TRIBUNAL REGIONAL ELEITORAL DA PARAÍBA
Avenida Princesa Isabel, 201 - Bairro Centro - CEP 58013-251 - João Pessoa - PB - http://www.tre-pb.jus.br

Contratação - Estudos Preliminares IN 1/2018TREPB nº 6/2022 - SESEC

ESTUDO PRELIMINAR DA CONTRATAÇÃO

Caracterização da Demanda

1. Descrição da Solução de TIC a ser contratada

Registro de preço para contratação de ferramenta de Auditoria de Segurança no Active Directory.

1.1. DOD(s) que compõe(m) a solução de TIC

DOD que compõe a solução de TIC descrito neste estudo: 1223063.

2. Equipe de planejamento da contratação

Integrante	Nome	Ramal	E-mail	Setor
Demandante	*Felipe Cavalcanti Alves*	1420	felipe.alves@tre-pb.jus.br	SESEC
Administrativo	Aline Correa dos Santos	1277	aline.correa@tre-pb.jus.br	SECONT
Técnico	Adailton Ventura da Silva	1322	adailton.ventura@tre-pb.jus.br	SESEC

3. Necessidade da contratação

O Active Directory (AD) é um banco de dados e um conjunto de serviços que conectam os usuários aos recursos de rede de que precisam para realizar seu trabalho. O banco de dados (ou diretório) contém informações essenciais sobre o seu ambiente, incluindo os usuários com todas as suas informações cadastradas, computadores existentes e quem tem permissão para fazer o quê. Os serviços controlam grande parte da atividade do seu ambiente de TI. Especificamente, eles se certificam de que cada pessoa é quem afirma ser (autenticação), geralmente verificando a ID do usuário e a senha inserida, e permitem que acessem apenas os dados que têm permissão para usar (autorização).

Nos últimos anos, cada vez mais, tem surgido brechas de segurança e implementações não seguras do Active Directory (AD). O AD tornou-se o alvo preferido dos invasores para elevar os privilégios e facilitar o movimento lateral por meio do aproveitamento de falhas e configurações incorretas conhecidas. A maioria das organizações luta com a segurança do Active Directory devido a configurações incorretas que se acumulam à medida que os domínios aumentam em complexidade, impedindo as equipes de segurança de encontrarem e corrigirem falhas antes que se tornem problemas que afetam os negócios. A aquisição de ferramenta para proteção do AD é essencial pois permite que você veja tudo, preveja o que é importante e aja para lidar com os riscos no Active Directory para interromper as vias de ataque antes que os invasores os explorem.

4. Alinhamento estratégico

Objetivo 4 do PEI: Aperfeiçoar a comunicação e a informação.

Objetivo 8 do PEI: Aperfeiçoar a governança e gestão.

Seção I - Análise da Viabilidade da Contratação

5. Requisitos da contratação

O presente estudo objetiva a contratação de ferramenta de Auditoria de Segurança no Active Directory para atender as necessidades do Tribunal Regional Eleitoral da Paraíba.

5.1 Necessidades do negócio

Necessidade: Descobrir fraquezas ocultas nas configurações do Active Directory;

Necessidade: Descobrir problemas subjacentes que ameacem a segurança do AD;

Necessidade: Analisar detalhadamente os erros de configuração;

Necessidade: Obter recomendações de correções para cada problema;

Necessidade: Descobrir relacionamentos de confiança perigosos;

Necessidade: Descobrir todas as mudanças em seu AD;

Necessidade: Monitorar em tempo real ataques ao domínio no AD;

Necessidade: Estabelecer a ligação entre mudanças do AD e ações mal-intencionadas;

Necessidade: Analisar os detalhes de um ataque contra o AD.

Ator(es) Envolvido(s): STIC.

