TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS
Avenida Aristeu de Andrade nº 377 - Bairro Farol - CEP 57051-090 - Maceió - AL

Termo de Referência - TIC nº 28 / 2020

Termo de Referência - Soluções de Tecnologia da Informação

QUADRO RESUMO

01. Objeto	Formação de Ata de Registro de Preços para Solução unificada de gestão de vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo aquisição de serviços de software e suporte técnico, de acordo com as quantidades, especificações e condições descritas neste Termo de Referência.
02. Quantidade(s)	

Lote 1

Item	Qtd Registrada	Pedido Inicial	CATMAT/CATSER	Descrição
1	1	0	24333	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 128 endereços IP, por 36 meses de uso e suporte pelo fabricante.
2	1	0	24333	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 128 endereços IP, por 60 meses de uso e suporte pelo fabricante.
4	1	0	24333	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por 36 meses de uso e suporte pelo fabricante.
5	1	0	24333	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos

				de rede, contemplando no mínimo 250 endereços IP, por 60 meses de uso e suporte pelo fabricante.
6	1	0	24333	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 500 endereços IP, por 36 meses de uso e suporte pelo fabricante.
7	1	0	24333	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 500 endereços IP, por 60 meses de uso e suporte pelo fabricante.
8	1	0	24333	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 36 meses de uso e suporte pelo fabricante.
9	1	0	24333	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 60 meses de uso e suporte pelo fabricante.
10	1	0	24333	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 10 domínios (FQDN), por 36 meses de uso e suporte pelo fabricante.
11	1	0	24333	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 10 domínios (FQDN), por 60 meses de uso e suporte pelo fabricante.
12	1	0	26972	Instalação e configuração da solução.
13	1	0	26972	Repasse tecnológico, com período mínimo de 20 horas.
14	50	0	26972	4 Horas de Serviço Especializado.

03. Resumo da Especificação do Objeto	Os descritivos dos itens que compõem o lote já resumem de forma adequada,
04. Valor Estimado	Conforme os Estudos Preliminares (doc. 0778219), valor a ser confirmado pela SEIC.

05. Justificativa	Com o auto grau de dependência de ativos de tecnologia da informação para fornecimento de serviços e sistemas (SEI, ELO, acesso à Internet. Intranet, ASI, sistema de diárias, SADP, SJUR, etc.) se faz necessário adotar ferramentas avançadas que possibilitem o gerenciamento e monitoramento de vulnerabilidades no ambiente de TIC.
06. Prazo de Entrega	O prazo máximo para o fornecimento é de 05 (cinco) dias úteis após o recebimento da ordem de fornecimento, nota de empenho ou documento equivalente.
07. Adjudicação	Por Lote. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao principio 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 em cada lote deverão ser fornecidos por um único fabricante, o qual será responsável também pelo suporte e garantia da plataforma como um todo.
08. Classificação Orçamentária	(A cargo da COFIN). Sugere-se custeiro de TI.
09. Local de Entrega	Deve ser realizada por meio eletrônico para o e-mail coinf@tre-al.jus.br.
10. Unidade Fiscalizadora	SEGI/COINF/STI
11. Unidade Gestora	SEGEC/COMAP/SAD
12. Sanções Administrativas	Vide Item 3.2 Forma de Execução e de Gestão do Contrato (Art. 18, § 3º, III, a) Subitem Penalidades (Art. 18, § 3º, III, a, 11)
13. Prazo de Pagamento	Vide Item 3.2 Forma de Execução e de Gestão do Contrato (Art. 18, § 3º, III, a) Subitem Forma de Pagamento (Art. 18, § 3º, III, a, 7)
14. Estratégia de Recebimento	Vide Item 3.2 Forma de Execução e de Gestão do Contrato (Art. 18, § 3º, III, a) Subitem Recebimento do Objeto:
15. Modalidade e Tipo de Licitação	Vide 2.11 Modalidade, Tipo de Licitação, Critérios de Habilitação e Atendimento aos Requisitos (Art. 18, § 3º, II, j, IV e V)

1. OBJETO (Art. 18, §3º,I):

Solução unificada de gestão de vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo aquisição de serviços de software e suporte técnico, de acordo com as quantidades, especificações e condições descritas neste Termo de Referência.

1.1 Definição (Art. 18, §3º, I)

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO (Art. 18, § 3º, II)

2.1 Motivação (Art. 18, § 3º, II, a)

A área de Tecnologia da Informação e Comunicação - TIC - se tornou crítica para organizações de qualquer tamanho ou ramo de atuação. Assim, no âmbito do TRE/AL, qualquer perda de dados ou informações pode causar o comprometimento da imagem e dos serviços prestados por este órgão, com efeito no plano interno e no atendimento ao público.

Neste contexto, é de extrama necessidade a utilização de compoentnes para ssolução de gestão de vulnerabilidades para diminuir a superfície de ataques quanto aos ativos de TIC gerenciados.

