Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Tocantins
Reitoria

PROCESSO DE GESTÃO DE REGISTRO DE LOGS DE AUDITORIA

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
05/01/2024	1	Elaboração do processo de gestão de registro de *logs* 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 pelo IFTO é responsável por coletar, alertar, analisar e reter *logs* de auditoria de eventos que podem ajudar a detectar, compreender ou recuperar-se de um ataque cibernético.

Este processo é uma estratégia utilizada pelo IFTO 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 o IFTO 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 e abarca várias áreas dentro do IFTO. 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 os seguintes 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* sobre o 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 o IFTO 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 uma ataque (CIS, 2023). A partir da execução das fases deste processo, o IFTO 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 do IFTO.

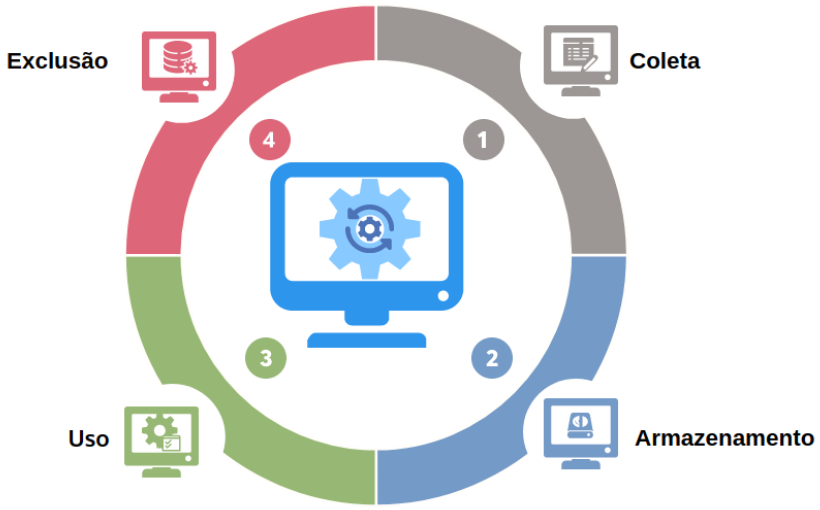

Figura 1 - Processo de gestão de registro de *logs* de auditoria

As fases do processo de gestão de registro (*logs*) de auditoria serão detalhadas na tabela 1.

Tabela 1 - Detalhamento do processo de gestão de registro de *logs* de auditoria

Processo de gerenciamento de registro de *logs* de auditoria	
Entrada	Registro de eventos de recursos, sistemas, softwares, aplicativos, banco de dados, sistemas de informação e serviços de TI.
Fases	1. Coleta. 2. Armazenamento. 3. Uso. 4. Exclusão.
Saída	*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.

3.1.2. Armazenamento

Fase responsável por garantir a integridade, disponibilidade e acessibilidade das informações registradas nos *logs* de auditoria. Na medida do possível, o IFTO centralizará a retenção de *logs* de auditoria de eventos realizados pelos usuários em seus ativos de informação com o objetivo de aperfeiçoar o gerenciamento destes *logs*. Nesta fase podem ser realizadas as seguintes atividades:

a) estabelecimento de normas para retenção de *logs*, determinar por quanto tempo os registros devem ser mantidos conforme requisitos legais, regulatórios e de conformidade;

b) escolha do local seguro para armazenamento dos *logs* (servidores dedicados, armazenamento em nuvem seguro ou outras soluções de armazenamento de dados);

c) implementação de medidas de segurança para proteger os registros armazenados;

d) configuração de controles de acesso para garantir que apenas usuários autorizados possam acessar os registros de auditoria;

e) reter registros de auditoria;

f) estabelecimento de mecanismos para monitorar a integridade dos *logs* armazenados;

g) implementação de plano de backup regular para garantir a recuperação de dados em caso de falhas de hardware, corrupção de dados ou outros eventos adversos;

h) indexação e catalogação de registros para facilitar a pesquisa e recuperação eficientes de informações específicas;

i) utilização de técnicas de compactação para otimizar o armazenamento e reduzir o espaço necessário para registros de *logs*;

j) manutenção de um formato de *log* padronizado para facilitar a análise e a interpretação dos dados;

k) realização de auditorias regulares no armazenamento de *logs* para garantir conformidade com normas estabelecidas e requisitos regulatórios; e

l) documentação detalhada de normas e procedimentos relacionados ao armazenamento de *logs*.

