https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1712112&crc=397BEB07, informando, caso não preenchido, o código verificador 1712112 e o código CRC 397BEB07.
2021.00.000004104-1

ATOS DO DIRETOR-GERAL

PORTARIA

PORTARIA TSE Nº 459 DE 13 DE JULHO DE 2021.

Institui norma de gerenciamento e monitoramento de *logs* relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral.

O DIRETOR-GERAL DA SECRETARIA DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições legais e regimentais, 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), e 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,

RESOLVE:

Capítulo I

DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a norma de gerenciamento e monitoramento de *logs* (conjunto de registros de eventos), em consonância com a Política de Segurança da Informação do Tribunal Superior Eleitoral (TSE).

Art. 2º Para os efeitos da Política de Segurança da Informação do TSE, aplicam-se os termos e definições conceituados na Portaria TSE nº 444, de 8 de julho de 2021.

Capítulo II

DO REGISTRO DE EVENTOS (*LOGS*)

Seção I

COMPOSIÇÃO E RETENÇÃO DOS REGISTROS DE EVENTOS

Art. 3º Os registros de eventos devem conter informações mínimas e relevantes, especialmente:

I - identificação inequívoca do usuário que acessou o recurso;

II - identificação dos usuários de origem e destino do evento, quando for o caso;

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

IV - *timestamp*, formado por data, hora e fuso horário;

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

VI - endereços, serviços e protocolos de rede utilizados;

VII - arquivos acessados e tipo de acesso;

VIII - alarmes provocados pelo sistema de controle de acesso.

Art. 4º Os ativos de processamento que não permitam os registros de eventos conforme indicado devem ser mapeados e documentados quanto ao tipo e ao formato de registro de eventos que o sistema permite armazenar.

Art. 5º Os registros de eventos devem ser armazenados na rede corporativa, pelo período de 30 (trinta) dias, e em mídias não regraváveis, por um período mínimo de 12 (doze) meses, sem prejuízo de outros prazos previstos em referências legais e normativas específicas.

Seção II

MONITORAMENTO DOS EVENTOS DE ACESSO OU USO

Art. 6º 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 a bem-sucedida quanto a malsucedida;

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

IV - uso de privilégios;

V - troca de senhas;

VI - modificação de política de senhas, como tamanho, 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 - alteração na configuração de sistemas operacionais, serviços e sistemas de informação;

IX - inicialização, suspensão e reinicialização de serviços;

X - uso de aplicativos e utilitários do sistema operacional;

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 magnético ou biometria em área de segurança com ativos de processamento críticos como *data center*, sala de roteadores, entre outros;

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

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

Art. 7º 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.

§ 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 a intervalos regulares para ajustar sua 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 na manutenção dos ativos de processamento, a fim de manter sua adequação às mudanças ocorridas.

Art. 8º Os usuários devem estar cientes de que os ativos de processamento estão suscetíveis a monitoramento e auditoria sempre que houver suspeita ou constatação de quebra de segurança.

Seção III

MONITORAMENTO DOS EVENTOS DE INCIDENTE OU FALHA

Art. 9º Todos os eventos contrários ao ordenamento jurídico em vigor e às normas constantes da Política de Segurança da Informação do TSE, inclusive os discriminados nos incisos deste artigo, devem ser registrados formalmente e analisados, com adoção das 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 III

DA PROTEÇÃO DAS INFORMAÇÕES DOS REGISTROS DE EVENTOS

Art. 10. Os arquivos de registros de eventos devem ser protegidos para que não sejam possíveis o acesso não autorizado às informações registradas e/ou a falsificação destas.
Parágrafo único. A fim de assegurar a proteção de que trata o *caput*, os seguintes controles mínimos devem ser implementados:
I - armazenamento, no mínimo, em 2 (dois) arquivos de mesmo conteúdo, sendo um deles em local centralizado e protegido contra acessos indevidos;
II - guarda da cópia centralizada 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 - 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 - execução de auditorias legais e forenses por, no mínimo, dois profissionais de áreas diferentes;
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 IV

DOS REGISTROS DE EVENTOS DE ADMINISTRADOR E OPERADOR

Art. 11. 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, 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, a 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;
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. 12. 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. 13. O horário dos ativos de processamento deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a Hora Legal Brasileira, de acordo com o serviço oferecido e assegurado pelo Observatório Nacional.

Art. 14. O estabelecimento correto dos relógios nos ativos de processamento da rede corporativa é importante para 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:

I - uso de, pelo menos, 3 (três) fontes de tempo sincronizadas, 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;

II - preferencialmente, compartilhamento ou sincronização das mesmas fontes de tempo com outros controles de acesso lógico e físico, como catracas, pontos eletrônicos, entre outros, para integrar cronologicamente os sistemas de gerenciamento.

Capítulo VI

DISPOSIÇÕES FINAIS

Art. 15. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação (CSI) do TSE.

Art. 16. A revisão desta portaria ocorrerá a cada 3 (três anos) ou sempre que se fizer necessário ou conveniente para o TSE.

Art. 17. O descumprimento desta portaria deve ser imediatamente registrado como incidente de segurança e comunicado à CSI para apuração e consequente adoção das providências cabíveis.

Art. 18. Esta portaria entra em vigor na data de sua publicação e sua implementação se fará no prazo de 12 (doze) meses a contar dessa data.

RUI MOREIRA DE OLIVEIRA

Documento assinado eletronicamente em 20/07/2021, às 14:34, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1706379&crc=9BAC2FE1, informando, caso não preenchido, o código verificador 1706379 e o código CRC 9BAC2FE1.

2020.00.000004513-0

PORTARIA TSE Nº 458 DE 13 DE JULHO DE 2021.

Institui norma de gestão de ativos, relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral.

O DIRETOR-GERAL DA SECRETARIA DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições legais e regimentais, 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), e 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,

RESOLVE:

Capítulo I