2.2 Objetivos (Art. 18, § 3º, II, b)

Implementar uma solução de software capaz de testar os ativos de TI e as aplicações web periodicamente em busca de quaisquer vulnerabilidades, sejam elas relativas a atualização de sistemas operacionais e servidores de aplicação, configurações de serviços ou outras falhas técnicas. Além disso, é preciso que a solução forneça relatórios para que seja possível o acompanhamento deste trabalho de identificação e mitigação de riscos.

2.3 Benefícios (Art. 18, § 3º, II, c)

Gerenciamento de vulnerabilidades, 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.

2.4 Alinhamento Estratégico (Art. 18, § 3º, II, d)

1. Planejamento Estratégico Institucional (PEI): melhoria da infraestrutura e governança de tecnologia da informação;

2. Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC): viabilizar serviços e soluções de TIC;

Alinhamento com os Objetivos Estratégicos de TIC da Justiça Eleitoral de Alagoas – 2017/2022 nos seguintes aspectos:

1. Viabilizar serviços e soluções de TIC; e
2. Aprimorar a segurança da informação.

3. Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC):

a) aprimorar as medidas de segurança do serviço de acesso à rede ;

b) aprimorar as medidas de segurança do serviço de conexão de dados ;

c) aprimorar as medidas de segurança de dados .

Há,igualmente, alinhamento com o Plano de Contratações de TIC/2022

Item 09 - Softwares de Gerenciamento de Rede e de Inventário e

Item 11 - Software para gerenciamento de logs

2.5 Referência aos Estudos Preliminares (Art. 18, § 3º, II, e)

Este Termo de Referência foi elaborado considerando o Documento de Oficialização de Demanda (DOD), demais instruções e os Estudos Preliminares constantes do Procedimento SEI nº 0007757-43.2020.6.02.8000.

2.6 Relação entre a Demanda Prevista e a Contratada (Art. 18, §3º, II, f)

A estimativa inicial para a pretendida contratação necessária para atender à demanda do TRE/AL, foi realizada durante a fase de Estudos Preliminares e visa minimizar ricsco sdecorrente de falhas em servidores, equipamentos, serviços e sistemas deste Regional, bem assim alta disponibilidade de sistemas e serviços informatizados.

2.7 Análise de Mercado de TIC (Art. 18, § 3º, II, g)

Conforme destalhado nos Estudos Preliminares, existem vários fabricantes que comercializam soluções que são aderentes às especificações técnicas exigidas**.**

2.8 Natureza do Objeto (Art. 18, § 3º, II, h)

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;

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.

2.9 Parcelamento e Adjudicação do Objeto (Art. 18, § 3º, II, i)

Não haverá parcelamento.

Adjudicação será por Lote.

2.10 Vigência

A depender do item.

2.11 Modalidade, Tipo de Licitação, Critérios de Habilitação e Atendimento aos Requisitos (Art. 18, § 3º, II, j, IV e V)

A aquisição pretendida deverá ser realizada por meio de licitação do tipo Pregão Eletrônico, como é de praxe neste Regional, salvo entendimento superior contrário.

A sugestão da equipe de planejamento, por se tratar de fornecimento de serviço, é pela contratação por licitação via pregão.

O DECRETO Nº 7.174, DE 12 DE MAIO DE 2010 que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União deve ser aplicado nesta aquisição por se tratar de bem de informática.

A ressalva que a equipe aponta é em relação ao artigo 3º, item II que versa sobre a necessidade de exigências, na fase de habilitação, de certificações emitidas por instituições públicas ou privadas credenciadas pelo Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (Inmetro), que atestem, conforme regulamentação específica, a adequação à segurança para o usuário e instalações, compatibilidade eletromagnética e consumo de energia.

Tal exigência inviabiliza e restringe a competição deste certame, vez que a certificação para este tipo de produto, segundo o próprio INMETRO, é voluntária, conforme Portaria Inmetro n.º 170 de 10/04/2012.

(fonte:http://www.inmetro.gov.br/legislacao/rtac/pdf/RTAC001808.pdf).

pretendida deverá ser realizada por meio de licitação do tipo Pregão Eletrônico, como é de praxe neste Regional, salvo entendimento superior contrário.

A sugestão da equipe de planejamento, por se tratar de fornecimento de equipamento, é pela contratação por licitação via pregão.

O DECRETO Nº 7.174, DE 12 DE MAIO DE 2010 que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União deve ser aplicado nesta aquisição por se tratar de bem de informática.

A ressalva que a equipe aponta é em relação ao artigo 3º, item II que versa sobre a necessidade de exigências, na fase de habilitação, de certificações emitidas por instituições públicas ou privadas credenciadas pelo Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (Inmetro), que atestem, conforme regulamentação específica, a adequação à segurança para o usuário e instalações, compatibilidade eletromagnética e consumo de energia.

Tal exigência inviabiliza e restringe a competição deste certame, vez que a certificação para este tipo de produto, segundo o próprio INMETRO, é voluntária, conforme Portaria Inmetro n.º 170 de 10/04/2012.

(fonte:http://www.inmetro.gov.br/legislacao/rtac/pdf/RTAC001808.pdf).

