PORTARIA PRE Nº 223, DE 16 DE SETEMBRO DE 2024

Institui Norma de Segurança Cibernética — NSC10 — Gestão do Monitoramento de Ativos de TIC e dos respectivos registros de eventos (logs) do Tribunal Regional Eleitoral de Minas Gerais.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS, no uso de suas atribuições conferidas pelo inciso XV do art. 22 da Resolução TRE-MG nº 1.277, de 29 de maio de 2024, o Regimento Interno, considerando o disposto no art. 4° da Resolução TRE-MG nº 1.240, de 6 de fevereiro de 2023, que determina que a "revisão e a atualização das normas complementares de Segurança da Informação ocorrerão sempre que necessário, por meio de portaria da Presidência do Tribunal.",

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1° Fica instituída a Norma de Segurança Cibernética — NSC10 – Gestão do Monitoramento de Ativos de TIC e dos respectivos registros de eventos (*logs*) do Tribunal Regional Eleitoral de Minas Gerais.

Parágrafo único. A norma de segurança de que trata o *caput* estabelece as principais estratégias para o monitoramento e a gestão de registro de atividades (*logs*) no ambiente computacional do Tribunal Regional Eleitoral de Minas Gerais.

Art. 2° Esta portaria integra a Política de Segurança da Informação do Tribunal Regional Eleitoral de Minas Gerais, regulamentada pela Resolução TRE-MG nº 1.240, de 6 de fevereiro de 2023.

Art. 3° Para efeitos desta portaria, aplicam-se os termos e definições da Norma de Segurança Cibernética — NSC1 — Termos e Siglas de Segurança da Informação.

Art. 4° Esta portaria aplica-se aos magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço, colaboradores e usuários externos, outros órgãos públicos ou entidades privadas contratadas ou com parcerias celebradas, acordos de cooperação de qualquer tipo, convênios e termos congêneres que façam ou venham a fazer uso dos ativos de TIC na Justiça Eleitoral Mineira.

CAPÍTULO II

DO REGISTRO DE EVENTOS *(LOGS)*

Art. 5° Serão monitorados, com registro centralizado de *logs* e através de ferramentas apropriadas, no mínimo, os seguintes tipos de ativos do ambiente de produção:

I — servidores *web*;

II — servidores de arquivos;

III — servidores de bancos de dados;

IV — servidores de *e-mails*;

V — servidores de aplicação;

VI — *firewalls* de rede;

VII — *firewalls* de aplicação;

VIII — roteadores de acesso à *internet* e às redes da Justiça Eleitoral;

IX — *switches* e roteadores de núcleo de rede (*core*);

X — servidores controladores de domínio e demais serviços de autenticação;

XI — serviços de gerenciamento de cópias de segurança (*backups*);

XII— serviços de gerenciamento de infraestrutura de virtualização e conteinerização, incluídas as baseadas em nuvem pública, quando for o caso;

XIII — soluções *antimalware*;

XIV — soluções controle de acesso físico e lógico;

XV — soluções gerais de cibersegurança;

XVI — serviços de *Dynamic Host Configuration Protocol* — DHCP;

XVII — serviços de *Domain Name System* — DNS.

Art. 6° Os *logs* com os registros de eventos conterão, quando possível, informações relevantes, especialmente:

I — identificação do usuário que acessou o recurso;

II — natureza do evento, como sucesso ou falha de autenticação, tentativa de troca de senha, entre outros;

III — carimbo de tempo (*timestamp*), formado por data, hora e fuso horário;

IV — endereço IP (*Internet Protocol*), identificador do ativo de processamento, coordenadas geográficas, se disponíveis, e outras informações que permitam identificar a origem e destino do evento;

V — recursos acessados e seus respectivos tipos de acesso;

VI — alarmes provocados pelos sistemas de controle de acesso;

VII — informações de falhas nas aplicações ou recursos acessados;

VIII — outras informações que permitam identificar a possível origem e destino do evento.

Art. 7° Os ativos de processamento que não permitam os registros de eventos conforme indicado, ou que estejam em ambiente seguro de nuvem administrado por terceiros, serão mapeados e documentados quanto ao tipo e formato de registro de eventos que o sistema permite armazenar, a temporalidade do armazenamento, assim como o nível de segurança obtido.

Art. 8° Os *logs* com os registros de eventos serão armazenados para acesso direto pelo período de 60 (sessenta) dias e em cópias de segurança por um período de 12 (doze) meses, sem prejuízo de outros prazos previstos em referências legais e normativos específicos.

Art. 9º Os ativos de processamento em produção serão configurados de forma a gerar registros de eventos relevantes que afetem a segurança da informação, armazenando-os para utilização posterior, incluindo:

I — acesso remoto à rede corporativa;

II — autenticação, tanto as bem-sucedidas quanto as malsucedidas;

III — criação, alteração e remoção de usuários, perfis e grupos privilegiados;

IV — uso de privilégios;

V — troca de senhas;

VI — modificações de política de senhas, como tamanho, tempo de expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico, entre outras;

VII — acesso ou modificação de arquivos, serviços e sistemas de informação considerados críticos;

VIII — alterações na configuração de sistemas operacionais de servidores, serviços e sistemas de informação;

IX — inicialização, suspensão e reinicialização de serviços;

X — uso de aplicativos e utilitários do sistema operacional de servidores;

XI — ativação e desativação dos sistemas de proteção, como sistemas de antivírus e sistemas de detecção e prevenção de intrusão;

XII — acesso físico por senha, cartão inteligente ou biometria em área de segurança com ativos de processamento críticos como *datacenters*, salas de equipamentos e telecomunicações, dentre outros;

XIII — acoplamento e desacoplamento de dispositivos de *hardware*, com especial atenção para mídias removíveis em servidores;

XIV — acesso e alteração nos registros de eventos (*logs*).

