Art. 24. A revisão desta portaria ocorrerá a cada 3 (três) anos ou sempre que se fizer necessário ou conveniente para o TRE/RN.
Art. 25. O descumprimento desta portaria deve ser imediatamente registrado como incidente de segurança e comunicado à CPSI para apuração e consequente adoção das providências cabíveis.
Art. 26. Esta portaria entra em vigor na data de sua publicação e sua implementação se fará no prazo de 12 (doze) meses a contar desta data.
Natal/RN, 12 de dezembro de 2023.
Desembargador Cornélio Alves
Presidente

PORTARIA N.° 238/2023 - GP

Dispõe sobre a gestão de vulnerabilidades em sistemas de informação no âmbito 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 garantir a disponibilidade, a confidencialidade e a integridade dos dados e dos sistemas de informação;
CONSIDERANDO a necessidade de adequação dos sistemas de informação às boas práticas de gestão previstas na norma ABNT/ISO/IEC 27001:2013;
CONSIDERANDO a necessidade de definir as políticas de gestão de vulnerabilidades em sistemas de informação no Tribunal Regional Eleitoral do Rio Grande do Norte;
CONSIDERANDO a Resolução CNJ nº 370, de 28 de janeiro de 2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
CONSIDERANDO a Resolução TSE nº 23.501, de 19 de dezembro de 2016, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral e PSI do TRE/RN;
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 a necessidade de adequação à Lei Geral de Proteção de Dados (Lei nº 13.709 /2018); e
CONSIDERANDO que a segurança da informação é condição essencial para a prestação dos serviços jurisdicionais e administrativos da Justiça 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 Gestão de Vulnerabilidades, em consonância com a Política de Segurança da Informação do Tribunal Regional Eleitoral do Rio Grande do Norte, observará as disposições contidas nesta Portaria.
CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES
Art. 2º Para efeitos desta norma, consideram-se as seguintes definições:
I - Ameaça: causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;
II - Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;
III - Risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;

IV - 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; e

V - *Hardening:* é o processo de tornar seus sistemas, redes, *softwares*, *hardwares* e *firmwares*, bem como infraestruturas de TI mais resistentes a ataques.

CAPÍTULO III

DA CLASSIFICAÇÃO QUANTO AO RISCO

Art. 3º Para os efeitos desta norma deverá ser realizada a classificação de risco dos dados manipulados/armazenados no ativo corporativo contemplando três níveis:

I - Ativos de Alto Risco: os expostos à internet, os controladores de domínio, os servidores de banco de dados, os ativos da infraestrutura de virtualização e *firewall* de borda;

II - Ativos de Médio Risco: os ativos de informação não classificados como de alto risco e que suportam serviços essenciais para o tribunal, lidam com dados sensíveis ou com dados pessoais cujo acesso não seja público; e

III - Ativos de Baixo Risco: os ativos de informação não classificados como de alto ou médio risco.

CAPÍTULO IV

DAS AÇÕES PREVENTIVAS

Art. 4º Os Ativos de informação devem possuir suporte para recebimento de atualizações de segurança.

§ 1º Os ativos de informação não podem passar mais de 04 (quatro) meses sem aplicação de atualização de segurança disponível, contados a partir da data de liberação oficial da atualização de segurança.

§ 2º Os ativos de informação de alto ou médio risco também devem ser atualizados assim que surgir uma atualização de segurança com criticidade alta.

§ 3º Os ativos de informação que estão com versão prestes a perder o suporte para recebimento de atualizações de segurança devem ser atualizados ou migrados para uma versão que possua esse suporte.

