PROCESSO DE GESTÃO DE REGISTRO DE LOGS DE AUDITORIA

1. INTRODUÇÃO

Os registros de *logs* de auditoria servem como uma ferramenta crítica para a segurança, conformidade, investigação, análise e gestão eficiente de sistemas e redes em um ambiente digital. O processo de gestão de registro de *logs* de auditoria utilizado pela UX INNOVATION é responsável por coletar, alertar, analisar e reter *logs* de auditoria de eventos que podem ajudara detectar, compreender ou recuperar-se de um ataque cibernético.

Este processo é uma estratégia utilizada pela UX INNOVATION para garantir a segurança, conformidade, responsabilidade e integridade dos sistemas operacionais, redes, *softwares*, aplicativos, sistemas de informação, serviços e outros ambientes de tecnologia da informação. Ele auxilia a execução de diversas atividades relacionadas à segurança da informação, tais como: monitoramento e detecção de problemas, investigação forense, conformidade com regulamentações e padrões, análise de tendências e padrões, responsabilização, rastreabilidade e suporte à tomada de decisões.

O processo de gestão de registro de *logs* de auditoria define os requisitos de registro para o tratamento da coleta, revisão e retenção de *logs* de auditoria para ativos institucionais. Para que este processo seja executado com eficiência o documento está estruturado em uma breve introdução, definições, registro de *logs* de auditoria, papéis e responsabilidades, matriz RACI, indicador de desempenho, processos relacionados, práticas recomendadas e referências.

1.1 Escopo

O escopo do processo de gestão de registro de *logs* de auditoria envolve uma série de atividades e práticas para garantir que os registros de atividades de um sistema sejam adequadamente coletados, armazenados, protegidos e analisados para garantir a segurança, conformidade e integridade das operações evitando possíveis ameaças ou incidentes de segurança. Esse processo geralmente inclui:

a) coleta de l*ogs*: Identificação dos eventos significativos a serem registrados, como acesso ao sistema, alterações de configuração, atividades de usuários, entre outros;

b) armazenamento seguro: garantia de que os *logs* sejam armazenados de forma segura e protegida contra alterações não autorizadas ou exclusões acidentais. Isso pode envolver criptografia, controle de acesso e backups regulares;

c) padronização e formato: definição de um formato padronizado para os registros de *log*, facilitando a análise e o entendimento desses registros. Por exemplo, uso de formatos como JSON, XML ou syslog;

d) monitoramento e análise: implementação de ferramentas e processos para monitorar e analisar os *logs* em tempo real ou periodicamente, identificando padrões, anomalias ou eventos suspeitos que possam indicar atividades maliciosas;

e) retenção e descarte: definição de políticas claras sobre o período pelo qual os *logs* devem ser mantidos para atender a requisitos regulatórios e de conformidade, assim como a forma como devem ser descartados ao fim desse período;

f) integração com SIEM: Integração dos logs de auditoria com sistemas de gerenciamento de informações e eventos de segurança (SIEM) para correlacionar dados de diferentes fontes e identificar ameaças em potencial;

g) conformidade e relatórios: preparação de relatórios e documentação para demonstrar conformidade com regulamentações e políticas internas, muitas vezes necessárias para auditorias internas ou externas; e

h) melhoria contínua: revisão regular do processo de gestão de registros de *logs* de auditoria para identificar possíveis melhorias e atualizações necessárias para acompanhar as mudanças na tecnologia e nos requisitos regulatórios.

1.2 Objetivos

O objetivo geral do processo é estabelecer requisitos para coletar, armazenar, usar e eliminar *logs* de auditoria de eventos de forma que a UX INNOVATION possa se proteger contra ataques cibernéticos. Para isso foram definidos os seguintes objetivos específicos:

a) monitoramento de segurança: registrar e monitorar atividades para identificar possíveis ameaças de segurança, como acessos não autorizados, tentativas de invasão ou atividades suspeitas;

b) conformidade: garantir que as práticas e operações do sistema estejam em conformidade com regulamentações e padrões específicos, e fornecer evidências para auditorias;

c) detecção de incidentes: facilitar a detecção precoce de incidentes de segurança, permitindo uma resposta rápida e eficaz para mitigar danos ou interromper atividades maliciosas;

d) rastreabilidade e responsabilidade: manter um registro detalhado das atividades do sistema para atribuir responsabilidades, rastrear mudanças e identificar a origem de problemas ou violações de segurança;

e) análise forense: fornecer dados valiosos para investigações forenses após um incidente de segurança, permitindo a reconstrução de eventos para entender o que aconteceu e como;

f) melhoria da eficiência operacional: usar dados de *logs* para identificar tendências, otimizar processos e melhorar a eficiência operacional do sistema;

g) prevenção de fraudes: identificar padrões de atividades incomuns que possam indicar possíveis atividades fraudulentas ou comportamento anômalo;

h) suporte à tomada de decisão: oferecer informações valiosas para tomada de decisões estratégicas relacionadas à segurança e ao funcionamento do sistema.

