      | 1      |
| TRE-GO           | 1300   | 1      | 1      | 1      |
| TRE-MA           | 1200   | 1      | 1      | 1      |
| TRE-MS           | 700    | 1      | 1      | 1      |
| TRE-MT           | 1600   | 1      | 1      | 1      |
| TRE-PA           | 1500   | 1      | 1      | 1      |
| TRE-PB           | 2000   | 1      | 1      | 1      |
| TRE-PE           | 2200   | 1      | 1      | 1      |
| TRE-PI           | 1600   | 1      | 1      | 1      |
| TRE-RJ           | 3122   | 1      | 1      | 1      |
| TRE-RN           | 1300   | 1      | 1      | 1      |
| TRE-RO           | 700    | 1      | 1      | 1      |
| TRE-SC           | 1250   | 1      | 1      | 1      |
| TRE-SE           | 904    | 1      | 1      | 1      |
| TRE-SP           | 7500   | 1      | 1      | 1      |
| TRE-TO           | 900    | 1      | 1      | 1      |
| TOTAL REGISTRADO | 38581  | 23     | 23     | 23     |

### Especificações técnicas do lote 01 :

#### 4.1 SOLUÇÃO DE AUDITORIA DE SEGURANÇA NO ACTIVE DIRECTORY (COM GERENCIAMENTO E ARMAZENAMENTO LOCAL)

##### *Características técnicas mínimas:*

- 4.1.1. Características gerais à solução de análise em ambiente Microsoft Active Directory
- 4.1.1.1. A solução deve identificar fraquezas ocultas em configurações do dedicadas ao Active Directory;
- 4.1.1.2. A solução deve possuir ações preventivas de hardening para o Active Directory;
- 4.1.1.3. A solução deve identificar ataque específicos para a estrutura do Active Directory;

- 4.1.1.4. A solução deve possuir funcionalidade para analisar em detalhes cada configuração incorreta que acarreta riscos de segurança – com uma linguagem simples, contextualizando tal risco para os times envolvidos;
- 4.1.1.5. A solução deve possuir recomendações de correção para cada configuração incorreta no Active Directory;
- 4.1.1.6. A solução deve avaliar relações de confiança perigosas entre florestas e domínios;
- 4.1.1.7. A solução deve capturar as mudanças que ocorrem no AD e demonstrar na console de administração;
- 4.1.1.8. A solução deve possuir dashboard com os principais ataques e vulnerabilidades por domínio;
- 4.1.1.9. A solução deve permitir a correlação de mudanças no Active Directory e desvios de segurança;
- 4.1.1.10. A solução deve analisar em detalhes um ataque explorando as descrições através do framework MITRE ATT&CK;
- 4.1.1.11. A solução deve prover interface web para gerenciamento de todas as funcionalidades;
- 4.1.1.12. A solução deve possuir capacidade nativa de criação de dashboards customizados;
- 4.1.1.13. A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;
- 4.1.1.14. A solução não deve realizar alterações no Active Directory, seus objetos e atributos;
- 4.1.1.15. A solução não deve armazenar ou sincronizar nenhuma credencial de objetos do Active Directory;
- 4.1.1.16. A solução deve suportar ambientes com múltiplas florestas e domínios;
- 4.1.1.17. A solução deve suportar monitoramento contínuo de ambientes com Active Directory com o nível funcional de floresta e domínio a partir do 2003;
- 4.1.1.18. A solução deve suportar reter os eventos coletados por no mínimo um ano;
- 4.1.1.19. A solução deve descobrir e mapear a superfície de ataque do Active Directory e seus domínios monitorados com os seguintes padrões:
  - 4.1.1.19.1. Não depender de agentes ou sensores para coleta de informações do AD;
  - 4.1.1.19.2. A solução deve seguir as boas práticas de menor privilégio, a conta de serviço utilizada para conexão com o Active Directory, sendo o menor nível de acesso esperado para a conta de serviço como parte do grupo Domain User;
  - 4.1.1.19.3. Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles;
- 4.1.1.20. A solução deve analisar continuamente a postura de segurança do AD, minimamente avaliando:
  - 4.1.1.20.1. Validação de GPOs desvinculadas, desabilitadas ou órfãs;
  - 4.1.1.20.2. Validação de contas desativadas em grupos privilegiados;
  - 4.1.1.20.3. Domínio usando uma configuração perigosa de compatibilidade com versões anteriores por meio de alterações no atributo dSHeuristics;
  - 4.1.1.20.4. Validação de atributos relacionados a roaming de credenciais vulneráveis (ms-PKI-DPAPIMasterKeys) gerenciados por um usuário sem privilégios;
  - 4.1.1.20.5. Validação de domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como NTLMv1;
  - 4.1.1.20.6. Validação de contas com senhas que nunca expiram;
  - 4.1.1.20.7. Validação de senhas reversíveis em GPOs;
  - 4.1.1.20.8. Validação de uso de senhas reversíveis em contas de usuário;
  - 4.1.1.20.9. Validação de utilização de protocolo criptográfico fraco (Ex. DES) em contas de usuário;
  - 4.1.1.20.10. Validação de uso do LAPS (Solução de senha de administrador local) para gerenciar senhas de contas locais com privilégios;
  - 4.1.1.20.11. Validação se o domínio possui um nível funcional desatualizado;
  - 4.1.1.20.12. Validação de contas de usuário utilizando senha antiga;
  - 4.1.1.20.13. Validação se o atributo AdminCount está definido em usuários padrão;
  - 4.1.1.20.14. Validação do uso recente da conta de administrador padrão;
  - 4.1.1.20.15. Validação de usuários com permissão para ingressar computadores no domínio;

