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-015	V1.0 - FEV 2025	SEGURANÇA DA INFORMAÇÃO

Norma de Configuração Segura de Ambientes

Referência(s):

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

Resolução CNJ 396/2021 – ENSEC-PJ

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 | 5 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

Dispõe sobre a configuração segura de ambientes no âmbito do Tribunal Regional Eleitoral do Espírito Santo (TRE-ES).

3. Das disposições preliminares

3.1. Para os efeitos desta norma deverá ser realizada a classificação de risco dos dados manipulados/armazenados no ativo corporativo contemplando pelo menos três níveis:

3.1.1. Risco alto

3.1.2. Risco moderado

3.1.3. Risco baixo.

4. **Da classificação dos tipos de ativos corporativos**

4.1. Os controles mínimos estabelecidos nos incisos deste artigo visam estabelecer e manter a configuração segura de ativos corporativos (dispositivos de usuário(a) final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não computacionais/ IoT; e servidores) e software (sistemas operacionais e aplicações) no ambiente da rede corporativa da justiça eleitoral de acordo com a seguinte classificação: (CIS Controls 04.01)

4.1.1. ATIVOS DE INFRAESTRUTURA REDE, quais sejam os dispositivos de rede (ex. firewall, roteadores, switches, etc.);

4.1.2. ATIVOS DE APLICAÇÕES, quais sejam os sistemas operacionais e aplicações;

4.1.3. ATIVOS DE USUÁRIOS, quais sejam os(as) usuários(as) finais;

4.1.4. ATIVOS DE DISPOSITIVOS, quais sejam os dispositivos de usuário(a) final, incluindo portáteis, dispositivos não computacionais/ IoT e móveis, e equipamentos servidores;

5. **Da configuração segura para os ativos de infraestrutura de redes**

5.1. Deverá ser estabelecido e mantido um processo de configuração segura para os ativos de rede contemplando no mínimo: (CIS Controls 04.02)

5.1.1. Revisão e atualização da documentação anualmente ou quando ocorrerem mudanças significativas no ambiente que possam impactar esta medida de segurança; (CIS Controls 04.02)

5.1.2. Uso de infraestrutura como código (IaC) qual seja o gerenciamento e provisionamento da infraestrutura por meio de códigos, em vez de processos manuais.

5.1.3. Aplicação de procedimentos de *hardening* nos ativos de rede e servidores contemplando no mínimo a limitação do acesso à interface de gerência em interfaces e/ou endereços IP controlados.

5.1.4. A infraestrutura de rede deve ser mantida atualizada, executando sempre a versão mais recente e estável do software e verificando se ainda é suportado pelo fabricante. (CIS Controls 12.01)

6. Da configuração segura para os ativos de aplicações

6.1.1. Gerenciamento dos ativos e software corporativos com implementações de gestão de configuração que no mínimo seja contemplado:

6.1.1.1. Acesso a interfaces administrativas por meio de protocolos de rede seguros, como Secure Shell (SSH) e Hypertext Transfer Protocol Secure (HTTPS); (CIS Controls 04.06)

6.1.1.2. Não utilização de protocolos de gestão inseguros, como Telnet (Teletype Network) e HTTP, a menos que seja operacionalmente essencial; (CIS Controls 04.06)

7. Da configuração segura para os ativos de usuários

7.1. Deverá ser estabelecido e mantido um processo de configuração segura para os ativos de usuários da rede corporativa da Justiça Eleitoral que contemple:

7.1.1. Configuração de bloqueio automático de sessão nos ativos corporativos após um período definido de inatividade.

7.1.1.1. Para sistemas operacionais de uso geral, o período não deve exceder 15 minutos. (CIS Controls 04.03)

7.1.1.2. Para dispositivos móveis de usuário(a) final, o período não deve exceder 2 minutos. (CIS Controls 04.03)

7.1.2. Desativação ou inutilização das contas padrão nos ativos e software corporativos quando possível. (CIS Controls 04.07)

8. Da configuração segura para os ativos de dispositivos

8.1. Deverá ser estabelecido e mantido um processo de configuração segura para os ativos de dispositivos dos(as) usuários(as) da rede corporativa da Justiça Eleitoral que contemple:

8.1.1. A implementação e gerenciamento de firewall nos servidores, onde houver suporte. Essas implementações podem incluir firewall virtual, firewall do sistema operacional ou um agente de firewall de terceiros. (CIS Controls 04.04)

8.1.2. A implementação e gerenciamento de firewall baseado em host ou uma ferramenta de filtragem de porta nos dispositivos de usuário(a) final, com uma regra de negação padrão de bloqueio de todo o tráfego, exceto os serviços e portas que são explicitamente permitidos. (CIS Controls 04.05)

8.1.3. A desinstalação ou desativação de todos os serviços desnecessários nos ativos e software corporativos. (CIS Controls 04.08)

8.1.4. Configuração de servidores DNS confiáveis nos ativos corporativos, preferencialmente servidores DNS controlados pela Justiça Eleitoral e/ou servidores DNS confiáveis acessíveis externamente caso seja imprescindível para a operação; (CIS Controls 04.09)

8.1.5. A imposição de bloqueio automático do dispositivo seguindo um limite pré-determinado de tentativas de autenticação local com falha nos dispositivos portáteis de usuário final, quando compatível. (CIS Controls 04.10)

8.1.5.1. Para laptops, não deve ser permita mais de 5 tentativas de autenticação com falha;

8.1.5.2. Para tablets e smartphones, não mais do que 3 tentativas de autenticação com falha.

8.1.6. A limpeza remota dos dados corporativos de dispositivos portáteis de usuário final de propriedade da Justiça Eleitoral para dispositivos perdidos ou roubados, ou quando do desligamento do usuário das atividades exercidas na Justiça Eleitoral. (CIS Controls 04.12)

9. Disposições finais

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

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

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

9.4. Esta norma entra em vigor na data de sua publicação e sua implementação se fará no prazo de 12 meses a contar da data de sua publicação.