§ 4º As atualizações de segurança devem ser aplicadas para, no mínimo, os ativos de informação elencados abaixo:

I - Os sistemas em uso pelo Tribunal, sejam eles adquiridos ou obtidos da comunidade de software livre ou obtidos de outros Órgãos Públicos;

II - As bibliotecas e dependências utilizadas pelos sistemas de informação;

III - Os servidores de aplicação e os ambientes de execução;

IV - Os sistemas gerenciadores de banco de dados;

V - Os sistemas operacionais em conjunto com pacotes, serviços e programas de máquinas servidoras da rede, físicas ou virtuais;

VI - O *firmware* dos equipamentos de rede, físicos ou virtuais;

VII - A infraestrutura de virtualização;

VIII - Os sistemas operacionais e aplicativos das estações de trabalho, físicas ou virtuais; e

IX - Os sistemas de "Internet das Coisas" - IOT.

Parágrafo único. Toda atualização deve ser precedida de análise de compatibilidade e, se aplicável, testes em ambiente de homologação com o intuito de garantir a disponibilidade e integridade dos sistemas e minimizar o risco de incompatibilidades que possam produzir incidentes e perturbações indesejáveis no ambiente de TI.

CAPÍTULO V

DAS DESCOBERTAS DE VULNERABILIDADES

Art. 5º Devem ser realizadas varreduras e testes periódicos em todos os ativos de informação inventariados conectados à rede do TRE/RN, em busca de vulnerabilidades.

Art. 6º As atividades de varreduras e testes podem ser feitas de forma automatizada ou manual, de acordo com a disponibilidade de recursos e da necessidade.

Art. 7º OS principais tipos de varreduras a serem realizados e considerados durante as análises de riscos são:

I - Completa: É composta por testes para todas as vulnerabilidades conhecidas de aplicativos da w *eb*, sistemas operacionais e redes, usando ferramentas manuais e automatizadas; e

II - Rápida: É composta por testes das principais vulnerabilidades conhecidas, tipicamente realizada de forma automatizada.

§ 1º Deve ser feita, no mínimo, uma varredura completa por dia nos ativos de informação classificados como de alto ou médio risco.

§ 2º Deve ser feita, no mínimo, uma varredura rápida por semana em toda faixa de endereçamentos IP dos ativos de informação do Tribunal.

§ 3º A varredura nas estações de trabalho pode ser feita por amostragem levando em consideração os diferentes tipos de imagem de estação de trabalho.

§ 4º A varredura nas impressoras, *switches*, roteadores, equipamentos *NAS - Network Attached Storage* e dispositivos *IOT - Internet of Things* pode ser feita por amostragem levando em consideração os diferentes tipos de dispositivos.

CAPÍTULO VI

DA AVALIAÇÃO E DA PRIORIZAÇÃO

Art. 8º Os controles mínimos estabelecidos nos incisos deste artigo visam estabelecer e manter a configuração segura de ativos corporativos (dispositivos de usuário 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:

I - Ativos de infraestrutura de rede, quais sejam os dispositivos de rede;

II - Ativos de aplicações, quais sejam os sistemas operacionais e aplicações;

III - Ativos de usuários, quais sejam os usuários finais; e

IV Ativos de dispositivos, quais sejam os dispositivos de usuário final, incluindo portáteis, dispositivos não computacionais/*IoT* e móveis e servidores.

Art. 9º As vulnerabilidades de maior criticidade deverão ser tratadas no menor tempo possível.

Art. 10. No caso de impossibilidade de tratamento de alguma vulnerabilidade classificada como crítica o Gestor de Segurança da Informação deverá ser imediatamente comunicado pela área técnica responsável pelo tratamento.

CAPÍTULO VII

DA CORREÇÃO

Art. 11. A área responsável pelo ativo de informação cuja vulnerabilidade for encontrada, deve atuar para diminuir a exposição ao risco a um nível aceitável, de acordo com o nível de criticidade do ativo.

Art. 12. Os processos de correção de vulnerabilidade de criticidade alta em ativos definidos como prioritários ao negócio devem ter suas atividades priorizadas em relação às demais atividades rotineiras das unidades técnicas.

Art. 13. Caso um ativo de informação vulnerável tenha sido desenvolvido, ou seja, mantido por outro órgão público, este deverá ser comunicado.

CAPÍTULO VIII

DA MEDIÇÃO

Art. 14. Deverão ser acompanhados, ao longo do tempo, o surgimento de novas vulnerabilidades, o tempo de tratamento das vulnerabilidades descobertas e o nível de exposição dos principais ativos de informação.

