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

Estudos Preliminares

1. Análise de Viabilidade da Contratação (Resolução CNJ nº 182/2013 – Arts.12 e 14)

1.1. Contextualização

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 interno e no atendimento ao público.

O monitoramento das vulnerabilidades de segurança num ambiente computacional é absolutamente necessário para se manter a confidencialidade, a disponibilidade e a integridade das informações.

Neste contexto, buscamos 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. Definição e Especificação dos Requisitos da Demanda (Art. 14, I)

2.1. Especificações Técnicas

Especificações 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 maliciososconhecidos (malware) para no mínimo 250 IPs;
2. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através darede;
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 possibilitaro 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 seguintescaracterísticas:
    1. Por sistema operacional;
    2. Por determinado software instalado;
    3. Por Ativos impactados por determinada vulnerabilidade.
11. A solução deve possuir suporte para a adição de detecções personalizadas usando o OVAL (Open VulnerabilityAssessment 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 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 de 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, aextração de dados para carga no SIEM;
19. Deve possuir uma API para automação de processos e integração com aplicações ITSM do órgão para asvulnerabilidades 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 diretamenteno sistema operacional;
21. Se for baseada em nuvem, a solução deve possuir conectores para, no mínimo, as seguintes plataformas:a) Amazon Web Service (AWS);b) Microsoft Azure;c) Google Clound Platform.
22. A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV ou HTML;
23. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novosdispositivos e desvios de padrões observados;
24. A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento emtempo real;
25. 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;

26. Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinadoativo;
27. A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no minímo:
    1. Bancos de dados;
    2. Hypervisors (no mímino VMWare ESX/ESXi);
    3. Dispositivos móveis;
    4. Dispositivos de rede;
    5. Endpoints;
    6. Aplicações;
28. A solução deve ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento derede;
29. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;
30. A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBMQRadar, Microfocus ArcSight e Splunk.
31. A solução deve possibilitar a realização de cópias de segurança, funcionamento em alta disponibilidade e criptografiade todos os dados armazenados, além de incluir todo o software e licenciamento necessários para o funcionamento completode acordo com as funcionalidades previstas neste Termo de Referência.
32. A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.
33. 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 transito devem usar ao menos o algoritimo TLS 1.2 de chave 2048 bits;
    3. Os dados em transito devem ser criptografados ao menos com o algoritimo AES-128 bits;
    4. Os algoritimos de hash devem usar ao menos o algoritimo 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 algoritimo 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 einiciado pelos scanners (on-premises).
    10. Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site dofabricante.
34. Dos Relatórios:
    1. Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bemcomo a geração de relatórios sob demanda;
    2. A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção detodos 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 deacordo com a necessidade;
38. A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites deendereços IPs.
39. A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades para no mínimo 250 IPs;
40. A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);
41. Deve permitir a configuração de vários painéis e widgets;
42. Deve ser capaz de medir e reportar ameaças;
43. Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;
44. A plataforma de software deve realizar varreduras em uma variedade de sistemas operacionais, suportando pelomenos hosts baseados em Windows, Linux e Mac OS, bem como appliances virtuais;A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades eregiões e gerenciar todos por uma console central;
45. A plataforma de software deve fornecer agentes instaláveis em sistemas operacionais, pelo menos Windows, Linux eMac OS, para o monitoramento contínuo de configurações e vulnerabilidades;
46. A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licençasadquiridas, para varredura diretamente no sistema operacional.
47. A plataforma de software deve permitir o monitoramento sem a necessidade de agentes instalados, até o limite delicenças adquiridas, para varredura diretamente no sistema operacional.
48. A plataforma de software deve incluir a capacidade de programar períodos de tempo e data onde varreduras nãopodem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia;
49. No caso onde uma atividade de varredura seja interrompida por invadir o período não permitido, o mesmo deve sercapaz de ser reiniciado de onde parou;
50. A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;
51. A plataforma de software deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindocontas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;

A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuáriopadrão até acesso de sistema ou administrativo;

