TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ

Portaria Presidência Nº 93/2023 TRE/PRESI/DG/ASSDG, de 16 de fevereiro de 2023

Dispõe sobre a regulamentação para a Gestão e Monitoramento de Registro de Atividades (logs) no âmbito do Tribunal Regional Eleitoral do Piauí.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de apoiar a gestão do processo de tratamento e resposta a incidentes em redes computacionais no TRE-PI;

CONSIDERANDO a necessidade de definir processos para o gerenciamento e o monitoramento de logs (registro de eventos) em sistemas computacionais;

CONSIDERANDO a Resolução nº 396, de 7 de junho de 2021, do Conselho Nacional de Justiça, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Resolução nº 23.644, de 1º de julho de 2021, do Tribunal Superior Eleitoral, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a Resolução nº 448, de 24 de maio de 2022, que adota a PSI da Justiça Eleitoral estabelecida pela Resolução nº 23.644, de 1º de julho de 2021, do Tribunal Superior Eleitoral;

CONSIDERANDO as boas práticas em segurança da informação previstas nas normas ABNT ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013;

CONSIDERANDO as boas práticas em segurança da informação previstas no modelo *CIS Controls V.8*;

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 Piauí;

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída, por meio deste normativo, a regulamentação para a Gestão e Monitoramento de Registro de Atividades (logs) no âmbito do Tribunal Regional Eleitoral do Piauí.

Art. 2º Esta norma integra a Política de Segurança de Informação da Justiça Eleitoral, estabelecida pela Resolução nº 448, de 24 de maio de 2022.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 3º Para efeitos desta norma consideram-se os termos e definições a seguir:

I - Agente público: todo aquele que exerce, ainda que transitoriamente com ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da APF, direta e indireta;

II - Assinatura digital: tipo de assinatura eletrônica que usa operações matemáticas com base em algoritmos criptográficos, de criptografia assimétrica, para garantir segurança quanto a autenticidade das documentações. Para assinar digitalmente um documento é necessário possuir um certificado digital. Entre as principais vantagens do uso de assinatura digital estão o não repúdio e tempestividade;

III - Ativo de processamento: patrimônio composto por todos os elementos de hardware, software e infraestrutura de comunicação necessários à execução das atividades precípuas da Justiça Eleitoral;

IV - Ativo de TI: o mesmo que ativo de processamento;

V - Ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

VI - Autenticidade: propriedade que garante que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

VII - Hora Legal Brasileira (HLB): gerada pelo Observatório Nacional a partir de um conjunto de 7 padrões atômicos de feixe de césio e 2 padrões atômicos de MASER de hidrogênio, é a referência brasileira das grandezas de tempo e frequência;

VIII - Incidente de segurança em redes computacionais: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

IX - Incidente em segurança da informação: qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações do negócio ou ameaçar a segurança da informação;

X - Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XI - Integridade: propriedade que garante que a informação mantém todas as características originais estabelecidas pelo proprietário;

XII - Proprietário do ativo de informação: refere-se à parte interessada do órgão ou entidade, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;

XIII - Recurso: além da própria informação, é todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;

XIV - Recursos de Tecnologia da Informação: são o conjunto de bens e serviços de tecnologia da informação que constituem a infraestrutura tecnológica de suporte automatizado ao ciclo da informação, que envolve as atividades de produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação;

XV - Rede de computadores: rede formada por um conjunto de máquinas eletrônicas com processadores capazes de trocar informações e partilhar recursos, interligados por um subsistema de comunicação, ou seja, existência de dois ou mais computadores, e outros dispositivos interligados entre si de modo a poder compartilhar recursos físicos e lógicos, sendo que estes podem ser do tipo dados, impressoras, mensagens (e-mails), entre outros;

XVI - Registro de eventos (log): processo com a finalidade de registrar eventos durante o seu ciclo de vida, podendo ser gerado por sistemas operacionais, aplicações, entre outros, e armazenado durante um período pré-determinado;

XVII - Resumo criptográfico: resultado da ação de algoritmos que fazem o mapeamento de bits de tamanho arbitrário para uma sequência de bits de tamanho fixo menor - conhecida como resultado *hash* - de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado *hash* (resistência à colisão) e que o processo reverso também não seja realizável (utilizando-se apenas o *hash* não é possível recuperar a mensagem que o gerou);

XVIII - Risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;

XIX - Serviços de DHCP *(Dynamic host configuration protocol)* - servidores que fornecem endereços IP e outras configurações de forma dinâmica para o ambiente de rede de computadores;

XX - Serviços de DNS *(Domain name system)* - servidores que fazem localização e tradução de nomes de *hosts* e serviços de rede para números de endereços IP;

XXI - SIEM - *Security information event management* – solução de software que faz a centralização de eventos de rede e de sistemas, com capacidade para busca e correlação entre esses eventos, possibilitando o monitoramento por parte das equipes de segurança e outros administradores de rede;

XXII - SOAR - *Security orchestration, automation and response* – Possui as mesmas funções do SIEM, com capacidade adicional de abertura de chamados e automação da resposta ao incidente, como bloqueio de usuários e geração de regras de firewall;

XXIII - Usuário: aquele que utiliza, de forma autorizada, recursos inerentes às atividades precípuas da Justiça Eleitoral;

XXIV - Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO III

DO REGISTRO DE EVENTOS (*LOGS*)

Art. 4º Devem ser monitorados, com registro centralizado de logs em servidores específicos, no mínimo, os seguintes tipos de ativos em 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 *backups* (cópias de segurança);

XII - serviços de gerenciamento de infraestrutura de virtualização e conteinerização, incluídas as baseadas em nuvem pública;