5.2 Requisitos Tecnológicos e Não Funcionais

5.2.1. Requisitos Tecnológicos

5.2.1.1. Características gerais à solução de análise em ambiente Microsoft Active Directory
5.2.1.1.1. A solução deve identificar fraquezas ocultas em configurações do dedicadas ao Active Directory;
5.2.1.1.2. A solução deve possuir ações preventivas de hardening para o Active Directory;
5.2.1.1.3. A solução deve identificar ataque específicos para a estrutura do Active Directory;
5.2.1.1.4. 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;
5.2.1.1.5. A solução deve possuir recomendações de correção para cada configuração incorreta no Active Directory;
5.2.1.1.6. A solução deve avaliar relações de confiança perigosas entre florestas e domínios;
5.2.1.1.7. A solução deve capturar as mudanças que ocorrem no AD e demostrar na console de administração;
5.2.1.1.8. A solução deve possuir dashboard com os principais ataques e vulnerabilidades por domínio;
5.2.1.1.9. A solução deve permitir a correlação de mudanças no Active Directory e desvios de segurança;
5.2.1.1.10. A solução deve analisar em detalhes um ataque explorando as descrições através do framework MITRE ATT&CK;
5.2.1.1.11. A solução deve prover interface web para gerenciamento de todas as funcionalidades;
5.2.1.1.12. A solução deve possuir capacidade nativa de criação de dashboards customizados;
5.2.1.1.13. A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;
5.2.1.1.14. A solução não deve realizar alterações no Active Directory, seus objetos e atributos;
5.2.1.1.15. A solução não deve armazenar ou sincronizar nenhuma credencial de objetos do Active Directory;
5.2.1.1.16. A solução deve suportar ambientes com múltiplas florestas e domínios;
5.2.1.1.17. A solução deve suportar monitoramento continuo de ambientes com Active Directory com o nível funcional de floresta e domínio a partir do 2003;
5.2.1.1.18. A solução deve suportar reter os eventos coletados por no mínimo um ano;
5.2.1.1.19. A solução deve descobrir e mapear a superfície de ataque do Active Directory e seus domínios monitorados com os seguintes padrões:
5.2.1.1.19.1. Não depender de agentes ou sensores para coleta de informações do AD;
5.2.1.1.19.2. 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;
5.2.1.1.19.3. Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles;
5.2.1.1.20. A solução deve analisar continuamente a postura de segurança do AD, minimamente avaliando:
5.2.1.1.20.1. Validação de GPOs desvinculadas, desabilitadas ou órfãs;
5.2.1.1.20.2. Validação de contas desativadas em grupos privilegiados;
5.2.1.1.20.3. Domínio usando uma configuração perigosa de compatibilidade com versões anteriores por meio de alterações no atributo dSHeuristics;
5.2.1.1.20.4. Validação de atributos relacionados a roaming de credenciais vulneráveis (ms-PKI-DPAPIMasterKeys) gerenciados por um usuário sem privilégios;
5.2.1.1.20.5. Validação de domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como NTLMv1;
5.2.1.1.20.6. Validação de contas com senhas que nunca expiram;
5.2.1.1.20.7. Validação de senhas reversíveis em GPOs;
5.2.1.1.20.8. Validação de uso de senhas reversíveis em contas de usuário;
5.2.1.1.20.9. Validação de utilização de protocolo criptográfico fraco (Ex. DES) em contas de usuário;
5.2.1.1.20.10. Validação de uso do LAPS (Solução de senha de administrador local) para gerenciar senhas de contas locais com privilégios;
5.2.1.1.20.11. Validação se o domínio possui um nível funcional desatualizado;
5.2.1.1.20.12. Validação de contas de usuário utilizando senha antiga;
5.2.1.1.20.13. Validação se o atributo AdminCount está definido em usuários padrão;
5.2.1.1.20.14. Validação do uso recente da conta de administrador padrão;
5.2.1.1.20.15. Validação de usuários com permissão para ingressar computadores no domínio;
5.2.1.1.20.16. Validação de contas dormentes;
5.2.1.1.20.17. Validação de computadores executando um sistema operacional obsoleto;
5.2.1.1.20.18. Validação de restrições de logon para usuários privilegiados em ambiente com múltiplos tiers (1, 2 e 3) de segregação de ativos;
5.2.1.1.20.19. Validação de direitos perigosos configurados no Schema do AD;
5.2.1.1.20.20. Validação de relação de confiança perigosa com outras Florestas e Domínios;
5.2.1.1.20.21. Validação de contas que possuem um atributo perigoso de histórico SID (SID History);
5.2.1.1.20.22. Validação de contas utilizando controle de acesso compatível com Windows 2000;
5.2.1.1.20.23. Validação da última alteração de senha do KDC;
5.2.1.1.20.24. Validação da última alteração da senha da conta SSO do Azure AD;
5.2.1.1.20.25. Validação de contas que podem ter senha em branco/vazia;
5.2.1.1.20.26. Validação de utilização do grupo nativo Protected Users;
5.2.1.1.20.27. Validação de privilégios sensíveis (Ex. Debug a program, Replace a process level token, etc.) perigosos atribuídos aos usuários;
5.2.1.1.20.28. Validação de possível senha em clear-text;
5.2.1.1.20.29. Validação de sanidade das GPOs e componentes CSEs (Client-Side Extension);
5.2.1.1.20.30. Validação de uso de algoritmos de criptografia fracos na PKI do Active Directory;
5.2.1.1.20.31. Validação de contas de serviço com SPN (Service Principal Name) que fazem parte de grupos privilegiados;
5.2.1.1.20.32. Validação de contas anormais nos grupos administrativos padrão do AD;
5.2.1.1.20.33. Validação de consistência no container adminSDHolder;
5.2.1.1.20.34. Validação de delegação Kerberos perigosa;
5.2.1.1.20.35. Validação em permissões de objetos raiz que permitem ataques do tipo DCSync;
5.2.1.1.20.36. Validação de políticas de senha fracas aplicadas aos usuários;
5.2.1.1.20.37. Validação das permissões relacionadas às contas do Azure AD Connect;
5.2.1.1.20.38. Validação do ID do grupo primário do usuário (Primary Group ID);
5.2.1.1.20.39. Validação de permissões em GPOs sensíveis associadas aos Containers Configuration, Sites, Root Partition e OUs sensíveis como Domain Controllers;
5.2.1.1.20.40. Controladores de domínio gerenciados por usuários ilegítimos;

5.2.1.1.20.41. Validação de certificado mapeado através de atributo altSecurityIdentities em contas privilegiadas;
5.2.1.1.20.42. Validação de uso de protocolo Netlogon inseguro (Zerologon/CVE-2020-1472);
5.2.1.1.21. A solução deve identificar vulnerabilidades e configurações incorretas do AD à medida que são introduzidas sendo:
5.2.1.1.21.1. Identificar todas as vulnerabilidades e configurações incorretas no AD;
5.2.1.1.21.2. Monitorar relações de confiança perigosas em toda a estrutura AD;
5.2.1.1.21.3. Apresentar ameaças e alterações sem a necessidade de scans estáticos e programados no Active Directory e sua infraestrutura;
5.2.1.1.21.4. Apresentar as ameaças e alterações em tempo real ou em menos de cinco minutos;
5.2.1.1.22. Em relação a detecção e resposta a ataques a solução deve:
5.2.1.1.22.1. 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;
5.2.1.1.22.2. Detecção de ataques ao AD em tempo real ou em menos de um minuto;
5.2.1.1.22.3. Análise detalhada do ataque, apresentando ativo de origem, vetor de ataque, controlador de domínio afetado, técnica aplicada;
5.2.1.1.22.4. Apresentação de ataques em uma linha do tempo;
5.2.1.1.22.5. Investigar ameaças, reproduzir ataques e procurar por backdoors;
5.2.1.1.22.6. Permitir busca ágil de eventos específicos na base da solução através de queries customizadas;
5.2.1.1.23. A solução deve ser capaz de enviar alertas por e-mail;
5.2.1.1.24. A solução nativamente deve ser capaz de se integrar com SIEM através de protocolo SYSLOG;
5.2.1.1.25. A solução deve ser capaz de filtrar e enriquecer os eventos que serão enviados para o SIEM;
5.2.1.1.26. A solução deve produzir regras YARA na detecção de ataques (Ex. DCSync, Golden Ticket) identificados pela ferramenta;
5.2.1.1.27. A solução deve possuir conjunto de APIs REST, todas as chamadas disponíveis devem estar contidas na documentação;
5.2.1.1.28. A solução deve permitir a criação de listas de exclusões, suportando minimamente Exclusão por domínios do AD monitorados e por itens analisados;
5.2.1.1.29. A solução deve ser licenciada pelo número de usuários habilitados;