1.3. Abrangência

A abrangência do processo de gestão de registro de log de auditoria é ampla eabarca várias áreas dentro da UX INNOVATION. Ela engloba:

a) sistemas e aplicações: inclui *logs* de sistemas operacionais, aplicativos, servidores, *firewalls*, bancos de dados, dispositivos de rede e outros dispositivos conectados;

b) ambientes diversificados: abrange ambientes locais, nuvem, ambientes virtualizados e híbridos, garantindo a coleta e gestão dos registros em diferentes plataformas;

c) diversidade de fontes de *logs*: incorpora registros de diversas fontes, como *logs* de segurança, *logs* de acesso, registros de eventos, *logs* de transações, entre outros;

d) conformidade: atende aos requisitos de conformidade impostos por regulamentações governamentais, padrões da indústria e políticas internas da organização;

e) monitoramento contínuo: envolve monitoramento em tempo real, análise periódica e alertas para identificar e responder a eventos de segurança ou anomalias;

f) segurança da informação: contribui para a segurança global da informação ao rastrear atividades suspeitas, identificar ameaças e manter a integridade dos sistemas;

g) análise e resposta a incidentes: fornece dados para investigações forenses e respostas a incidentes, facilitando a compreensão do que aconteceu durante um incidente de segurança;

h) gestão de riscos: ajuda na identificação proativa de riscos ao analisar padrões nos *logs*, permitindo a mitigação antes que se tornem problemas maiores;

i) integração de ferramentas e tecnologias: integração com sistemas de gerenciamento de informações e eventos de segurança (SIEM), ferramentas de análise de *logs*, entre outros, para uma abordagem mais holística na gestão dos *logs;*

j) melhoria contínua: Inclui revisões periódicas do processo de gestão de *log* para identificar áreas de melhoria, atualizar políticas e procedimentos de acordo com as mudanças tecnológicas e regulatórias.

1.4. Benefícios esperados

A execução do processo de gestão de registro de *logs* de auditoria traz osseguintes benefícios:

a) transparência e responsabilidade: a manutenção de registros de auditoria cria transparência nos processos organizacionais. Isso ajuda a estabelecer responsabilidades claras, pois os registros fornecem um histórico detalhado de quem realizou quais ações e quando;

b) conformidade regulatória: possibilita cumprir requisitos legais e regulatórios;

c) detecção de anomalias e fraudes: detectar atividades incomuns ou potencialmente fraudulentas. O monitoramento constante dos registros pode ajudar a identificar desvios de comportamento ou atividades suspeitas;

d) análise de tendências e padrões: ao longo do tempo, os registros de auditoria acumulam dados valiosos que podem ser analisados para identificar tendências, padrões e áreas de melhoria nos processos operacionais da organização;

e) suporte a decisões estratégicas: os registros de auditoria podem servir como uma fonte confiável de informações para a tomada de decisões estratégicas. Eles fornecem *insights* sobreo desempenho passado e atual da organização;

f) aprimoramento da segurança cibernética: em um contexto de segurança da informação, os registros de auditoria são fundamentais para rastrear atividades e identificar potenciais ameaças à segurança cibernética. Eles ajudam a responder rapidamente a incidentes de segurança;

g) avaliação de riscos: os registros de auditoria são úteis na avaliação de riscos. Eles ajudam a identificar áreas de vulnerabilidade e a implementar medidas preventivas para mitigar esses riscos;

h) melhoria contínua dos processos: analisar os registros de auditoria pode revelar oportunidades de melhoria nos processos operacionais, permitindo ajustes e refinamentos para aumentar a eficiência e a eficácia; e

i) evidências em casos legais: em situações legais ou disputas, os registros de auditoria podem servir como evidências críticas para apoiar a posição da organização ou para contestar alegações.