- 4.1.1.20.16. Validação de contas dormentes;
- 4.1.1.20.17. Validação de computadores executando um sistema operacional obsoleto;
- 4.1.1.20.18. Validação de restrições de logon para usuários privilegiados em ambiente com múltiplos tiers (1, 2 e 3) de segregação de ativos;
- 4.1.1.20.19. Validação de direitos perigosos configurados no Schema do AD;
- 4.1.1.20.20. Validação de relação de confiança perigosa com outras Florestas e Domínios;
- 4.1.1.20.21. Validação de contas que possuem um atributo perigoso de histórico SID (SID History);
- 4.1.1.20.22. Validação de contas utilizando controle de acesso compatível com Windows 2000;
- 4.1.1.20.23. Validação da última alteração de senha do KDC;
- 4.1.1.20.24. Validação da última alteração da senha da conta SSO do Azure AD;
- 4.1.1.20.25. Validação de contas que podem ter senha em branco/vazia;
- 4.1.1.20.26. Validação de utilização do grupo nativo Protected Users;
- 4.1.1.20.27. Validação de privilégios sensíveis (Ex. Debug a program, Replace a process level token, etc.) perigosos atribuídos aos usuários;
- 4.1.1.20.28. Validação de possível senha em clear-text;
- 4.1.1.20.29. Validação de sanidade das GPOs e componentes CSEs (Client-Side Extension);
- 4.1.1.20.30. Validação de uso de algoritmos de criptografia fracos na PKI do Active Directory;
- 4.1.1.20.31. Validação de contas de serviço com SPN (Service Principal Name) que fazem parte de grupos privilegiados;
- 4.1.1.20.32. Validação de contas anormais nos grupos administrativos padrão do AD;
- 4.1.1.20.33. Validação de consistência no container adminSDHolder;
- 4.1.1.20.34. Validação de delegação Kerberos perigosa;
- 4.1.1.20.35. Validação em permissões de objetos raiz que permitem ataques do tipo DCSync;
- 4.1.1.20.36. Validação de políticas de senha fracas aplicadas aos usuários;
- 4.1.1.20.37. Validação das permissões relacionadas às contas do Azure AD Connect;
- 4.1.1.20.38. Validação do ID do grupo primário do usuário (Primary Group ID);
- 4.1.1.20.39. Validação de permissões em GPOs sensíveis associadas aos Containers Configuration, Sites, Root Partition e OUs sensíveis como Domain Controllers;
- 4.1.1.20.40. Controladores de domínio gerenciados por usuários ilegítimos;
- 4.1.1.20.41. Validação de certificado mapeado através de atributo altSecurityIdentities em contas privilegiadas;
- 4.1.1.20.42. Validação de uso de protocolo Netlogon inseguro (ZeroLogon/CVE-2020-1472);
- 4.1.1.21. A solução deve identificar vulnerabilidades e configurações incorretas do AD à medida que são introduzidas sendo:
  - 4.1.1.21.1. Identificar todas as vulnerabilidades e configurações incorretas no AD;
  - 4.1.1.21.2. Monitorar relações de confiança perigosas em toda a estrutura AD;
  - 4.1.1.21.3. Apresentar ameaças e alterações sem a necessidade de scans estáticos e programados no Active Directory e sua infraestrutura;
  - 4.1.1.21.4. Apresentar as ameaças e alterações em tempo real ou em menos de cinco minutos;
- 4.1.1.22. Em relação a detecção e resposta a ataques a solução deve:
  - 4.1.1.22.1. Monitorar continuamente os indicadores de possíveis ataque como DCSync, DCShadow, Password Spraying, Password Guessing/Brute Force, Lsaas Injecton nos controladores de domínio, Golden Ticket, NTLM Relay, entre outros;
  - 4.1.1.22.2. Detecção de ataques ao AD em tempo real ou em menos de um minuto;
  - 4.1.1.22.3. Análise detalhada do ataque, apresentando ativo de origem, vetor de ataque, controlador de domínio afetado, técnica aplicada;
  - 4.1.1.22.4. Apresentação de ataques em uma linha do tempo;
  - 4.1.1.22.5. Investigar ameaças, reproduzir ataques e procurar por backdoors;
  - 4.1.1.22.6. Permitir busca ágil de eventos específicos na base da solução através de queries customizadas;
- 4.1.1.23. A solução deve ser capaz de enviar alertas por e-mail;
- 4.1.1.24. A solução nativamente deve ser capaz de se integrar com SIEM através de protocolo SYSLOG;

- 4.1.1.25. A solução deve ser capaz de filtrar e enriquecer os eventos que serão enviados para o SIEM;
- 4.1.1.26. A solução deve produzir regras YARA na detecção de ataques (Ex. DCSync, Golden Ticket) identificados pela ferramenta;
- 4.1.1.27. A solução deve possuir conjunto de APIs REST, todas as chamadas disponíveis devem estar contidas na documentação;
- 4.1.1.28. A solução deve permitir a criação de listas de exclusões, suportando minimamente Exclusão por domínios do AD monitorados e por itens analisados;
- 4.1.1.29. A solução deve ser licenciada pelo número de usuários habilitados;
- 4.1.1.30. Os Solução deverá possuir gerenciamento e armazenamento dos dados na rede local do tribunal, com scanners próprios localizados e instalados na infraestrutura do cliente (on-premise).
- 4.1.1.31. A solução proposta deve ser de mesmo fabricante, sem adaptações ou alterações não efetuadas pelo fabricante, disponível para gerenciamento em console central unificado.
- 4.1.1.32. A solução deve possibilitar a realização de cópias de segurança, funcionamento em alta disponibilidade e criptografia de todos os dados armazenados, além de incluir todo o software e licenciamento necessários para o funcionamento completo de acordo com as funcionalidades previstas neste Termo de Referência.
- 4.1.1.33. A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.
- 4.1.1.34. Todas as licenças de uso de software devem ser registradas, em nome da Contratante no site do fabricante.
- 4.1.1.35. O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Confidencialidade, em que se comprometerá a não acessar, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.
- 4.1.1.36. A CONTRATADA ou o CONTRATANTE poderá não conseguir realizar o registro e licenciamento da solução junto ao fabricante, no caso de o número de usuários ativos dos domínios cadastrados ser superior ao número de licenças adquiridas.
- 4.1.1.37. No caso de transbordo do número de usuários ativos do AD permitidos (quando o número de usuários ativos dos domínios cadastrados ultrapassar o número de licenças habilitadas), após o registro e licenciamento da solução junto ao fabricante:
  - 4.1.1.37.1 O CONTRATANTE poderá perder o direito de atualização e suporte do fabricante, enquanto persistir o transbordo;
  - 4.1.1.37.2 Será garantido ao CONTRATANTE o direito de uso da solução, mesmo enquanto durar o transbordo;
  - 4.1.1.37.3 Será garantido ao CONTRATANTE o direito ao suporte técnico especializado pela CONTRATADA, mesmo enquanto durar o transbordo.

#### 4.1.2. Configurações básicas para o usuário:

- 4.1.2.1. Preferências do usuário para:
  - 4.1.2.1.1. Selecionar a linguagem da ferramenta;
  - 4.1.2.1.2. Selecionar o perfil de usuário;
  - 4.1.2.1.3. Alterar a senha o perfil do usuário da solução;
  - 4.1.2.1.4. Gerenciar as chaves de API.
- 4.1.2.2. A navegação pela plataforma da solução deve ser de maneira clara e simples contendo, no mínimo, os seguintes elementos:
  - 4.1.2.2.1. Painel de controle: para permitir o gerenciamento e monitoramento de forma visual e eficiente sobre a infraestrutura do Active Directory;
  - 4.1.2.2.2. Notificações: que contenham alertas de ataque e/ou exposição aguardando sua confirmação e verificação.
  - 4.1.2.2.3. Conectividade: visualização indicativa de conexão ao Active Directory e, ainda

apresentar alerta quando houver indisponibilidade entre a solução e o elemento de infraestrutura supracitado;

4.1.2.2.4. Acessibilidade: para acessar documentos que ajudem e esclareçam dúvidas ao usuário ou administrador da solução;

4.1.2.2.5. Perfis de segurança: permitindo diferentes tipos de usuários para revisar as análises de segurança a partir de ângulos variados sobre relatórios disponibilizados;

4.1.2.2.6. Tela de fluxo: monitoramento e análise de eventos que afetam o Active Directory em tempo real;

4.1.2.2.7. Indicadores de Exposição (IoE): medidor de maturidade de segurança para o Active Directory atribuindo níveis de gravidade (Crítico, alto, médio ou baixo) junto ao fluxo de eventos que monitora e analisa os eventos;

4.1.2.2.8. Indicadores de ataque: detecção de ataques ao Active Directory em tempo real;

4.1.2.2.9. Topologia: página na solução que forneça uma visualização gráfica e interativa do Active Directory. A visualização deve apresentar minimamente: as florestas, domínios e relações de confiança que existem entre eles.