5.2.1.2. Configurações básicas para o usuário:

5.2.1.2.1. Preferências do usuário para:
5.2.1.2.1.1. Selecionar a linguagem da ferramenta;
5.2.1.2.1.2. Selecionar o perfil de usuário;
5.2.1.2.1.3. Alterar a senha o perfil do usuário da solução;
5.2.1.2.1.4. Gerenciar as chaves de API.

5.2.1.2.2. A navegação pela plataforma da solução deve ser de maneira clara e simples contendo, no mínimo, os seguintes elementos:
5.2.1.2.2.1. Painel de controle: para permitir o gerenciamento e monitoramento de forma visual e eficiente sobre a infraestrutura do Active Directory;
5.2.1.2.2.2. Notificações: que contenham alertas de ataque e/ou exposição aguardando sua confirmação e verificação.
5.2.1.2.2.3. Conectividade: visualização indicativa de conexão ao Active Directory e, ainda apresentar alerta quando houver indisponibilidade entre a solução e o elemento de infraestrutura supracitado;
5.2.1.2.2.4. Acessibilidade: para acessar documentos que ajudem e esclareçam dúvidas ao usuário ou administrador da solução;
5.2.1.2.2.5. Perfis de segurança: permitindo diferentes tipos de usuários para revisar as análises de seguranças a partir de ângulos variados sobre relatórios disponibilizados;
5.2.1.2.2.6. Tela de fluxo: monitoramento e análise de eventos que afetam o Active Directory em tempo real;
5.2.1.2.2.7. 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;
5.2.1.2.2.8. Indicadores de ataque: detecção de ataques ao Active Directory em tempo real;
5.2.1.2.2.9. 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.
5.2.1.2.2.10. Caminho do ataque: página na solução que forneça representações gráficas dos relacionamentos do Active Directory como:
5.2.1.2.2.10.1. Avaliação de movimentos laterais no AD sobre um ativo potencialmente comprometido (Blast Radius);
5.2.1.2.2.10.2. Antecipação sobre técnicas de escalonamento de privilégios para alcançar um ativo a partir de um determinado ponto de entrada (Attack Path);
5.2.1.2.2.10.3. Medição sobre a vulnerabilidade de um ativo, usando sua visualização e exposição para abordar os caminhos de escalação (Asset Exposure);
5.2.1.2.2.10.4. Preferencias do usuário: permitindo a configuração de linguagem, perfil e senha dentro da solução;
5.2.1.2.2.10.5. Log out: Opção para saída de forma simples do perfil dentro da solução.
5.2.1.2.2.11. Widgets: que possibilitem um conjunto de dados personalizáveis para exibição do painel da solução. Devem conter minimamente:
5.2.1.2.2.11.1. Gráficos de barras;
5.2.1.2.2.11.2. Gráficos de linhas; e
5.2.1.2.2.11.3. Contadores.

5.2.1.3. Notificações:

5.2.1.3.1. A solução deve notificar e realizar contagem sobre alertas de ataque e/ou alertas de exposição aguardando conhecimento dos responsáveis pela solução;
5.2.1.3.2. Ao receber novos alertas a contagem deve permanecer crescente de forma transparente e visual;
5.2.1.3.3. Os detalhes dos eventos devem conter as seguintes informações no painel exibido dentro das notificações:
5.2.1.3.3.1. Origem (da coleta do evento);
5.2.1.3.3.2. Tipo de objeto;
5.2.1.3.3.3. Caminho para o arquivo;
5.2.1.3.3.4. Domínios afetados;
5.2.1.3.3.5. Data;
5.2.1.3.3.6. Lista de atributos com valores no momento do evento e o valor atual.
5.2.1.3.4. Possibilidade de arquivamento do aleta

5.2.1.4. Painel de controle

5.2.1.4.1. O painel de controle da solução deve permitir a visualização de dados e tendências que afetem a segurança do AD;
5.2.1.4.2. O painel de controle deve ser personalizável com widgets para exibição de gráficos e contadores de acordo com as necessidades do ambiente.
5.2.1.4.3. As configurações dos painéis de controle devem permitir:
5.2.1.4.3.1. Criação;
5.2.1.4.3.2. Renomeação; e
5.2.1.4.3.3. Exclusão de um painel de controle.

5.2.1.5. Widgets

5.2.1.5.1. 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.
5.2.1.5.2. Deve ser permitido a criação de novos widgets no painel ou a partir de existentes.
5.2.1.5.3. As configurações do widget devem incluir:
5.2.1.5.3.1. Contagem de usuários: o número de usuários ativos para o domínio;
5.2.1.5.3.2. Contagem de desvios: o número de desvios ou violações de segurança detectadas;
5.2.1.5.3.3. 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.
5.2.1.5.3.4. Duração (para gráfico de linhas): exibindo a duração.

