ESTUDO TÉCNICO PRELIMINAR

INTRODUÇÃO

O presente documento caracteriza a primeira etapa da fase de planejamento e apresenta os devidos estudos para a contratação de solução que atenderá à necessidade abaixo especificada. O objetivo principal é estudar detalhadamente a necessidade e identificar no mercado a melhor solução para supri-la, em observância às normas vigentes e aos princípios que regem a Administração Pública.

A redundância é um conceito crucial quando se trata de soluções de armazenamento de logs, em especial no que tange a proteger a integridade dos dados, facilitar a recuperação de desastres, atender aos requisitos de conformidade e garantir escalabilidade e desempenho adequados. Desse modo, é essencial para a estratégia de segurança e operações de TI de deste Tribunal.

1 - DESCRIÇÃO DA NECESSIDADE

Fundamentação: Descrição da necessidade da contratação, considerado o problema a ser resolvido sob a perspectiva do interesse público (inciso I do § 1° do art. 18 da Lei 14.133/2021 e art. 9°, inciso I, da IN 58/2022).

A aquisição do equipamento FortiAnalyzer-300G ou equivalente compatível, para compor o ambiente em alta disponibilidade garante que a equipe especializada do Tribunal tenha acesso contínuo aos recursos de análise e registro, mesmo em caso de falha de hardware. Isso aumenta a confiabilidade e a disponibilidade desse importante sistema de segurança.

Benefícios gerais a serem obtidos:

- Contornar instabilidades causadas por falhas de dados;
- Evitar perda de dados críticos;
- Maior disponibilidade do ambiente de logs dos firewalls.

2 – PREVISÃO NO PLANO DE CONTRATAÇÕES ANUAL

Fundamentação: Demonstração da previsão da contratação no plano de contratações anual, sempre que elaborado, de modo a indicar o seu alinhamento com o planejamento da Administração (inciso II do § 1° do art. 18 da Lei 14.133/21), bem como com os instrumentos de planejamento do órgão ou entidade (Art. 9°, inciso IX da IN 58/2022).

PORTARIA PRESIDÊNCIA Nº 418/2023 - Plano de Contratações Anual (PCA) do Tribunal Regional Eleitoral de Alagoas para o exercício de 2024.

Item 18 - AQUISIÇÃO EQUIPAMENTOS DE TIC - ATIVOS DE REDE

NECESSIDADE DE ATUALIZAÇÃO DO PARQUE DE ATIVOS DE REDE

R$ 98.818,00

3 – REQUISITOS DA CONTRATAÇÃO

Fundamentação: Descrição dos requisitos da contratação necessários e suficientes à escolha da solução (inciso III do § 1° do art. 18 da Lei 14.133/2021), bem como a previsão de critérios e práticas de sustentabilidade, observadas as leis ou regulamentações específicas, inclusive com a observância dos padrões mínimos de qualidade e desempenho (Art. 9°, inciso II da IN 58/2022).

- O equipamento fornecido deverá ser plenamente compatível com o gerenciador de logs Fortinet FortiAnalyzer-300G, em uso pelo TRE-AL;
- Deve ter capacidade de armazenamento igual ou superior à atual;
- Incluir o serviço acessório de ativação da solução;
- 36 meses de garantia.

4 – ESTIMATIVA DAS QUANTIDADES

Fundamentação: Estimativa das quantidades a serem contratadas, acompanhada das memórias de cálculo e dos documentos que lhe dão suporte, considerando a interdependência com outras contratações, de modo a possibilitar economia de escala (inciso IV do § 1° do art. 18 da Lei 14.133/21 e art. 9°, inciso V da IN 58/2022).

A quantidade relacionada à pretendida aquisição é de 01 (um) equipamento, incluindo o respectivo serviço de instalação.

5 – LEVANTAMENTO DE MERCADO

Fundamentação: Levantamento de mercado, que consiste na análise das alternativas possíveis, e justificativa técnica e econômica da escolha do tipo de solução a contratar (inciso V do § 1° do art. 18 da Lei 14.133/2021), podendo, entre outras opções (Art. 9°, inciso III da IN 58/2022):

a) serem consideradas contratações similares feitas por outros órgãos e entidades públicas, bem como por organizações privadas, no contexto nacional ou internacional, com o objetivo de identificar a existência de novas metodologias, tecnologias ou inovações que melhor atendam às necessidades da Administração;

b) ser realizada audiência e/ou consulta pública, preferencialmente na forma eletrônica, para coleta de contribuições;

c) em caso de possibilidade de compra, locação de bens ou do acesso a bens, serem avaliados os custos e os benefícios de cada opção para escolha da alternativa mais vantajosa, prospectando-se arranjos inovadores em sede de economia circular; e

d) serem consideradas outras opções logísticas menos onerosas à Administração, tais como chamamentos públicos de doação e permutas.

Por se tratar de aquisição de equipamento para compor solução em uso, baseada no Fortinet Fortianalyzer, qualquer revenda autorizada do fabricante poderá participar da concorrência, não havendo dispositivo de outra marca que possa ser utilizado para o mesmo fim, de forma satisfatória.

