I - Privacy By Design: assegura que a proteção de dados pessoais deverá ser estabelecida desde a concepção do software ou componente compreendendo todo o ciclo de vida, devendo a equipe realizar uma abordagem proativa na proteção de dados pessoais; e

II - Privacy By Default: o software deverá resguardar a exposição de dados pessoais salvaguardando a privacidade, sendo o mais restritivo possível tanto na exposição/visualização de dados pessoais quanto na coleta;

Art. 17. As vulnerabilidades com dados pessoais terão prioridade sobre as demais, para as suas correções.

T. V

DAS DISPOSIÇÕES FINAIS

Art. 18. Esta portaria deverá ser revisada a cada 12 meses.

Art. 19. Os casos omissos e eventuais dúvidas quanto à aplicação desta norma serão dirimidos pela Comissão Permanente de Segurança da Informação deste Tribunal.

Art. 20. Esta Portaria entra em vigor na data de sua publicação e sua implementação iniciará imediatamente e deverá estar totalmente implantada no prazo de 24 (vinte e quatro) meses a contar desta data.

Natal/RN, 12 de dezembro de 2023.

Desembargador Cornélio Alves

Presidente

PORTARIA N° 242/2023 - GP

Dispõe sobre a implantação e gestão de sistemas com foco na segurança da informação do Tribunal Regional Eleitoral do Rio Grande do Norte.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE, no uso das atribuições que lhe são conferidas pelo artigo 20, inciso XIX, da Resolução nº 09/2012 - TRE/RN, e

CONSIDERANDO a necessidade de apoiar a gestão dos riscos de segurança da informação do TRE/RN, cuja avaliação periódica é condição para implementação e operação do SGSI - Sistema de Gestão de Segurança da Informação;

CONSIDERANDO a Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Resolução CNJ nº 370/2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO a Portaria DG/TSE nº 444/2021, que dispõe sobre a instituição da norma de termos e definições relativas à Política de Segurança da Informação do Tribunal Superior Eleitoral;

CONSIDERANDO a Resolução TRE/RN nº 110/2023, que institui a Política de Segurança da Informação (PSI) no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte;

CONSIDERANDO as boas práticas em segurança das informações previstas nas normas ABNT ISO/IEC 27001 e ABNT NBR ISO/IEC 27002;

CONSIDERANDO as boas práticas em gestão de riscos de segurança cibernéticos na norma ABNT ISO/IEC 27005 versão 2019 baseada no Processo de Gestão de Riscos estabelecido na ISO 31:000:2018;

CONSIDERANDO a necessidade de gerenciar os riscos que envolvem o tratamento de dados pessoais, de acordo com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados);

CONSIDERANDO que a segurança da informação e a proteção de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos do Tribunal Regional Eleitoral do Rio Grande do Norte, e tendo em vista o que consta no Processo PAE nº 10.487/2023;

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º A Implantação e Gestão de Sistemas com foco na segurança da informação, no âmbito do Tribunal, observará as disposições contidas nesta portaria.

Art. 2º 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)

Art. 3° Esta norma se aplica a:

I - Sistemas de informação desenvolvidos pela equipe técnica do TRE/RN;

II - Sistemas de informação desenvolvidos por outros órgãos, candidatos a serem implantados na infraestrutura tecnológica do Tribunal; e

III - *Softwares* infraestruturantes relacionados aos serviços de TI, a exemplo do Moodle, GLPI, Tenable, Gitlab, Jenkins, dentre outros.

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

CAPÍTULO II
DO DESENVOLVIMENTO DE SISTEMAS DE INFORMAÇÃO
COM FOCO NA SEGURANÇA

Art. 4º O desenvolvimento de Sistemas de Informação no âmbito do TRE/RN deve ter foco no desenvolvimento seguro e na proteção dos dados pessoais, com utilização de técnicas próprias para esses fins.

