Tribunal Regional Eleitoral
do Espírito Santo

Sede: Vitória/ES
Av. João Batista Parra, 575
Praia do Suá - Vitória - ES
CEP 72620-000
Tel.: (27) 2121.8595
Endereço eletrônico:
www.tre-es.jus.br

Comissão de Segurança da Informação

NSI-012	V1.0 - FEV-2025	SEGURANÇA DA INFORMAÇÃO

Norma de Gerenciamento de Vulnerabilidades

Referência(s):

Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)

Resolução CNJ 396/2021 – ENSEC-PJ

Resolução-CNJ 370/2021 - ENTIC-JUD

Resolução TSE 23.644/2021 – PSI/JE

Resolução TSE 23.650/2021 – Política Geral de Privacidade e Proteção de Dados Pessoais

Palavras Chave: segurança, norma, configuração, ambientes | 8 páginas

1. Prefácio

A presente norma está alinhada às diretrizes de Segurança da Informação e dos Dados Pessoais estabelecidas na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) e na Política de Segurança da Informação da Justiça Eleitoral (PSI-JE).

2. Objetivo

Garantir a segurança da infraestrutura tecnológica, com adoção das seguintes ações:

2.1. **Prevenção da Exploração:** visando evitar a exploração de vulnerabilidades técnicas na infraestrutura de sistemas e redes, reduzindo a probabilidade de ataques maliciosos.

2.2. **Identificação Oportuna:** visando detectar e identificar vulnerabilidades de forma rápida e eficaz, possibilitando uma resposta imediata para minimizar o tempo de exposição a potenciais ameaças.

2.3. **Classificação de Riscos:** visando classificar as vulnerabilidades de acordo com sua criticidade e potencial impacto, permitindo uma abordagem estratégica para priorização e alocação de recursos.

2.4. **Avaliação de Exposição:** visando avaliar a exposição da organização a vulnerabilidades, considerando a interconexão de sistemas e identificando áreas críticas que requerem atenção prioritária.

2.5. **Adoção de Medidas Preventivas**: visando implementar ações técnicas preventivas, conforme normas e boas práticas, para fortalecer a segurança dos ativos de TI e reduzir a superfície de ataque.

2.6. **Obtenção de Informações Atualizadas:** visando manter a equipe técnica atualizada com informações relevantes sobre novas vulnerabilidades e ameaças, garantindo uma abordagem proativa na gestão de riscos.

2.7. **Resposta Eficaz:** visando adotar medidas corretivas e tempestivas para lidar com os riscos identificados, minimizando o impacto de possíveis incidentes de segurança.

2.8. **Melhoria Contínua:** visando promover a melhoria contínua do processo, aprendendo com eventos passados, atualizando políticas e procedimentos, e fortalecendo constantemente a postura de segurança da organização.

3. Abrangência

Esta norma se aplica à infraestrutura tecnológica do Tribunal, incluindo os ativos: rede de dados, equipamentos servidores, computadores de uso geral, banco de dados e sistemas corporativos.

4. Das definições

Para efeitos desta norma consideram-se as seguintes definições:

4.1. **Ameaça:** causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;

4.2. **Vulnerabilidade:** fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

4.3. **Risco:** potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;

4.4. **Ativo de informação:** todo dado ou informação gerado, adquirido, utilizado ou custodiado pela Justiça Eleitoral, assim como qualquer equipamento, software ou recurso utilizado para seu processamento ou armazenamento.

4.5. **Common Vulnerabilities and Exposures (CVE):** é um banco de dados que registra vulnerabilidades e exposições relacionadas a segurança da informação conhecidas publicamente.

5. Do monitoramento de bases de vulnerabilidades

5.1. Constituem-se controles mínimos para definição das fontes de dados de vulnerabilidades:

5.1.1. **Qualidade das informações:** verificar se as informações fornecidas pela fonte são precisas e atualizadas (algumas apenas repassam notícias ou informações de outras fontes);

5.1.2. **Disponibilidade das informações:** verificar a frequência de atualização das informações fornecidas pela fonte (a vulnerabilidade técnica pode ser explorada por um período mais longo se a fonte demorar muito para atualizar suas informações);

5.1.3. **Legitimidade da fonte:** verificar se a fonte é representante autorizado do responsável pela informação (como fóruns específicos de fabricantes para comunicação com seus clientes ou fornecimento de patches) ou reconhecida como confiável pela comunidade de segurança da informação:

5.2. Os controles mínimos estabelecidos **no subitem 5.1** devem ser aplicados para monitorar regularmente sítios de fabricantes, fóruns especializados, grupos especiais e outras fontes de consulta para obter informações relacionadas a vulnerabilidades técnicas e medidas de correção.