4.1.2.2.10. Caminho do ataque: página na solução que forneça representações gráficas dos relacionamentos do Active Directory como:

4.1.2.2.10.1. Avaliação de movimentos laterais no AD sobre um ativo potencialmente comprometido (Blast Radius);

4.1.2.2.10.2. Antecipação sobre técnicas de escalonamento de privilégios para alcançar um ativo a partir de um determinado ponto de entrada (Attack Path);

4.1.2.2.10.3. Medição sobre a vulnerabilidade de um ativo, usando sua visualização e exposição para abordar os caminhos de escalação (Asset Exposure);

4.1.2.2.10.4. Preferencias do usuário: permitindo a configuração de linguagem, perfil e senha dentro da solução;

4.1.2.2.10.5. Log out: Opção para saída de forma simples do perfil dentro da solução.

4.1.2.2.11. Widgets: que possibilitem um conjunto de dados personalizáveis para exibição do painel da solução. Devem conter minimamente:

4.1.2.2.11.1. Gráficos de barras;

4.1.2.2.11.2. Gráficos de linhas; e

4.1.2.2.11.3. Contadores.

#### 4.1.3. Notificações:

4.1.3.1. A solução deve notificar e realizar contagem sobre alertas de ataque e/ou alertas de exposição aguardando conhecimento dos responsáveis pela solução;

4.1.3.2. Ao receber novos alertas a contagem deve permanecer crescente de forma transparente e visual;

4.1.3.3. Os detalhes dos eventos devem conter as seguintes informações no painel exibido dentro das notificações:

4.1.3.3.1. Origem (da coleta do evento);

4.1.3.3.2. Tipo de objeto;

4.1.3.3.3. Caminho para o arquivo;

4.1.3.3.4. Domínios afetados;

4.1.3.3.5. Data;

4.1.3.3.6. Lista de atributos com valores no momento do evento e o valor atual.

4.1.3.4. Possibilidade de arquivamento do alerta

#### 4.1.4. Painel de controle

4.1.4.1. O painel de controle da solução deve permitir a visualização de dados e tendências que afetem a segurança do AD;

4.1.4.2. O painel de controle deve ser personalizável com widgets para exibição de gráficos e contadores de acordo com as necessidades do ambiente.

4.1.4.3. As configurações dos painéis de controle devem permitir:

4.1.4.3.1. Criação;

- 4.1.4.3.2. Renomeação; e
- 4.1.4.3.3. Exclusão de um painel de controle.

#### 4.1.5. Widgets

- 4.1.5.1. Os widgets no painel de controle devem permitir a visualização dos dados do AD na forma de gráficos de barras, linhas gráficos e contadores, possibilitando que sejam arrastados ao redor para reposicioná-los no painel, incluindo a personalização para exibir informações específicas.
- 4.1.5.2. Deve ser permitido a criação de novos widgets no painel ou a partir de existentes.
- 4.1.5.3. As configurações do widget devem incluir:
  - 4.1.5.3.1. Contagem de usuários: o número de usuários ativos para o domínio;
  - 4.1.5.3.2. Contagem de desvios: o número de desvios ou violações de segurança detectadas;
  - 4.1.5.3.3. Pontuação de conformidade: uma pontuação de 0 a 100 que a solução compute levando em conta o número de desvios detectados e seus níveis de gravidade.
  - 4.1.5.3.4. Duração (para gráfico de linhas): exibindo a duração.
- 4.1.5.4. Os conjuntos de dados devem exibir:
  - 4.1.5.4.1. Status (contagem de usuários): Ativo, inativo ou todos;
  - 4.1.5.4.2. Indicadores (Indicadores de exposição): a seleção pode ser feita de forma singular ou de vários através de uma lista, mas opcionalmente pode:
    - 4.1.5.4.2.1. Ser digitada através do nome do indicador em caixa de pesquisa;
    - 4.1.5.4.2.2. Seleção de todos os indicadores: a partir dos níveis de gravidade (crítico, alto, médio ou baixo).
  - 4.1.5.4.3. Domínios: A seleção pode ser feita de através de todos os domínios, mas opcionalmente pode ser digitada através do nome do domínio em caixa de pesquisa;

#### 4.1.6. Topologia

- 4.1.6.1. A solução deve prover através da funcionalidade de topologia:
  - 4.1.6.1.1. Uma visualização gráfica interativa do Active Directory;
  - 4.1.6.1.2. Gráfico de Topologia exibindo as florestas, domínios e relações de confiança que existem entre eles;
  - 4.1.6.1.3. Pesquisa por um domínio específico;
  - 4.1.6.1.4. Exibição do link entre dois domínios;
  - 4.1.6.1.5. Exibição de detalhes sobre um domínio.
- 4.1.6.2. A solução deve exibir relações de confiança;
- 4.1.6.3. Deve haver compreensão do código de cores das relações de confiança dependendo do seu nível de ameaça;
- 4.1.6.4. As informações do atributo de confiança devem indicar a direção de confiança como unidirecional ou bidirecional (entrada/saída).

#### 4.1.7. Investigação de Eventos no Active Directory

- 4.1.7.1. A solução deve conter funcionalidade de investigação sobre eventos que monitorem continuamente a infraestrutura e detecte regressões à medida que elas acontecem;
- 4.1.7.2. A solução deve ter painel intuitivo, para identificar rapidamente as vulnerabilidades mais críticas e suas recomendações de correção;
- 4.1.7.3. A página inicial deve exibir o monitoramento e a análise em tempo real de eventos que afetam as infraestruturas do AD;
- 4.1.7.4. A solução deve permitir carregar eventos anteriores e voltar no tempo;
- 4.1.7.5. A solução deve permitir a caixa de pesquisa para executar a caça a ameaças e detectar padrões maliciosos;
- 4.1.7.6. A solução deve ter elementos interativos como:
  - 4.1.7.6.1. Permitir clicar nos elementos de entrada exibidos na página;
  - 4.1.7.6.2. Os detalhes dos elementos devem incluir quais atributos mudaram de valor;