Art. 5º O desenvolvimento seguro de Sistemas de Informação deve considerar as seguintes melhores práticas, dentre outras:

I - *Modelagem de ameaças*: analisar a arquitetura de software e identificar potenciais ameaças de segurança e vulnerabilidades;

II - *Codificação segura de software*: adesão a práticas de codificação seguras, tais como validação de entrada de dados, armazenamento seguro de dados e uso de protocolos de comunicação seguros;

III - *Revisão de código*: revisar o código escrito pelos desenvolvedores para identificar possíveis problemas de segurança;

IV - *Testes*: realizar testes de segurança regularmente, incluindo testes de penetração e varreduras de vulnerabilidades;

V - *Gerenciamento de configuração de segurança*: configurar controles de acesso e configurações de redes;

VI - *Controle de acesso*: garantir que somente pessoal autorizado pode acessar o software, por meio da implementação de mecanismos de autenticação e autorização;

VII - *Atualizações e patches regulares*: manter o software atualizado com patches de segurança e atualizações de todos os componentes, de forma a corrigir vulnerabilidades de segurança e reduzir o risco de violações de segurança;

VIII - *Treinamento em segurança*: capacitar a equipe envolvida em todo o processo de desenvolvimento para entender e implementar as melhores práticas para desenvolvimento de software seguro;

IX - *Resposta a incidentes*: ter um plano bem definido para responder a incidentes de segurança, de modo a permitir recuperação em incidentes de segurança; e

X - *Monitoramento contínuo*: permitir detectar e responder a incidentes de segurança em tempo real, por meio do monitoramento de logs de sistemas e tráfego de rede.

XI - *Uso de ferramentas para análise estática de código (SAST)*: detectar e prevenir falhas de segurança introduzidas a nível de código-fonte.

CAPÍTULO III

DA IMPLANTAÇÃO DE SISTEMAS DE INFORMAÇÃO

Art. 6º A implantação de Sistemas de Informação na infraestrutura tecnológica do TRE/RN deve ser precedida de avaliação de segurança efetuada pela área técnica responsável pela Segurança da Informação.

§ 1º A avaliação de segurança a que se refere o caput deve ser realizada a partir de um Relatório Técnico de Segurança (*Anexo A*) a ser apresentado pelos setores responsáveis pela implantação dos Sistemas de Informação, podendo ser subsidiado com informações técnicas a serem fornecidas pelas áreas de redes, banco de dados, implantação de sistemas e desenvolvimento, quando solicitados.

§ 2º O fruto da avaliação de segurança consiste na elaboração de um Parecer de Segurança (*Anexo B*), que, juntamente com o Relatório Técnico de Segurança, devem ser armazenados em repositório próprio visando a Gestão da Segurança da Informação.

Art. 7º O Relatório Técnico de Segurança deve conter os seguintes elementos, quando possíveis:

§ 1º Identificação do Sistema de Informação a ser implantado, incluindo o sistema operacional e as plataformas necessárias para sua implantação.

§ 2º A matriz de comunicação do Sistema de Informação com outras aplicações e serviços.

§ 3º Características gerais do sistema, como o seu tipo de acesso (interno ou externo); o mecanismo de autenticação a ser utilizado; o seu nível de disponibilidade e de *backup*.

§ 4º Informação sobre aplicação ou não de técnicas de desenvolvimento seguro na codificação do sistema, descrevendo-as, de forma sucinta.

§ 5º Informação sobre a linguagem de programação e/ou ferramentas tecnológicas usadas no desenvolvimento da solução, com informações sucintas sobre eventuais fragilidades de segurança nessa linguagem/ferramenta.

§ 6º Informação sobre como se dará o processo de atualização de segurança da solução, incluindo a indicação das áreas responsáveis.

§ 7º Informação sobre adequação de segurança do Sistema de Informação quanto à proteção dos dados pessoais.

§ 8º Resultado da análise de vulnerabilidades da solução, preferencialmente efetuada em *software* próprio para esse fim.

