



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-005

V4.0 - JUN 2025

SEGURANÇA DA INFORMAÇÃO

Norma de Desenvolvimento, Implantação e Gestão de Sistemas com foco na Segurança da Informação

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

Portaria DG/TSE 444/2021, instituição da norma de termos e definições relativa
à Política de Segurança da Informação do Tribunal Superior Eleitoral

ABNT ISO/IEC 27001 e ABNT NBR ISO/IEC 27002

ABNT ISO/IEC 27005 e ABNT ISSO/IEC 27701

Palavras-Chave: segurança, norma, sistemas, implantação

10 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), na Política de Segurança da Informação da Justiça Eleitoral (PSI-JE) e na Lei Geral de Proteção de Dados Pessoais (LGPD).

2. Objetivo

Estabelecer as diretrizes de segurança para desenvolvimento, implantação e gestão de Sistemas de Informação no âmbito do Tribunal Regional Eleitoral do Espírito Santo.

3. Abrangência

Esta norma se aplica a todos os Sistemas de Informação desenvolvidos pela equipe técnica do TRE/ES e aos Sistemas de Informação desenvolvidos por outros órgãos, candidatos a serem implantados na infraestrutura tecnológica do Tribunal – Intranet e Internet. Essa

norma não se aplica aos Sistemas Eleitorais homologados pelo TSE, que possuem normativos de segurança próprios para implantação e gestão.

4. Do Desenvolvimento de Sistemas de Informação com foco na segurança

- 4.1. O desenvolvimento de Sistemas de Informação no âmbito do TRE/ES deve ter foco no desenvolvimento seguro e na proteção dos dados pessoais, com utilização de técnicas próprias para esses fins.
- 4.2. Devem ser mantidos ambientes logicamente separados para desenvolvimento, homologação e produção de sistemas, com controles técnicos e administrativos que garantam a independência e o isolamento entre eles.
- 4.3. É vedada a execução de testes em ambiente de produção.
- 4.4. Toda migração de código ou base de dados entre ambientes deve ser auditável, com registro de responsáveis, datas e justificativas.
- 4.5. Para sistemas cujo desenvolvimento ou homologação ocorra utilizando cópias parciais ou totais de bases de dados de produção, devem ser adotadas medidas específicas para proteção dos dados pessoais e sensíveis.
- 4.6. É obrigatório operar com dados anonimizados em ambientes de desenvolvimento e homologação, exceto se houver impedimento técnico devidamente justificado, caso em que se deve adotar as seguintes medidas adicionais de proteção:
 - a) Controle de acesso baseado em funções e mínima atribuição de privilégios;
 - b) Monitoramento contínuo de acessos e atividades;
 - c) Todos os demais controles de segurança aplicados ao ambiente de produção.
- 4.7. A disponibilização das bases de dados de produção para desenvolvimento ou homologação deve ser obrigatoriamente precedida de:
 - 4.7.1. Solicitação em processo formalizado iniciado pela área responsável pelo desenvolvimento de sistemas, indicando:
 - a) Conjunto de dados a ser disponibilizado

- b) Campos que devem ser mascarados, caso haja dados pessoais envolvidos
 - c) Justificativa técnica, caso haja campos com dados pessoais que não podem ser mascarados.
 - d) Indicação dos técnicos que terão acesso e o tipo de acesso
 - e) Período de disponibilização, para as bases de homologação.
- 4.7.2. Informação da área de administração e inteligência de dados sobre a forma anonimização ou proteção utilizada.
- 4.7.3. Aprovação do responsável pela unidade solicitante.
- 4.8. As informações previstas em 4.7.1, “a” a “d” só são necessárias quando houver a solicitação de cópia de uma nova base de dados ou quando houver mudança estrutural que implique na necessidade de mascaramento de novos campos.
- 4.9. O acesso aos ambientes de desenvolvimento e homologação será concedido exclusivamente a perfis autorizados formalmente e mediante registro de aceite de termo específico de confidencialidade, com identificação clara do tipo de vínculo (servidor, estagiário, terceirizado);
- 4.10. Devem ser mantidos registros de log de acesso às bases de dados de desenvolvimento e homologação pelo período mínimo de 12 meses.