1. A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais;
2. A solução deve possuir módulo para realizar análise dinâmica em aplicações Web:
3. A solução deve possuir módulo para realizar varreduras de vulnerabilidades para no mínimo 5 aplicações Web,cobrindo no mínimo, mas não limitando-se a base de ameaças apontadas pelo OWASP Top 10, CWE e WASC:
4. A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web;
5. A solução de análise deverá ser capaz de executar varreduras em sistemas Web através de seus endereços IP ouFQDN (DNS);
6. A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento deinformações de identificação pessoal;
7. 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;
8. Deverá também permitir a execução da função crawler, que consiste na navegação para descoberta das URLsexistentes na aplicação;
9. A solução de análise deve suportar a integração com o softwares de automação de testes para permitir sequênciasde autenticação complexas;
10. A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamentelimitadas ao número de licenças;
11. A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foidetectada anteriormente no aplicativo Web;
12. Deve ser capaz de utilizar scripts customizados de crawling com parâmetros definidos pelo usuário;
13. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;
14. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;
15. 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. Número máximo de elementos DOM;
    4. Tamanho máximo de respostas;
    5. Tempo máximo para a varredura;
    6. Número máximo de conexões HTTP(S) ao servidor hospedando a aplicação Web;
    7. Número máximo de requisições HTTP(S) por segundo;
16. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal,mensal e anual;
17. Deve suportar o envio de notificações por email;
18. Deverá ser compatível com avaliação de web services REST e SOAP;
19. A solução de análise deve suportar os seguintes esquemas de autenticação:
    1. Autenticação Básica (Digest);
    2. NTLM;
    3. Autenticação de Cookies;
20. Deve ser capaz de importar scripts de autenticação previamente configurados pelo usuário;
21. A solução de análise deve ser capaz de exibir os resultados das varreduras de forma temporal paraacompanhamento de correções e introdução de novas vulnerabilidades;
22. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
23. Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências;

24. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;
25. Serviço de Detecção de Malware:
    1. A solução de análise deve utilizar a plataforma de gerenciamento de vulnerabilidades existente;
    2. A solução de análise deve permitir visualizar o acompanhamento das atividades de verificação, páginas infectadas etendências de infecção por malware;
    3. A solução de análise deve fornecer relatórios de resumo geral de todas as aplicações web e resumo de uma aplicaçãoespecífica, que serão exportados para os formatos XML, HTML ou PDF.
26. 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 5.2.1.41.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.

3. 3. Soluções Disponíveis no Mercado de TIC (Art. 14, I, a):

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

a. **Utilização de softwares livres**
- Nome da Solução: Softwares livres OpenVas e Nmap
- Fornecedor: Comunidades Open Source e páginas específicas dos projetos.
- Descrição: Utilizar ferramentas livres ou gratuitas, como os softwares OpenVas e Nmap.

b. **Solução paga com gerenciamento e armazenamento na nuvem (On Cloud)**
   - Nome da Solução: Ferramenta de Gestão de Vulnerabilidades On Cloud
   - Possíveis Fornecedores: Qualys, Tenable, Rapid7, entre outros.
   - Descrição: Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseadoem nuvem, com modelo de subscrição por 36 meses.

c. **Solução paga com gerenciamento e armazenamento na rede local do Tribunal (On premise)**
   - Nome da Solução: Ferramenta de Gestão de Vulnerabilidades On premises
   - Possíveis Fornecedores: Tenable, Rapid7, entre outros.
   - Descrição: Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseadoem gerenciamento e armazenamento na rede local do tribunal, com modelo de subscrição por 36 meses ou de licençaperpetua com suporte de 36 meses.

4. Contratações Públicas Similares (Art. 14, I, b):

- Governo do Distrito Federal - Secretaria de Estado da Fazenda, Pregão Eletrônico 16/2018
- Ministério Público do Trabalho, Pregão de Eletrônico 21/2017
- Tribunal de Contas da União, Pregão Eletrônico 78/2018

5. Outras Soluções Disponíveis (Art. 14, II, a):

Não se aplica, smj, por se tratar de licenciamento e serviços de suporte padrão de mercado.

6. Portal do Software Público Brasileiro (Art. 14, II, b):

Não se aplica, smj, por se tratar de licenciamento e serviços de suporte padrão de mercado.

