



TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO
Rua João Batista Parra 575 - Bairro Praia do Suá - CEP 29052-123 - Vitória - ES

ESTUDO TÉCNICO PRELIMINAR (TIC) Nº STIC 09/2023 - TRE-ES/PRE/DG/STI/CIS/SGIR

(este documento deve seguir as orientações da Resolução TRE/ES nº 261/2018)

SUMÁRIO

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO.

- 1. Caracterização da Demanda.**
- 2. Especificação dos Requisitos Funcionais.**
- 3. Especificação dos Requisitos Tecnológicos.**
- 4. Identificação e Comparação das Soluções Aderentes aos Requisitos.**
- 5. Indicação da STIC Escolhida.**
- 6. Indicação da Necessidade de Adequação Ambiental**

ANÁLISE DE RISCOS.

- 7. Identificação dos Riscos.**
- 8. Relação dos Riscos e Ações de Mitigação.**

ANÁLISE DE SUSTENTAÇÃO DO CONTRATO.

- 9. Recursos Materiais e Humanos.**
- 10. Descontinuidade do Fornecimento.**

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1. CARACTERIZAÇÃO DA DEMANDA

1.1. DESCRIÇÃO SUCINTA

Contratação de suporte técnico e do direito de atualização (no modelo de subscrição) para solução de gestão de vulnerabilidades dos ativos de tecnologia da informação utilizada pelo TRE-ES.

1.2. JUSTIFICATIVA DA NECESSIDADE E RESULTADOS

A gestão de vulnerabilidades é um processo que se preocupa com a descoberta e remediação de vulnerabilidades que podem estar presentes nos sistemas de informação. Uma vulnerabilidade pode surgir pela utilização de uma versão comprometida de um software ou por uma configuração inadequada de uma aplicação. Essa vulnerabilidade pode ser explorada por um atacante para prejudicar a disponibilidade, integridade e confidencialidade dos ativos de informação. Existem inúmeras ações maliciosas que podem explorar um vasto número de vulnerabilidades existentes. Dentre elas podemos citar:

- Utilização de usuários e senhas padrões: A maioria de aplicações possuem usuários e senhas padrões, de conhecimento público, que caso não sejam alteradas ou desabilitadas podem ser utilizadas por invasores para acessar os sistemas e obter informações importantes ou sigilosas;

- Problemas de criptografia: Ocorre quando aplicações ou sites utilizam algoritmos de criptografia "fracos" que possibilitem ao invasor quebrar a chave e obter dados sensíveis que podem ser utilizados para obter acesso a servidores, banco de dados, sistemas essenciais, etc.

- CRLF Injection: Ocorre quando um invasor pode injetar uma sequência CRLF - "Carriage Return (Retorno de carro)" e "Line Field (Avanço de linha)" - em um fluxo HTTP. Ao introduzir esta injeção de CRLF inesperada, o invasor é capaz de explorar vulnerabilidades de CRLF de forma mal-intencionada para manipular as funções do aplicativo da web.

- Cross-site Scripting (XSS): Acontece quando um invasor explora uma área de um site que possui conteúdos dinâmicos. O invasor consegue rodar seu código dentro do site da vítima, causando o roubo de contas de usuários, controle do navegador da vítima, e muito mais. Esse problema é comum em formulários de contato que permitem a inserção de caracteres utilizados em linguagens de programação como pontos de interrogação ou barras.

- Acesso a diretórios restritos: Ocorre quando o invasor consegue se aproveitar de sites desprotegidos, conseguindo acesso a um grande número de arquivos de sistema, tendo acesso a nome de usuários, senhas, documentos importantes e até mesmo o código fonte do site/aplicativo.

- SQL Injection: Ocorre quando o invasor se aproveita de falhas em sistemas que interagem com bases de dados através de comandos SQL, onde o atacante consegue inserir uma instrução SQL personalizada e indevida dentro de uma consulta (SQL query) através da entradas de dados de uma aplicação, como formulários ou páginas de uma aplicação.

- Varredura em redes (*Scan*): Varredura em redes, ou *scan*, é uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados. Com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados.

- Interceptação de tráfego (*Sniffing*): Interceptação de tráfego, ou *sniffing*, é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de *sniffers*.

- Força bruta (*Brute force*): Um ataque de força bruta, ou *brute force*, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar *sites*, computadores e serviços em nome e com os mesmos privilégios deste usuário.