5. Da implantação de Sistemas de Informação com foco na segurança

- 5.1. A implantação de Sistemas de Informação na infraestrutura tecnológica administrada pelo TRE/ES deve ser precedida de avaliação de segurança efetuada pela área técnica responsável pela gestão de Sistemas de Informação, com apoio das áreas de segurança cibernética, redes e banco de dados.
- 5.2. A avaliação de Segurança deverá ter como produto um Relatório Técnico com Parecer, que deverá ser armazenado em repositório próprio visando à Gestão da Segurança da Informação.
- 5.3. O Relatório Técnico, fruto da avaliação de segurança, deve conter, no mínimo:

- 5.3.1. Resultado da Análise de Vulnerabilidades do Sistema de Informação, efetuada em softwares próprios para esse fim.
- 5.3.2. Informação sobre aplicação ou não de técnicas de desenvolvimento seguro na codificação do sistema, descrevendo-as, de forma sucinta, quando estiverem presentes.
- 5.3.3. Informação sobre a linguagem de programação e/ou ferramentas tecnológicas usadas no desenvolvimento do Sistema de Informação, com informações sucintas sobre eventuais fragilidades de segurança nessa linguagem/ferramenta.
- 5.3.4. Informação sobre como se dará o processo de atualização de segurança do Sistema de Informação durante o seu ciclo de vida, incluindo as responsabilidades.
- 5.3.5. Informação sobre adequação de segurança do Sistema de Informação quanto à proteção dos dados pessoais, com indicação do responsável de negócio pelos dados.
- 5.4. O Parecer, fruto da avaliação de segurança, deve indicar, com base nas informações constantes no Relatório Técnico, se o sistema possui requisitos mínimos de segurança para ser implantado na infraestrutura tecnológica do TRE/ES.
 - 5.4.1. É permitida a implantação de Sistemas de Informação cujo Parecer Técnico indicar o cumprimento dos requisitos de segurança.
 - 5.4.2. Pareceres Técnicos que indicarem riscos de segurança insanáveis na implantação de Sistemas de Informação, serão encaminhados ao demandante que poderá submetê-los, motivadamente, à apreciação da Comissão de Segurança da Informação, que poderá:
 - 5.4.2.1. Justificadamente, autorizar a implantação do Sistema de Informação.
 - 5.4.2.2. Ratificar o Parecer Técnico

6. Da implantação de Sistemas de Informação por determinação normativa

- 6.1. Quando houver determinação expressa em lei ou em regulamento para implantação de um Sistema de Informação, ficam dispensadas, caso não seja possível obtê-las, as informações constantes nos subitens 5.3.2 a 5.3.5.

6.2. Caso seja viável, deverá ser efetuada a análise de vulnerabilidades do Sistema da Informação prevista no subitem 5.3.1.

6.2.1. Havendo indicação de riscos de segurança insanáveis, o resultado deve ser submetido à Comissão de Segurança da Informação, para fins de ciência e providências que entender cabíveis.

7. Da implantação de Sistemas de Informação desenvolvidos por outros Órgãos

7.1. No processo de acordo para disponibilização de Sistema de Informação desenvolvido em outro Órgão, devem constar as informações necessárias à produção do Relatório Técnico previsto em 5.3, sendo:

7.1.1. Aplicação ou não de técnicas de desenvolvimento seguro, descrevendo-as, de forma sucinta, quando estiverem presentes.

7.1.2. Informação sobre a linguagem de programação e/ou ferramentas tecnológicas usadas no desenvolvimento do sistema de informação.

7.1.3. Informações e/ou artefatos necessários que indiquem como devem ser efetuadas as atualizações de segurança ao longo do ciclo de vida.