- 4.1.7.6.3. Mostrar ao usuário o valor do atributo antes e depois;
- 4.1.7.6.4. Mostrar se o evento possui uma exploração potencial dentro da entrada;
- 4.1.7.6.5. Chaves de alternância para ativar ou desativar a exibição de eventos;
- 4.1.7.6.6. Botões de ação para carregar eventos anteriores. O fluxo da trilha deve parar automaticamente para permitir que o usuário procure um evento que ocorreu dentro de um determinado período de tempo.
- 4.1.7.6.7. Caixas de seleção para selecionar as florestas e domínios a serem incluídos na pesquisa ou na exibição.
- 4.1.7.7. Deve monitorar e permitir visualização em tempo real da análise de eventos que afetam o AD;
- 4.1.7.8. A funcionalidade deve atender aos seguintes requisitos dentro de sua exibição:
  - 4.1.7.8.1. Recursos indicando a origem de qualquer alteração relacionada à segurança em suas infraestruturas do AD, correlacionando no mínimo duas fontes possíveis:
    - 4.1.7.8.1.1. Lightweight Directory Access Protocol (LDAP): usado para se comunicar com seu Infraestrutura AD.
    - 4.1.7.8.1.2. Server Message Block (SMB): protocolo usado para compartilhar arquivos, impressoras, etc.
  - 4.1.7.9. A solução deve analisar minuciosamente o tráfego LDAP e SMB através da rede para detectar anomalias e ameaças potenciais;
  - 4.1.7.10. A solução deve possibilitar aprimoramento dos tipos de elementos característicos que podem ser de interesse para usuários, como entrar em um grupo, criar uma nova conta de usuário, sendo os tipos de evento enquadrados no mínimo como:
    - 4.1.7.10.1. ACL changed
    - 4.1.7.10.2. SPN changed
    - 4.1.7.10.3. Member removed
    - 4.1.7.10.4. New member
    - 4.1.7.10.5. New trust
    - 4.1.7.10.6. Unknown file type added
    - 4.1.7.10.7. New object
    - 4.1.7.10.8. Object removed
    - 4.1.7.10.9. Password changed
    - 4.1.7.10.10. UAC changed
    - 4.1.7.10.11. New GPO linked
    - 4.1.7.10.12. GPO link removed
    - 4.1.7.10.13. Owner change
    - 4.1.7.10.14. File renamed
    - 4.1.7.10.15. SPN created
    - 4.1.7.10.16. Failed auth reset
    - 4.1.7.10.17. Failed authentication
  - 4.1.7.11. Deve indicar a classe ou extensão de arquivo associada a um objeto AD, possibilitando a procura por um objeto de diretório (usuário, computador, etc.) ou um arquivo com uma extensão de nome de arquivo específica (ini, xml, csv).
  - 4.1.7.12. Deve indicar o caminho completo para um objeto AD, permitindo a identificação da localização exclusiva desse objeto no AD.
  - 4.1.7.13. Deve indicar de qual diretório vem a alteração em sua infraestrutura do AD.
  - 4.1.7.14. Deve indicar a hora em que ocorreu a alteração na infraestrutura do AD.
  - 4.1.7.15. Visto a volumetria de resultados na investigação de eventos para acomodar entradas que continuarão aumentando ao longo do tempo, a solução deverá possibilitar, no mínimo, as funcionalidades de:
    - 4.1.7.15.1. pausar;
    - 4.1.7.15.2. reiniciar.
  - 4.1.7.16. Deve permitir o filtro sobre eventos e resultados obtidos em tempo real;
  - 4.1.7.17. Deve permitir a pesquisa sobre eventos e resultados obtidos em tempo real;
  - 4.1.7.18. A pesquisa poderá ser realizada utilizando expressões para refinar os resultados da pesquisa usando os operadores booleanos \*, AND e OR, com possibilidade de encapsulamento das instruções OR para modificar a prioridade de pesquisa capacitando filtrar eventos que correspondem à sequência de caracteres ou padrão específico que foram



inseridos no caixa de pesquisa.

4.1.7.19. A solução deve permitir consultas rápidas através de um campo disponibilizado como assistente em seu painel;

4.1.7.20. A solução deve permitir que as expressões usadas frequentemente sejam adicionadas a uma lista de favoritos, facilitando a seleção de qualquer entrada na lista para usar novamente sem precisar digitar novamente toda a expressão;

4.1.7.21. A solução deve permitir que as expressões de consulta sejam salvas através de um histórico, de forma automática em lista;

4.1.7.22. A solução deve permitir que as expressões permitam combinadores AND ou OR para a consulta.

4.1.7.23. Em casos específicos de consulta, a solução deve restringir a pesquisa a objetos desviantes, permitindo expressão para facilitar o filtro de busca.

4.1.7.24. A solução deve permitir:

4.1.7.24.1. exclusão de atributos na expressão de consulta;

4.1.7.24.2. adição de novas condições na expressão de consulta;

4.1.7.24.3. adição de novas regras para as expressões de consulta

4.1.7.24.4. adição de atributos nas expressões de consulta.

4.1.7.24.5. adição de combinadores como AND ou OR;

4.1.7.25. A solução deve incluir campo de pesquisa para inserção das sintaxes utilizadas nas expressões de consulta;

4.1.7.26. A solução deve possuir funcionalidade para validar as expressões de consulta;

4.1.7.27. A solução deve permitir gerenciamento das expressões favoritas para:

4.1.7.27.1. procurar um marcador específico na lista;

4.1.7.27.2. limitar a pesquisa a uma pasta específica;

4.1.7.27.3. editar um nome de marcador;

4.1.7.27.4. excluir uma expressão da página dos favoritos;

4.1.7.27.5. editar o nome de uma pasta de favoritos (se houver);

4.1.7.27.6. excluir uma pasta de favoritos (se houver);

4.1.7.28. A pesquisa deve incluir florestas e domínios específicos como alvo;

4.1.7.29. A solução deve fornecer informações detalhadas sobre cada evento que afeta suas infraestruturas AD, visto que um evento específico permitirá a revisão das informações técnicas e tomada de medidas corretivas, se necessário para o Indicador do nível de gravidade da Exposição (Crítico, Alto, Médio ou Baixo);

4.1.7.30. A solução deve permitir a visualização de alterações de todos os atributos, com no mínimo os seguintes status:

4.1.7.30.1. adição;

4.1.7.30.2. exclusão;

4.1.7.30.3. inalterado.

4.1.7.31. A solução deve permitir a visualização sobre domínios impactados, incluindo os seguintes indicadores:

4.1.7.31.1. informação;

4.1.7.31.2. detalhes da Vulnerabilidade;

4.1.7.31.3. objetos desviantes; e

4.1.7.31.4. recomendações.

4.1.8. Visualização sobre vulnerabilidades:

4.1.8.1. A solução deve oferecer visualização em representação gráfica sobre potenciais vulnerabilidades para os ativos críticos;

4.1.8.2. Mostrar os possíveis caminhos que um invasor pode seguir para comprometer um ativo de um ponto de entrada;

4.1.8.3. Mostrar os possíveis movimentos laterais no Active Directory de qualquer ativo;

4.1.8.4. Mostrar todos os caminhos que podem potencialmente assumir o controle de um ativo;

4.1.8.5. Ajuste e manuseio de forma intuitiva aos gráficos exibidos.

#### 4.1.9. Detecção a ataques em tempo real:

4.1.9.1. A solução deve ter a capacidade de detectar ataques em tempo real e interrupção imediata contemplando:

4.1.9.1.1. Visualização de todas as ameaças a partir de uma linha do tempo do ataque de forma precisa;

4.1.9.1.2. Consolidando a distribuição de ataques em uma visualização única.

4.1.9.1.3. Análise detalhada sobre um ataque ao Active Directory;

4.1.9.1.4. Explorar as descrições do MITRE ATT&CK diretamente dos incidentes detectados.

4.1.9.2. A solução deve ter a capacidade de detectar ataques que afetam as infraestruturas AD por meio de Indicadores de Ataque (IoAs) e atribuir níveis de gravidade ao fluxo constante de ataques que estão sendo monitorados e analisados das seguintes formas:

4.1.9.2.1. Crítica;

4.1.9.2.2. Alta;

4.1.9.2.3. Média;

4.1.9.2.4. Baixa.

4.1.9.3. A visualização deve exibir blocos de domínio organizados por:

4.1.9.3.1. Ordem alfabética;

4.1.9.3.2. Criticidade; e

4.1.9.3.3. Florestas;

4.1.9.4. Deve conter no mínimo as seguintes funcionalidades:

4.1.9.4.1. Distribuição de ataques mostrando os níveis de gravidade relacionados ao fluxo constante de ataques;

4.1.9.4.2. Top 3 dos principais ataques e seus números de ocorrências.

4.1.9.4.3. Capacidade de atualizar a visualização.

4.1.9.5. Capacidade de editar o tipo de gráfico exibido na página.

4.1.9.6. Capacidade de gerar e exportar relatórios listando os ataques;

4.1.9.7. Capacidade de selecionar data e hora iniciais para mostrar uma linha do tempo dos ataques;

4.1.9.8. A solução deve possibilitar a aplicação de filtros a incidentes;

4.1.9.9. Possibilidade de definir critérios de pesquisa para execução;

4.1.9.10. Acesso a explicações detalhadas sobre os ataques que afetam as infraestruturas do AD;

4.1.9.11. Capacidade de fechar ou reabrir um incidente;

4.1.9.12. Extração de relatório mostrando todos os incidentes.

#### 4.1.10. Gestão de segurança das infraestruturas do AD:

4.1.10.1. A solução deve medir a maturidade de segurança das infraestruturas do AD por meio de Indicadores de Exposição e atribuir níveis de gravidade ao fluxo constante de eventos que estão sendo analisados e monitorados.

4.1.10.2. São os níveis do subitem anterior:

4.1.10.2.1. Crítico;

4.1.10.2.2. Alto;

4.1.10.2.3. Médio; e

4.1.10.2.4. Baixo.

4.1.10.3. A solução deve exibir blocos sobre os indicadores com os seguintes requisitos:

4.1.10.3.1. Por severidade e código de cores;

4.1.10.3.2. Verticalmente, por ordem de severidade;

4.1.10.3.3. Horizontalmente, por ordem de complexidade;

4.1.10.3.4. Em ordem alfabética;

4.1.10.3.5. Por nome de domínio.

4.1.10.4. A solução deve possibilitar mostrar todos os Indicadores de Exposição de maneira fácil;

4.1.10.5. A solução deve ter a capacidade de restringir a seleção a florestas e domínios específicos;

4.1.10.6. A solução deve ter a capacidade de diferenciar os seguintes elementos:

4.1.10.6.1. Indicadores de exposição;

- 4.1.10.6.2. Eventos;
- 4.1.10.6.3. Objetos desviantes;
- 4.1.10.7. A solução deve possibilitar a visibilidade sobre vulnerabilidades para ver uma descrição completa e sua potencial ameaça;
- 4.1.10.8. A solução deve revelar objetos desviantes que revelam fraquezas ou comportamentos potencialmente perigosos às infraestruturas do AD;
- 4.1.10.9. Possibilitar as seguintes ações sobre objetos desviantes:
  - 4.1.10.9.1. Recuperar objetos afetados no AD;
  - 4.1.10.9.2. Ignorar objetos afetados no AD por um período de tempo;
  - 4.1.10.9.3. Seleção de florestas e domínios para executar uma pesquisa.
  - 4.1.10.9.4. Acesso a explicações sobre os atributos incriminadores que afetam os indicadores de exposição;
  - 4.1.10.9.5. Exportação de relatório informando todos os objetos desviantes.
- 4.1.11. Configuração de segurança e acesso à gerência da solução:
  - 4.1.11.1 A solução deve possuir proteção contra ataques de força bruta bloqueando as contas após um número determinado de tentativas de login malsucedidas;
  - 4.1.11.2 Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;
  - 4.1.11.3 Os dados em trânsito devem usar ao menos o algoritmo TLS 1.2 de chave 2048 bits;
  - 4.1.11.4 Os dados em trânsito devem ser criptografados ao menos com o algoritmo AES-128 bits;
  - 4.1.11.5 Os algoritmos de hash devem usar ao menos o algoritmo SHA-256;
  - 4.1.11.6 Será aceito como comprovação critérios de criptografia publicação em site do fabricante ou declaração do próprio fabricante;
  - 4.1.11.7 Os dados armazenados devem ser criptografados ao menos com o algoritmo AES-256 bits;
  - 4.1.11.8 Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;
  - 4.1.11.9 A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;

## 4.2 INSTALAÇÃO E CONFIGURAÇÃO ITEM 02

### *Características técnicas mínimas:*

- 4.2.1. Efetuar a instalação e configuração, em conjunto com a Contratante, para uso da solução proposta, contendo no mínimo os seguintes itens:
  - a) Validação que as máquinas virtuais e/ou servidores físicos atendem os requisitos de CPU, Memória e Rede definidos pelo fabricante conforme documentação;
  - b) Validação do espaço de armazenamento das máquinas virtuais e/ou servidores físicos atendem os requisitos pelo fabricante conforme documentação;
  - c) Validação das liberações necessárias no firewall junto a CONTRATANTE para confirmar se atendem os requisitos pelo fabricante conforme documentação;
  - d) Configuração do endereçamentos de IP, DNS, GATEWAY e NTP da solução e dos seus componentes;
  - e) Criação dos logins de acesso iniciais para administração da solução e dos seus componentes;
  - f) Criação dos logins de acesso para outras atividades não administrativas da solução e dos seus componentes;
  - g) Licenciamento da solução e dos seus componentes;

- h) Configuração dos domínios e servidores Active Directory a serem monitorados;
- i) Configurações iniciais da investigação de Eventos;
- j) Configurações dos Indicadores de Exposição;
- l) Configurações das Topologias Gráficas de comunicação;
- m) Configurações dos Indicadores de Ataques;
- n) Configurações iniciais dos dashboards de análise e monitoramento.
- o) Configurações iniciais dos relatórios de análise e monitoramento.

4.2.2. A instalação e configuração da solução poderá ser feita por meio de acesso remoto;

4.2.3. A CONTRATADA deverá aceitar as especificações de softwares e protocolos de segurança estabelecidos pela CONTRATANTE para a realização do acesso remoto;

4.2.4. Não serão aceitos softwares "beta" ou em desenvolvimento;

4.2.5. Somente será aceita a instalação por técnico certificado na fabricante da solução, da CONTRATADA ou do fabricante;

4.2.6. A CONTRATADA deverá elaborar documentação, contendo no mínimo os seguintes itens:

4.2.6.1 Cronograma;

4.2.6.2 Levantamento de informações sobre o ambiente atual;

4.2.6.3 Definição dos parâmetros de configuração básicos e avançados a serem implementados;

4.2.6.4 Mapa de rede contendo a topologia a ser implementada ou atualizada;

4.2.6.5 Gerenciamento de mudanças, contemplando análise de riscos de implementação da solução;

4.2.6.6 Procedimentos de implementação e de rollback no caso de problemas não previstos previamente.

### 4.3 REPASSE TECNOLÓGICO ITEM 03

*Características técnicas mínimas:*

4.3.1. A contratada deverá ministrar treinamento, na língua portuguesa, para até 10 (dez) servidores indicados pelo órgão, com carga horária mínima de 20 horas.