6 – ESTIMATIVA DO PREÇO DA CONTRATAÇÃO

Fundamentação: Estimativa do valor da contratação, acompanhada dos preços unitários referenciais, das memórias de cálculo e dos documentos que lhe dão suporte, que poderão constar de anexo classificado, se a administração optar por preservar o seu sigilo até a conclusão da licitação (inciso VI do § 1° da Lei 14.133/21 e art. 9°, inciso VI da IN 58/2022).

Órgão	Fonte	Item	Valor	Observações
Defensoria Pública da Bahia	ATA DE REGISTRO DE PREÇOS 03/2023	04	R$ 160.656,30	• Apesar do valor do item na licitação ter sido de R$ 267.760,50, estimamos o valor proposcional a 36 meses.

TRE-AL	ATA DE REGISTRO DE PREÇOS n.º 12/2022	10	R$90.951,90	

Diante dos valores inicalmente coletados e se aplicando a média, estíma-se o valor de R$ 125.801,10 para a pretendida aquisição, a serem validados e/ou complementados pela SEIC/COMAP/SAD.

7 - DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

Fundamentação: Descrição da solução como um todo, inclusive das exigências relacionadas à manutenção e à assistência técnica, quando for o caso (inciso VII do § 1° do art. 18 da Lei 14.133/21 e art. 9°, inciso IV da IN 58/2022).

1. **CARACTERISTICAS GERAIS**
    1. Deve ser totalmente compatível com o equipamento FortiAnalyzer-300G, em uso pelo Tribunal.
    2. Solução deverá ser baseado em appliance físico, possuir garantia e licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 36 (trinta e seis) meses.
    3. **Deverá possuir no mínimo:**
        a. Capacidade de receber pelo menos 90 GB de logs diários;
        b. Taxa analítica de 1.500 (um mil e quinhentos) logs por segundo;
        c. 04 (quatro) interfaces RJ45 1GE;
        d. Capacidade de armazenamento de no mínimo 04 (quatro) TB.
2. **REQUISITOS MINIMOS DE FUNCIONALIDADES**
    1. Deverá suportar o acesso via SSH e WEB (HTTPS) para gerenciamento de soluções
    2. Deverá possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) e via linha de comando no console de gerenciamento.
    3. Deverá permitir o acesso simultâneo à administração, bem como permitir que pelo menos 2 (dois) perfis sejam criados para administração e monitoramento.
    4. Deverá suportar SNMP versão 2 e 3
    5. Deverá permitir a virtualização do gerenciamento e administração dos dispositivos, nos quais cada administrador só tem acesso aos computadores autorizados.
    6. Deverá permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução.
    7. Deverá permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS, SSH
    8. Deverá possuir **a**utenticação de usuários para acesso à plataforma via LDAP, Radius, TACACS + ;
    9. Deverá possuir geração de relatórios de tráfego em tempo real, em formato de mapa geográfico, em formato de gráfico de bolhas e em formato gráfico;
    10. Deverá possuir definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais.
    11. Deverá possuir um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha.
    12. Deverá possuir visualização da quantidade de logs enviados de cada dispositivo monitorado
    13. Deverá possuir mecanismos de apagamento automático para logs antigos.
    14. Deverá permitir importação e exportação de relatórios;
    15. Deverá ter a capacidade de criar relatórios no formato HTML, PDF, XML e CSV;
    16. Deverá permitir exportar os logs no formato CSV;

17. Deverá gerar logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário.

18. Deverá permitir que os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar.

19. Deverá ter relatórios predefinidos.

20. Deverá poder enviar automaticamente os logs para um servidor FTP externo para a solução

21. Deverá permitir a duplicação de relatórios existentes, deve ser possível para edição posterior.

22. Deverá ter a capacidade de personalizar a capa dos relatórios obtidos.

23. Deverá permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos mesmos logs.

24. Deverá ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas

25. Deverá ter um mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo real.

26. Deverá permitir que os arquivos de log sejam baixados da plataforma para uso externo.

27. Deverá ter a capacidade de gerar e enviar relatórios periódicos automaticamente.

28. Deverá permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades.

29. Deverá permitir o envio por e-mail relatórios automaticamente.

30. Deverá permitir que o relatório seja enviado por email ao destinatário específico.

31. Deverá permitir a programação da geração de relatórios, conforme calendário definido pelo administrador.

32. Deverá exibir graficamente em tempo real a taxa de geração de logs para cada dispositivo gerenciado.

33. Deverá permitir o uso de filtros nos relatórios.

34. Deverá permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros.

35. Deverá permitir especificar o idioma dos relatórios criados

36. Deverá gerar alertas automáticos por email, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros.

37. Deverá permitir o envio automático de relatórios para um servidor SFTP ou FTP externo.

38. Deverá ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios.

39. Deverá possibilitar visualizar nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros.

40. Deverá ter uma ferramenta que permita analisar o desempenho na geração de relatórios, a fim de detectar e corrigir problemas na geração deles.