XIII - soluções *antimalware*;

XIV - soluções controle de acesso físico e lógico;

XV - soluções gerais de cibersegurança;

XVI - serviços de DHCP;

XVII - serviços de DNS;

Art. 5º Os registros de eventos devem conter informações mínimas e relevantes, especialmente:

I - identificação da usuária ou 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 possível 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. 6º Os ativos de processamento que não permitam os registros de eventos conforme indicado, ou que estejam em ambiente seguro de nuvem administrado por terceiros, devem ser 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.7º Os registros de eventos devem ser armazenados na rede corporativa pelo período de 180 (cento e oitenta) 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. 8º Os ativos de processamento em produção devem ser 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 intrusos;

XII - acesso físico por senha, cartão inteligente ou biometria em área de segurança com ativos de processamento críticos como *Data Center*, salas de 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. 9º O monitoramento deve ser 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/SOAR*).

§ 1º O monitoramento deve ser 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 devem ser 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 devem ser revisados na implantação ou manutenção dos ativos de processamento, a fim de manter sua adequação às mudanças ocorridas.

§ 5º Os administradores devem monitorar os registros impedindo o armazenamento indevido de dados pessoais.

Art. 10. As usuárias ou os usuários devem estar 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.

Art. 11. Todos os eventos contrários ao ordenamento jurídico em vigor e às normas constantes da Política de Segurança da Informação, inclusive os

discriminados nos incisos deste artigo, devem ser registrados formalmente e analisados, adotando-se as ações apropriadas para sua correção:

I - divulgação não autorizada de dado ou informação sigilosa contida em sistema, arquivo ou base de dados da Administração Pública, nos termos do art. 153, § 1º-A do Código Penal;

II - invasão de dispositivo informático, nos termos do art. 154-A do Código Penal;

III - interrupção de serviço telemático ou de informação de utilidade pública, previsto no § 1º do art. 266 do Código Penal;

IV - inserção ou facilitação de inserção de dados falsos, alteração ou exclusão de dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública, nos termos do art. 313-A do Código Penal;

V - modificação ou alteração por agente público de sistema de informação ou programa de informática sem autorização, nos termos do art. 313-B do Código Penal;

VI - distribuição, armazenamento ou conduta vinculada a pornografia infantil, nos termos dos arts. 240, 241, 241-A, 241-B, 241-C e 241-D da Lei nº 8.069, de 13 de julho de 1990;

VII - interceptação telemática clandestina, nos termos do art. 10 da Lei nº 9.296, de 24 de julho de 1996.

CAPÍTULO IV

DA PROTEÇÃO DAS INFORMAÇÕES DOS REGISTROS DE EVENTOS

Art. 12. Os arquivos de registros de eventos devem ser protegidos para que não estejam sujeitos a falsificação ou ao acesso não autorizado às informações registradas.

Parágrafo único. A fim de assegurar a proteção de que trata o *caput* deste artigo, os seguintes controles mínimos devem ser implementados:

I - armazenamento, no mínimo, em 2 (dois) registros de mesmo conteúdo, sendo ambos protegidos contra acessos indevidos e adulteração, e um deles em local centralizado;

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

III - espaço de armazenamento adequado e alertas preventivos de seu esgotamento;

IV - localização física em área sujeita a controles de segurança;

V - emprego de protocolos seguros para acesso remoto;

VI - capacidade de assinatura digital ou resumo criptográfico para verificar a integridade;

VII - possibilidade de execução de auditorias legais e forenses;

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

IX - geração de registros de eventos (*logs*) para todos os trabalhos

executados nos arquivos;

X - conservação de documentação atualizada dos procedimentos de:

a) configuração, instalação e manutenção;

b) administração e operação;

c) cópia de segurança e restauração.

CAPÍTULO V

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 super usuários, administradores de rede, entre outros, devem ter mecanismos adicionais de gerenciamento e monitoramento, considerando, no mínimo, os seguintes aspectos:

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

II - os administradores e operadores da rede corporativa não devem fazer 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 devem ter 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 VI

DA SINCRONIZAÇÃO DOS RELÓGIOS

Art. 15. O horário dos ativos de processamento deve ser ajustado por meio de mecanismos de sincronização de tempo (servidor 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.

Art. 16. O estabelecimento correto dos relógios nos ativos de processamento da rede corporativa deve assegurar a exatidão dos registros de eventos, que podem ser requeridos para investigações ou como evidências em casos legais ou disciplinares, devendo atender, no mínimo, à seguinte rotina:

I - Usar 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 VII

DAS DISPOSIÇÕES FINAIS

Art. 17. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação.

Art. 18. A Secretaria de Tecnologia da Informação elaborará, em até 180 dias, os procedimentos operacionais para aplicação desta norma, que levem em conta as boas práticas de cibersegurança e os recursos tecnológicos disponíveis.

Art. 19. Qualquer descumprimento desta norma deve ser imediatamente comunicado e registrado como incidente de segurança da informação, para apuração pela Comissão de Segurança da Informação, com consequente adoção das providências cabíveis.

Art. 20. Esta norma complementar deve ser revisada a cada 12 meses pelo Núcleo de Segurança da Informação e encaminhada para nova apreciação da Comissão de Segurança da Informação.

Art. 21. Esta Portaria entra em vigor na data de sua publicação.

Desembargador ERIVAN LOPES

Presidente do TRE-PI

Documento assinado eletronicamente por **Erivan José da Silva Lopes**, **Presidente**, em 16/02/2023, às 15:12, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1775200** e o código CRC **A526BC82**.