7.1.4. Informação sobre adequação de segurança do sistema de informação quanto à proteção dos dados pessoais, se couber.

7.1.5. Informações completas sobre a documentação do sistema ou acesso ao repositório com a documentação.

8. Da disponibilização de Sistemas de Informação e Serviços na Internet

8.1. Os Sistemas de Informação disponibilizados na Internet devem, obrigatoriamente, prover:

8.1.1. Mecanismo de autenticação de múltiplo fator (MFA).

8.1.2. Mecanismo de registro de acesso com retenção de 1 ano.

8.1.3. Mecanismo de tráfego criptografado de senhas e dados pessoais.

8.2. Os Serviços disponibilizados na Internet devem, obrigatoriamente, prover mecanismo de tráfego criptografado.

8.3. Outros mecanismos de segurança podem ser implementados, conforme necessidade.

9. Da conformidade dos sistemas com os requisitos de negócio

- 9.1. Todo sistema implantado no âmbito do TRE deve ser homologado pela área de negócio que utilizará o sistema.
- 9.2. O prazo de homologação é de até 30 dias, podendo ser estendido por mais 15 dias, mediante solicitação tempestiva à área de desenvolvimento, salvo o disposto em 9.5.
- 9.3. Ao término do prazo de 45 dias, caso a área de negócio não consiga efetuar os testes, deve, solicitar, justificadamente, novo prazo ao Comitê Gestor de TIC (CETIC), demonstrando as ações efetuadas no decorrer do período e indicando o que ainda precisa ser verificado.
- 9.4. O CETIC deverá avaliar o pedido e deliberar sobre novo período de homologação, que pode ser imediato ou não, considerando outros sistemas em desenvolvimento e homologação e a disponibilidade da equipe para apoio à homologação.
- 9.5. Caso o sistema em homologação esteja sendo implantado em substituição a outro que apresenta risco de segurança insanável e encontra-se em produção, a solicitação de ampliação do prazo de 30 dias deverá ser submetida à Comissão de Segurança da informação que deverá deliberar sobre:
 - 9.5.1. Ampliação do prazo.
 - 9.5.2. Manutenção, em produção, do sistema vulnerável.

10. Da Gestão de Segurança dos Sistemas de Informação

- 10.1. A área técnica responsável pela gestão dos Sistemas de Informação deve efetuar Análise de Vulnerabilidades periódica dos Sistemas de Informação, corrigir vulnerabilidades classificadas como críticas ou altas e, caso não seja possível, apresentar à Comissão da Segurança da Informação qualquer resultado que indique risco de segurança insanável à Infraestrutura.
- 10.2. A área técnica responsável pela gestão dos Sistemas de Informação deve efetuar atualizações periódicas de segurança nos Sistemas de Informação e nos Servidores de Aplicação, com apoio da área responsável pela infraestrutura de redes, no que couber.
- 10.3. Com o intuito de promover a segurança da rede, em situações iminentes de ataques ou identificação de vulnerabilidades críticas de alto impacto, a área

técnica responsável pela gestão dos Sistemas de Informação poderá bloquear e/ou limitar o acesso ou retirar o sistema ou serviço de produção, comunicando imediatamente à Comissão de Segurança da Informação e à Administração do Tribunal.

11. Das responsabilidades

11.1. Do Comitê Gestor de TIC (CETIC):

- 11.1.1. Avaliar ampliação de prazo de homologação de sistema, desde que não esteja sendo implementado em substituição a sistema que apresente risco de segurança insanável.

11.2. Da Comissão de Segurança da Informação:

- 11.2.1. Apreciar os Pareceres Técnicos que indiquem riscos insanáveis de segurança na implantação de um Sistema de Informação.
- 11.2.2. Adotar providências em relação a Sistemas de Informação com determinação normativa para implantação e que apresentem riscos de segurança insanáveis.
- 11.2.3. Decidir sobre o bloqueio de Sistemas de Informação em produção nos quais forem identificadas vulnerabilidades críticas insanáveis por ocasião de análise de vulnerabilidades periódica.
- 11.2.4. Deliberar sobre ampliação de prazo de homologação de sistema que esteja sendo implantado para substituir sistema em produção que apresenta vulnerabilidade crítica insanável.
- 11.2.5. Manter atualizados os dispositivos desta norma.