41. Deverá importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios.

42. Deverá ser possível definir o espaço que cada instância de virtualização pode usar para armazenamento de log.

43. Deverá fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado.

44. Deverá ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma.

45. Deverá permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos

46. Deverá permitir visualizar em tempo real os logs recebidos.

47. Deverá permitir o encaminhamento de log no formato syslog e no formato CEF (Common Event Format).

48. Deverá permitir a criação de painéis personalizados para monitorar operações SOC

49. Deverá gerar alertas de eventos a partir de logs recebidos
50. Deverá permitir a criação de incidentes a partir de alertas de eventos para o terminal
51. Deverá permitir a integração ao sistema de tickets do ServiceNow
52. Deverá permitir o suporte a logs na nuvem pública do Amazon S3, na nuvem pública do Microsoft Azure e de nuvem pública do Gooogle Cloud.
53. Suportar o padrão SAML para autenticação do usuário administrador

3. **FUNCIONALIDADES DE RELATORIOS DE FIREWALL**
    1. Deverá possuir relatório de conformidade com o PCI DSS;
    2. Deverá possuir um relatório de uso do aplicativo SaaS
    3. Deverá possuir um relatório de prevenção de perda de dados (DLP)
    4. Deverá possuir um relatório de VPN
    5. Deverá possuir um relatório IPS (Intruder Prevention System)
    6. Deverá possuir um relatório de reputação do cliente
    7. Deverá possuir um relatório de análise de segurança do usuário
    8. Deverá possuir um relatório de análise de ameaças cibernéticas
    9. Deverá possuir um breve relatório resumido diário de eventos e incidentes de segurança
    10. Deverá possuir um relatório de tráfego DNS
    11. Deverá possuir um relatório de tráfego de e-mail
    12. Deverá possuir um relatório dos 10 principais aplicativos usados na rede
    13. Deverá possuir um relatório dos 10 principais sites usados na rede
    14. Deverá possuir um relatório de uso de mídia social.

8 – JUSTIFICATIVA PARA PARCELAMENTO

Fundamentação: Justificativas para o parcelamento ou não da solução (inciso VIII do § 1° do art. 18 da Lei 14.133/21 e art. 9°, inciso VII da IN 58/2022).

Não se vislumbra a hipótese de parcelamento.

9 - DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS

Fundamentação: Demonstrativo dos resultados pretendidos em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis (inciso IX do § 1° do art. 18 da Lei 14.133/21 e Art. 9°, inciso X da IN 58/2022).

- Contornar instabilidades causadas por falhas de dados;
- Evitar perda de dados críticos;
- Maior disponibilidade do ambiente de logs dos firewalls.

10 – PROVIDÊNCIAS PRÉVIAS AO CONTRATO

Fundamentação: Providências a serem adotadas pela administração previamente à celebração do contrato (inciso X do § 1° do art. 18 da Lei 14.133/21), inclulsive com a observância de adaptações no ambiente do órgão ou da entidade, devendo-se atentar para a necessidade de obtenção de licenças, outorgas ou autorizações, bemo como para a capacitação de servidores ou de empregados para fiscalização e gestão contratual (art. 9°, inciso XI da IN 58/2022).

Por se tratar de equipamento para compor solução em utilização, não se vislumbra providências prévias ao contrato.

11 – CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

Fundamentação: Contratações correlatas e/ou interdependentes (inciso XI do § 1° do art. 18 da Lei 14.133/21 e art. 9°, inciso VIII da IN 58/2020).

Não se vislumbra a necessidade de contratações correlatas/independentes.

12 – IMPACTOS AMBIENTAIS

Fundamentação: Descrição de possíveis impactos ambientais e respectivas medidas mitigadoras, incluídos requisitos de baixo consumo de energia e de outros recursos, bem como logística reversa para desfazimento e reciclagem de bens e refugos, quando aplicável (inciso XII do § 1° do art. 18 da Lei 14.133/21 e Art. 9°, inciso XII da IN 58/2022).

Por se tratar de solução de hardware, com baixo consumo de energia, não se vislumbra impactos ambientais decorrentes.

13 – VIABILIDADE DA CONTRATAÇÃO

Fundamentação: Posicionamento conclusivo sobre a adequação da contratação para o atendimento da necessidade a que se destina (inciso XIII do § 1° do art. 18 da Lei 14.133/21 e Art. 9°, inciso XIII da IN 58/2022).

Considerando que há necessidade da solução, considerando que há previsão orçamentária - Item 2 e a considerar que o custo estimado - Item 6, esta comissão entende, smj, que há viabilidade para a contratação, mesmo que seja necessária complementação orçamentária.

Documento assinado eletronicamente por **DANIEL MACÊDO DE CARVALHO SOUTO**, **Membro da Comissão**, em 06/05/2024, às 18:44, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **CRISTINO HERMANO DE BULHÕES**, **Membro da Comissão**, em 06/05/2024, às 18:44, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **NEILTON SOUZA SILVA JÚNIOR**, **Chefe de Seção**, em 08/05/2024, às 16:04, 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 **1463914** e o código CRC **F6232143**.