1. OBJETIVO

Este procedimento estabelece as diretrizes e responsabilidades para a configuração, monitoramento e manutenção da trilha de auditoria, assegurando que eventos críticos sejam registrados de maneira consistente e que os logs sejam gerenciados de forma segura, contribuindo para a mitigação de riscos de segurança, preservação da confidencialidade dos dados e resposta proativa a eventos adversos.

2. ABRANGÊNCIA

Este procedimento é aplicável a todos os sistemas e ambientes tecnológicos nos quais os registros de log são utilizados para monitorar e registrar eventos. A abrangência deste procedimento inclui, mas não se limita a sistemas de informação, redes de computadores, dispositivos físicos e virtuais, usuários autorizados e administração de sistemas.

3. DOCUMENTOS DE REFERÊNCIA

3.1 Norma ABNT NBR ISO/IEC 27001 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos

4. DEFINIÇÕES

4.1 Sistemas de Informação: todos os sistemas, servidores, aplicativos e dispositivos que processam, armazenam ou transmitem informações sensíveis e críticas para as operações da organização.

4.2 Rede de Computadores: roteadores, switches, firewalls e outros dispositivos de rede que são parte integrante da infraestrutura de rede.

4.3 Dispositivos Físicos e Virtuais: servidores, sistemas de armazenamento em rede (NAS), sistemas de armazenamento conectados à rede (SAN), máquinas virtuais, contêineres e outros recursos de computação que compõem a infraestrutura.

4.4 Usuários Autorizados: todos os usuários autorizados a acessar os sistemas e informações registradas nos logs, incluindo administradores de sistemas, pessoal de TI e outros usuários com privilégios específicos.

4.5 Administração de Sistemas: profissionais responsáveis pela configuração, monitoramento e manutenção da trilha de auditoria e dos registros de log.

5. DIRETRIZES

5.1 Políticas de retenção e dos eventos a serem registrados

5.1.1 Configurar as políticas de retenção de logs de acordo com os requisitos legais e regulatórios.

5.1.2 Garantir a sincronização dos relógios dos sistemas e aplicações, para assegurar o correto correlacionamento dos eventos.

5.1.3 Determinar os eventos a serem armazenados, quando aplicável os seguintes eventos deverão ser registrados: tentativas de acesso ao sistema bem sucedidas ou rejeitadas; tentativas de acesso a recursos bem sucedidas ou rejeitadas; alterações em configurações; uso de privilégios; uso de chamadas de sistema; acessos ao sistema de arquivos, seja para leitura, exclusão, criação ou modificação; ativação e desativação de recursos de segurança; criação, modificação ou exclusão de identidades; transações executadas pelo usuários.

5.1.4 Especificar o formato e o conteúdo dos registros de logs. É adequado que os registros incluam para cada evento, conforme aplicável: ID do usuário; atividades do sistema; datas, horários e detalhes dos eventos; identidade do dispositivo, identificador do sistema e localização; endereços e protocolos de rede.

5.1.5 Definir os eventos críticos que devem ser observados.

5.2 Armazenamento seguro dos logs

- Armazenar os logs em local seguro, protegido contra acessos não autorizados.
- Realizar backups periódicos dos logs.
- Preservar os registros de log, conforme orientações das normas regulatórias.
- Logs dos ambientes de produção deverão ser retidos por 5 anos, e dos demais ambientes por 6 meses.

5.3 Monitoramento contínuo dos log

- Tratar as entradas de logs, tornando-as legíveis para administradores.
- Realizar o monitoramento contínuo dos logs em tempo real.
- Implementar ferramentas IDS (*Intrusion Detecction System*) para descoberta de atividades maliciosas e violações de políticas.

Elaborador: Evertton de Lima Silva, Analista de Redes, em 2025-04-30 13:26
Revisor: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-05-01 19:59
Aprovador: André Magno Costa de Araújo, , em 2025-05-07 18:41

5.4 Análise e resposta a eventos

- Designar as responsabilidades para análise de logs e resposta a incidentes.
- Investigar imediatamente qualquer atividade suspeita ou violação de segurança.
- Implementar ferramentas IPS (*Intrusion Prevetion System*) para executar medidas de resposta automáticas a eventos comuns.

5.5 Treinamento e conscientização

- Fornecer treinamento regular aos administradores de sistemas, gerentes de projetos e usuários autorizados sobre a importância da trilha de auditoria e o tratamento adequado dos logs.

6. REGISTROS

Devem ser mantidos registros de todas as configurações de logs, eventos monitorados, análises de incidentes e revisões periódicas. As ferramentas adotadas para esses registros são:

- FortiAnalyzer: armazena e analisa logs de firewall, acessos e eventos críticos de segurança de rede.
- Graylog: centraliza logs de servidores, aplicações e dispositivos, permitindo análises e correlação de eventos.

Os registros relacionados com este procedimento são:

- Relatórios gerados pelo Graylog e FortiAnalyzer.
- Histórico de ocorrências e ações corretivas, registrando incidentes identificados e medidas adotadas.
- Alertas de eventos, como sucessivo erros de senha.

7. DISTRIBUIÇÃO E CONTROLE

Este documento está disponível e controlado através do sistema INTEGRA, módulo conhecimento/ ISO27001/Procedimentos. Deve ser atualizado anualmente.

8. HISTÓRICO DE ALTERAÇÕES

Revisão	Data	Descrição	Responsável
01	18/04/2024	Criação do documento.	Francisco Meneses
02	01/04/2025	Revisão da estrutura de todo o documento e inclusão do controle de documentos e assinaturas, via sistema INTEGRA. Revisão dos subitens 5.1, 5.2 e do item 6.	Shirley Vital, Evertton Silva e Francisco Menezes

Elaborador: Evertton de Lima Silva, Analista de Redes, em 2025-04-30 13:26
Revisor: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-05-01 19:59
Aprovador: André Magno Costa de Araújo, , em 2025-05-07 18:41