11.3. Da área técnica responsável pela gestão dos Sistemas de Informação:

- 11.3.1. Produzir relatório técnico de segurança e emitir parecer relativo a riscos de implantação de Sistemas de Informação.
- 11.3.2. Comunicar à Comissão de Segurança da Informação sobre sistemas em produção que apresentem riscos à segurança.
- 11.3.3. Bloquear e/ou limitar o acesso, bem como retirar de produção, sistema ou serviço que esteja em risco iminente de ataque.

- 11.3.4. Apoiar tecnicamente a Comissão de Segurança de Informação nas deliberações sobre implantação e gestão segura de sistemas de informação.
- 11.3.5. Efetuar a gestão de segurança dos Sistemas de Informação.
- 11.3.6. Informar à Comissão de Segurança de Informação violações à norma identificadas.
- 11.3.7. Comunicar os usuários quanto à realização de manutenções programadas nos Sistemas de Informação que venham a causar indisponibilidade.
- 11.4. Das áreas técnicas responsáveis pela Segurança Cibernética, Rede de Comunicação de Dados e Administração e Inteligência de Dados:
 - 11.4.1. Efetuar atualizações de segurança de servidores e bases de dados sob sua responsabilidade, para fins de garantia da segurança dos Sistemas de Informação, comunicando à área técnica responsável pela gestão dos Sistemas de Informação, quando houver impacto nos Sistemas de Informação.
 - 11.4.2. Apoiar, no que couber, a área responsável de gestão dos Sistemas de Informação, quanto à realização de Análise de Vulnerabilidades das aplicações e segurança dos dados pessoais.
- 11.5. Da área técnica responsável pela Administração e Inteligência de Dados:
 - 11.5.1. Documentar a forma de anonimização ou de proteção de dados utilizada nas bases de dados de desenvolvimento e homologação.
 - 11.5.2. Implantar os controles de segurança exigidos para bases de dados de desenvolvimento ou homologação não anonimizadas.
- 11.6. Do responsável pela unidade solicitante da cópia da base de dados de produção para desenvolvimento ou homologação.
 - 11.6.1. Encaminhar as informações necessárias para viabilizar a cópia das bases de acordo com os parâmetros estabelecidos nesta norma.

12. Das disposições Transitórias

- 12.1. Até o final do ano de 2027 todos os Sistemas de Informação implantados na infraestrutura tecnológica do Tribunal deverão estar adequados aos termos desta norma.
- 12.2. No prazo máximo de 12 meses, todas as bases de dados já disponibilizadas em ambiente de desenvolvimento e homologação devem passar por processos de adequação aos termos estabelecidos nesta norma.
- 12.3. O código-fonte de aplicações legadas que contenham credenciais sensíveis embutidas deve ser submetido a processo gradual de **refatoração segura**, com prioridade para os sistemas acessíveis por rede externa ou que manipulem dados pessoais.
- 12.4. Até a conclusão da refatoração, devem ser adotadas barreiras compensatórias, como:
- a) Controle de acesso estrito ao repositório;
 - b) Segmentação de rede dos servidores que executam tais aplicações;
 - c) Monitoramento em tempo real das conexões e logs de execução.

13. Das disposições Finais

- 13.1. Os Relatórios, Pareceres e Registros de Acesso deverão estar disponíveis para fins de auditoria autorizada pela Administração, e de investigação de ilícitos cibernéticos.
- 13.2. As áreas técnicas responsáveis pela Rede de Comunicação de Dados e pelos Sistemas de Informação devem adotar as providências para prover e manter atualizadas as ferramentas de Gestão de Vulnerabilidades, a fim de garantir o cumprimento desta norma.
- 13.3. Os casos omissos nesta norma deverão ser resolvidos pela Comissão de Segurança da Informação.

14. Da vigência e atualização

- 14.1. Esta norma operacional entra em vigor a partir da data de sua publicação e sua atualização ocorrerá sempre que se fizer necessária.