5.2.1.5.4. Os conjuntos de dados devem exibir:
5.2.1.5.4.1. Status (contagem de usuários): Ativo, inativo ou todos;
5.2.1.5.4.2. Indicadores (Indicadores de exposição): a seleção pode ser feita de forma singular ou de vários através de uma lista, mas opcionalmente pode:
5.2.1.5.4.2.1. Ser digitada através do nome do indicador em caixa de pesquisa;
5.2.1.5.4.2.2. Seleção de todos os indicadores: a partir dos níveis de gravidade (crítico, alto, médio ou baixo).
5.2.1.5.4.3. 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;

5.2.1.6. Topologia

5.2.1.6.1. A solução deve prover através da funcionalidade de topologia:
5.2.1.6.1.1. Uma visualização gráfica interativa do Active Directory;
5.2.1.6.1.2. Gráfico de Topologia exibindo as florestas, domínios e relações de confiança que existem entre eles;
5.2.1.6.1.3. Pesquisa por um domínio específico;
5.2.1.6.1.4. Exibição do link entre dois domínios;
5.2.1.6.1.5. Exibição de detalhes sobre um domínio.

5.2.1.6.2. A solução deve exibir relações de confiança;
5.2.1.6.3. Deve haver compreensão do código de cores das relações de confiança dependendo do seu nível de ameaça;
5.2.1.6.4. As informações do atributo de confiança devem indicar a direção de confiança como unidirecional ou bidirecional (entrada/saída).

5.2.1.7. Investigação de Eventos no Active Directory

5.2.1.7.1. A solução deve conter funcionalidade de investigação sobre eventos que monitorem continuamente a infraestrutura e detecte regressões à medida que elas acontecem;
5.2.1.7.2. A solução deve ter painel intuitivo, para identificar rapidamente as vulnerabilidades mais críticas e suas recomendações de correção;
5.2.1.7.3. A página inicial deve exibir o monitoramento e a análise em tempo real de eventos que afetam as infraestruturas do AD;
5.2.1.7.4. A solução deve permitir carregar eventos anteriores e voltar no tempo;
5.2.1.7.5. A solução deve permitir a caixa de pesquisa para executar a caça a ameaças e detectar padrões maliciosos;
5.2.1.7.6. A solução deve ter elementos interativos como:
5.2.1.7.6.1. Permitir clicar nos elementos de entrada exibidos na página;
5.2.1.7.6.2. Os detalhes dos elementos devem incluir quais atributos mudaram de valor;
5.2.1.7.6.3. Mostrar ao usuário o valor do atributo antes e depois;
5.2.1.7.6.4. Mostrar se o evento possui uma exploração potencial dentro da entrada;
5.2.1.7.6.5. Chaves de alternância para ativar ou desativar a exibição de eventos;
5.2.1.7.6.6. 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.
5.2.1.7.6.7. Caixas de seleção para selecionar as florestas e domínios a serem incluídos na pesquisa ou na exibição.
5.2.1.7.7. Deve monitorar e permitir visualização em tempo real da análise de eventos que afetam o AD;
5.2.1.7.8. A funcionalidade deve atender aos seguintes requisitos dentro de sua exibição:
5.2.1.7.8.1. Recursos indicando a origem de qualquer alteração relacionada à segurança em suas infraestruturas do AD, correlacionando no mínimo duas fontes possíveis:
5.2.1.7.8.1.1. Lightweight Directory Access Protocol (LDAP): usado para se comunicar com seu Infraestrutura AD.
5.2.1.7.8.1.2. Server Message Block (SMB): protocolo usado para compartilhar arquivos, impressoras, etc.
5.2.1.7.9. A solução deve analisar minuciosamente o tráfego LDAP e SMB através da rede para detectar anomalias e ameaças potenciais;
5.2.1.7.10. 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:
5.2.1.7.10.1. ACL changed
5.2.1.7.10.2. SPN changed
5.2.1.7.10.3. Member removed
5.2.1.7.10.4. New member
5.2.1.7.10.5. New trust
5.2.1.7.10.6. Unknown file type added
5.2.1.7.10.7. New object
5.2.1.7.10.8. Object removed
5.2.1.7.10.9. Password changed
5.2.1.7.10.10. UAC changed
5.2.1.7.10.11. New GPO linked
5.2.1.7.10.12. GPO link removed

5.2.1.7.10.13. Owner change
5.2.1.7.10.14. File renamed
5.2.1.7.10.15. SPN created
5.2.1.7.10.16. Failed auth reset
5.2.1.7.10.17. Failed authentication

5.2.1.7.11. 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).
5.2.1.7.12. Deve indicar o caminho completo para um objeto AD, permitindo a identificação da localização exclusiva desse objeto no AD.
5.2.1.7.13. Deve indicar de qual diretório vem a alteração em sua infraestrutura do AD.
5.2.1.7.14. Deve indicar a hora em que ocorreu a alteração na infraestrutura do AD.
5.2.1.7.15. 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:
5.2.1.7.15.1. pausar;
5.2.1.7.15.2. reiniciar.

5.2.1.7.16. Deve permitir o filtro sobre eventos e resultados obtidos em tempo real;
5.2.1.7.17. Deve permitir a pesquisa sobre eventos e resultados obtidos em tempo real;
5.2.1.7.18. 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.
5.2.1.7.19. A solução deve permitir consultas rápidas através de um campo disponibilizado como assistente em seu painel;
5.2.1.7.20. 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;
5.2.1.7.21. A solução deve permitir que as expressões de consulta sejam salvas através de um histórico, de forma automática em lista;
5.2.1.7.22. A solução deve permitir que as expressões permitam combinadores AND ou OR para a consulta.
5.2.1.7.23. Em casos específicos de consulta, a solução deve restringir a pesquisa a objetos desviantes, permitindo expressão para facilitar o filtro de busca.
5.2.1.7.24. A solução deve permitir:
5.2.1.7.24.1. exclusão de atributos na expressão de consulta;
5.2.1.7.24.2. adição de novas condições na expressão de consulta;
5.2.1.7.24.3. adição de novas regras para as expressões de consulta
5.2.1.7.24.4. adição de atributos nas expressões de consulta.
5.2.1.7.24.5. adição de combinadores como AND ou OR;