4.3.2. O conteúdo do treinamento a ser ministrado deverá contemplar os seguintes itens:

a. Procedimentos de instalação;

b. Todos os procedimentos necessários à configuração técnica;

c. Todos os procedimentos necessários à completa operação do produto;

d. Todos os procedimentos de manutenção do produto que devem ser realizados pelos técnicos do órgão.

4.3.3. O treinamento poderá ser realizado virtualmente por profissional certificado pelo fabricante do produto ofertado;

4.3.4. O treinamento deverá ser ministrado em horário definido pelo tribunal, em dias úteis;

4.3.5. O treinamento será dado como concluído após a avaliação dos participantes, com o preenchimento da Planilha de Avaliação de Treinamento, devendo ser obtida média superior a 70%, caso contrário a CONTRATANTE poderá solicitar a realização de novo treinamento, com a reformulação que achar necessária.

### 4.4 SUPORTE TÉCNICO ESPECIALIZADO ITEM 04

*Características técnicas mínimas:*

4.4.1 O suporte técnico especializado será solicitado pela contratante sob demanda e prestada por meio de acesso remoto, pelo período de 60 (sessenta) meses em língua portuguesa, de acordo com as necessidades elencadas, nos dias úteis (de segunda a sexta-feira), no horário de 08hs as 18hs, e deverão executar as seguintes atividades:

- a) Acompanhar, quando solicitado pela CONTRATANTE, todas as operações realizadas no sistema durante determinado período de tempo, sempre que constatada a necessidade pela contratada e notificado a contratante através da Web, E-mail ou telefone;
- b) Esclarecer dúvidas de usuários em relação à operação do sistema e/ou solução ofertada;
- c) Prestar serviços de suporte técnico para a solução de problemas que impeçam o perfeito funcionamento do sistema e/ou solução ofertada de acordo com o tempo de resposta citado abaixo;
- d) Reportar à CONTRATANTE quaisquer outros problemas verificados durante o atendimento, relativos ou não à solução ofertada;
- e) Fornecer informações aos usuários da CONTRATANTE sobre a situação e o andamento de serviços de manutenção e/ou consultivos solicitados;
- f) Diagnosticar a performance do solução em seus aspectos operacionais;
- g) Identificar e notificar problemas inerentes ao software e/ou solução;
- h) Notificar possíveis problemas de performance oriundos do ambiente onde a solução se encontra instalada;
- i) Discutir implementações de melhorias e atualizações, visando possíveis adequações;
- j) Na prestação dos serviços, quando solicitado pela CONTRATANTE, a CONTRATADA utilizará profissionais com qualificação e treinamento adequados para o desenvolvimento das tarefas relacionadas;
- k) Apoiar na criação de dashboards e relatórios da software e/ou solução;
- l) Apoiar na solução de problemas relativos a solução e às licenças adquiridas para chamados Nível 1 (padrão);
- m) Intermediação, acompanhamento e suporte entre a CONTRATANTE e o fabricante da solução para chamados Nível 2, 3 e 4;
- n) Documentação e transferência de conhecimento das atividades técnicas e consultivas realizadas;
- o) Relatório final através da Web, E-mail ou telefone formalizando o início e o término de cada solicitação;

4.4.2 A CONTRATADA deverá aceitar as especificações de softwares e protocolos de segurança estabelecidos pela CONTRATANTE para a realização do acesso remoto.

## **5 – DAS CONDIÇÕES DE INSTALAÇÃO E GARANTIA**

### **5.1 – Do local onde os softwares e licenças poderão ser entregues:**

5.1.1. As licenças deverão ser entregues em formato digital, por e-mail, ou disponibilizada para download em site do fabricante do produto.

### **5.2 – Condições de participação e realização dos serviços**

5.2.1. A solução será constituída de softwares, licenças e serviços relacionados nos itens do lote, sendo todos de um mesmo fabricante, garantindo a entrega e execução dos serviços por uma única empresa e a total compatibilidade entre eles;

5.2.2. A escolha do agrupamento dos itens em lote visa que a empresa fornecedora que prestará os serviços de fornecimento será a mesma que prestará os serviços de instalação, configuração, repasse tecnológico e consultoria especializada durante a vigência do contrato de garantia dos softwares e licenças, garantindo a total compatibilidade entre os softwares solicitados e a capacidade técnica de manter a solução em operação.

### **5.3 – Garantia e suporte técnico**

5.3.1. Os softwares e licenças fornecidos deverão estar cobertos por garantia que ofereça atualizações necessárias para a correção de vícios, pelo período especificado no item 1, a contar da data do aceite provisório do software, conforme Art. 73, I, "a", da Lei 8.666/1993;

5.3.1.1 O suporte pelo fabricante será obrigatório;

5.3.2. Devem estar explícitos na proposta os part numbers de garantia oficial do fabricante no Brasil;

5.3.3 O tempo da garantia e suporte estarão explicitadas nas especificações específicas dos respectivos itens.

5.3.4. A empresa deve indicar, na assinatura do contrato, os procedimentos para abertura de suporte técnico, cabendo a este órgão a abertura do chamado com intermediação da empresa fornecedora dos produtos ou diretamente com o fabricante;

5.3.5. A empresa deve possuir, no momento da assinatura do contrato, pelo menos 1 (um) profissional com certificação técnica emitida pelo fabricante, capaz de prestar o Serviço de Suporte Técnico Especializado registrado no item 4;

5.3.6. Os chamados telefônicos deverão estar disponibilizados de segunda à sexta-feira, das 8 às 18 horas, adotando-se para tanto o horário de Brasília;

5.3.6.1 O tempo para a resposta dos chamados dependerá da severidade do problema conforme abaixo:

5.3.6.2 Não poderá ser superior a 2 horas, após abertura do chamado, para problemas com severidade crítica (Funcionalidade do produto completamente degradada, impacto crítico nas operações);

5.3.6.3 Não poderá ser superior a 12 horas, após abertura do chamado, para problemas com severidade alta (Funcionalidade do produto severamente degradada, impacto severo nas operações);

5.3.6.4 Não poderá ser superior a 2 (dois) dias úteis, após abertura do chamado, para problemas com severidade média (Erros, problemas gerais, produto danificado, no entanto, as operações permanecem funcionais );

5.3.7. A empresa contratada ou o fabricante deverão disponibilizar, cumulativamente, abertura de suporte técnico por meio de atendimento telefônico, website e e-mail;

5.3.8. Os serviços de garantia aos produtos deverão ser prestados por empresa credenciada pelo fabricante ou pelo próprio fabricante dos produtos fornecidos.