5.3. Constituem-se informações técnicas essenciais para a gestão de vulnerabilidades a serem buscadas em fontes de dados confiáveis:

5.3.1. Notícias e alertas sobre ameaças, vulnerabilidades, ataques e *patches*, com especial atenção às vulnerabilidades de dia zero;

5.3.2. Melhores práticas de segurança da informação adotadas pelo mercado: políticas, procedimentos, diretrizes e listas de verificação;

5.3.3. Tendências do mercado de segurança da informação relacionadas ao setor: leis e regulamentos, requisitos de clientes e soluções de fornecedores;

5.3.4. Dados sobre segurança da informação de consultorias especializadas, outras organizações, polícia, agências de segurança do governo ou congêneres;

5.3.5. Notícias relacionadas a novas tecnologias e produtos.

6. Da descoberta de vulnerabilidades técnicas

6.1. Constituem-se controles mínimos a serem aplicados na descoberta de vulnerabilidade técnicas:

6.1.1. Utilização de ferramentas automatizadas atualizadas e de rotinas regulares de varreduras;

6.1.2. Utilização da fonte Common Vulnerabilities and Exposures (CVE) como base para a verificação de vulnerabilidades nos ativos de processamento;

6.1.3. Assegurar-se que somente varreduras de vulnerabilidades autorizadas possam ser executadas, local ou remotamente, e configuradas com direitos elevados nos ativos de processamento que estão sendo testados

6.1.4. Utilização de credencial (ou conta de acesso) dedicada para varreduras de vulnerabilidades, que não deve ser usada para outras atividades administrativas e deve estar vinculada aos equipamentos específicos em endereços de *Internet Protocol (IP)* específicos.

7. Da avaliação da exposição

7.1. Constituem-se controles mínimos a serem aplicados para analisar e avaliar os riscos de uma vulnerabilidade afetar o ambiente da rede corporativa:

7.1.1. Consulta ao inventário de ativos visando identificar quais ativos de processamento serão afetados pela vulnerabilidade, o valor dos ativos para a organização, os requisitos de segurança da informação e a classificação de segurança;

7.1.2. Verificação de como a vulnerabilidade técnica pode afetar o ambiente da rede corporativa, considerando interfaces e interdependências internas e externas, requisitos de segurança da informação implementados e classificação de segurança dos ativos de processamento considerados críticos;

7.1.3. Avaliação quanto à necessidade de criar ambiente de teste, realizar provas de conceito (*Proofs of Concept ou PoCs*), desativar serviços/funcionalidades ou aplicar *patches* de correção;

8. Do tratamento de vulnerabilidades técnicas

8.1. Constituem-se controles mínimos a serem aplicados para corrigir as vulnerabilidades técnicas ou minimizar a probabilidade de exploração:

8.1.1. Observância do Processo de Gerenciamento de Incidentes vigente;

8.1.2. Adoção de testes e homologação da correção da vulnerabilidade técnica antes de ser instalada no ambiente da rede corporativa;

8.1.3. Registro dos procedimentos para correção da vulnerabilidade técnica, contemplado instalação, configuração, regras estabelecidas e procedimentos de restauração, quando for o caso;

8.1.4. Geração de registros de eventos (*logs*) das ações realizadas para correção da vulnerabilidade técnica.

8.2. Quando não existir a possibilidade de correção de uma vulnerabilidade crítica ou alta - seja por impossibilidade de atualização de software ou alteração de configuração - desde que devidamente justificado, a situação deverá ser repassada para a CSI, para decidir sobre outras formas de tratamento, como:

8.2.1. Desativação de serviços relacionados à vulnerabilidade;

8.2.2. Aumento do monitoramento relacionado ao ativo para detectar ou prevenir ataques reais;

8.2.3. Aumento da conscientização sobre a vulnerabilidade;

8.2.4. Implementação de controles de segurança compensatórios, quando possível.

8.3. As mudanças no ambiente da rede corporativa motivadas pelas correções das vulnerabilidades técnicas devem ser implantadas de forma a causar o menor impacto possível na utilização dos sistemas administrativos.

