/01/2023 a 20/01/2023, devido ao afastamento do Juiz Eleitoral Titular, DUARTE HENRIQUE RIBEIRO DE SOUZA.
Dê-se ciência. Publique-se. Cumpra-se.
Gabinete da Corregedoria Regional Eleitoral do Maranhão, em 11/01/2023.
Desembargador JOSE LUIZ OLIVEIRA DE ALMEIDA
Vice-Presidente e Corregedor Regional Eleitoral

PORTARIA Nº 27/2023-CRE

O Corregedor Regional Eleitoral do Maranhão, Desembargador José Luiz Oliveira de Almeida, no uso de suas atribuições legais e regimentais, e com base na Resolução nº 3734, de 25/04/2002, deste TREMA,
RESOLVE:
DESIGNAR o magistrado RÔMULO LAGO E CRUZ, Juiz de Direito titular da 1ª Vara da comarca de Vitorino Freire/MA, para responder pela 74ª Zona Eleitoral de LAGO DA PEDRA, no período de 09/01/2023 a 18/01/2023, devido ao afastamento do Juiz Eleitoral Titular, MARCELO SANTANA FARIAS .
Dê-se ciência. Publique-se. Cumpra-se.
Gabinete da Corregedoria Regional Eleitoral do Maranhão, em 11/01/2023.
Desembargador JOSE LUIZ OLIVEIRA DE ALMEIDA
Vice-Presidente e Corregedor Regional Eleitoral

PORTARIA Nº 25/2023-CRE

O Corregedor Regional Eleitoral do Maranhão, Desembargador José Luiz Oliveira de Almeida, no uso de suas atribuições legais e regimentais, e com base na Resolução nº 3734, de 25/04/2002, deste TREMA, bem como nos artigos 2º, 3º e 5º do Provimento nº. 001/2015-CRE,
RESOLVE:
DESIGNAR o magistrado SAMIR ARAÚJO MOHANA PINHEIRO, Juiz da 77ª Zona Eleitoral, com sede no município de SANTA INÊS, para exercer a Diretoria do Fórum Eleitoral, no período de 21 /01/2023 a 21/01/2024.
Dê-se ciência. Publique-se. Cumpra-se.
Gabinete da Corregedoria Regional Eleitoral do Maranhão, em 11/01/2023.
Desembargador JOSE LUIZ OLIVEIRA DE ALMEIDA
Vice-Presidente e Corregedor Regional Eleitoral

NORMAS E PORTARIAS - DG

NORMAS

INSTRUÇÃO NORMATIVA Nº 1/2023 INSTITUI NORMA DE CONFIGURAÇÃO SEGURA DE AMBIENTES NO ÂMBITO DO TRE-MA.

O DIRETOR-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO, 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 23.644, de 01 de julho de 2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a Resolução TRE-MA nº 9888/2021, de 21 de outubro de 2021, que adota, no âmbito do Tribunal Regional Eleitoral do Maranhão, as diretrizes da Política de Segurança da Informação 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 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, 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 softwares corporativos com implementações de gestão de configuração que no mínimo seja contemplado:

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

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

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

ii.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 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 organização 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:
iii.a Instalação do software básico do sistema operacional e posterior aplicação dos patches de segurança apropriados.
iii.b Instalação apenas dos pacotes, ferramentas e utilitários de software de aplicações apropriadas e posterior atualizações apropriadas ao software instalado.
iii.c Instalação do software antimalware e posterior aplicação dos patches de segurança apropriados, onde houver suporte.
iii.d Execução automatizada de processos de configuração de segurança.
iv Execução de testes 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.
i.a Para sistemas operacionais de uso geral, o período não deve exceder 15 minutos.
i.b Para dispositivos móveis de usuário final, o período não deve exceder 2 minutos.
ii 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. 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 todo o tráfego, exceto os serviços e portas que são explicitamente permitidos.
iii A implementação e gerenciamento de solução antimalware nos dispositivos de usuário final e nos servidores, onde houver suporte.
iv A implementação de solução de gerenciamento de acessos privilegiados nos servidores, onde houver suporte.
v A desinstalação ou desativação todos os serviços desnecessários nos ativos e software corporativos.
vi 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;
vii 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.
vii.a Para laptops, não deve ser permita mais de 10 tentativas de autenticação com falha;
vii.b 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 funções 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 TRE-MA.
Art. 10º 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 o plano de ação para sua implementação será apresentado no prazo de 60 dias a contar dessa data.
Cientifique-se. Publique-se. Cumpra-se.
Hebert Pinheiro Leite
Diretor-Gera

INSTRUÇÃO NORMATIVA Nº 2/2023 INSTITUI NORMA DE GERENCIAMENTO DE VULNERABILIDADES NO ÂMBITO DO TRE-MA.

O DIRETOR-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO, 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 23.644, de 01 de julho de 2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
CONSIDERANDO a Resolução TRE-MA nº 9888/2021, de 21 de outubro de 2021, que adota, no âmbito do Tribunal Regional Eleitoral do Maranhão, as diretrizes da Política de Segurança da Informação da Justiça Eleitoral,
RESOLVE:
Capítulo I
DISPOSIÇÕES PRELIMINARES
Art. 1º Fica instituída a norma de Gerenciamento de Vulnerabilidades, em consonância com a Política de Segurança da Informação da Justiça Eleitoral (PSI-JE).
Capítulo II
DEFINIÇÕES
Art. 2º Para efeitos desta norma consideram-se as seguintes definições:
I - 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.
II - Ameaça - causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;
III - Vulnerabilidade - fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;
IV - Risco - potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo para o negócio da organização;
Capítulo III