5.3.9. A contratada ou o fabricante deverão disponibilizar um portal web com disponibilidade de 24 horas por dia, 7 dias por semana e 365 dias por ano, com sistema de help-desk para abertura de chamados de suporte técnico;

5.3.10. A equipe técnica da contratante poderá abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico, mediante login e senha de acesso ao Sistema;

5.3.11. Os chamados abertos por e-mail deverão ter sua abertura automática no portal web;

5.3.12. Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk;

5.3.13. A contratante poderá solicitar o escalonamento de incidentes ao fabricante quando se tratarem de correções especiais, defeitos nos programas ou defeito em hardware;

5.3.14. A contratada poderá prestar o suporte técnico dos produtos, sendo facultado a ela o escalonamento das questões para o respectivo fabricante, ficando, entretanto, a contratada responsável pelo gerenciamento do chamado e prestação de informações junto à contratante;

5.3.15. A garantia iniciará sua contagem a partir da data de emissão da NF dos softwares, serviços ou licenças;

5.3.16. Havendo discrepâncias entre o que está especificado no item específico e o que consta nestas condições gerais, prevalecerá o que está no item específico.

## 5.4 - Atualizações

5.4.1. A contratada deverá disponibilizar, na vigência do contrato, todas as atualizações dos softwares dos componentes da solução, concebidas em data posterior ao seu fornecimento, pelo período especificado no item 1 (60 meses), sem qualquer ônus adicional para o contratante;

5.4.2. As atualizações incluídas devem ser do tipo "minor release" e "major release", permitindo manter todos componentes atualizados em sua última versão de software/firmware.

## **5.5 - Condições de entrega e recebimento**

5.5.1. O fornecimento das licenças de software deverá ocorrer em até 10 (dez) dias úteis após a assinatura do contrato.

5.5.2. A entrega do item 2 (Instalação e Configuração) deverá ocorrer em até 10 (dez) dias úteis após o fornecimento das licenças de software.

5.5.3. A entrega do item 3 (Repasse tecnológico de 20 horas) será agendado conforme disponibilidade de agenda das partes, podendo ser efetuado em outro exercício financeiro, mas em prazo não superior a 90 dias da data de assinatura do contrato e a contratada terá um prazo de 10 dias úteis para iniciar a prestação do serviço após o recebimento da solicitação.

5.5.4. Para itens de software, devem ser apresentados chave única tipo serial ou qualquer outra forma de validação da ferramenta, comprovando perante o fabricante que trata-se de uma ferramenta devidamente licenciada;

5.5.5. O Termo de Recebimento Provisório será emitido por servidor ou comissão do tribunal, devidamente constituída para este fim, em **até 10 dias úteis após a entrega dos itens 1 e 2;**

5.5.6. O Termo de Recebimento Definitivo será emitido por servidor ou comissão do tribunal, devidamente constituída para este fim **em até 15 dias úteis após a entrega dos itens 1 ,2 e 3.**

## **5.6 - Condições de aceite**

5.6.1. O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente especificação técnica;

5.6.2. Para comprovação de pleno atendimento aos requisitos deste edital, serão consultados folhetos, prospectos, manuais e toda documentação pública disponível diretamente do site do fabricante. Em caso de dúvida ou divergência na comprovação da especificação técnica, este órgão poderá solicitar amostra do produto ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 5 (cinco) dias úteis após a solicitação deste órgão. Para a amostra, a empresa deverá apresentar as mesmas versões do produto ofertado no certame, com técnico certificado na solução para configuração e comprovação dos itens pendentes, nas dependências deste órgão, conforme itens 1.1.1 e 1.1.2, TC-006.806/2006-4, Acórdão nº 838/2006-TCU-2ª Câmara.

## **5.7 - Condições de pagamento**

5.7.1. O pagamento será feito em duas etapas:

5.7.1.1 O valor da primeira etapa será o somatório dos valores dos itens 1,2 e 4 e será pago após a entrega dos itens 1 e 2;

5.7.1.2 O valor da segunda etapa será o valor do item 3 e será pago após a entrega do item 3.

## **6 - HABILITAÇÃO E QUALIFICAÇÃO DO FORNECEDOR**

**6.1. A PROPONENTE deverá:**

6.1.1. Comprovar pertencer ao ramo de atividade pertinente ao objeto da contratação, através de cartão CNPJ, estatuto ou contrato social em vigor devidamente registrado na Junta Comercial;

6.1.2. Comprovar aptidão do desempenho de atividade pertinente e compatível em tecnologia com a solução global especificada neste Termo de Referência. A comprovação deverá acontecer através de:

6.1.2.1. Apresentação de declaração do fabricante da solução ofertada no lote garantindo que a empresa revendedora é capaz de fornecer, instalar, configurar e prestar suporte da solução ofertada, não implicando em perda de garantia no Brasil e;

6.1.2.2 Atestados ou certidões de capacidade técnica, em nome da licitante, expedidos por pessoas jurídicas de direito público ou privado, registrado nas entidades profissionais competentes, que comprove o regular fornecimento, instalação e configuração de solução de gestão/gerenciamento de vulnerabilidade em ambiente de infraestrutura que compreenda Active Directory no parque tecnológico, sendo da mesma marca da solução que pretende fornecer a este órgão no âmbito da presente contratação.

6.1.3. Possuir no mínimo 1 (um) profissional com certificação técnica do fabricante da solução que pretende fornecer a este órgão no âmbito da presente contratação;

6.1.3.1. O técnico deverá estar devidamente contratado pela empresa fornecedora da solução.

6.2. Todas as comprovações exigidas neste item deverão ser enviadas durante a fase de habilitação.

**7 - DAS PENALIDADES**

7.1 - O CONTRATANTE poderá aplicar à CONTRATADA as penalidades previstas no artigo 49 do Decreto nº 10.024/2019. A Administração poderá, ainda, a seu critério, utilizar-se subsidiariamente das sanções previstas na Lei nº 8.666/93, no que couber.

7.2. A recusa injustificada do adjudicatário em assinar o contrato, se for o caso, no prazo de 05 (cinco) dias, contados da notificação do CONTRATANTE, caracteriza o descumprimento total da obrigação assumida, sujeitando-o à penalidade de multa no percentual de até 30% (trinta por cento) sobre o valor global da obrigação não cumprida.

7.3 - Fica estabelecido como falta grave, caracterizado como falha em sua execução, a não manutenção de todas as condições de habilitação e qualificação exigidas na licitação, que poderá dar ensejo à rescisão do contrato, sem prejuízo da aplicação da multa compensatória estabelecida no item 7.4 e do impedimento para licitar e contratar com a União, nos termos do art. 49 do Decreto nº 10.024/2019.

7.4 - Com fundamento no art. 49 do Decreto nº 10.024/2019, ficará impedida de licitar e contratar com a União e será descredenciada no SICAF, pelo prazo de até 5 (cinco) anos, sem prejuízo das demais cominações legais e de multa compensatória de até 30% (trinta por cento), no caso de inexecução total, sobre o valor total da contratação, ou de até 15% (quinze por cento), no caso de inexecução parcial, sobre o valor do saldo da contratação, respectivamente, a Contratada que:

7.4.1 - não assinar o contrato ou a ata de registro de preços;

7.4.2 - não entregar a documentação exigida no edital;

7.4.3 - apresentar documentação falsa;

7.4.4 - causar o atraso na execução do objeto;

7.4.5 - não manter a proposta;

7.4.6 - falhar na execução do contrato;

7.4.7 - fraudar a execução do contrato;

7.4.8 - comportar-se de modo inidôneo;

7.4.9 - declarar informações falsas; e

7.4.10 - cometer fraude fiscal.