- Negação de serviço (DoS e DDoS): Negação de serviço, ou DoS (*Denial of Service*), é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (*Distributed Denial of Service*). O objetivo destes ataques não é invadir e nem coletar informações, mas sim exaurir recursos e causar indisponibilidades ao alvo.

Devido à complexidade e quantidade de ativos de informação utilizados no nosso ambiente de TIC, o processo de gestão de vulnerabilidades necessita ser suportado por uma solução de gestão de vulnerabilidades.

Em 2020 um grupo da Justiça Eleitoral, formado pelo TSE e vários Tribunais Regionais, adquiriu a solução denominada TenableSC para suprir essa demanda, que é essencial para a Segurança da Informação no âmbito da Justiça Eleitoral. O contrato atual, que permite a atualização e o suporte da solução tem vigência até 21 de fevereiro de 2024 e se a subscrição não for renovada, não conseguiremos mais atualizar a base de vulnerabilidades e o software que compõe a solução, perderíamos o direito de suporte, e não seria possível atingir os objetivos (resultados) esperados:

- Manter a base de vulnerabilidades atualizada para permitir a identificação e priorização de tratamento de vulnerabilidades nos ativos de TIC (roteadores, switches, estações de trabalho, hosts de virtualização, bancos de dados, máquinas virtuais, sistemas operacionais, servidores de aplicação, etc) do TRE-ES;

- Reduzir o nível de risco através da redução da probabilidade de ameaças explorarem vulnerabilidades de nossos ativos.

2. ESPECIFICAÇÃO DOS REQUISITOS FUNCIONAIS

2.1. REQUISITOS RELACIONADOS AO NEGÓCIO

- Gerenciamento de Vulnerabilidades em Sistemas Operacionais: testar os hosts (físicos e virtuais), comparando a bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por grandes fabricantes de software;
- Gerenciamento de Vulnerabilidades em Sistemas e páginas Web: Testar as aplicações e páginas web, internas e externas, comparando a bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por grandes fabricantes de software;
- Emissões de Relatórios: emitir relatórios de acompanhamento dos testes e das vulnerabilidades encontradas, apontando quando forem solucionadas;

2.2. REQUISITOS DE CAPACITAÇÃO, AMBIENTAIS, CULTURAIS E SOCIAIS

Não se aplica á atual contratação.

2.3. REQUISITOS DE MANUTENÇÃO E GARANTIA

Não se aplica á atual contratação.

2.4. REQUISITOS TEMPORAIS

O contrato deve ter início no dia 22 de fevereiro de 2024.

O contrato deve ter vigência de 60 (sessenta) meses;

2.5. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

Não se aplica á atual contratação.

3. ESPECIFICAÇÃO DOS REQUISITOS TECNOLÓGICOS

3.1. CARACTERÍSTICAS GERAIS

Aquisição de suporte técnico e direito de atualização de software para a solução de Gestão de Vulnerabilidades TenableSC on premise no modelo de subscrição por 60 meses:

a) Informações do Produto:

- Nome do Produto: Tenable.sc Continuous View
- Part Numbers - TSCCV-M e TSCCV-STNDC-M
- Hostname a ser vinculado: TRE-ES-37-2020
- Quantidade de IP's licenciados: 500

b) Deve ser vinculada à conta do TRE-ES (**Customer ID = 889020**) no portal da fabricante Tenable (<https://community.tenable.com/>);

c) Deve permitir suporte técnico e direito de atualização do software e da base de vulnerabilidades por 60 meses;

4. IDENTIFICAÇÃO E COMPARAÇÃO DAS SOLUÇÕES ADERENTES AOS REQUISITOS

4.1 - Solução Única: Aquisição de suporte técnico e direito de atualização de software para a solução de Gestão de Vulnerabilidades

Descrição da Solução: Aquisição de suporte técnico e direito de atualização de software para a solução de Gestão de Vulnerabilidades Tenable.sc on premise no modelo de subscrição.

Fornecedor da Solução: Empresas de Mercado.

Órgão /Entidade Proprietário da Solução: Não se aplica à presente contratação.

Aderência da Solução ao MNI: Não se aplica à presente contratação.

Aderência da Solução ao ICP-Brasil: Não se aplica à presente contratação.

Aderência da Solução ao Moreq-Jus: Não se aplica à presente contratação.