2.12 Adequação do Ambiente (Art. 18, § 3º, II, k)

Não se aplica por se tratar solução baseada em appliance virtual..

2.13 Conformidade Técnica e Legal (Art. 18, § 3º, II, l)

Será realizada, por equipe designada pelo TRE/AL, a verificação de conformidade no momento da entrega da documentação de contratação.

2.14 Obrigações do Contratante (Art. 18, § 3º, II, m)

1. Efetuar o pagamento à Contratada, após o recebimento definitivo;
2. Acompanhar e fiscalizar a execução do objeto e do(s) contrato(s) dela decorrentes, por meio de servidor(es) designado(s), de modo a garantir o fiel cumprimento do mesmo e da proposta;
3. Manter arquivo, junto ao processo administrativo ao qual está vinculado o presente termo, toda a documentação referente ao mesmo;
4. Proporcionar todas as facilidades indispensáveis à boa execução das obrigações contratuais; e
5. Aplicar as sanções conforme previsto no contrato, assegurando à Contratada o contraditório e ampla defesa.

2.15 Obrigações da Contratada (Art. 18, § 3º, II, m)

As obrigações abaixo são aplicáveis ao objeto a ser contratado.

1. Fornecer o(s) serviços(s) e/ou produto(s) conforme especificações, quantidades, prazos e demais condições estabelecidas no Edital, na Proposta e no Contrato;
2. Fornecer a documentação necessária à instalação e à operação dos produtos (manuais, termos de garantia, etc.), completa, atualizada e em português do Brasil, caso exista, ou em inglês;
3. Disponibilizar Central de Atendimento para a abertura e fechamento de chamados técnicos, conforme períodos, horários e condições estabelecidas no Edital e em seus Anexos;
4. Comunicar formal e imediatamente ao Gestor ou Responsável Técnico da Administração sobre mudanças nos dados para contato com a Central de Atendimento;
5. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo representante da Administração, referentes a qualquer problema detectado ou ao andamento de atividades da garantia;
6. Responder por quaisquer prejuízos que seus profissionais causarem ao patrimônio da Administração ou a terceiros, por ocasião da execução do objeto, procedendo imediatamente aos reparos ou às indenizações cabíveis e assumindo o ônus decorrente;
7. Responsabilizar-se integralmente pelo fornecimento dos equipamentos e pela execução dos serviços de garantia técnica, primando pela qualidade, desempenho, eficiência e produtividade na execução dos trabalhos, dentro dos prazos estipulados e cujo descumprimento será considerado infração passível de aplicação das penalidades previstas neste Termo de Referência;

8. Comunicar ao Gestor ou Responsável Técnico, formal e imediatamente, todas as ocorrências anormais e/ou que possam comprometer a execução do objeto;
9. Manter sigilo sobre todo e qualquer assunto de interesse da Administração ou de terceiros de que tomar conhecimento em razão da execução do objeto, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa;
10. Cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação do TRE/AL;
11. Responsabilizar-se pela conservação dos ambientes onde desempenhe as atividades necessárias para prestar a garantia on-site.
12. Prestar as informações e os esclarecimentos que venham a ser solicitados pela Administração, referentes a qualquer problema detectado ou ao andamento de atividades da garantia técnica.

DETALHAMENTO DO OBJETO (Art. 18, § 3º, III)

3.1 Descrição do Objeto

REQUISITOS GERAIS

Características técnicas mínimas:

1. A solução deve estar licenciadas e inclusas todas as funcionalidades para realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance), indícios e padrões de códigos maliciosos conhecidos (malware);
2. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;
3. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;
4. Deve ser capaz de identificar no mínimo 50.000 CVEs (Common Vulnerabilities and Exposures);
5. A solução deve ter a capacidade de adicionar etiquetas (tags) aos ativos de maneira automática, manual e possibilitar o uso de regras com parâmetros específicos para aplicação das mesmas;
6. Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score;
7. A solução deve calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança, sistema e conformidade, bem como hierarquias e prioridades;
8. A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades;
9. A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente;
10. Deve possuir um sistema de busca de informações de um determinado ativo com no mínimos as seguintes características:
    1. Por sistema operacional;
    2. Por um determinado software instalado;
    3. Por Ativos impactados por uma determinada vulnerabilidade.
11. A solução deve possuir suporte para a adição de detecções personalizadas usando o OVAL (Open Vulnerability Assessment Language);
12. Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;
13. Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;
14. A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades;
15. A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina (machine learning) para analisar as características relacionadas a vulnerabilidades;
16. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
    1. CVSSv3 Impact Score;
    2. Idade da Vulnerabilidade;
    3. Se existe ameaça ou exploit que explore a vulnerabilidade;
    4. Número de produtos afetados pela vulnerabilidade;
17. Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindo feeds de inteligência de ameaças ao vivo;
18. Deve possuir uma API para automação de processos e integração com aplicações terceiras permitindo, no mínimo, a extração de dados para carga no SIEM.
19. Deve possuir uma API para automação de processos e integração com aplicações ITSM do órgão para as vulnerabilidades encontradas, permitindo o agrupamento no chamado por ações corretivas;
20. A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;
21. A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e HTML;
22. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
23. A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real;