9. Da avaliação de resultados

9.1. Constituem-se controles mínimos a serem aplicados para analisar criticamente os resultados da gestão de vulnerabilidades:

9.1.1. Comparação regular de resultados consecutivos de varreduras para verificar se as vulnerabilidades encontradas foram corrigidas em tempo hábil;

9.1.2. Acompanhamento regular do nível de exposição dos principais ativos de processamento;

9.1.3. Acompanhamento regular do resultado das varreduras, visando verificar a evolução do número de vulnerabilidades encontradas no ambiente da rede corporativa;

9.1.4. Comunicação à Comissão de Segurança da Informação (CSI) sobre os resultados de detecção e tratamento das vulnerabilidades críticas e altas insanáveis no ambiente computacional;

9.1.5. Proposição à CSI de melhorias nos processos de gestão de vulnerabilidades.

10. Das responsabilidades

10.1. À área técnica responsável pela cibersegurança caberá:

10.1.1. Monitorar regularmente sítios de fabricantes, fóruns especializados, grupos especiais e outras fontes de consulta, para obter informações relacionadas a vulnerabilidades técnicas e medidas de correção;

10.1.2. Acionar ferramentas automatizadas e métodos para a identificação de vulnerabilidades técnicas no ativo, assegurando a execução de verificações na periodicidade mínima definida para cada tipo de ativo no procedimento vigente de Gestão de Vulnerabilidades;

10.1.3. Analisar e avaliar os riscos das vulnerabilidades técnicas detectadas;

10.1.4. Comunicar-se com a ETIR (Equipe Técnica de Resposta a Incidentes de Segurança Cibernética) e com as áreas da Secretaria de TI responsáveis pelos ativos, a fim de informar e obter informações acerca de vulnerabilidades existentes;

10.1.5. Acompanhar a detecção e o tratamento das vulnerabilidades através de ferramenta automatizada específica e documentação produzida pelas unidades;

10.1.6. Reportar à CSI sobre vulnerabilidades críticas e altas insanáveis detectadas nos ativos do TRE-ES.

10.2. Para efeitos desta norma, fica estabelecido o Núcleo de Segurança Cibernética da Secretaria de Tecnologia da informação como a área técnica responsável pela cibersegurança.

10.3. À unidade responsável pela administração do ativo deverá:

10.3.1. Configurar as ferramentas para detecção de vulnerabilidades nos ativos sob sua responsabilidade;

10.3.2. Planejar e corrigir as vulnerabilidades técnicas encontradas ou aplicar controles para minimizar a probabilidade de exploração enquanto não for possível a correção definitiva;

10.3.3. Implementar as correções das vulnerabilidades de forma a gerar o menor impacto para os usuários da infraestrutura do TRE-ES;

10.3.4. Informar aos usuários sempre que uma correção de vulnerabilidade possa gerar interrupção nos serviços do TRE-ES;

10.3.5. Informar à área técnica responsável pela segurança cibernética sobre vulnerabilidades críticas e altas insanáveis detectadas em seus ativos.

10.3.6. Guardar os registros de logs relativos às correções de vulnerabilidades;

10.4. Para efeitos desta norma, fica estabelecida a:

10.4.1. Seção de Gestão de Infraestrutura e Redes como área técnica responsável pelos ativos de rede, incluindo equipamentos servidores;

10.4.2. Seção de Administração e Inteligência de Dados como área técnica responsável pelos ativos de banco de dados;

10.4.3. Seção de Gestão de Serviços de TIC e Microinformática como área responsável pelos ativos de microinformática, incluindo computadores *desktops e notebooks.*

10.4.4. Coordenadoria de Sistemas Corporativos, Governança e Inovação Tecnológica como área responsável pelos ativos de *software*.

11. Disposições finais

11.1. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação (CSI).

11.2. A revisão desta norma ocorrerá sempre que se fizer necessário ou conveniente para o TRE-ES.

11.3. O descumprimento desta norma deve ser imediatamente registrado como incidente de segurança e comunicado à CSI para apuração e consequente adoção das providências cabíveis.

11.4. Esta norma entra em vigor na data de sua publicação.