Art. 8º O Parecer de Segurança, fruto da avaliação de segurança, deve indicar, com base nas informações constantes no Relatório Técnico de Segurança, se o sistema possui requisitos mínimos de segurança para ser implantado na infraestrutura tecnológica do TRE/RN.

§ 1º É permitida a implantação de Sistemas de Informação cujo Parecer de Segurança indique o cumprimento dos requisitos de segurança.

§ 2º Pareceres de Segurança que indiquem riscos de segurança insanáveis na implantação de Sistemas de Informação devem ser submetidos à apreciação do Comitê Gestor de Tecnologia da Informação e Comunicação (COGESTIC), que poderá:

I - Justificadamente, autorizar a implantação do Sistema de Informação; e

II - Ratificar o Parecer Técnico e submetê-lo à Comissão Permanente de Segurança da Informação (CPSI).

§ 3º Caberá à Comissão Permanente de Segurança da Informação (CPSI) a decisão final sobre a implantação ou não de um Sistema de Informação com parecer técnico desfavorável à implantação.

CAPÍTULO IV

DA DISPONIBILIZAÇÃO DE SISTEMAS DE INFORMAÇÃO

E SERVIÇOS NA INTERNET

Art. 9º Os Sistemas de Informação disponibilizados na Internet devem, preferencialmente, prover:

I - mecanismo de autenticação de múltiplo fator (MFA), preferencialmente de caráter físico, como tokens e autenticações biométricas;

II - mecanismo de registro de logs de acesso com retenção de um ano; e

III - mecanismo de tráfego criptografado de senhas e dados pessoais.

Parágrafo único. Outros mecanismos de segurança adicionais podem ser implementados, conforme necessidade.

CAPÍTULO V

DA GESTÃO DE SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

Art. 10. As áreas técnicas responsáveis pela implantação e desenvolvimento dos Sistemas de Informação devem revisar periodicamente a necessidade de efetuar atualizações de segurança em seus componentes arquiteturais, bem como quaisquer outros que possam influenciar a segurança do ambiente, com apoio da área responsável pela infraestrutura de redes, no que couber.

Parágrafo único. Define-se o período de revisão das atualizações como não superior a um mês, podendo ser reduzido este período a critério da área técnica responsável pela gestão de Sistemas de Informação, devendo haver, preferencialmente, sempre que possível, atualizações automáticas nos ambientes.

Art. 11. Com o intuito de promover a segurança da rede, em situações iminentes de ataques ou identificação de vulnerabilidades críticas de alto impacto, as áreas técnicas da STIE ligadas à COSIS e à COINF poderão bloquear e/ou limitar o acesso ou retirar o sistema ou serviço de produção, comunicando imediatamente ao Comitê Gestor de Tecnologia da Informação e Comunicação (COGESTIC) e à Comissão Permanente de Segurança da Informação (CPSI).

CAPÍTULO VI

DAS ATRIBUIÇÕES

Art. 12. Ao Comitê Gestor de Tecnologia da Informação e Comunicação (COGESTIC) compete:

I - decidir sobre a implantação de Sistema de Informação, tomando por base a avaliação de segurança efetuada pela área técnica responsável pela Segurança da Informação e, quando necessário, submeter a referida demanda à análise da Comissão Permanente de Segurança da Informação (CPSI);

II - apreciar os Pareceres de Segurança que indiquem risco insanáveis de segurança na implantação de um sistema de Informação;

III - adotar providências em relação a Sistemas de Informação com determinação normativa para implantação e que apresentem riscos de segurança insanáveis;

IV - decidir sobre o bloqueio de Sistemas de Informação em produção nos quais forem identificadas vulnerabilidades críticas insanáveis por ocasião de análise periódica de vulnerabilidade; e

V - manter atualizados os dispositivos desta norma.