24. A solução deve possuir sensores, no mínimo, com as seguintes funcionalidades:
    1. Execução de verificação completa do sistema (rede), adequada para qualquer host;
    2. Verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação;
    3. Autenticação de hosts e enumeração de atualizações ausentes;
    4. Execução de varredura simples para descobrir hosts ativos e portas abertas;
    5. Utilização de um scanner para verificar aplicativos da web;
    6. Avaliação de dispositivos móveis
    7. Auditoria de configuração de serviços em nuvem de terceiros;
    8. Auditoria de configuração dos gerenciadores de dispositivos móveis;
    9. Auditoria de configuração dos dispositivos de rede;
    10. Auditoria de configurações do sistema em relação a uma linha de base conhecida;
    11. Detecção de desvio de segurança Intel AMT;
    12. Verificação de malware nos sistemas Windows e Unix;
25. Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;
26. A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no mínimo:
    1. Bancos de dados;
    2. Hypervisors (no mímino VMWare ESX/ESXi);
    3. Dispositivos móveis;
    4. Dispositivos de rede;Endpoints;
    5. Aplicações;
27. A solução deve ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento de rede;
28. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;
29. A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk.
30. 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.
31. A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.
32. Configuração de segurança e acesso à gerência da solução:
    1. Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;
    2. Os dados em trânsito devem usar ao menos o algoritmo TLS 1.2 de chave 2048 bits;
    3. Os dados em trânsito devem ser criptografados ao menos com o algoritmo AES-128 bits;
    4. Os algoritmos de hash devem usar ao menos o algoritmo SHA-256;
    5. Será aceito como comprovação critérios de criptografia publicação em site do fabricante ou declaração do próprio fabricante;
    6. Os dados armazenados devem ser criptografados ao menos com o algoritmo AES-256 bits;
    7. Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;
    8. A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;
    9. A empresa contratada não deverá ter acesso a rede interna da contratante e todo trafego de dados deverá ser de saída e iniciado pelos scanners (on-premise).
33. Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.
34. Dos Relatórios:
    1. Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como ageração de relatórios sob demanda;
    2. A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes;
    3. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);
    4. A solução deve suportar o envio automático de relatórios para destinatários específicos;
    5. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
    6. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
    7. A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;
    8. A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;
35. A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;
36. A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:
    1. Hosts verificados sem credenciais;
    2. Top 100 Vulnerabilidades mais criticas;

3. Top 10 Hosts infectados por Malwares;
4. Hosts exploráveis por Malwares;
5. Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
6. Vulnerabilidades críticas e exploráveis;
7. Máquinas com vulnerabilidades que podem ser exploradas;

37. A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;
38. A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.
39. 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.

ESPECIFICAÇÕES TÉCNICAS COMUNS DO LOTE 01

Características técnicas mínimas:

1. Os Solução do lote 02 deverá possuir gerenciamento e armazenamento dos dados na rede local do tribunal, com scanners próprios localizados e instalados na infraestrutura do cliente (on-premise).
2. A aquisição da plataforma de software de gestão de vulnerabilidades é pré-requisito para a contratação do módulo de análise dinâmica de aplicações web.
3. Caso a licença da plataforma de software de gestão de vulnerabilidades contemple a análise dinâmica de aplicações web o licitante deverá apresentar R$ 0,00 (zero reais) como o preço dos itens relacionados a análise dinâmica de aplicações web (itens 20, 21, 22, 23 do lote 02).
4. A solução proposta no lote 02 deve ser de mesmo fabricante, sem adaptações ou alterações não efetuadas pelo fabricante, disponível para gerenciamento em console central unificado.
5. A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o período de garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução;
6. A aquisição dos itens poderá ser composta em relação ao tempo e a quantidade de ativos e aplicações Web:
    1. Para uma solução, por 3 anos, deverão ser adquiridos uma combinação dos itens 1,3,5,7 e 9. Por exemplo, para atender 250 ativos e 15 aplicações web (FQDNs simultâneos), por 3 anos, serão adquiridos os itens 3, 7 e 9.
    2. Para uma solução, por 5 anos, deverão ser adquiridos uma combinação dos itens 2,4,6,8 e 10. Por exemplo, para atender 378 ativos e 10 aplicações web (FQDNs simultâneos), por 5 anos, serão adquiridos os itens 2,3 e 10.

