TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
GABINETE DA PRESIDÊNCIA

PORTARIA N.° 237/2023 - GP

Dispõe sobre a configuração segura de ambientes, relativa à Política de 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 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;

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);

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 configuração segura de ambientes, em consonância com as Políticas de Segurança da Informação do Tribunal Superior Eleitoral e Tribunal Regional Eleitoral do Rio Grande do Norte, observará as disposições contidas nesta portaria.

Art. 2º Para os efeitos das Políticas de Segurança da Informação do TSE, aplicam-se os termos e definições conceituados na Portaria TSE nº 444/2021 e na Resolução TRE-RN nº 110/2023

Art. 3º 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; e

III - Risco baixo.

CAPÍTULO II
DA PREPARAÇÃO DA INSTALAÇÃO

Art. 4º Os controles mínimos estabelecidos nos incisos deste artigo devem ser aplicados na instalação de serviços ou sistemas de informação no ambiente da rede corporativa:

I - planejamento e documentação da instalação, definindo o seguinte conjunto mínimo de informações:

a) propósito do serviço ou sistema de informação a ser instalado;

b) funcionalidades que serão disponibilizadas;

c) configuração de segurança;

d) configuração de hardware;

e) estratégia de particionamento

f) imagem da instalação utilizada.

II - obtenção prévia de todas as documentações e mídias de instalação que serão utilizadas;

III - instalação preferencialmente a partir de dispositivos de armazenamento locais (CD, fita ou disco) desconectados da rede corporativa ou em um segmento isolado acessível apenas pela rede corporativa;

IV - geração de registros de eventos (*logs*) das ações realizadas para instalação e configuração dos serviços ou sistemas de informação, identificados de forma distinta.

Art. 5º É recomendado evitar a concentração de serviços ou sistemas de informação em um único servidor, para aumentar sua disponibilidade na rede corporativa e reduzir a extensão de um eventual comprometimento a partir de um desses serviços ou sistemas.

CAPÍTULO III
DA ESTRATÉGIA DE PARTICIONAMENTO

Art. 6º A estratégia de particionamento deve ser definida conforme as necessidades e características dos serviços ou sistemas de informação, mas deve ser analisada com especial atenção nas seguintes situações:

I - quando os serviços ou sistemas de informação forem suscetíveis a problemas de esgotamento do espaço de armazenamento por usuário ou programa mal-intencionado que tenha permissão de escrita, como áreas temporárias e de armazenamento de registros de eventos (*logs*), a demandar, como forma de evitar o travamento do serviço ou sistema de informação, a instalação de programas de computador e o espaço de armazenamento em partições diferentes;

II - quando for necessário definir determinadas características individuais para cada partição, como o uso em modo somente leitura;

III - quando forem necessárias múltiplas operações de disco em paralelo, isolada ou conjuntamente com o uso de otimizações individuais para cada partição, o que pode aumentar significativamente o desempenho dos serviços ou sistemas de informação;

IV - quando for necessário flexibilizar o procedimento de cópia de segurança (backup) dos serviços ou sistemas de informação, pois simplifica funções como copiar partições inteiras de uma só vez; excluir partições individuais do procedimento ou fazer cópia de segurança em intervalos diferentes para cada partição.

Art. 7º Na definição da estratégia de particionamento, é recomendado avaliar a conveniência dos seguintes controles:

I - divisão de disco em várias partições em vez de usar uma única partição ocupando o disco inteiro;

II - dimensionamento de cada partição de acordo com os requisitos de cada serviço ou sistema de informação, seguindo orientações de tamanho ocupado indicado na documentação do fornecedor;

III - implementação de partições específicas para:

a) programas do sistema operacional;
b) dados dos usuários;
c) registros de eventos (*logs*);
d) arquivos temporários;
e) filas de envio e recepção de e-mails;
f) filas de impressão;
g) repositórios de arquivos;
h) páginas web.

CAPÍTULO IV
DAS SENHAS DE ADMINISTRADOR

Art. 8º Caso seja solicitada a criação de senha de administrador durante a instalação de um serviço ou sistema de informação, considerar, minimamente, as seguintes ações:

I - definição de senha tão cedo quanto possível, preferencialmente antes da instalação;

II - substituição de senha padrão do fabricante;

III - utilização de senha forte com base nos padrões estabelecidos pela Portaria TSE nº 454, de 13 de junho de 2021, que institui a Norma de Controle de Acesso Físico e Lógico relativos à Segurança das Informações e Comunicações do

Tribunal Superior Eleitoral, bem como a Portaria GP nº 231/2023 - GP que dispõe sobre o Controle de Acesso Físico e Lógico ao ambiente cibernético do Tribunal Regional Eleitoral do Rio Grande do Norte.