2. DEFINIÇÕES

Para fins de compreensão dos termos utilizados neste processo serão utilizados os seguintes conceitos e definições:

a) alta administração: representa o mais alto nível estratégico e decisório de um órgão ou entidade, seja ela parte da administração pública federal;

b) ataque: evento de exploração de vulnerabilidades. Ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;

c) evento: qualquer mudança de estado que tenha significância para o gerenciamento de um serviço de TI ou outro item de configuração. O termo também pode ser usado para significar um alerta ou notificação criada por qualquer serviço de TI, Item de Configuração ou uma ferramenta de monitoramento. Os eventos normalmente exigem que o pessoal de operações de TI tome medidas e muitas vezes levam a incidentes, os quais devem ser registrados;

d) incidente: interrupção não planejada (imprevista) de um serviço ou redução na qualidade de um serviço. Qualquer evento que cause ou possa causar uma interrupção ou uma redução da qualidade do serviço prestado;

e) informação: qualquer conjunto de dados que resulte em algum significado compreensível. A informação pode possuir algum valor, seus clientes, parceiros e colaboradores, bem como pode ser de propriedade da empresa ou estar sob sua custódia;

f) resposta a incidentes: medidas tomadas para a preparação, detecção, resposta, contenção e recuperação de um incidente de segurança, além de todas as atividades pós incidente e de conscientização;

g) vulnerabilidade: situação que coloca a UX INNOVATION em uma posição mais suscetível a ataques e ações mal-intencionadas. Exemplo: vulnerabilidades de rede, softwares desatualizados e ausência de uma política de segurança da informação bem estruturada; e

h) usuário: qualquer indivíduo com direitos de acesso aprovado.

3. GESTÃO DE REGISTRO DE LOGS DE AUDITORIA

O gerenciamento de registro de *logs* de auditoria é uma abordagem que envolve a coleta, armazenamento, uso e exclusão de eventos registrados em recursos, sistemas, softwares, aplicativos, sistemas de informação e serviços de TI de modo a reduzir os riscos de ataques cibernéticos e violações de segurança da informação (CIS, 2023). Este processo é composto por fases que serão detalhadas nas próximas seções.

3.1. Processo de gestão de registro de auditoria

Segundo Unicamp (2020) a ausência de registros confiáveis de auditoria pode inviabilizar ações jurídicas para remediação de prejuízos financeiros ou da imagem da instituição. Neste

sentido, o processo de gestão de registro de *logs* de auditoria tem como objetivo garantir a segurança, integridade e conformidade das operações de um sistema ou ambiente de tecnologia da informação.

O processo de gestão de registro de logs de auditoria é responsável por coletar, alertar, analisar e reter *logs* de auditoria de eventos que podem ajudar a detectar, compreender ou recuperar de um ataque (CIS, 2023). A partir da execução das fases deste processo, a UX INNOVATION pode diminuir suas superfícies de ataque cibernético, identificar e remover erros de configuração e problemas de segurança que possam ser explorados.

Com a execução do processo será possível gerenciar recursos, sistemas e serviços de TI de forma mais eficiente e segura. A partir do processo é possível assegurar a análise de eventos que possam impactar diretamente na segurança da informação relaciona à recursos, sistemas e serviços de TI. A figura 1 apresenta as 4 (quatro) fases que compõem o processo de gestão de registros de *logs* de auditoria da UX INNOVATION.

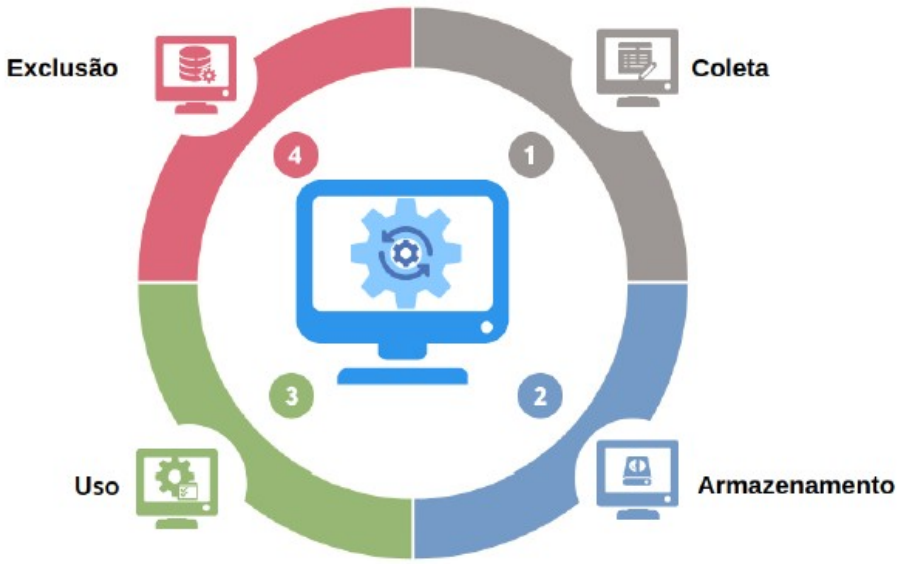

Figura 1 - Processo de gestão de registro de *logs* de auditoria

3.1.1. Coleta

Fase responsável pelo registro detalhado de eventos significativos para a segurança da informação. Esta fase registra os eventos realizados pelos usuários nos ativos de TI.