5.2.1.7.25. A solução deve incluir campo de pesquisa para inserção das sintaxes utilizadas nas expressões de consulta;
5.2.1.7.26. A solução deve possuir funcionalidade para validar as expressões de consulta;
5.2.1.7.27. A solução deve permitir gerenciamento das expressões favoritas para:
5.2.1.7.27.1. procurar um marcador específico na lista;
5.2.1.7.27.2. limitar a pesquisa a uma pasta específica;
5.2.1.7.27.3. editar um nome de marcador;
5.2.1.7.27.4. excluir uma expressão da página dos favoritos;
5.2.1.7.27.5. editar o nome de uma pasta de favoritos (se houver);
5.2.1.7.27.6. excluir uma pasta de favoritos (se houver);

5.2.1.7.28. A pesquisa deve incluir florestas e domínios específicos como alvo;
5.2.1.7.29. 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);
5.2.1.7.30. A solução deve permitir a visualização de alterações de todos os atributos, com no mínimo os seguintes status:
5.2.1.7.30.1. adição;
5.2.1.7.30.2. exclusão;
5.2.1.7.30.3. inalterado.

5.2.1.7.31. A solução deve permitir a visualização sobre domínios impactados, incluindo os seguintes indicadores:
5.2.1.7.31.1. informação;
5.2.1.7.31.2. detalhes da Vulnerabilidade;
5.2.1.7.31.3. objetos desviantes; e
5.2.1.7.31.4. recomendações.

5.2.1.8. Visualização sobre vulnerabilidades:

5.2.1.8.1. A solução deve oferecer visualização em representação gráfica sobre potenciais vulnerabilidades para os ativos críticos;
5.2.1.8.2. Mostrar os possíveis caminhos que um invasor pode seguir para comprometer um ativo de um ponto de entrada;
5.2.1.8.3. Mostrar os possíveis movimentos laterais no Active Directory de qualquer ativo;
5.2.1.8.4. Mostrar todos os caminhos que podem potencialmente assumir o controle de um ativo;
5.2.1.8.5. Ajuste e manuseio de forma intuitiva aos gráficos exibidos.

5.2.1.9. Detecção a ataques em tempo real:

5.2.1.9.1. A solução deve ter a capacidade de detectar ataques em tempo real e interrupção imediata contemplando:
5.2.1.9.1.1. Visualização de todas as ameaças a partir de uma linha do tempo do ataque de forma precisa;
5.2.1.9.1.2. Consolidando a distribuição de ataques em uma visualização única.
5.2.1.9.1.3. Análise detalhada sobre um ataque ao Active Directory;
5.2.1.9.1.4. Explorar as descrições do MITRE ATT&CK diretamente dos incidentes detectados.
5.2.1.9.2. 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:
5.2.1.9.2.1. Crítica;
5.2.1.9.2.2. Alta;
5.2.1.9.2.3. Média;
5.2.1.9.2.4. Baixa.
5.2.1.9.3. A visualização deve exibir blocos de domínio organizados por:

5.2.1.9.3.1. Ordem alfabética;
5.2.1.9.3.2. Criticidade; e
5.2.1.9.3.3. Florestas;
5.2.1.9.4. Deve conter no mínimo as seguintes funcionalidades:
5.2.1.9.4.1. Distribuição de ataques mostrando os níveis de gravidade relacionados ao fluxo constante de ataques;
5.2.1.9.4.2. Top 3 dos principais ataques e seus números de ocorrências.
5.2.1.9.4.3. Capacidade de atualizar a visualização.
5.2.1.9.5. Capacidade de editar o tipo de gráfico exibido na página.
5.2.1.9.6. Capacidade de gerar e exportar relatórios listando os ataques;
5.2.1.9.7. Capacidade de selecionar data e hora iniciais para mostrar uma linha do tempo dos ataques;
5.2.1.9.8. A solução deve possibilitar a aplicação de filtros a incidentes;
5.2.1.9.9. Possibilidade de definir critérios de pesquisa para execução;
5.2.1.9.10. Acesso a explicações detalhadas sobre os ataques que afetam as infraestruturas do AD;
5.2.1.9.11. Capacidade de fechar ou reabrir um incidente;
5.2.1.9.12. Extração de relatório mostrando todos os incidentes.

5.2.1.10. Gestão de segurança das infraestruturas do AD:
5.2.1.10.1. 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.
5.2.1.10.2. São os níveis do subitem anterior:
5.2.1.10.2.1. Crítico;
5.2.1.10.2.2. Alto;
5.2.1.10.2.3. Médio; e
5.2.1.10.2.4. Baixo.
5.2.1.10.3. A solução deve exibir blocos sobre os indicadores com os seguintes requisitos:
5.2.1.10.3.1. Por severidade e código de cores;
5.2.1.10.3.2. Verticalmente, por ordem de severidade;
5.2.1.10.3.3. Horizontalmente, por ordem de complexidade;
5.2.1.10.3.4. Em ordem alfabética;
5.2.1.10.3.5. Por nome de domínio.
5.2.1.10.4. A solução deve possibilitar mostrar todos os Indicadores de Exposição de maneira fácil;
5.2.1.10.5. A solução deve ter a capacidade de restringir a seleção a florestas e domínios específicos;
5.2.1.10.6. A solução deve ter a capacidade de diferenciar os seguintes elementos:
5.2.1.10.6.1. Indicadores de exposição;
5.2.1.10.6.2. Eventos;
5.2.1.10.6.3. Objetos desviantes;
5.2.1.10.7. A solução deve possibilitar a visibilidade sobre vulnerabilidades para ver uma descrição completa e sua potencial ameaça;
5.2.1.10.8. A solução deve revelar objetos desviantes que revelam fraquezas ou comportamentos potencialmente perigosos às infraestruturas do AD;
5.2.1.10.9. Possibilitar as seguintes ações sobre objetos desviantes:
5.2.1.10.9.1. Recuperar objetos afetados no AD;
5.2.1.10.9.2. Ignorar objetos afetados no AD por um período de tempo;
5.2.1.10.9.3. Seleção de florestas e domínios para executar uma pesquisa.
5.2.1.10.9.4. Acesso a explicações sobre os atributos incriminadores que afetam os indicadores de exposição;
5.2.1.10.9.5. Exportação de relatório informando todos os objetos desviantes.

