Tribunal Regional Eleitoral
do Espírito Santo

Sede: Vitória/ES
Av. João Batista Parra, 575
Praia do Suá - Vitória - ES
CEP 72620-000
Tel.: (27) 2121.8595
Endereço eletrônico:
www.tre-es.jus.br

Comissão de Segurança da Informação

NSI-007	V2.0 - JUL 2022	SEGURANÇA DA INFORMAÇÃO

Norma de gestão e monitoramento de registro de atividades (logs)

Referência(s):

Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)

Resolução CNJ 396/2021 – ENSEC-PJ

Resolução TSE 23.644/2021 – PSI/JE

Resolução TSE 23.650/2021 – Política Geral de Privacidade e Proteção de Dados Pessoais

Portaria DG/TSE 444/2021, instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral

Normas ABNT ISO/IEC 27001 e ABNT NBR ISO/IEC 27002

Boas práticas em segurança da informação previstas no modelo CIS Controls V.8.

Palavras Chave: segurança, norma, monitoramento, logs | 07 páginas

1. Prefácio

1.1. A presente norma está alinhada às diretrizes de Segurança da Informação e dos Dados Pessoais estabelecidas na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) e na Política de Segurança da Informação da Justiça Eleitoral (PSI-JE).

2. Objetivo

2.1. Dispõe sobre as regras e os procedimentos para a realização da gestão e monitoramento de registro de atividades (logs) no ambiente computacional do Tribunal Regional Eleitoral do Espírito Santo.

3. Definições

3.1. Para efeitos desta norma, consideram-se os termos e definições previstos na portaria DG/TSE 444/2021, além das seguintes:

3.1.1. 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.

3.1.2. 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.

3.1.3. 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.

3.1.4. SOAR – Security orchestration, automation and response – solução de software que 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.

4. Abrangência

4.1. Devem ser monitorados, com registro centralizado de logs em servidores específicos, no mínimo, os seguintes tipos de ativos de processamento em produção:

4.1.1. servidores web;

4.1.2. servidores de arquivos;

4.1.3. servidores de bancos de dados;

4.1.4. servidores de e-mails;

4.1.5. servidores de aplicação;

4.1.6. firewalls de rede;

4.1.7. firewalls de aplicação;

4.1.8. switches de núcleo de rede (core);

4.1.9. servidores controladores de domínio e demais serviços de autenticação;

4.1.10. servidores de gerenciamento de backups (cópias de segurança);

4.1.11. servidores de gerenciamento de infraestrutura de virtualização e conteinerização, incluídas as baseadas em nuvem pública.

4.1.12. soluções anti-malware;

4.1.13. soluções controle de acesso físico e lógico;

4.1.14. soluções gerais de cibersegurança;

4.1.15. serviços de DHCP;

4.1.16. serviços de DNS.

5. Do detalhamento dos registros de atividades e eventos geradores

5.1. Os registros de eventos devem conter informações mínimas e relevantes, especialmente:

5.1.1. Identificação do usuário que acessou o recurso;

5.1.2. Natureza do evento, como sucesso ou falha de autenticação, tentativa de troca de senha, entre outros;

5.1.3. Carimbo de tempo (timestamp), formado por data, hora e fuso horário;

5.1.4. Endereço IP (Internet Protocol), identificador do ativo de processamento, coordenadas geográficas, se disponíveis, endereços, serviços e protocolos de rede utilizados, recursos acessados e seus respectivos tipos de acesso, ou outras informações que permitam identificar a possível origem e destino do evento.

5.2. Os serviços e ativos 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.

5.3. Os registros de eventos devem ser armazenados na rede corporativa pelo período de 30 (trinta) 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.