Garantia e suporte técnico:

1. Os softwares e licenças fornecidos deverão estar cobertos por garantia que ofereça atualizações necessárias para a correção de vícios, pelo período especificado no termo de referência, a contar da data do aceite provisório do software, conforme Art. 73, I, “a”, da Lei 8.666/1993;
2. O suporte pelo fabricante será obrigatório;
3. O suporte pela CONTRATADA será opcional e ela poderá subcontratar uma empresa autorizada pelo fabricante para prestar o suporte técnico de primeiro nível;
4. Devem estar explícitos na proposta os part numbers de garantia oficial do fabricante no Brasil;
5. O tempo da garantia e suporte técnico dos lotes 1 e 2 estarão explicitadas nas especificações específicas dos respectivos itens.
6. 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;
7. 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 Especializado registrado no item 12;
8. Os chamados telefônicos deverão estar disponibilizados de segunda à sexta-feira, das 8 às 18 horas, adotando-se para tanto o horário de Brasília;
9. O tempo para a resposta dos chamados dependerá da severidade do problema conforme abaixo:
    1. 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);

Atualizações:

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 constante do termo de referência (36 meses ou 60 meses, a depender da garantia explicitada para o item em questão), sem qualquer ônus adicional para o contratante;
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.

CARACTERÍSTICAS DA PLATAFORMA DE SOFTWARE PARA GESTÃO DE VULNERABILIDADES DOS ITENS 1,2,3,4,5, 6 e 7
Características técnicas mínimas:

1. A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades, de acordo com a quantidade de endereços IP licenciados;
2. A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);
3. Deve permitir a configuração de vários painéis e widgets;
4. Deve ser capaz de medir e reportar ameaças;
5. Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;
6. A plataforma de software deve realizar varreduras em uma variedade de sistemas operacionais, suportando pelo menos hosts baseados em Windows, Linux e Mac OS, bem como appliances virtuais;
7. A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;
8. A plataforma de software deve fornecer agentes instaláveis em sistemas operacionais, pelo menos Windows, Linux e Mac OS, para o monitoramento contínuo de configurações e vulnerabilidades;
9. A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.
10. A plataforma de software deve permitir o monitoramento sem a necessidade de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.
11. A plataforma de software deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia;
12. No caso onde uma atividade de varredura seja interrompida por invadir o período não permitido, o mesmo deve ser capaz de ser reiniciado de onde parou;
13. A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;
14. A plataforma de software deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;
15. A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
16. A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais.

CARACTERÍSTICAS COMUNS DO MÓDULO DE ANÁLISE DINÂMICA EM APLICAÇÕES WEB ITENS 8,9,10 e 11
Características técnicas mínimas:

1. A solução de análise deve realizar varreduras de vulnerabilidades em aplicações Web, cobrindo no mínimo, mas não limitando-se a base de ameaças apontadas pelo OWASP Top 10, CWE e WASC;
2. A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web;
3. A solução de análise deverá ser capaz de executar varreduras em sistemas Web através de seus endereços IP ou FQDN (DNS);
4. A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal;
5. Para varreduras do tipo extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:
    1. Cookies, Headers, Formulários e Links;
    2. Nomes e valores de parâmetros da aplicação;
    3. Elementos JSON e XML;
    4. Elementos DOM;
6. Deverá também permitir a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;
7. A solução de análise deve suportar a integração com o softwares de automação de testes para permitir sequências de autenticação complexas;
8. A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamente limitadas ao número de licenças;
9. A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada anteriormente no aplicativo Web;
10. Deve ser capaz de utilizar scripts customizados de crawling com parâmetros definidos pelo usuário;
11. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;

12. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;
13. Deve ser capaz de instituir no mínimo os seguintes limites:
    1. Número máximo de URLs para crawling e navegação;
    2. Número máximo de diretórios para varreduras;
    3. Tamanho máximo de respostas;
    4. Tempo máximo para a varredura;
14. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
15. Deve suportar o envio de notificações por email;
16. Deverá ser compatível com avaliação de web services REST e SOAP;
17. A solução de análise deve suportar os seguintes esquemas de autenticação:
    1. Autenticação Básica (Digest);
    2. NTLM;
    3. Autenticação de Cookies;
18. A solução de análise deve ser capaz de exibir os resultados das varreduras de forma temporal para acompanhamento de correções e introdução de novas vulnerabilidades;
19. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
20. Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências;
21. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;
22. A solução de análise deve fornecer relatórios de resumo geral de todas as aplicações web e resumo de uma aplicação específica, que serão exportados para os formatos XML, HTML ou PDF.
23. A solução deve ser capaz de realizar varreduras nos seguintes componentes/aplicações:
    1. WordPress;
    2. IIS 6.x e IIS 10.x;
    3. ASP 6;
    4. NET 2;
    5. Apache HTTPD 2.2.x e 2.4.x;
    6. Tomcat 6.x, 7.x, 8.x e superiores;
    7. Jetty 8 e superiores;
    8. Nginx;
    9. PHP 5.3.x, 5.4.x, 5.6.x, 7.0.x e 7.1.x e superiores;
    10. Java 1.5, 1.6, 1.7 e 1.8 e superiores;
    11. Jboss 4.x e 7.x e superiores;
    12. WildFly 8 e 10 e superiores;
    13. Plone 2.5.x e 4.3.x e superiores;
    14. Zope;
    15. Python 2.4.4 e superiores;
    16. J2EE;
    17. Ansible;
    18. Joomla;
    19. Moodle;
    20. Docker Conteiner;
    21. Elk;
    22. GIT;
    23. Grafana; e
    24. Redmine.

