Documento assinado eletronicamente por ADRIANO NOGUEIRA BATISTA, Diretor-Geral, em 24/08/2022, às 18:29, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-rr.jus.br/autenticidade informando o código verificador 0715831 e o código CRC A2981869.

PORTARIA Nº 455/2022

PORTARIA Nº 455/2022

Institui norma de configuração segura de ambientes de tecnologia da informação âmbito do Tribunal Regional Eleitoral de Roraima.

O Diretor-Geral do Tribunal Regional Eleitoral de Roraima, no uso de suas atribuições legais e regimentais,

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;

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a norma de configuração segura de ambientes, em consonância com a Política de Segurança da Informação da Justiça Eleitoral (PSI-JE).

Art. 2º Para os efeitos desta norma deverá ser realizada a classificação de risco dos dados manipulados/armazenados no ativo corporativo contemplando pelo menos três níveis:

I - risco alto;

II - risco moderado;

III - risco baixo.

CAPÍTULO II

DA CLASSIFICAÇÃO DOS TIPOS DE ATIVOS CORPORATIVOS

Art. 3º 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 de acordo com a seguinte classificação:

I - ativos de infraestrutura 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;

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

CAPÍTULO III

DA CONFIGURAÇÃO SEGURA PARA OS ATIVOS DE INFRAESTRUTURA DE REDE

Art. 4º 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;

II - gerenciamento dos ativos e software corporativos com implementações de gestão de configuração que no mínimo seja contemplado;

III - uso de infraestrutura como código (IaC) qual seja o gerenciamento e provisionamento da infraestrutura por meio de códigos, em vez de processos manuais;

IV - acesso a interfaces administrativas por meio de protocolos de rede seguros, como Secure Shell (SSH) e Hypertext Transfer Protocol Secure (HTTPS);
V - não utilização de protocolos de gestão inseguros, como Telnet (Teletype Network) e HTTP, a menos que seja operacionalmente essencial;
VI - 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 IV

DA CONFIGURAÇÃO SEGURA PARA OS ATIVOS DE APLICAÇÕES

Art. 5º 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;
III - utilização de configurações de baseline de segurança com base nos requisitos de segurança ou classificação dos dados no ativo corporativo contemplando;
IV - instalação do software básico do sistema operacional e posterior aplicação dos patches de segurança apropriados;
V - instalação apenas dos pacotes, ferramentas e utilitários de software de aplicação apropriados e posterior atualizações apropriadas ao software instalado;
VI - execução processos automatizados de configuração de segurança;
VII - execução de testes para aferição que possam aferir a qualidade das implementações de segurança.

CAPÍTULO V

DA CONFIGURAÇÃO SEGURA PARA OS ATIVOS DE USUÁRIOS

Art. 6º 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;
II - para sistemas operacionais de uso geral, o período não deve exceder 15 minutos;
III - para dispositivos móveis de usuário final, o período não deve exceder 2 minutos;
IV - desativação ou inutilização das contas padrão nos ativos e software corporativos quando possível.

CAPÍTULO VI

DA CONFIGURAÇÃO SEGURA PARA OS ATIVOS DE DISPOSITIVOS

Art. 7º Deverá ser estabelecido e mantido um processo de configuração segura para os ativos de dispositivos dos usuários da rede corporativa da Justiça Eleitoral que contemple:
I - a implementação e gerenciamento de firewall nos servidores, onde houver suporte, que 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 todo o tráfego, exceto os serviços e portas que são explicitamente permitidos;
III - a desinstalação ou desativação todos os serviços desnecessários nos ativos e software corporativos;
IV - 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;

V - 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;
VI - para laptops, não deve ser permita mais de 10 tentativas de autenticação com falha;
VII - para tablets e smartphones, não mais do que 7 tentativas de autenticação com falha;
VIII - 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 exercidas na Justiça Eleitoral;
IX - 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 VII
DISPOSIÇÕES FINAIS
Art. 8º Os casos omissos serão resolvidos pela Comissão de Segurança da Informação (CSI).
Art. 9º A revisão desta portaria ocorrerá a cada ano ou sempre que se fizer necessário ou conveniente para o TRERR.
Art. 10. O descumprimento desta portaria deve ser imediatamente registrado como incidente de segurança e comunicado à CSI para apuração e consequente adoção das providências cabíveis.
Art. 11. Esta portaria entra em vigor na data de sua publicação e sua implementação se fará no prazo de 4 meses a contar dessa data.
Boa Vista, 24 de agosto de 2022.
Adriano Nogueira Batista
Diretor-Geral do TRE/RR
(documento assinado eletronicamente)

Documento assinado eletronicamente por ADRIANO NOGUEIRA BATISTA, Diretor-Geral, em 24/08/2022, às 18:29, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-rr.jus.br/autenticidade informando o código verificador 0715849 e o código CRC 318CDFA6.

PORTARIA Nº 454/2022

PORTARIA Nº 454/2022
Dispõe sobre as regras e os procedimentos para gestão de incidentes de segurança da informação do Tribunal Regional Eleitoral de Roraima.
O Diretor-Geral do Tribunal Regional Eleitoral de Roraima, no uso de suas atribuições legais e regimentais,
CONSIDERANDO a necessidade de apoiar a gestão de incidentes de segurança da informação do TRERR;
CONSIDERANDO a Res. CNJ 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO a Res. TSE 23.644/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
CONSIDERANDO a Portaria DG/TSE 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 gestão de incidentes de segurança da informação previstas nas normas ABNT ISO/IEC 27035(1,2 e 3);