5.4. 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:

5.4.1. acesso remoto à rede corporativa;

5.4.2. autenticação, tanto as bem-sucedidas quanto as malsucedidas;

5.4.3. criação, alteração e remoção de usuários, perfis e grupos privilegiados;

5.4.4. acesso com privilégios administrativos;

5.4.5. troca de senhas;

5.4.6. modificações de política de senhas, como tamanho, tempo de expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico, entre outras, quando aplicável;

5.4.7. acesso ou modificação de arquivos, serviços e sistemas de informação considerados críticos, quando aplicável;

5.4.8. alterações na configuração de sistemas operacionais, serviços e sistemas de informação considerados críticos, quando aplicável;

5.4.9. inicialização, suspensão e reinicialização de serviços;

5.4.10. uso de aplicativos e utilitários do sistema operacional;

5.4.11. ativação e desativação dos sistemas de proteção, como sistemas de antivírus e sistemas de detecção e prevenção de intrusos;

5.4.12. 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;

5.4.13. acoplamento e desacoplamento de dispositivos de hardware, com especial atenção para mídias removíveis, aplicável somente aos equipamentos físicos;

5.4.14. acesso e alteração nos registros de eventos (logs);

5.4.15. informações de falhas nas aplicações ou recursos acessados.

5.5. 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).

5.6. 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.

5.7. O monitoramento deve ser realizado de forma a manter inalterada a rotina de trabalho do ambiente de produção.

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

5.9. Os processos de monitoramento devem ser revisados na implantação ou manutenção dos ativos de processamento de produção, a fim de manter sua adequação às mudanças ocorridas.

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

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

5.12. Todos os eventos contrários ao ordenamento jurídico em vigor e às normas integrantes da Política de Segurança da Informação, inclusive os discriminados nos subitens abaixo, devem ser registrados formalmente e analisados, adotando-se as ações apropriadas para sua correção:

5.12.1. 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;

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

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

5.12.4. 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;

5.12.5. 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;

5.12.6. 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 8.069/90);

5.12.7. interceptação telemática clandestina, nos termos do art. 10 da Lei nº 9.296/96.

6. Da proteção das informações dos registros de eventos

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

6.2 Os seguintes controles mínimos devem ser implementados:

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

6.2.2. guarda da cópia centralizada preferencialmente em segmento isolado da rede corporativa, com proteção de dispositivos de segurança suficientes para a preservação da sua integridade;

6.2.3. espaço de armazenamento adequado e alertas preventivos de seu esgotamento;

6.2.4. localização física em área sujeita a controles de segurança;

6.2.5. emprego de protocolos seguros para acesso remoto;

6.2.6. possibilidade de execução de auditorias legais e forenses;

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

6.2.8. geração de registros de eventos (logs) para todos os trabalhos executados nos arquivos;

6.2.9. conservação de documentação atualizada dos procedimentos de:

6.2.9.1. configuração, instalação e manutenção;

6.2.9.2. administração e operação;

6.2.9.3. cópia de segurança e restauração.

7. Dos registros de eventos de administrador e operador

7.1. 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:

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

7.1.2. 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;

7.1.3. os administradores e operadores da rede corporativa não devem ter permissão para apagar, alterar ou desativar os registros de eventos de suas próprias atividades.

7.2. 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.

8. Da sincronização dos relógios

8.1. O horário dos ativos de processamento de produção 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.

8.2. O estabelecimento correto dos relógios nos ativos de processamento de produção 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, às seguintes rotinas:

8.2.1. Usar fontes de tempo sincronizadas para todos os ativos monitorados, a partir das quais os ativos de processamento de produção recuperem regularmente as informações de data, hora e fuso horário, de forma que os registros de eventos (logs) sejam cronologicamente consistentes.

9. Disposições finais

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

9.2. A Secretaria de Tecnologia da Informação elaborará, em até 120 dias, os procedimentos operacionais para aplicação desta norma, que levem em conta as boas práticas de cibersegurança e os recursos tecnológicos disponíveis.

9.3. 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.

9.4 Esta norma complementar deve ser revisada, pelo menos, a cada 3 anos e encaminhada para nova apreciação da Comissão de Segurança da Informação.

9.5. Esta norma entra em vigor na data de sua publicação, sua implementação iniciará imediatamente e deverá estar totalmente implantada no prazo de 12 (doze) meses a contar da data de sua publicação.