CAPÍTULO IX

DA CONFIGURAÇÃO SEGURA PARA OS ATIVOS DE INFRAESTRUTURA DE REDE

Art. 15. Deverá ser estabelecido e mantido um processo de configuração segura para os ativos de rede contemplando no mínimo:

I - Revisão e atualização da documentação anualmente ou quando ocorrerem mudanças significativas no ambiente que possam impactar esta medida de segurança; e

II - Gerenciamento dos ativos de infraestrutura de rede e software corporativos com implementações de gestão de configuração que no mínimo seja contemplado:

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

b) Acesso a interfaces administrativas por meio de protocolos de rede seguros, como *Secure Shell (SSH) e Hypertext Transfer Protocol Secure (HTTPS)*;

c) Não utilização de protocolos de gestão inseguros, como *Telnet (Teletype Network) e HTTP*, a menos que seja operacionalmente essencial; e

d) 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.

CAPÍTULO X

DA CONFIGURAÇÃO SEGURA PARA OS ATIVOS DE APLICAÇÕES

Art. 16. Deverá ser estabelecido e mantido um processo de configuração segura para os softwares de sistemas operacionais e aplicações utilizados nos ativos corporativos que contemple:

I - Revisão e atualização da documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança;

II - Criação de processos automatizados de configuração de segurança que definam as configurações de segurança dos sistemas para atender aos requisitos mínimos de proteger os dados usados nos ativos corporativos; e

III - Utilização de configurações de *baseline* de segurança com base nos requisitos de segurança ou classificação dos dados no ativo corporativo contemplando:

a) Instalação do software básico do sistema operacional e posterior aplicação dos *patches* de segurança apropriados;

b) Instalação apenas dos pacotes, ferramentas e utilitários de software de aplicações apropriadas e posterior atualizações apropriadas ao software instalado;

c) Execução de processos automatizados de configuração de segurança; e

d) Execução de testes para aferição que possam estimar a qualidade das implementações de segurança.

CAPÍTULO XI

DA CONFIGURAÇÃO SEGURA PARA OS ATIVOS DE USUÁRIOS

Art. 17. Deverá ser estabelecido e mantido um processo de configuração segura para os ativos de usuários da rede corporativa da Justiça Eleitoral que contemple:

I - Configuração de bloqueio automático de sessão nos ativos corporativos após um período definido de inatividade:

a) Para sistemas operacionais de uso geral, o período não deve exceder 15 (quinze) minutos; e

b) Para dispositivos móveis de usuário final, o período não deve exceder 02 (dois) minutos.

II - Desativação ou inutilização das contas padrão nos ativos e software corporativos quando possível.

CAPÍTULO XII

DA CONFIGURAÇÃO SEGURA PARA OS ATIVOS DE DISPOSITIVOS

Art. 18. Deverá ser estabelecido e mantido um processo de configuração segura para os ativos de dispositivos dos usuários da rede corporativa da Justiça Eleitoral do Rio Grande do Norte que contemple:

I - 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;

II - A implementação e gerenciamento de *firewall* baseado em *host* ou uma ferramenta de filtragem de porta nos dispositivos de usuário final, com uma regra de negação padrão de bloqueio de todo o tráfego, exceto os serviços e portas que são explicitamente permitidos;

III - A desinstalação ou desativação de todos os serviços desnecessários nos ativos e *software* corporativos;

IV - Configuração de servidores *DNS - Domain Name System* - confiáveis nos ativos corporativos, preferencialmente servidores *DNS* controlados pela Justiça Eleitoral e/ou servidores *DNS* confiáveis acessíveis externamente caso seja imprescindível para a operação;

V - A imposição de bloqueio automático do dispositivo seguindo um limite de 03 (três) tentativas sequenciais de autenticação com falha, quando compatível;

VI - A limpeza remota dos dados corporativos de dispositivos portáteis de usuário final de propriedade da Justiça Eleitoral do Rio Grande do Norte para dispositivos perdidos ou roubados, ou quando do desligamento do usuário da Justiça Eleitoral; e

VII - A implementação da segmentação dos espaços de trabalho corporativos que sejam utilizados nos dispositivos móveis de usuário final, onde houver suporte, para garantir a separação das aplicações e dados corporativos das aplicações e dados pessoais.