Os *logs* coletados nesta fase são gerados por diversas fontes, incluindo *software* de segurança, antivírus, *firewalls* e sistemas de prevenção e detecção de intrusão, sistemas operacionais em servidores, estações de trabalho e equipamentos de rede e aplicações.
Nesta fase podem ser realizadas as seguintes atividades:

a) identificação de fontes de registro: sistemas operacionais, servidores de aplicativos, *firewalls*, bancos de dados, dispositivos de rede e outros componentes do ambiente de TI;

b) configuração de parâmetros de registro em sistemas, servidores, dispositivos de rede, aplicativos e outros componentes do ambiente de TI para geração de *logs*;

c) especificação dos eventos a serem registrados e a quantidade de detalhes necessários para análise eficaz;

d) padronização do formato de *log* para garantir consistência;

e) implementação de protocolos seguros para a transmissão de *logs*;

f) configuração de coleta de *logs* em tempo real;

g) definição de intervalos apropriados para garantir que as informações estejam atualizadas;

h) implementação de mecanismos para lidar com o *overflow* de *logs*;

i) garantia de que apenas usuários autorizados tenham acesso aos registros de auditoria;

j) implementação de controles de acesso para proteger contra manipulação não autorizada dos *logs*;

k) coleta de *logs* de auditoria;

l) realização de testes regulares para garantir que os sistemas estão registrando os eventos conforme esperado; e

m) validação da qualidade e integridade dos *logs* coletados para evitar lacunas nas informações.

Fernando Shiguero Shimada
Gestor de Segurança da Informação

Alexandre Lopes Ambrósio
Diretor de Operações

8 páginas - Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON)
Certificado de assinaturas gerado em 05 de November de 2024, 15:17:37

Processo De Gestão De Registro De Logs De Auditoria UX docx

Código do documento 243671e5-c5f4-42cd-9b18-cb973372e4e5

Assinaturas

Fernando Shiguero Shimada
fernando.shiguero@uxinnovation.com.br
Assinou

Fernando Shiguero Shimada

Alexandre Lopes Ambrosio
alexandre.ambrosio@uxinnovation.com.br
Assinou

Alexandre Lopes Ambrosio

Eventos do documento

05 Nov 2024, 12:43:06
Documento 243671e5-c5f4-42cd-9b18-cb973372e4e5 **criado** por ALEXANDRE LOPES AMBROSIO (623ed979-d47e-439d-92ea-bd1e4b98cd3b). Email:contato@uxinnovation.com.br. - DATE_ATOM: 2024-11-05T12:43:06-03:00

05 Nov 2024, 12:44:13
Assinaturas **iniciadas** por ALEXANDRE LOPES AMBROSIO (623ed979-d47e-439d-92ea-bd1e4b98cd3b). Email: contato@uxinnovation.com.br. - DATE_ATOM: 2024-11-05T12:44:13-03:00

05 Nov 2024, 13:59:36
ALEXANDRE LOPES AMBROSIO **Assinou** - Email: alexandre.ambrosio@uxinnovation.com.br - IP: 134.238.232.174 (134.238.232.174 porta: 21478) - Geolocalização: -23.568255196553242 -46.68878241472178 - Documento de identificação informado: 286.056.418-78 - DATE_ATOM: 2024-11-05T13:59:36-03:00

05 Nov 2024, 15:17:05
FERNANDO SHIGUERO SHIMADA **Assinou** - Email: fernando.shiguero@uxinnovation.com.br - IP: 187.101.79.185 (187-101-79-185.dsl.telesp.net.br porta: 33306) - Documento de identificação informado: 326.434.668-02 - DATE_ATOM: 2024-11-05T15:17:05-03:00

Hash do documento original
(SHA256):7994836f18dcbd4c2f04df8f3b7a6d2ddd3ee416e7c73eb7da0f2d5d9a06f61d
(SHA512):784a936dd7cc4f53920d57fe02765c9211724efc4309f84cb0e5e2202158ac11d798fe35b76910b13e0e99378c7bbec17ed5f1ee18c53e87911bbd82591cad8d

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

Esse documento está assinado e certificado pela D4Sign