5. INDICAÇÃO DA STIC ESCOLHIDA

5.1. DESCRIÇÃO DA SOLUÇÃO

Aquisição de suporte técnico e direito de atualização de software para a solução de Gestão de Vulnerabilidades Tenable.sc on premise no modelo de subscrição por 60 meses:

5.2. JUSTIFICATIVA/MOTIVAÇÃO DA ESCOLHA

A solução indicada no subitem 5.1 foi escolhida por ser a única alternativa que atende às necessidades desta contratação..

5.3. ESTIMATIVA DE CUSTO

O valor estimado da atual contratação é de R\$ 295.000,00

5.4. ADERÊNCIA AOS REQUISITOS

Os requisitos tecnológicos estão aderentes e atendem aos requisitos funcionais estabelecidos pelo demandante.

5.5. RELAÇÃO ENTRE DEMANDA PREVISTA E A STIC

Hoje o TRE-ES possui uma solução para Gestão de Vulnerabilidades cujo contrato de subscrição permite atualização e suporte da mesma expira em 21 de fevereiro de 2024. Para que possamos continuar a executar as análises de vulnerabilidades nos ativos TIC e necessário a aquisição de uma nova subscrição da solução atual a partir do dia 22 de fevereiro de 2024.

Considerando que a solução em questão tem seu uso padronizado pela Justiça Eleitoral, que não existe perspectiva para a substituição dessa solução nos próximos 5 anos, que o processo de gestão de vulnerabilidades tem natureza crítica, que as bases de dados da ferramenta da solução devem se manter atualizadas sem interrupções e que um contrato de longo prazo oferece condições financeiras mais favoráveis, evidencia-se a necessidade e vantajosidade de definirmos uma contratação de 60 meses.

5.6 COMPOSIÇÃO DE BENS/SERVIÇOS DA SOLUÇÃO

- Serviço: Suporte com atualização.

6. PARCELAMENTO DO OBJETO

Não haverá parcelamento do objeto.

7. INDICAÇÃO DA NECESSIDADE DE ADEQUAÇÃO AMBIENTAL

Não existem necessidades de adequação ambiental.

ANÁLISE DE RISCOS

8. IDENTIFICAÇÃO DOS RISCOS

O principal risco identificado foi :

- Atraso no trâmite processual.

9. RELAÇÃO DOS RISCOS E AÇÕES DE MITIGAÇÃO

9.1. ANÁLISE DOS RISCOS

Probabilidade e impacto, ações de prevenção/contingência, responsáveis. Incluídos nas tabelas abaixo.

| RISCO 1 | | ATRASSO NO TRÂMITES PROCESSUAL |
|---|---|--------------------------------|
| Probabilidade (Alta, média ou baixa) | | Baixa |
| | Efeito (Dano) | *Impacto |
| 1 | Impossibilidade de realizar análises de vulnerabilidades de ativos com a base de vulnerabilidades atualizada | Alto |
| | Ações de Mitigação e Contingência | Responsável |
| 1 | Consultar empresas do ramo sobre adequação das especificações técnicas às características dos equipamentos fornecidos pelo mercado. | Integrante técnico |
| 2 | Acompanhar todo o trâmite processual | Equipe de contratação |

*Impacto (Baixo, Médio ou Alto)

ANÁLISE DE SUSTENTAÇÃO DO CONTRATO

10. RECURSOS MATERIAIS E HUMANOS

A contratação não necessita de recursos materiais e humanos para sua implantação. Caberá aos técnicos da SGIR monitorar o funcionamento e realizar a atualização da ferramenta e acionar o suporte técnico em caso de falhas que não possam ser solucionadas pelos técnicos da seção.

11. DESCONTINUIDADE DO FORNECIMENTO

Caso a contratada não forneça adequadamente o suporte técnico, o TRE deverá e aplicar as penalidades previstas no contrato.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Integrante Demandante: Rommel Baia Silva (substituto: Lucas Ribeiro Carlin)

Integrante Técnico: Lucas Ribeiro Carlin (substituto: Rommel Baia Silva)

Integrante Administrativo: Marcos Venturott Ferreira (substituto: Carlos Alberto da Rocha Pádua Filho)

Vitória, 29 de maio de 2023.



Documento assinado eletronicamente por **MARCOS VENTUROT FERREIRA, Integrante Administrativo**, em 06/07/2023, às 13:53, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **LUCAS RIBEIRO CARLIN, Integrante Técnico**, em 06/07/2023, às 13:56, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ROMMEL BAIA SILVA, Chefe de Seção**, em 06/07/2023, às 14:00, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site http://sei.tre-es.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0963250** e o código CRC **91A5B1E1**.