CARACTERÍSTICAS DO ITEM 12

Características técnicas mínimas:

1. Efetuar as configurações iniciais, em conjunto com a Contratante, para uso da solução proposta, incluindo criação de scans, relatórios, filtros, permissões de usuários e demais funcionalidades da solução;
2. Apoio na instalação de scanners e agentes on-premises;
3. A instalação e configuração da solução poderá ser feita por meio de acesso remoto;
4. A CONTRATADA deverá aceitar as especificações de softwares e protocolos de segurança estabelecidos pela CONTRATANTE para a realização do acesso remoto;
5. Não serão aceitos softwares “beta” ou em desenvolvimento;
6. Somente será aceita a instalação por técnico certificado na fabricante da solução, da CONTRATADA ou do fabricante;
7. A CONTRATADA deverá elaborar documentação, contendo no mínimo os seguintes itens:
    1. Cronograma;
    2. Levantamento de informações sobre o ambiente atual;
    3. Definição dos parâmetros de configuração básicos e avançados a serem implementados;
    4. Mapa de rede contendo a topologia a ser implementada ou atualizada;
    5. Gerenciamento de mudanças, contemplando análise de riscos de implementação da solução;
8. Procedimentos de implementação e de rollback no caso de problemas não previstos previamente.
9. A CONTRATADA poderá subcontratar uma empresa autorizada pelo fabricante para atender as atividades relacionadas ao

CARACTERÍSTICAS DO ITEM 13
Características técnicas mínimas:

1. A contratada deverá ministrar treinamento, na língua portuguesa, para até 10 (dez) servidores indicados pelo órgão, com carga horária mínima de 20 horas.
2. O conteúdo do treinamento a ser ministrado deverá contemplar os seguintes itens:
    1. Procedimentos de instalação física e lógica;
    2. Todos os procedimentos necessários à configuração técnica;
    3. Todos os procedimentos necessários à completa operação do produto; e
    4. Todos os procedimentos de manutenção do produto que devem ser realizados pelos técnicos do órgão.
3. O treinamento poderá ser realizado virtualmente por profissional certificado pelo fabricante do produto ofertado;
4. O treinamento deverá ser ministrado em horário definido pelo tribunal, em dias úteis;
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.
6. A CONTRATADA poderá subcontratar uma empresa autorizada pelo fabricante para atender as atividades relacionadas ao Repasse Tecnológico.

CARACTERÍSTICAS DO ITEM 14
Características técnicas mínimas:

1. A operação assistida e consultoria especializada será solicitada pela contratante sob demanda e prestada por meio de acesso remoto, 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:
    1. Acompanhar, quando solicitado por um usuário, todas as operações realizadas no sistema durante determinado período de tempo;
    2. Esclarecer dúvidas de usuários em relação à operação do sistema;
    3. Prestar serviços de suporte técnico para a solução de problemas que impeçam o perfeito funcionamento do sistema;
    4. Reportar à Coordenação de informática do órgão quaisquer outros problemas verificados durante o atendimento, relativos ou não à solução fornecida;
    5. Fornecer informações aos usuários sobre a situação e o andamento de serviços de manutenção solicitados;
    6. Diagnosticar a performance do software em seus aspectos operacionais;
    7. Identificar problemas inerentes ao software e ao ambiente onde este se encontra instalado;
    8. Discutir implementações de melhorias, visando possíveis adequações;
    9. Na prestação dos serviços de operação assistida, a Contratada deverá utilizar profissionais com qualificação e treinamento adequados para o desenvolvimento das tarefas relacionadas anteriormente;
    10. apoio no desenvolvimento de dashboad´s e solução de problemas internos, relativos às licenças adquiridas.

11. Integração da solução com ferramentas de ITSM.
12. Documentação e transferência de conhecimento das atividades técnicas realizadas.

2. A CONTRATADA deverá aceitar as especificações de softwares e protocolos de segurança estabelecidos pela CONTRATANTE para a realização do acesso remoto.
3. O licitante poderá apresentar R$ 0,00 (zero reais) como o preço dos itens relacionados ao Bloco de 04 Horas de Serviço Especializado caso os serviços elencados estejam incluídos no preço da solução ofertada da ferramenta de gestão de vulnerabilidades;
4. A CONTRATADA poderá subcontratar uma empresa autorizada pelo fabricante para atender as atividades relacionadas ao Bloco de 04 Horas de Serviço Especializado;

3.2 Forma de Execução e de Gestão do Contrato (Art. 18, § 3º, III, a)

A execução do objeto pressupõe a existência dos seguintes papéis e responsabilidades (Art. 18, § 3º, III, a, 1):

1. Patrocinador da Contratação: é o titular da área demandante, responsável por representar os interesses do órgão no contexto da Contratação, pela aprovação da necessidade e, por fim, pela negociação das ações necessárias para que os objetivos sejam alcançados;
2. Gestor do Contrato (art. 3º, IV, da Resolução TRE/AL nº 15.787/2017): servidor designado para coordenar e comandar o processo da fiscalização da execução contratual. Na forma do Art. 17 da mesma Resolução, o gestor do contrato responsabiliza-se pela condução da gestão e fiscalização do contrato, nos termos do Art. 67, da Lei nº 8.666/93.
3. Fiscal do Contrato (art. 3º, VI, da Resolução TRE/AL nº 15.787/2017): servidor designado para auxiliar o gestor do contrato quanto à fiscalização do objeto do contrato. Neste sentido, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos técnicos da solução.