7. Alternativa no Mercado de TIC (Art. 14, II, c):

Não se aplica, smj, por se tratar de c licenciamento e serviços de suporte padrão de mercado.

8. Modelo Nacional de Interoperabilidade – MNI (Art. 14, II, d):

Não se aplica, smj, por se tratar de licenciamento e serviços de suporte padrão de mercado.

9. Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (Art. 14, II, e):

Não se aplica, smj, por se tratar de licenciamento e serviços de suporte padrão de mercado.

10. Modelo de Requisitos Moreq-Jus (Art. 14, II, f):

Não se aplica, smj, por se tratar de licenciamento e serviços de suporte padrão de mercado.

11. Análise dos Custos Totais da Demanda (Art. 14, III):

Valor Estimado (baseado na melhor proposta da Tenable on premise): R$ 165.314,00 (Cento e sessenta e cinco mil trezentos e quatorze reais), com base nos valores obtidos em procedimento com o mesmo objeto em trâmite no TRE-PB, que terá como copartícipes vários outros TRE.

Eventos: 0782025, 0782027 e 0782030.

12. Escolha e Justificativa da Solução (Art. 14, IV):

A solução 1 baseada em Software Livre atende apenas parte da necessidade, pois a utilização desse cenário implica em não contar com suporte técnico especializado, além disso a atualização da base de vulnerabilidades e falhas não possui a mesma frequência de cenários com softwares pagos. Outro ponto desfavorável ao uso do Software Livre 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 adequado e facilidade nas atualizações da solução que serão todas feitas pelo fabricante. Todas os requisitos de funcionalidades do projeto são
atendidos por esse cenário. As soluções analisadas Qualys (VM e módulo WAS), Tenable (Tenable.io e módulo WAS) e Rapid7 (IVM e módulo IAS) conseguem fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web. Porém como os dados armazenados pela ferramenta (vulnerabilidades dos ativos de TIC) são muito sensíveis não é recomendável estarem armazenados em nuvem pública.

A solução 3 baseada em gerenciamento em rede local do tribunal (On premises) fornecida pela Tenable apresenta um valor de aquisição adequado e menor do que a Solução 2 (On cloud). Apesar de a solução 3 (On premise) trazer o trabalho de atualização para a equipe de infraestrutura de rede, ela possui um menor risco de vazamento de dados sensíveis que são as vulnerabilidades dos ativos de TIC do tribunal 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 soluções analisadas Tenable (Tenable.sc) e Rapid7 (Nexpose e módulo AppSpider) conseguem fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web. Outro ponto favorável a solução 3 fornecida pela Tenable é o fato de que após o término do suporte a STIC continuará a ter acesso a ferramenta embora sem o direito de recebimento de atualizações de versão e de novas vulnerabilidades.

Sendo assim, não resta outra alternativa para o TRE-AL no momento senão a solução 3 baseada no gerenciamento em rede local do tribunal, tendo em vista o menor preço da Solução 3 e o fato de fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web sem armazenar em nuvem pública os dados sensíveis que são as vulnerabilidades dos ativos de TIC do tribunal.

Solução Escolhida

Nome: Solução paga com gerenciamento e armazenamento na rede local do tribunal (On Premise).
Descrição: Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em gerenciamento e armazenamento na rede local do tribunal, com modelo de subscrição por 36 meses ou de licença perpetua com suporte de 36 meses.

Justificativa

Com a solução escolhida será possível realizar o Gerenciamento de vulnerabilidades, mitigando riscos de ataques cibernéticos e protegendo os sistemas de tecnologia da informação da Justiça Eleitoral.

13. Descrição da Solução (Art. 14, IV, a):

Contratação de solução de análise de vunerabilidades computacionais em servidores e serviços informatizados e serviços relacionados.

14. Alinhamento da Solução (Art. 14, IV, b):

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

15. Benefícios Esperados (Art. 14, IV, 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.

16. Relação entre a Demanda Prevista e a Contratada (Art. 14, IV, d):

Assegurar a salva guarda de dados e informações armazenadas nos servidores deste Regional, bem assim alta disponibilidade de sistemas e serviços informatizados.

