Tribunal Regional Eleitoral - RJ
Diretoria Geral
Secretaria de Administração
Coordenadoria de Gestão Documental, Informação e Memória

INSTRUÇÃO NORMATIVA DG TRE-RJ Nº 07, DE 03 DE JULHO DE 2023.

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 Rio de Janeiro.

A DIRETORA-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO, no uso das atribuições que lhe são conferidas pelo **art. 9º, I, da Resolução TRE nº 1.266 de 31 de janeiro de 2023 (Regulamento Administrativo do Tribunal Regional Eleitoral do Rio de Janeiro) (https://www.tre-rj.jus.br/legislacao/regulamento-administrativo-do-tribunal-regional-eleitoral-do-rio-de-janeiro) ,**

CONSIDERANDO a **Resolução CNJ nº 396, de 7 de junho de 2021 (https://atos.cnj.jus.br/atos/detalhar/3975)** , que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a **Resolução TSE nº 23.644, de 1º de julho de 2021 (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-644-de-1o-de-julho-de-2021)** , que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

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

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

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

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 Rio de Janeiro; e

CONSIDERANDO, ainda, o disposto no processo SEI nº 2023.0.000017456-1,

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1° Fica instituída a Instrução Normativa para Gestão e Monitoramento de Registro de Atividades (logs) no âmbito do TRE-RJ.

Art. 2° Esta norma integra a Política de Segurança de Informação da Justiça Eleitoral, estabelecida pela **Resolução TSE nº 23.644/2021 (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-644-de-1o-de-julho-de-2021)** .

CAPÍTULO II

DAS DEFINIÇÕES

Art. 3° Para efeitos desta norma consideram-se os termos e definições previstos na **Portaria DG /TSE nº 444/2021 (https://www.tse.jus.br/legislacao/compilada/prt/2021/portaria-no-444-de-08-de-julho-de-2021)** , além dos seguintes:

I - 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;
II - 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;
III - 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.

CAPÍTULO III

DO REGISTRO DE EVENTOS (LOGS)

Art. 4° Devem ser monitorados, preferencialmente 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;
VII - switches e roteadores de núcleo de rede (core);
VIII - servidores controladores de domínio e demais serviços de autenticação;
IX - serviços de gerenciamento de backups (cópias de segurança);
X - serviços de gerenciamento de infraestrutura de virtualização e conteinerização, incluídas as baseadas em nuvem pública;
XI - soluções anti-malware;
XII - soluções controle de acesso físico e lógico;
XIII - soluções gerais de cibersegurança;
XIV - serviços de DHCP;
XV - serviços de DNS.

Art. 5° Os registros de eventos devem conter informações mínimas e 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, modificação ou execução de arquivos, 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.

Art. 6° 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 - recursos acessados e seus respectivos tipos de acesso;
II - informações de falhas nas aplicações ou recursos acessados;
III - outras informações que permitam identificar a possível origem e destino do evento;
IV - criação, alteração e remoção de usuários, perfis e grupos privilegiados;
V - uso de privilégios;
VI - troca de senhas;
VII - modificações de política de senhas, como tamanho, tempo de expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico, entre outras;
VIII - acesso ou modificação de arquivos, serviços e sistemas de informação considerados críticos;
IX - inicialização, suspensão e reinicialização de serviços;
X - acesso físico por senha, cartão inteligente ou biometria em área de segurança com ativos de processamento críticos como Data Center, salas de telecomunicações, entre outros;
XI - logs de auditoria de linha de comando;
XII - logs de requisição de URL, desde que apropriado e suportado.

Art. 7° Os logs devem ser armazenados nos ativos originais de processamento por no mínimo 180 (cento e oitenta) dias, bem como devem estar armazenados em cópias de segurança, ao menos pelo mesmo período, sem prejuízo de outros prazos previstos em referências legais e normativos específicos.

Art. 8° Os registros de eventos no concentrador de logs devem ser armazenados por no mínimo 180 (cento e oitenta) dias, bem como devem estar armazenados em cópias de segurança, ao menos pelo mesmo período, sem prejuízo de outros prazos previstos em referências legais e normativos específicos.

Art. 9° 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.

§ 1° O monitoramento deve ser realizado de forma a manter inalterada a rotina de trabalho do ambiente de produção.
§ 2° 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.
§ 3° 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.
§ 4° Os processos de monitoramento devem ser revisados na implantação ou manutenção dos ativos de processamento, a fim de manter sua adequação às mudanças ocorridas.

Art. 10. 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 IV

DA PROTEÇÃO DAS INFORMAÇÕES DOS REGISTROS DE EVENTOS

Art. 11. 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 - espaço de armazenamento adequado e alertas preventivos de seu esgotamento;
II - localização física em área sujeita a controles de segurança;
III - emprego de protocolos seguros para acesso remoto;
IV - capacidade de assinatura digital ou resumo criptográfico para verificar a integridade;
V - possibilidade de execução de auditorias legais e forenses;
VI - fornecimento, para efeito de investigação, de cópia das informações relevantes, exceto nas hipóteses legais que exijam a apresentação da mídia original.

CAPÍTULO V

DOS REGISTROS DE EVENTOS DE ADMINISTRADOR E OPERADOR

Art. 12. 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.

CAPÍTULO VI

DA SINCRONIZAÇÃO DOS RELÓGIOS

Art. 13. 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. 14. 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 elementos de prova em processos judiciais ou processos administrativos disciplinares, devendo 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

DISPOSIÇÕES FINAIS

Art. 15. Os casos omissos serão resolvidos pela Diretoria-Geral, ouvida previamente a Comissão de Segurança da Informação (COMSI).

Art. 16. Essa norma deve ser revisada a cada 3 (três) anos, ou antes, se necessário, pela Assessoria de Segurança da Informação, com participação da Secretaria de Tecnologia da Informação, e encaminhada para nova apreciação da Comissão de Segurança da Informação.

Art. 17. Esta Instrução Normativa entra em vigor na data de sua publicação e sua implementação se fará no prazo de 24 (vinte e quatro) meses a contar desta data.

ELINE IRIS RABELLO GARCIA DA SILVA
Diretora-Geral

Este texto não substitui o publicado no **DJE TRE-RJ nº 165, de 05/07/2023, p. 3**

(https://dje.tse.jus.br/dje/pdf/v1/edicao/104814#page=3)

FICHA NORMATIVA

Data de Assinatura: 03/07/2023

Ementa: 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 Rio de Janeiro.

Situação: Não consta revogação.

Diretor(a)-Geral: ELINE IRIS RABELLO GARCIA DA SILVA

Data de publicação: DJE TRE-RJ nº 165, de 05/07/2023, p. 3 (https://dje.tse.jus.br/dje/pdf/v1/edicao/104814#page=3)

Alteração: Não consta alteração.