Dinâmica da Execução (Art. 18, § 3º, III, a, 2):

1. Os serviços ser entregues por meio eletrônico diretamente à unidade demandante;
2. A garantia dos serviços deve obedecer o detalhamento técnico feito e terá seu tempo contado por cada fornecimento individualmente;
3. Entende-se como garantia aquela prestada pelo próprio fabricante ou por rede credenciada pelo fabricante do(s) referido(s) serviço(s);
4. O pagamento será realizado individualmente para cada nota fiscal apresentada, após emissão do aceite definitivo pela unidade competente do TRE/AL;
5. Os serviços deverão atender rigorosamente a todas as especificações técnicas contidas neste Termo de Referência e em seus Anexos;
6. Ao TRE/AL é reservado o direito de efetuar diligência, a qualquer tempo, quanto aos documentos exigidos neste Termo de Referência e em seus Anexos.

Recebimento do Objeto:

1. O Tribunal designará Comissão para realizar o recebimento provisório, que só será emitido se os serviços estiverem de acordo com as especificações técnicas;
2. Após a entrega, os serviços serão submetidos à avaliação e homologação pelos responsáveis técnicos do Tribunal;
3. As especificações serão avaliadas também por meio de documentos técnicos, informações fornecidas pela Contratada e disponível no sítio do fabricante.
4. A comissão do Tribunal deverá, após a comprovação da adequação às especificações técnicas, emitir e assinar o Termo de Recebimento Definitivo.

Instrumentos Formais de Solicitação do(s) Bens e/ou Serviço(s) (Art. 18, § 3º, III, a, 3):

1. O envio da nota de empenho à licitante ganhadora será o instrumento formal de solicitação dos bens pertencentes ao escopo desta contratação.

Recebimento (Art. 18, § 3º, III, a, 6)

O recebimento, via de regra, ocorrerá com a verificação junto ao fabricante da solução das licenças fornecidas e o atesto pela comissão de recebimento quanto aos serviços prestados.

Forma de Pagamento (Art. 18, § 3º, III, a, 7)

1. O pagamento será efetuado mediante crédito em conta-corrente do Fornecedor, por ordem bancária, no prazo disposto nos artigos 5º, § 3º, ou 40, XIV, "a", da Lei n. 8.666/93, conforme o caso, quando mantidas as mesmas condições iniciais de habilitação e cumpridos os seguintes requisitos:
    a. Apresentação de nota fiscal de acordo com a legislação vigente à época da emissão (nota fiscaleletrônica, se for o caso), acompanhada da Certidão Negativa de Débito – CND, comprovando regularidade com o INSS; do Certificado de Regularidade do FGTS – CRF, comprovando regularidade com o FGTS; da Certidão Conjunta Negativa de

Débitos Relativos a Tributos Federais e à Dívida Ativa da União, expedida pela Secretaria da Receita Federal; e da Certidão Negativa de Débitos Trabalhistas – CNDT, emitida pela Justiça do Trabalho; e da prova de regularidade para com as Fazendas Estadual e Municipal do domicílio ou sede do Fornecedor; e

b. Inexistência de fato impeditivo para o qual tenha concorrido o Fornecedor.

2. Nenhum pagamento será efetuado à Contratada enquanto pendente de liquidação qualquer obrigação. Esse fato não será gerador de direito a reajustamento de preços ou a atualização monetária.

Direitos de Propriedade Intelectual (Art. 18, § 3º, III, a, 9):

1. Esse requisito não se aplica ao contexto desta contratação, uma vez que o objeto se refere ao fornecimento de software, cujos direitos autorais do fabricante são resguardados por legislação nacional e internacional.

Penalidades (Art. 18, § 3º, III, a, 11):