Art. 13. À Comissão Permanente de Segurança da Informação (CPSI) compete dar a decisão final sobre a implantação ou não de um Sistema de Informação com parecer técnico desfavorável à implantação.

Art. 14. Aos setores responsáveis pelo desenvolvimento e implantação dos Sistemas de Informação compete:

I - implementar melhores práticas para desenvolvimento de software seguro;

II - emitir, quando demandado, relatório sobre a linguagem de programação e/ou ferramentas tecnológicas usadas no desenvolvimento da solução, com informações sucintas sobre eventuais fragilidades de segurança nessa linguagem/ferramenta;

III - produzir o Relatório Técnico de Segurança visando subsidiar a análise de segurança a ser realizada pela área técnica responsável pela Segurança da Informação;
IV - comunicar à Seção de Segurança da Informação (SSI/COINF/STIE) e ao Comitê Gestor de Tecnologia da Informação e Comunicação (COGESTIC) sistemas em produção que apresentem riscos à segurança;
V - apoiar tecnicamente a Comissão Permanente de Segurança da Informação (CPSI) nas deliberações sobre implantação e gestão segura de Sistemas de Informação;
VI - efetuar a gestão de segurança dos Sistemas de Informação, realizando atualizações de segurança de servidores e bases de dados sob sua responsabilidade, para fins de garantia da segurança dos Sistemas de Informação; e apoiando, no que couber, a área técnica responsável pela Segurança da Informação, quanto à realização de análise de vulnerabilidades das aplicações e segurança dos dados pessoais;
VII - comunicar ao Comitê Gestor de Tecnologia da Informação e Comunicação (COGESTIC) acerca de violações à norma identificadas;
VIII - comunicar os usuários quanto à realização de manutenções programadas nos Sistemas de Informação que venham a causar indisponibilidade; e
IX - garantir a implementação de mecanismo de autenticação de múltiplo fator (MFA), preferencialmente de caráter físico, como tokens e autenticações biométricas, destinados aos Sistemas de Informação disponibilizados na Internet.
Art. 15. À área técnica responsável pela Segurança da Informação compete:
I - Emitir o Parecer de Segurança sobre Sistema de Informação a ser implantado em ambiente de produção;
II - Monitorar as análises de vulnerabilidades periódicas mensais dos Sistemas de Informação, produzindo relatório de Análise de Vulnerabilidade;
III - Garantir mecanismo de tráfego criptografado de senhas e dados pessoais para software a ser disponibilizado em ambiente de Internet; e
IV - Garantir mecanismo de registro de logs de acesso com retenção de um ano para os Sistemas de Informação disponibilizados na Internet.
CAPÍTULO VII
DAS RESPONSABILIDADES TRANSITÓRIAS
Art. 16. Os Sistemas de Informação já disponibilizados pelo TRE/RN na Internet devem ser adequados a esta norma no prazo máximo de um ano.
Art. 17. Todos os Sistemas de Informação implantados na infraestrutura tecnológica do TRE/RN devem ser adequados a esta norma no prazo máximo de dois anos.
CAPÍTULO VIII
DISPOSIÇÕES FINAIS
Art. 18. Os Relatórios, Pareceres e Registros de Acesso deverão estar disponíveis para fins de auditoria autorizada pela Administração e de investigação de ilícitos cibernéticos.
Art. 19. A área técnica responsável pela Segurança da Informação deve adotar as providências para prover e manter atualizadas as ferramentas de gestão de vulnerabilidades, a fim de garantir o cumprimento desta norma.
Art. 20. Os casos omissos deverão ser resolvidos pelo Comitê Gestor de Tecnologia da Informação e Comunicação (COGESTIC).
Art. 21. Esta Portaria entra em vigor na data de sua publicação.
Natal/RN, 12 de dezembro de 2023.
Desembargador Cornélio Alves
Presidente
Anexo Portaria 242 2023 - Implantação e gestão de sistemas.pdf