5.2.1.11. Serviço de Instalação e Configuração

5.2.1.11.1. A Contratada será inteiramente responsável pela instalação da solução, bem como pelas despesas diretas ou indiretas para execução das atividades pela sua equipe técnica;

5.2.1.11.2. A instalação da solução deverá ser realizada remotamente, no ambiente do tribunal;

5.2.1.11.3. A instalação da solução deverá ser realizada em dias úteis, podendo ocorrer no período de 10h às 19hs, considerando o fuso horário do contratante;

5.2.1.11.4. O processo de instalação da solução deverá ser acompanhado por servidores do Contratante;

5.2.1.11.5. Para garantir que a instalação não afetará o ambiente do Contratante, os procedimentos e atividades deverão ser realizados por técnicos certificados na solução;

5.2.1.11.6. A Contratada deverá se reunir com a equipe técnica do Contratante e elaborar um plano de instalação, contendo as etapas, modelos, arquiteturas, funcionalidades e configurações da solução que serão implantadas durante a execução do serviço;

5.2.1.11.7. A instalação da solução no ambiente do Contratante não poderá interferir no bom funcionamento de outros sistemas previamente instalados;

5.2.2. Requisitos de Capacitação

A contratação deve possuir um item de repasse tecnológico para capacitar os servidores da STIC a operacionalizar a ferramenta com os seguintes requisitos:

5.2.2.1. O repasse de conhecimento deverá ser fornecido para, no mínimo, 10 alunos e ter duração mínima de 20 (vinte) horas;

5.2.2.2 A Contratada deverá realizar a transferência de conhecimento para a equipe técnica do Contratante, por meio de repasse de conhecimento das tecnologias da solução;

5.2.2.3. A transferência de conhecimento deverá ser realizada de forma remota, por meio de ferramenta a ser acordada com o Contratante;

5.2.2.4. A transferência de conhecimento deverá conter conteúdo teórico e prático sobre a solução e deverá abordar, no mínimo, os seguintes itens:

5.2.2.5. Detalhamento dos componentes da solução, suas interconexões e todas as informações técnicas necessárias para o seu pleno funcionamento;

5.2.2.6. Orientar sobre a topologia lógica da solução implantada, mostrando a interligação dos componentes da solução, informando as interconexões realizadas com a infraestrutura existente no Contratante;

5.2.2.7. Orientar sobre os componentes, procedimentos de instalação e administração da solução, explorando as funcionalidades disponíveis na solução ofertada, ainda que não exigidas na especificação técnica;

5.2.2.8. A transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelo fabricante dos softwares da solução ofertada;

5.2.3. Requisitos Legais

5.2.3.1 - Margem de Preferência

Não há.

5.2.4. Requisitos de Manutenção

Não há requisitos de manutenção dos itens adquiridos, exceto quando houver mudança de versão do sistema operacional.

5.2.5. Requisitos Temporais

5.2.5.1. Prazos

5.2.5.1.1. O licitante terá 5 (cinco) dias contados da assinatura do contrato para fornecer os softwares ou as subscrições contratadas;

5.2.5.1.2. O atraso não justificado deverá ser punido de acordo com as sanções aplicadas ao contrato.

5.2.5.2. Suporte e garantia

A garantia de atualização do software e suporte do fabricante devem ser de, no mínimo, 60 (sessenta) meses.

A contratação também terá um item específico para suporte técnico de primeiro nível, durante 60 (sessenta) meses, pela contratada em língua portuguesa.

O suporte técnico de primeiro nível será acionado pela CONTRATANTE sob demanda e prestado por meio de acesso 100% remoto 8h x 5d (8 horas x 5 dias) e deverão contemplar 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 dashboad´s e relatórios da software e/ou solução;
l) Apoiar na solução de problemas relativos a solução e às licenças adquiridas para chamados Nivel 1 (padrão);
m) Intermediação, acompanhamento e suporte entre a CONTRATANTE e o fabricante da solução para chamados Nivel 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;

5.2.6. Requisitos de Segurança

5.2.6.1. A empresa contratada deverá respeitar as diretrizes constantes da Política de Segurança da Informação do da Justiça Eleitoral (Resolução TSE Nº 23.644/2021), obrigando-se a manter sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do Tribunal Regional Eleitoral da Paraíba aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa;

5.2.6.2. O Tribunal Regional Eleitoral da Paraíba terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação;

5.2.6.3. Os documentos eventualmente produzidos deverão ser repassados ao Tribunal tanto em formato não editável (PDF) como também em formato editável (.DOCX).

5.2.6.4. 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.

5.2.7. Requisitos Sociais, Ambientais e culturais

5.2.7.1. Logística Reversa

5.2.7.1.1. É de responsabilidade da CONTRATADA a disposição final responsável e ambientalmente adequada das embalagens e materiais que porventura venham a ser utilizados em observância à Logística Reversa disposta no art. 33 da Lei Nº 12.305/2010, que institui a Política Nacional de Resíduos Sólidos;

5.2.7.1.2. 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;

5.2.7.1.3. Qualquer material que venha a ser utilizado na embalagem dos produtos ofertados e/ou utilizados na execução dos serviços deverão ter sua reciclabilidade efetiva no Brasil.

6. Levantamento das Alternativas Disponíveis no Mercado

As soluções presentes no presente estudo resumem-se as seguintes opções.

6.1. Soluções

6.1.1. Utilização de software gratuito

Nome da Solução: Softwares gratuito Purple Knight

Fornecedor: Purple Knight.

Descrição: Utilizar ferramenta gratuita, como o Purple Knight.

