ANEXO XIV
NORMA DE REGISTROS DE EVENTOS

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo

Versionamento:

Versão:	1.0
Data:	03/04/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	12/06/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

A norma de registros de eventos complementa a Política de Segurança da Informação (PSI), definindo as diretrizes para gerenciar registros de eventos dos ativos de Tecnologia da Informação e Comunicação (TIC) do Poder Judiciário do Estado do Maranhão (PJMA).

Para fins desta norma, aplica-se a lista de termos do glossário com suas respectivas definições, conforme descrito no ANEXO I da PSI.

Esta norma obedece ao escopo definido na Política de Segurança da Informação.

2. OBJETIVOS

Registrar eventos, gerar evidências, assegurar a integridade das informações de registro, prevenir contra acesso não autorizado, identificar eventos de segurança da informação que possam levar a um incidente de segurança e apoiar investigações.

Utilizar tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de TIC e de ações dos(as) usuários(as), permitindo automatizar ações de segurança e oferecer inteligência à análise de eventos de segurança.

3. DIRETRIZES

A atividade de auditoria de registros de eventos de TIC é de competência da Diretoria de Informática e Automação (DIA). Os arquivos de registro de eventos deverão ser protegidos contra exclusão, alteração, inclusão indevida ou acesso não autorizado.

Habilitar nos ativos de TIC do PJMA, onde houver suporte para essa atividade, os registros de eventos, devendo ser armazenados por no mínimo 180 dias, exceto ativos de TIC que necessitem manter o registro de eventos por mais tempo, para atender algum normativo interno ou para cumprir alguma exigência legal.

Os ativos de TIC, principalmente os ativos de TIC críticos, deverão estar obrigatoriamente com as informações de data e hora sincronizadas via protocolo NTP (Network Time Protocol), caso haja suporte.

Ações de restabelecimento de serviços e sistemas afetados por incidentes de segurança, não deverão impossibilitar a coleta, a preservação e a disponibilidade de evidências em suas formas íntegras.

Os registros de eventos de ativos de TIC deverão ser criados e retidos na medida necessária para permitir o monitoramento, análise, investigação e relatório de atividades suspeitas ou não autorizadas. Os registros de eventos serão armazenados em pelo menos um repositório central.

Assegurar que os eventos dos ativos de TIC classificados como críticos, sejam registrados, armazenados e mantidos por pelo menos 365 dias, a contar do registro de cada evento.

Caso exista disponibilidade nos ativos de TIC, deverão ser registrados os eventos de:

I - tentativas de acesso (sistemas de informação, serviço de diretório e outros recursos) bem-sucedidas e fracassadas;

II - alterações na configuração do sistema;

III - uso de privilégios;

IV - arquivos acessados e tipo de acesso, incluindo a exclusão de arquivos importantes, a exemplo os arquivos de log de auditoria;

V - alarmes críticos ou importantes disparados pelo serviço de diretório;

VI - gerenciamento: criação, modificação ou exclusão de identidades;

VII - uso de programas e aplicações utilitários;

VIII - operações executadas pelos usuários em aplicações/sistemas, limitando-se ao que é exigido por lei;

IX - ativação e desativação de sistemas de segurança, como ferramenta de proteção contra códigos maliciosos (antivírus), sistemas de detecção de intrusão, etc.

Entradas de trilha de auditoria para componentes de sistema de informação podem ser registradas de forma classificada e personalizada, devendo ser registrados os eventos de:

I - identificação do usuário;

II - origem ou tipo do evento;

III - data e hora;

IV - indicação de sucesso ou falha;

V - endereços IP e portas de origem e destino, para eventos de rede;

VI - a identidade ou o nome dos dados afetados, componentes ou recursos do sistema.

Ativos de TIC críticos ou que contenham dados sensíveis deverão ser registrados os eventos de:

I - identificação do usuário;

II - origem ou tipo do evento;

III - data e hora;

IV - indicação de sucesso ou falha;

V - endereços IP e portas de origem e destino, para eventos de rede.

Uma ferramenta de gerenciamento de eventos de segurança da informação, tipo SIEM ou serviço equivalente, deverá ser utilizada para armazenar, correlacionar, normalizar e analisar informações de eventos e gerar alertas.

Quando não forem mais necessários para requisitos legais, regulatórios ou de negócios do PJMA, os registros dos eventos deverão ser removidos observando diretrizes de descarte seguro.

5. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

5.1 Diretoria de Informática e Automação

É responsabilidade da Diretoria de Informática e Automação, devendo a mesma:

I - possuir acesso irrestrito às informações necessárias ao bom desempenho de suas funções, ao executar as atividades de auditoria;

II - selecionar os registros de eventos e observar os respectivos tempos de guarda, bem como as demais características para utilização dos mesmos;

III - coletar e preservar os registros de eventos e as mídias de armazenamento dos ativos de TIC afetados, pelo tempo necessário para realizar as atividades de auditoria;

IV - configurar e manter a estrutura original dos registros de eventos, principalmente de ativos de TIC críticos ou de ativos que contenham dados sensíveis para o PJMA;

V - justificar formalmente, a impossibilidade de preservar as evidências dos registros de evento de segurança da informação;

VI - realizar análises de auditoria, periódicas e quando forem necessárias, para detectar anomalias ou eventos inusitados que possam indicar uma ameaça potencial;

VII - coletar e armazenar registros de eventos de rede de provedores de serviço, caso haja viabilidade técnica;

VIII - fornecer e gerir serviço de NTP para sincronização dos ativos de TIC do PJMA.

6. INFRAÇÕES E PENALIDADES

Infrações e penalidades serão aplicadas conforme previsto na Política de Segurança da Informação.

7. REVISÕES

Esta norma será alterada mediante necessidade de atualização, com apreciação e aprovação do Comitê de Governança de Segurança da Informação (CGSI).

8. APROVAÇÃO

A norma foi aprovada pelo Comitê de Governança de Segurança da Informação (CGSI), revogando-se todas as disposições em contrário.