7.5 - Para os fins do item 7.4.8, reputar-se-ão inidôneos atos como os descritos nos arts. 90, 92, 93, 94, 95 e 97 da Lei nº 8.666/93.

7.6 - A Contratada ficará sujeita, no caso de inexecução parcial ou total da obrigação, com fundamento no art. 86 da Lei nº 8.666/93, à seguinte penalidade:



7.7.1 - multa moratória de:

7.7.1.1 - 0,05% (zero vírgula zero cinco por cento) ao dia sobre o valor do contrato em caso de atraso na execução do serviço, limitada a incidência de 10 (dez) dias;

7.7.1.2 - Sendo o atraso superior a 10 (dez) dias, configurar-se-á inexecução total da obrigação, a ensejar a aplicação da multa compensatória, prevista no item 7.4, sem prejuízo da aplicação da multa moratória limitada a 0,5% (zero vírgula cinco por cento), oriunda do atraso referido no subitem anterior, bem como da rescisão unilateral da avença.

## **8. VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS E DO VALIDADE DO CONTRATO:**

8.1. A(s) ata(s) de registro de preços decorrente(s) desta contratação terão validade de 12 (doze) meses.

8.2. O(s) contrato(s) decorrentes das ARP's terá(ão) vigência de 60 meses, conforme o suporte do item contratado.

## **9. OBRIGAÇÕES DA CONTRATADA**

Além das demais obrigações descritas ao longo deste Termo de Referência, a CONTRATADA obriga-se a:

9.1. Fornecer todas as licenças de software necessárias para utilização completa da solução pelos períodos adquiridos, salvo o sistema operacional das máquinas utilizadas pela solução.

9.2. Registrar, junto aos fabricantes e em nome da contratante, todas as assinaturas de licenças de software ofertadas.

9.3. Cumprir fielmente as obrigações assumidas, conforme as especificações constante neste Termo de Referência, utilizando-se de todos os recursos materiais e humanos necessários para entregar os produtos/prestar os serviços, nos prazos indicados.

9.4. 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.

9.5. Prestar todos os esclarecimentos que forem solicitados pelo tribunal, credenciando junto ao órgão, um representante para prestar os devidos esclarecimentos e atender as reclamações que porventura surgirem durante a execução do objeto.

9.6. Assinar, através de seu responsável legal, Termo de Sigilo e Responsabilidade, garantindo o sigilo e a confidencialidade dos dados a que vier a ter contato durante a instalação e durante a utilização da solução de software.

9.7. A contratada obrigar-se-á em manter-se em compatibilidade com a habilitação e com as obrigações assumidas na licitação até o adimplemento total da contratação.

9.8. Executar os serviços nos prazos estabelecidos neste instrumento, nos locais indicados pela Administração, em estrita observância das especificações do Edital e da proposta;

9.9. Atender prontamente aos chamados da Administração, relacionados ao objeto da licitação;

9.10. Comunicar à Administração, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

9.11. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

9.12. Responsabilizar-se pelas despesas dos tributos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros, deslocamento de pessoal, prestação de garantia e quaisquer outras que incidam ou venham a incidir na execução do contrato.

9.13 Apresentar junto com a Fatura/Nota Fiscal dos serviços prestados, as comprovações de regularidade junto à Seguridade Social (CND), ao Fundo de Garantia por Tempo de Serviço (CRF) e às Fazendas Federal, Estadual e Municipal de seu domicílio ou sede, bem como a Certidão Negativa de Débitos Trabalhistas de que trata a Lei nº 12.440/2011; caso esses documentos não estejam disponíveis no SICAF.

9.14 Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que está obrigada, exceto nos casos e condições autorizadas pelo CONTRATANTE, já previstos neste Termo de Referência.

## 10. OBRIGAÇÕES DA CONTRATANTE

A Contratante obriga-se a:

10.1. Prover as máquinas virtuais ou físicas juntamente com sistema operacional de acordo com documentação do fabricante.

10.2. Receber provisoriamente o material, disponibilizando local, data e horário.

10.3. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivos.

10.4. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através do gestor e dos fiscais especialmente designados.

10.5. Efetuar o pagamento na forma e no prazo previsto neste instrumento e no contrato.

## 11. ADJUDICAÇÃO DO OBJETO

11.1 - A adjudicação será feita por lote único, tendo em vista trata-se de solução não divisíveis, bem como para fins de garantir total compatibilidade entre os itens agrupados.

## 12 - LOGÍSTICA REVERSA

12.1. É de responsabilidade da CONTRATADA a disposição final responsável e ambientalmente adequada das embalagens e dos materiais após o uso, em observância à Logística Reversa disposta no art. 33 da Lei Nº 12.305/2010 - que institui a Política Nacional de Resíduos Sólidos;

12.2. O Tribunal reserva-se o direito de assumir a responsabilidade a que se refere o item anterior, podendo dar outra destinação às embalagens e materiais após o uso, caso julgue mais conveniente para a Administração;

12.3. Os materiais utilizados na embalagem do produto ofertado deverão ter sua reciclabilidade efetiva no Brasil.

**FELIPE CAVALCANTI ALVES**  
**CHEFE DA SEÇÃO DE SEGURANÇA CIBERNÉTICA**



Documento assinado eletronicamente por FELIPE CAVALCANTI ALVES em 22/08/2022, às 14:18, conforme art. 1º, III, "b", da [Lei 11.419/2006](#).

**ADAILTON VENTURA DA SILVA**  
**TÉCNICO JUDICIÁRIO**



Documento assinado eletronicamente por ADAILTON VENTURA DA SILVA em 22/08/2022, às 14:19, conforme art. 1º, III, "b", da [Lei 11.419/2006](#).

**JOSÉ CASSIMIRO JUNIOR**  
**SECRETÁRIO(A) DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**



Documento assinado eletronicamente por JOSÉ CASSIMIRO JUNIOR em 22/08/2022, às 14:22, conforme art. 1º, III, "b", da [Lei 11.419/2006](#).

---

**GEORGE BEZERRA CAVALCANTI LEITE**  
**COORDENADOR(A) DE APOIO À GOVERNANÇA, GESTÃO DE TIC E SEGURANÇA CIBERNÉTICA**

---



Documento assinado eletronicamente por GEORGE BEZERRA CAVALCANTI LEITE em 22/08/2022, às 14:58, conforme art. 1º, III, "b", da [Lei 11.419/2006](#).

---

**ALINE CORRÊA DOS SANTOS**  
**TÉCNICO JUDICIÁRIO**

---



Documento assinado eletronicamente por ALINE CORRÊA DOS SANTOS em 22/08/2022, às 16:03, conforme art. 1º, III, "b", da [Lei 11.419/2006](#).



A autenticidade do documento pode ser conferida no site [https://sei.tre-pb.jus.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://sei.tre-pb.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0) informando o código verificador **1342396** e o código CRC **2C081873**.