IV - utilização de senhas que sejam únicas para o sistema em questão, quando a autenticação por múltiplos fatores não for suportada (como administrador local ou contas de serviço).

CAPÍTULO V
DA INSTALAÇÃO MÍNIMA

Art. 9º Os controles mínimos de proteção estabelecidos nos incisos deste artigo devem ser implementados para evitar que componentes e pacotes não utilizados pelos serviços ou sistemas de informação exponham o ambiente da rede corporativa a vulnerabilidades que possam vir a ser exploradas por um atacante, por falta de monitoramento regular ou pela não aplicação das correções previstas:

I - identificação de quais componentes e pacotes podem deixar de ser instalados sem comprometer a funcionalidade do serviço ou sistema de informação ou a estabilidade do ambiente da rede corporativa, via mecanismo de controle de dependências (que avisa quando determinado componente precisa de outro para funcionar), consulta à documentação ou apoio do suporte técnico do fornecedor;

II - abstenção de instalar componentes e pacotes cuja funcionalidade seja desconhecida ou cuja necessidade não seja justificada;

III - opção pela instalação personalizada, em detrimento da instalação típica, para instalar a base do serviço ou sistema de informação e selecionar cuidadosamente quais componentes extras serão adicionados;

IV - instalação do mínimo possível de componentes e pacotes, especialmente dos que implementam serviços de rede;

V - limitação do acesso às ferramentas de *scripting* exclusivamente a usuários administrativos ou de desenvolvimento que necessitem acessar tais funcionalidades.

CAPÍTULO VI
DA DESATIVAÇÃO DE FUNCIONALIDADES NÃO UTILIZADAS

Art. 10. Os controles mínimos de proteção estabelecidos nos incisos deste artigo devem ser implementados nos casos de instalação completa de serviço ou sistema de informação e de seus componentes e pacotes para poder utilizar um subconjunto das funcionalidades:

I - desativação de funcionalidades (locais e, principalmente, de rede) que não serão imediatamente utilizadas;

II - emprego de filtro de pacotes para definir as origens aceitáveis para os acessos às portas TCP/UDP utilizadas, evitando assim a possibilidade de acesso a partir de equipamentos que não tenham uma necessidade legítima de uso do serviço disponibilizado.

CAPÍTULO VII
DAS IMAGENS DE INSTALAÇÃO

Art. 11. Imagens das instalações seguras pré-configuradas devem ser estabelecidas e mantidas para todos os dispositivos móveis, notebooks, estações

de trabalho e servidores, com base nos padrões de configuração definidos pelas seções responsáveis pelas configurações dos respectivos ativos de processamento.

Art. 12. A quantidade de variações de imagens das instalações seguras pré-configuradas deve ser reduzida ao mínimo para melhor entendimento e gerenciamento dos requisitos de segurança de cada uma.

Art. 13. Os arquivos com imagens das instalações seguras pré-configuradas devem ser protegidos para que não sejam possíveis o acesso e a alteração não autorizados das informações.

Parágrafo único. Os controles mínimos de proteção estabelecidos nos incisos deste artigo devem ser implementados:

I - armazenagem em local centralizado e resguardado de acessos indevidos;

II - armazenagem em segmento isolado da rede corporativa, com proteção de dispositivos de segurança, tais como *firewall* sistema de detecção e prevenção de intrusões, entre outros;

III - localização física em área de segurança;

IV - utilização de protocolos seguros para acesso remoto;

V - capacidade de assinatura digital ou resumo criptográfico para verificação da integridade;

VI - geração de registros de eventos (*logs*) para todos os trabalhos executados nos arquivos;

VII - manutenção de documentação atualizada dos procedimentos de:

a) configuração, instalação e manutenção;

b) administração e operação;

c) cópia de segurança e restauração.

CAPÍTULO VIII
DA DOCUMENTAÇÃO E CONFIGURAÇÃO DAS IMAGENS

Art. 14. A instalação e as alterações na configuração dos serviços ou sistemas de informação e de seus componentes devem ser documentadas para registrar quais passos exatos foram seguidos para alcançar pleno êxito, de forma que seja possível reconstituir a partir dessas informações, a última configuração antes de uma falha, sem a necessidade de recorrer a cópias de segurança (backup).