CAPÍTULO XIII

DAS RESPONSABILIDADES

Art. 19. Cabe ao Gestor de Segurança da Informação:

I - Acompanhar a evolução das vulnerabilidades do ambiente computacional;

II - Acompanhar a evolução das ameaças de maior prevalência no tocante à segurança de ativos de informação;

III - Informar, quando necessário, as áreas de negócio, o Encarregado pela Proteção de Dados Pessoais e a Diretoria-Geral, sobre vulnerabilidade crítica descoberta e que não puder ser tratada em tempo adequado;

IV - Aceitar os riscos que não puderem ser tratados ou encaminhá-los para apreciação superior;

V - Comunicar-se com a Seção de Segurança da Informação - SSI e com as áreas da STIE responsáveis pelos ativos, a fim de informar e obter informações acerca de vulnerabilidades existentes; e

VI - Reportar-se à Comissão Permanente de Segurança da Informação sobre a evolução, os riscos e os achados dos testes e varreduras.

Art. 20. Cabe à Seção de Segurança da Informação:

I - Gerenciamento das vulnerabilidades do ambiente computacional;

II - Realizar ou acompanhar a realização de testes e varreduras nos ativos de informação;

III - Acionar as áreas técnicas responsáveis pelos ativos de informação, eventualmente vulneráveis, para que providenciem o tratamento; e

IV - Elaborar análises de risco de segurança dos ativos de informação, de acordo com as normas de gestão de riscos vigentes.

Art. 21. Cabe às unidades técnicas responsáveis pelos ativos de informação:

I - Providenciar as atualizações de que trata o art. 4º, de acordo com as boas práticas e planejamento;
II - Corrigir as vulnerabilidades encontradas em observância à priorização definida pelo Gestor de Segurança da Informação; e
III - Implementar medidas para mitigar o risco referente às vulnerabilidades que não puderem ser corrigidas tempestivamente.
CAPÍTULO XIV
DISPOSIÇÕES FINAIS
Art. 22. O Tribunal deverá observar o cumprimento das exigências técnicas deste normativo nos contratos e convênios com outros órgãos públicos ou empresas responsáveis pela manutenção de ativos de informação do TRE/RN.
Art. 23. Os casos omissos serão resolvidos pela Comissão Permanente de Segurança da Informação (CPSI).
Art. 24. A revisão desta portaria ocorrerá a cada ano ou sempre que se fizer necessário ou conveniente para o Tribunal.
Art. 25. O descumprimento desta portaria deve ser imediatamente registrado como incidente de segurança e comunicado à CPSI para apuração e consequente adoção das providências cabíveis.
Art. 26. Esta Portaria entra em vigor na data de sua publicação e sua implementação inicia-se imediatamente.
Natal/RN, 12 de dezembro de 2023.
Desembargador Cornélio Alves
Presidente

PORTARIA N° 239/2023 - GP

Dispõe sobre a realização da gestão e monitoramento de registro de atividades (logs) no ambiente computacional 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 do processo de tratamento e resposta a incidentes em redes computacionais no TRE-RN;
CONSIDERANDO a necessidade de definir processos para o gerenciamento e o monitoramento de logs (registro de eventos) em sistemas computacionais;
CONSIDERANDO a Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO a Resolução TSE nº 23.644/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça 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 a Portaria DG/TSE nº 444/2021, que dispõe sobre a instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral;
CONSIDERANDO as boas práticas em segurança da informação previstas nas normas ABNT ISO /IEC 27001 e ABNT NBR ISO/IEC 27002;
CONSIDERANDO as boas práticas em segurança da informação previstas no modelo CIS Controls V.8; e
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;