1. Com fundamento no artigo 7º da Lei nº 10.520/2002 e, subsidiariamente, nos artigos 86 e 87 da Lei 8.666/1993, a Contratada ficará sujeita, assegurada prévia e ampla defesa, às seguintes penalidades:
    1. Advertência:
        1. A Contratada será notificada formalmente em caso de descumprimento de obrigação contratual e terá que apresentar as devidas justificativas em um prazo de até 5 (cinco) dias úteis após o recebimento da notificação; e
        2. Caso não haja manifestação dentro desse prazo ou se entenda serem improcedentes as justificativas apresentadas, a Contratada será advertida;
    2. Multa de:
        1. 0,25% por dia, sobre o valor constante da Nota de Empenho ou instrumento contratual, no caso de atraso injustificado na entrega do bem, limitada a incidência a 20 (vinte) dias corridos;
            1. No caso de atraso injustificado na entrega dos bens por prazo superior a 20 (vinte) dias corridos, com a aceitação pela Administração, será aplicada a multa de 7,5% sobre o valor da Nota de Empenho ou instrumento contratual; e
            2. No caso de atraso injustificado na entrega do bem por prazo superior a 20 (vinte) dias corridos, com a não aceitação pela Administração, será aplicada a penalidade 12,5% sobre o valor da Nota de Empenho ou instrumento contratual, no caso de inexecução total da obrigação, podendo haver, ainda, o cancelamento do instrumento de fornecimento;
        2. 5% sobre o valor constante da Nota de Empenho ou instrumento contratual, no caso de inexecução parcial da obrigação assumida;
        3. 15% sobre o valor da Nota de Empenho ou instrumento contratual, no caso de inexecução total da obrigação, podendo haver, ainda, o cancelamento do instrumento de fornecimento.
    3. Impedimento de licitar e contratar com a União e descredenciamento do SICAF pelo prazo de até 5 (cinco) anos, sem prejuízo das demais penalidades legais; e
    4. Declaração de inidoneidade para licitar ou contratar com a Administração Pública.
2. O cometimento reiterado de atrasos injustificados dos prazos previstos para entrega/solução de ocorrências poderá resultar no cancelamento do instrumento de fornecimento com a Contratada.
3. As sanções previstas nos itens "1.a", “1.c” e “1.d” do item 1 poderão ser aplicadas, cumulativamente ou não, à pena de multa.
4. O valor da multa, aplicada após o regular processo administrativo, será descontado de pagamentos eventualmente devidos à contratada ou cobrado judicialmente;
5. Excepcionalmente, ad cautelam, a Administração poderá efetuar a retenção do valor presumido da multa, antes da instauração do regular procedimento administrativo.
6. Se a Contratada não recolher o valor da multa que lhe for aplicada, dentro de 5 (cinco) dias úteis a contar da data da intimação para o pagamento, a importância será descontada automaticamente, ou ajuizada a dívida, consoante o § 3º do art. 86 e § 1º do art. 87 da Lei nº 8.666/93, acrescida de juros moratórios de 0,5% (meio por cento) ao mês.
7. O período de atraso será contado em dias corridos.
8. No caso de aplicação de penalidade em que a contratada tenha que pagar multa através de Guia de Recolhimento da União – GRU, e não o faça no devido prazo, o índice utilizado para atualização do valor será o IPCA.
9. A data a ser utilizada como referência para a atualização do débito será a da publicação da decisão da aplicação da penalidade no diário eletrônico.

4. Requisitos Técnicos (Art. 18, § 3º, IV)

O requisitos técnicos foram abordados no Item 3 e seus subitens

5. Modelos (templates) propostos a serem utilizados na contratação (Art. 18, § 3º, III, V)

Proc. SEI Principal nº XXXXXXXXX

Pregão Eletrônico nº XX/YYYY – TRE/AL

Ata de Registro de Preços TRE/AL nº XX/YYYY

Fornecedor: AAAAAAAAAAA. - CNPJ 00.000.000/0000-00

ORDEM DE FORNECIMENTO Nº XXX/20YY – STI

Solicito, com base na Ata de Registro de Preços relativa ao Pregão Eletrônico suprarreferido, celebrada entre este Tribunal e essa Empresa, o fornecimento abaixo discriminado:

Item da Ata	Descrição	Qtd. Solicitada	Valor Unitário (R$)	Valor Total (R$)
TOTAL:				

Recursos Orçamentários: As despesas decorrentes da prestação dos serviços pretendido serão cobertas com recursos de MATERIAL PERMANENTE DE TI ou DE SERVIÇOS ou DESTINADOS À SOFTWARE (conforme caso concreto).

Prazo de Entrega: No máximo de XX (XXXXXXX) dias corridos após o recebimento da autorização de fornecimento, nota de empenho ou instrumento formal e equivalente, conforme contrato.

Valor Total: R$ XX.XXX,XX (XXXXXX reais e XXXXXXXa centavos).

RESUMO DE STATUS DA ATA

QUANTITATIVO TOTAL REGISTRADO:	
Quantitativo executado via	

Ordem de Fornecimento nº 00X/20YY	
Quantitativo executado via Ordem de Fornecimento nº 00X/20YY	
SALDO ATA:	

Gestor da Ata - Portaria TRE/AL nº XX/XXXX

Maceió, 28 de agosto de 2020.

Maceió, 14 de outubro de 2020.

Documento assinado eletronicamente por **DANIEL MACÊDO DE CARVALHO SOUTO**, **Membro da Comissão**, em 19/10/2020, às 13:46, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **CRISTINO HERMANO DE BULHÕES**, **Membro da Comissão**, em 19/10/2020, às 14:43, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **RODRIGO FERREIRA MOURA**, **Técnico Judiciário**, em 20/10/2020, às 17:45, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-al.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0785938** e o código CRC **9ABE76CB**.