6.1.2. Solução paga com gerenciamento e armazenamento na nuvem (On Cloud) Tenable.ep

Nome da Solução: Ferramenta de Auditoria de Segurança do Active Directory On Cloud

Fornecedores: Tenable.ep (Proposta Itprotect (1249539) baseada nos Itens 4,5,6 da Ata 1244084 do TRT8 com vencedor Itprotect)

Descrição: Aquisição de software de Auditoria de Segurança do Active Directory baseado em nuvem, com modelo de subscrição por 60 meses.

6.1.3. Solução paga com gerenciamento e armazenamento na rede local do Tribunal (On premise) Varonis

Nome da Solução: Ferramenta de Auditoria do Active Directory On premise Varonis

Fornecedores: Varonis (Baseado nos Itens 1, 5,6 e 7 da Ata 1238201 da Agência Nacional de Águas - ANA edital 1244309 e na planilha 1249641)

Descrição: Aquisição de software de Auditoria de Segurança do Active Directory baseado em gerenciamento e armazenamento na rede local do tribunal, com modelo de subscrição por 60 meses do fabricante Varonis.

6.1.4. Solução paga com gerenciamento e armazenamento na rede local do Tribunal (On premise) Tenable.ad

Nome da Solução: Ferramenta de Auditoria do Active Directory On premise Tenable.ad

Fornecedores: Tenable (Cotação ferramenta Tenable.ad da revenda SERVIX 1255132 e Cotação ferramenta Tenable.ad da revenda Qualitek 1238191)

Descrição: Aquisição de software de Auditoria de Segurança do Active Directory baseado em gerenciamento e armazenamento na rede local do tribunal, com modelo de subscrição por 60 meses do fabricante Tenable.

6.2. Análise de Custos Totais das Soluções de TIC Identificadas

Os custos estimados da contratação são conforme tabela abaixo.

Soluções de TIC - propostas de possíveis fornecedores/pesquisa no mercado de TIC

Item	Fornecedor	Descrição/Modelo	Quantidade Registrada	Valor Unitário	Valor Total
6.1.1	Comunidades	Softwares gratuito Purple Knight	0	R$ 0,00	R$ 0,00
6.1.2. - 01	Tenable.ep (on cloud)	Licença de subscrição de solução de auditoria do Active Directory por conta ativa de usuário do AD, durante 60 meses de uso e suporte do fabricante.	2000	R$ 1.453,00	R$ 2.906.000,00
6.1.2. - 02	Tenable.ep (on cloud)	Instalação e configuração.	1	R$ 0,00	R$ 0,00
6.1.2. - 03	Tenable.ep (on cloud)	Repasse Tecnológico com período mínimo de 20 horas.	1	R$ 8.600,00	R$ 8.600,00
6.1.2. - 04	Tenable.ep (on cloud)	Suporte de Primeiro Nível por 60 meses.	1	R$10.000,00	R$ 10.000,00
6.1.2	TOTAL Tenable.ep (on cloud)	----------	----------	----------	R$ 2.924.600,00
6.1.3-01	Varonis (on premise)	Licença de subscrição de solução de auditoria do Active Directory por conta ativa de usuário do AD, durante 60 meses de uso e suporte do fabricante.	2000	R$ 2.687,87	R$ 5.375.744,00
6.1.3-02	Varonis (on premise)	Instalação e configuração.	1	R$ 0,00	R$ 0.000,00
6.1.3-03	Varonis (on premise)	Repasse Tecnológico com período mínimo de 20 horas.	1	R$ 59.500,00	R$ 59.500,00
6.1.3-04	Varonis (on premise)	Suporte de Primeiro Nível por 60 meses.	1	R$ 1.740.000,00	R$ 1.740.000,00

6.1.4	TOTAL Varonis (on premise)	----------	----------	----------	R$ 7.175.244,00
6.1.4-01	Tenable.ad (on premise)	Licença de subscrição de solução de auditoria do Active Directory por conta ativa de usuário do AD, durante 60 meses de uso e suporte do fabricante.	2000	R$ 457,00	R$ 914.000,00
6.1.4-02	Tenable.ad (on premise)	Instalação e configuração	1	R$ 11.832,00	R$ 11.823,00
6.1.4-03	Tenable.ad (on premise)	Repasse Tecnológico com período mínimo de 20 horas	1	R$ 9.853,00	R$ 9.853,00
6.1.2-04	Tenable.ad (on premise)	Suporte de Primeiro Nível por 60 meses	1	R$ 9.853,00	R$ 9.853,00
6.1.2	TOTAL Tenable.ad (on premise)	----------	----------	----------	R$ 945.529,00

7. Justificativa da Solução Escolhida

A solução 1 baseada em Software Gratuito atende apenas parte da necessidade, pois a utilização desse cenário implica em não contar com suporte técnico especializado, além disso não possuí o monitoramento em tempo real e a base de vulnerabilidades é bem menor comparada com de cenários com softwares pagos. Outro ponto desfavorável ao uso do Software Gratuito é que os relatórios fornecidos pela ferramenta não apresentam rastreabilidade das atividades já realizadas nos ativos e sistemas.

A solução 2 baseada em nuvem (cloud computing) apresenta facilidade de gerenciamento, valor de aquisição elevado e facilidade nas atualizações da solução que serão todas feitas pelo fabricante. Todas os requisitos de funcionalidades do projeto são atendidos por esse cenário. A solução analisada Tenable.ep consegue fazer a auditoria do Active Directory e detecção em tempo real de eventos suspeitos no Active Directory. Porém como os dados armazenados pela ferramenta (indicadores de exposição do Active Directory) são muito sensíveis não é recomendável estarem armazenados em nuvem pública.

A solução 3 baseada em gerenciamento em rede local do tribunal (On premise) fornecida pelos fabricante Varonis apresenta um valor de aquisição extremamente elevado e não atende a todas os requisitos de funcionalidades do projeto.