Art. 15. Os registros de configuração da imagem devem conter informações mínimas e relevantes, especialmente:

I - data da modificação;

II - responsável pela modificação;

III - justificativa para a modificação;

IV - descrição da modificação;

V - sistema operacional utilizado;

VI - descrição de como o serviço ou sistema de informação foi instalado, quais componentes e pacotes foram implementados e quais funcionalidades foram desativadas e bloqueadas;

VII - configuração de segurança implementada;

VIII - indicação de como foi feito o particionamento;

IX - local onde pode ser encontrada a lista de pacotes instalados;

X - descrição de quais portas ficaram ativas após a instalação;

XI - indicação de quais os usuários criados (com seus respectivos *UIDs* e *GIDs*).

Art. 16. Os registros de configuração da imagem devem ser armazenados em local seguro e com acesso restrito aos administradores dos ativos de informação e de processamento.

Art. 17. A Equipe de Gestão de Segurança da Tecnologia da Informação deve analisar criticamente a documentação referente à configuração segura de ambientes para verificar sua aderência às regras descritas nesta portaria, incluindo:

I - procedimentos operacionais com a configuração técnica de serviços ou sistemas de informação a cada 12 (doze) meses;

II - registros de configuração da imagem com a configuração segura de serviços ou sistemas de informação a cada 12 (doze) meses.

CAPÍTULO IX
DA INSTALAÇÃO DE CORREÇÕES

Art. 18. Deverá ser implantado processo de gerenciamento de correções de sistemas operacionais e de softwares de terceiros, para assegurar que estejam executando as atualizações de segurança mais recentes disponibilizadas pelos fabricantes.

Art. 19. Os controles mínimos estabelecidos nos incisos deste artigo devem ser implementados para assegurar que as configurações estabelecidas não foram alteradas durante o processo de instalação de correções (*patches*, *fixes*, *service packs*) para vulnerabilidades conhecidas nos serviços ou sistemas de informação:

I - aplicação somente daquelas que corrigem problemas em componentes que estejam efetivamente instalados, pois a instalação indiscriminada de atualizações pode enfraquecer a segurança do ambiente da rede corporativa em vez de fortalecê-la;

II - revisão da configuração dos serviços ou sistemas de informação após instalar uma correção, para certificar-se de que a instalação não tenha revertido eventuais modificações realizadas (especialmente aquelas destinadas a desativar componentes e funcionalidades).

Art. 20. Os registros de configuração da imagem devem ser atualizados com as ações realizadas durante o processo de instalação de correções.

CAPÍTULO X
DAS FERRAMENTAS DE GERENCIAMENTO DE CONFIGURAÇÃO

Art. 21. Os controles mínimos estabelecidos nos incisos deste artigo devem ser implementados para assegurar que as configurações estabelecidas não sejam alteradas acidental ou intencionalmente durante o uso dos serviços ou sistemas de informação:

I - utilização de ferramenta de gerenciamento de configuração que automaticamente impõe as configurações estabelecidas de serviços ou sistemas de informação em intervalos agendados regularmente;

II - utilização de sistema de monitoramento de configuração para verificar se a configuração corrente permanece idêntica à configuração aprovada, catalogar exceções aprovadas e alertar quando ocorrerem alterações não autorizadas.

CAPÍTULO X
DO SUPORTE DOS FABRICANTES E COMUNIDADES

Art. 22. Todos os ambientes computacionais deverão ser mantidos em versões suportadas pelos respectivos fabricantes ou comunidades desenvolvedoras, de forma a garantir a existência de correções para os problemas de segurança identificados, bem como viabilizar a prestação de suporte técnico pelo fabricante.

§ 1º Para soluções baseadas em código aberto ou software gratuito, deve ser assegurado que seus projetos estejam ativos e suportados pelas respectivas comunidades.

§ 2º Caso algum ambiente se mantenha operacional em versão não suportada pelo fabricante ou pela comunidade, deverão ser analisadas medidas adicionais de segurança que assegurem a proteção do ativo de processamento e do respectivo ambiente

CAPÍTULO XII
DISPOSIÇÕES FINAIS

Art. 23. Os casos omissos serão resolvidos pela Comissão Permanente de Segurança da Informação (CPSI).

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