Devido a restrições orçamentárias e tendência natural de aumento da quantidade de ativos de TIC na rede interna do Tribunal optamos pela modalidade de Registro de preços.

17. Adequação do Ambiente (Art. 14, V, a, b, c, d, e, f):

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

18. Orçamento Estimado (Art. 14, II, g):

Conforme desclinado no Item 11

19. Sustentação do Contrato (Art.15)

19.1. Recursos Materiais e Humanos (Art. 15, I):

Não será necessária a disponibilização de recursos humanos e/ou materiais adicionais para sustentação da solução adquirida, após sua implantação.

19.2. Descontinuidade do Fornecimento (Art. 15, II):

Não se trata de um serviço de natureza contínua, logo não se aplica, smj.

19.3. Transição Contratual (Art. 15, III, a, b, c, d, e):

Não se aplica, smj, por se tratar de nova contratação/aquisição.

19.4. Estratégia de Independência Tecnológica (Art. 15, IV, a, b):

Não se trata de um serviço de natureza contínua, logo não se aplica, smj.

20. Estratégia para Contratação (Art.16)

20.1. Natureza do Objeto (Art. 16, I):

O objeto possui características comuns e usuais encontrados no mercado de TIC e trata-se de contrato de fornecimento de prorrogação de licenciamento de software com serviço de suporte e atualização, não consistindo de serviço continuado.

20.2. Parcelamento do Objeto (Art. 16, II):

Como se trata de RP é natural se pensar em parcelamento. Todavia, cada demanda, ou seja, cada ordem de fornecimento derivada do RP deverá ser realizada de maneira integral.

20.3. Adjudicação do Objeto (Art. 16, III):

Adjudicação por Lote devido a necessidade de compatibilidade e vinculos diretos entre seus itens componentes.

20.4. Modalidade e Tipo de Licitação (Art. 16, IV):

Pregão Eletrônico do Tipo Menor Preço.

20.5. Classificação e Indicação Orçamentária (Art. 16, V):

Plano de Contratação de TIC/2020

Item 11

Proposta orçamentária de 2020
Manutenção corretiva/adaptativa e sustentação de softwares
Código de classificação da fonte de recurso: 3390.40.07

20.6. Vigência da Prestação de Serviço (Art. 16, VI)

Neste caso é de 36 meses, considerando o período de garantia/suporte das licenças.

20.7. Equipe de Apoio à Contratação (Art. 16, VII):

Integrante Demandante:

Cargo ou Função: Coordenador de Infraestrutura

E-mail: coinf@tre-al.jus.br

Integrante Técnico:

Cargo ou Função: Chefe da Seção de Gerência de Infraestrutura

E-mail: segi@tre-al.jus.br

Integrante Administrativo:

Servidor: Rodrigo Ferreira Moura

E-mail: rodrigomoura@tre-al.jus.br

20.8. Equipe de Gestão da Contratação (Art. 16, VIII):

Gestor do Contrato: Indicação a cargo da Secretaria de Administração

21. Análise de Riscos:

A análise em questão é mínima, portanto, não exaustiva e focada em aspectos diretamente ligados ao procedimento nas suas etapas de aquisição e fornecimento.

Risco: 1	Não Aprovação dos documentos do Planejamento da Contratação	
Dano(s)	Atraso no processo de contratação	
Impacto(s)	Aumento de risco de vulnerabilidade exploráveis em servidores e serviços	
Ações	Responsável	Prazo
Adotar procedimentos para que a área administrativa acompanhe a elaboração dos documentos, evitando envios e devoluções do processo	Equipe de planejamento da contratação	Durante todo o processo de contratação
Reuniões com superiores para sensibilização e aprovação dos documentos.		