A solução 4 baseada em gerenciamento em rede local do tribunal (On premise) fornecida pelos fabricante Tenable (Tenable.ad) apresenta um valor de aquisição adequado e menor do que a Solução 2 e Solução 3. Apesar de a solução 4 (On premise) trazer o trabalho de atualização para a equipe de infraestrutura de rede, ela possui um menor risco de vazamento de dados sensíveis (indicadores de exposição do Active Directory), pois os mesmos serão armazenados na rede local do Tribunal e não em nuvem pública. Todas os requisitos de funcionalidades do projeto também são atendidos por esse cenário. As solução analisada Tenable (Tenable.ad) conseguem fazer a auditoria do Active Directory e detecção em tempo real de eventos suspeitos no Active Directory.

Sendo assim, não resta outra alternativa para o TRE no momento senão a solução 4 baseada no gerenciamento em rede local do tribunal, tendo em vista o menor preço da Solução 4 (Tenable.ad) e o fato de atender a todos os requisitos de funcionalidades do projeto sem armazenar em nuvem pública os dados sensíveis (indicadores de exposição do Active Directory).

7.1. Solução Escolhida

Nome: Solução paga com gerenciamento e armazenamento na rede local do tribunal (On Premise) Tenable.ad

Descrição: Aquisição de ferramenta para auditoria do Active Directory e monitoramento de eventos suspeitos no Active Directory, baseado em gerenciamento e armazenamento na rede local do tribunal, com modelo de subscrição por 60 meses do fabricante Tenable.

Valor Estimado (baseado na melhor proposta da Tenable.ad on premise): R$ 945.529,00 (novecentos e quarenta e cinco mil quinhentos e vinte e nove reais)

7.2. Justificativa

Com a solução escolhida será possível realizar o Gerenciamento dos indicadores de exposição e indicadores de ataques no Active Directory, mitigando riscos de ataques cibernéticos e protegendo os sistemas de tecnologia da informação da Justiça Eleitoral.

7.3. Benefícios Esperados

Gerenciamento dos dos indicadores de exposição e indicadores de ataques no Active Directory, mitigando riscos de ataques cibernéticos e protegendo os sistemas de tecnologia da informação da Justiça Eleitoral e Conformidade com normas de gestão de segurança da informação.

7.4. Alinhamento em relação às necessidades

A solução escolhida se alinha perfeitamente com as necessidades do negócio e com os requisitos tecnológicos.

7.5. Relação entre a demanda prevista e a quantidade dos bens e/ou serviços a serem contratados

Devido a tendência natural de aumento da quantidade de contas ativas no Active Directory do tribunal optamos pela modalidade de Registro de preços nos quantitativos previstos e registrados na tabela abaixo baseada na melhor solução.

Lote	Item		Unidade	Quantidade Total Registrada	Valor Unitário	Valor Total

1	1	Licença de subscrição de solução de auditoria do Active Directory por conta ativa de usuário do AD, durante 60 meses de uso e suporte do fabricante.	Licenças	2000	R$ 457,00	R$ 914.000,00
	2	Serviço de Instalação e Configuração.	Serviço	1	R$ 11.823,00	R$ 11.823,00
	3	Repasse Tecnológico de 20 horas para 10 alunos.	Serviço	1	R$ 9.853,00	R$ 9.853,00
	4	Suporte Técnico Especializado de primeiro nível por 60 meses.	Serviço	1	R$ 9.853,00	R$ 9.853,00
1	**VALOR TOTAL DO LOTE**					**R$ 945.529,00**

8. Necessidades de Adequação do Ambiente do Órgão

Não haverá necessidade de adequação do ambiente, tendo em vista que a contratação não alterará em nada o ambiente atualmente em uso.

Seção II - SUSTENTAÇÃO DO CONTRATO

Como não há nenhuma consideração a ser feita no tocante à estratégia de sustentação do contrato, estaremos suprimindo esta parte.

Seção III - ESTRATÉGIA PARA A CONTRATAÇÃO

9. Natureza do objeto

Trata-se de uma subscrição de uso de software, cujo uso é comum a diversas instituições da Administração Pública Federal, sendo assim um padrão de mercado.

10. Parcelamento do objeto

O objeto será composto por quatro itens que deverão ser fornecidos pela mesma empresa.

11. Adjudicação do objeto

A adjudicação do objeto será feita por lote único, tendo em vista que os itens do lote compõem uma solução global, interdependente e indivisível.

12. Modalidade e tipo de licitação

Após realização dos estudos técnicos chegou-se aos seguintes quantitativos de material, descrito por meio da tabela do item 6.2, a serem licitados em dois lotes único (por se tratar de soluções distintas e indivisíveis) e através do sistema de Registro de Preços (por não ser possível precisar de início o quantitativo a ser pedido durante a vigência da ata):

13. Classificação e indicação orçamentária

Recursos suplementares de cibersegurança oriundos de iniciativa do TSE

3.3.90.40.21.0021 - SERVIÇOS TÉCNICOS PROFISSIONAIS DE TIC

14. Vigência da prestação de serviço

A vigência dos itens registrados será de 60 meses.

15. Equipe de Apoio à Contratação

A equipe de apoio à contratação será composta pela mesma equipe do presente estudo preliminar constante do item 02 deste documento.

16. Equipe de Gestão da Contratação

Sugerimos como gestor titular do contrato o servidor Felipe Cavalcanti Alves e o substituto o servidor Adailton Ventura da Silva.

Seção IV - ANÁLISE DE RISCOS

17. Riscos do Processo de Contratação

Os riscos do processo da contratação e as respostas aos mesmos estão descritos na planilha 1249768.

FELIPE CAVALCANTI ALVES
CHEFE DA SEÇÃO DE SEGURANÇA CIBERNÉTICA

Documento assinado eletronicamente por FELIPE CAVALCANTI ALVES em 10/05/2022, às 15:30, 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 10/05/2022, às 15:42, 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 10/05/2022, às 17:00, 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 informando o código verificador **1254792** e o código CRC **8AF6DE98**.