Art. 10. O monitoramento será realizado, preferencialmente, com a utilização de ferramentas automatizadas que gerem alarmes imediatos de eventos críticos e permitam a correlação e análise dos registros de eventos gravados (SIEM — *Security Information and Event Management* —/SOAR — *Security Orchestration, Automation, and Response*).

§ 1º O monitoramento será realizado de forma a manter inalterada a rotina de trabalho do ambiente de produção.

§ 2º O nível de monitoramento pode ser reduzido em função da implementação de controles de acesso que minimizem o risco aos ativos de processamento e reduzam a exposição da informação a acessos indevidos.

§ 3º As ferramentas automatizadas serão analisadas criticamente em intervalos regulares para ajuste de configuração, de forma a melhorar a identificação de registros de eventos relevantes, falsos negativos e falsos positivos.

§ 4º Os processos de monitoramento serão revisados na implantação ou manutenção dos ativos de processamento, a fim de manter sua adequação às mudanças ocorridas.

§ 5º As configurações de monitoramento e registro de eventos em *logs* registrarão apenas dados pessoais suficientes para rastreamento da respectiva ação registrada em *log*.

Art. 11. Os usuários estarão cientes de que os ativos de processamento estão suscetíveis a monitoramento e auditoria a qualquer momento, bem como quando houver suspeita ou constatação de uma falha de segurança.

CAPÍTULO III

DA PROTEÇÃO DAS INFORMAÇÕES DOS REGISTROS DE EVENTOS

Art. 12. Serão adotadas medidas de segurança para proteger os arquivos de registros de eventos contra adulteração, falsificação e acesso não autorizado às informações registradas, de forma a preservar sua integridade e disponibilidade.

Parágrafo único. A fim de assegurar a proteção de que trata o *caput* deste artigo, sempre que disponíveis e tecnicamente viáveis, os seguintes controles serão implementados:

I — guarda da cópia centralizada em segmento isolado da rede corporativa, com proteção de dispositivos de segurança suficientes para a proteção da sua integridade;

II — espaço de armazenamento adequado e alertas preventivos de seu esgotamento;

III — localização física em área sujeita a controles de segurança;

IV — emprego de protocolos seguros para acesso remoto;

V — capacidade de assinatura digital ou resumo criptográfico para verificar a integridade;

VI — possibilidade de execução de auditorias legais e forenses;

VII — fornecimento, para efeito de investigação, de cópia das informações relevantes, exceto nas hipóteses legais que exijam a apresentação da mídia original;

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

IX — conservação de documentação atualizada dos procedimentos de:

a) instalação, configuração e manutenção;

b) administração e operação;

c) cópia de segurança e restauração.

CAPÍTULO IV

DOS REGISTROS DE EVENTOS DE ADMINISTRADOR E OPERADOR

Art. 13. Os registros de eventos de administradores e operadores com privilégios para ações e comandos especiais na rede corporativa, como superusuários, administradores de rede, entre outros, terão mecanismos adicionais de gerenciamento e monitoramento, considerando os seguintes aspectos:

I — os registros de eventos dos administradores e operadores da rede corporativa serão protegidos e analisados criticamente, em intervalos regulares;

II — os administradores e operadores da rede corporativa não farão parte da equipe de monitoramento e análise crítica de suas próprias atividades, respeitando o princípio da segregação de funções;

III — os administradores e operadores da rede corporativa não terão permissão para apagar, alterar ou desativar os registros de eventos de suas próprias atividades.

Art. 14. Um sistema de detecção e prevenção de intrusões gerenciado fora do controle dos administradores e operadores da rede corporativa pode ser utilizado para monitorar as atividades nos registros de eventos.

CAPÍTULO V

DA SINCRONIZAÇÃO DOS RELÓGIOS

Art. 15. O horário dos ativos de processamento será ajustado por meio de mecanismos de sincronização de tempo, através de serviço *Network Time Protocol* — NTP, de forma que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a "Hora Legal Brasileira — HLB", de acordo com o serviço oferecido e assegurado pelo Observatório Nacional — ON — ou outro equivalente.

Art. 16. A correta configuração dos relógios nos ativos de processamento da rede corporativa assegurará a exatidão dos registros de eventos, que podem ser requeridos para investigações ou como evidências em casos legais ou disciplinares.

Parágrafo único. Sempre que possível, serão utilizadas fontes de tempo sincronizadas para todos os ativos monitorados, a partir das quais os ativos de processamento recuperem regularmente as informações de data, hora e fuso horário, de forma que os registros de eventos *(logs*) sejam cronologicamente consistentes.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 17. O descumprimento desta portaria será imediatamente registrado como incidente de segurança e caberá ao Gestor de Segurança da Informação, a depender da gravidade do incidente, a comunicação ou não à Comissão de Segurança da Informação, para apuração e consequente adoção das providências complementares cabíveis.

Art. 18. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação.

Art. 19. Esta portaria entra em vigor na data de sua publicação.

Belo Horizonte, 16 de setembro de 2024.

Desembargador Ramom Tácio de Oliveira
Presidente

Documento assinado eletronicamente por **RAMOM TÁCIO DE OLIVEIRA**, **Presidente**, em 16/09/2024, às 16:51, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade deste documento pode ser conferida no site https://sei.tre-mg.jus.br/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&lang=pt_BR&id_orgao_acesso_externo=0, informando o código verificador **5680304** e o código CRC **0321490B**.