Risco: 2	Insuficiência de recursos orçamentários/financeiros para aquisição	
Dano(s)	Impossibilidade da contratação	
Impacto(s)	Aumento de risco de vulnerabilidade exploráveis em servidores e serviços	
Ações	Responsável	Prazo
Encontrar a maneira mais vantajosa economicamente para realizar a contratação	Equipe de planejamento da contratação	Durante todo o processo de contratação
Utilização de recursos destinados a outras aquisições para contemplar esta necessidade	STI	
Substituição dos equipamentos por outros equipamentos existentes, paralisando o andamento de outros projetos e demandas, tais como implementação de ambiente de banco de homologação e desenvolvimento.	STI	
Remanejar verbas de outros projetos previstos no plano de contratações mas que não serão executados por razões diversas	SAD	

Risco: 3	Atraso na Aquisição	
Dano(s)	Aumento de riscos na área de segurança da informação	
Impacto(s)	Eventual aumento de risco de vulnerabilidades exploráveis em servidores e serviços	
Ações	Responsável	Prazo
Solicitação de aceleração de trâmites internos	STI	Durante todo o processo de contratação
Substituição dos equipamentos por outros equipamentos existentes, paralisando o andamento de outros projetos e demandas, tais como implementação de ambiente de banco de homologação e desenvolvimento.	STI	

Risco: 4	Falha na prestação de serviços	
Dano(s)	Aumento de risco de vulnerabilidade exploráveis em servidores e serviços	
Impacto(s)	Eventual aumento de risco de vulnerabilidades exploráveis em servidores e serviços	
Ações	Responsável	Prazo
Aplicar sanções administrativas	Gestão contratual	Durante a execução do contrato
Substituição dos equipamentos por outros equipamentos existentes, caso possível, paralisando o andamento de outros projetos e demandas, tais como implementação de ambiente de banco de homologação e desenvolvimento.	STI	

A seguir se encontra a matriz de avaliação qualitativa dos riscos identificados:

Probabilidade / Impacto	Sem Impacto	Baixo	Médio	Alto
Baixa			Risco 1	
Média				Risco 2,3 e 4
Alta				

Lista de Potenciais Fornecedores

Nome: Netconn
Sítio: http://www.netconn.com.br
Telefone: (11) 3023 1500 / Ramal 5210
E-mail: comercial@netconn.com.br
Contato: Viviane Lopes

Nome: G3 Solutions
Sítio: http://www.g3solutions.com.br/
Telefone: 81 3471-8600 / 81 8173-7134
E-mail: alexandre.barros@g3solutions.com.br
Contato: Alexandre Barros

Nome: Servix
Sítio: http://www.servix.com
Telefone: (61) 3031-2960
E-mail: cristina.carvalho@servix.com
Contato: Cristina Carvalho

Nome: Service IT Security
Telefone: (11) 2595-1400
Sítio: http://www.service.com.br

Nome: SUPORTE INFORMÁTICA
Sítio: http://www.suporteinformatica.com
Telefone: 81 3202-9100 / 81 3244-9697 / 81 8178-6653
E-mail: andre.brasileiro@suporteinformatica.com
Contato: André Brasileiro

Nome: INFINIIT
Sítio: http://www.infiniit.com.br
E-mail: guilherme@infiniit.com.br
Contato: Guilherme

Nome: SWT
Sítio: http://www.swt.com.br/
Contato: Bernadete Sabino
Email: bsabino@swt.com.br
Telefone: 32213731

Nome: Plugnet
Sítio: http://www.plugnetshop.com.br/
Telefone: (81) 34267006
Contato: Breno
Email: breno@plugnetshop.com.br

Nome: PCT Informática
Sítio: http://www.pctinformatica.com.br/
Telefone: (82) 3241-5300
Contato: Zacarias
Email: pct@pctinformatica.com.br

Nome: 3A Tecnologia
Sítio: www.3atecnologia.com.br

Nome: Drive A
Sítio: www.drivea.com.br

Maceió, 04 de outubro de 2020.

Documento assinado eletronicamente por **DANIEL MACÊDO DE CARVALHO SOUTO**, **Membro da Comissão**, em 08/10/2020, às 18:11, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **CRISTINO HERMANO DE BULHÕES**, **Membro da Comissão**, em 08/10/2020, às 18:13, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **RODRIGO FERREIRA MOURA**, **Técnico Judiciário**, em 13/10/2020, às 23:36, 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 **0778219** e o código CRC **6278CAE5**.

0007757-43.2020.6.02.8000 0778219v53