3.1.3. Uso

Esta fase responsável pela análise e interpretação ativa dos dados registrados nos *logs* de auditoria para tomar decisões informadas, responder a incidentes de segurança, garantir conformidade e otimizar o desempenho do sistema. Na medida do possível o IFTO deve garantir que os *logs* de auditoria estejam disponíveis para o acesso quando for necessário, e manter o controle de acesso lógico aos diretórios onde os *logs* estão armazenados. Nesta fase podem ser realizadas as seguintes atividades:

a) uso de ferramentas de análise de *logs* ou sistemas de gerenciamento de eventos de segurança para examinar os registros de auditoria;

b) identificação de padrões, anomalias e eventos significativos que possam indicar atividades suspeitas ou não conformidades;

c) configuração de alertas em tempo real para eventos críticos, possibilitando uma resposta rápida a possíveis ameaças ou incidentes de segurança;

d) uso de registros de auditoria para reconstruir a sequência de eventos, entender a natureza do incidente e determinar a extensão do impacto;

e) avaliação regular de registros de auditoria em relação a políticas de segurança e conformidade;

f) criação de relatórios periódicos de auditoria para documentar eventos relevantes, a conformidade com normas estabelecidas e outras métricas importantes;

g) correlação de eventos para entender melhor as relações entre diferentes registros com a finalidade de revelar padrões que não seriam evidentes ao analisar eventos isolados;

h) utilização de registros de auditoria para identificar potenciais ameaças e vulnerabilidades no ambiente de TI de forma a orientar a implementação de medidas de segurança adicionais;

i) análise os *logs* para identificar possíveis melhorias no desempenho do sistema, podendo incluir ajustes em configurações, otimização de recursos e resolução de problemas de desempenho;

j) integração da análise de *logs* aos processos de resposta a incidentes;

k) realização de revisões regulares do processo de uso de registros de *logs* para identificar áreas de melhoria;

l) ajuste de análises de *logs* sobre novas ameaças, conforme o necessário;

m) realização de treinamento aos profissionais de segurança, operadores de sistemas e outros *stakeholders* para garantir que saibam como interpretar e agir com base nos registros de auditoria; e

n) integração da análise de *logs* com outras ferramentas de segurança da informação, como sistemas de prevenção de intrusões (IPS) e antivírus, para obter uma visão mais abrangente das ameaças.

3.1.4. Exclusão

Fase responsável por gerenciar de forma adequada a remoção ou exclusão de registros de *logs* de auditoria conforme as normas, requisitos legais e regulamentares. Os eventos de auditoria em ativos de TI considerados críticos devem ser armazenados por um período pré-estabelecido e quando este prazo vencer, o IFTO deve ser capaz de realizar a eliminação de *logs* de forma eficiente, com base nas melhores práticas de segurança da informação e normativos como LGPD e LAI. Nesta fase podem ser realizadas as seguintes atividades:

a) estabelecimento de normas de retenção de *logs*, indicando por quanto tempo os registros devem ser mantidos para atender a requisitos legais, regulatórios e de conformidade;

b) definição de normas de exclusão segura de registros após o período de retenção expirar;

c)implementação de processos automatizados para exclusão de registros conforme as normas estabelecidas de forma a garantir consistência e conformidade com os prazos definidos;

d) realização de verificações regulares para garantir que a exclusão de registros esteja em conformidade com as políticas estabelecidas e requisitos regulatórios;

e) garantia de que a exclusão de registros seja feita de maneira segura, minimizando a chance de recuperação por partes não autorizadas, podendo envolver a sobrescrição segura dos dados ou outros métodos de exclusão segura;

f) manutenção de registros ou trilhas de auditoria que documentem as atividades de exclusão de registros para rastrear quem, quando e por que os registros foram excluídos; e

g) exclusão de registros de *logs* em conformidade com a legislação vigente no âmbito da administração pública federal.

4. PAPÉIS E RESPONSABILIDADES

Um papel é um conjunto de responsabilidades, atividades e autoridades definidas em um processo e atribuídas a uma pessoa, equipe ou função. Os papéis e responsabilidades dos envolvidos no processo de gestão de registro de logs de auditoria são:

4.1. Alta Administração

Representa o mais alto nível estratégico e decisório de um órgão ou entidade, seja ela parte da administração pública federal. Compete ao representante deste nível as

seguintes responsabilidades:

a) prover a orientação e o apoio necessário às ações de gestão de registro de *logs* de auditoria, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes; e

b) garantir os recursos (humanos, tecnológicos e financeiros) para a execução da gestão de registro de *logs* de auditoria no âmbito do IFTO.

4.2. Comitê de Segurança da Informação

Grupo de pessoas que representam áreas finalísticas do IFTO. Compete a este grupo de pessoas as seguintes responsabilidades:

a) deliberar sobre norma interna complementar de registro de *logs* de auditoria;

b) assessorar a implementação das ações para o registro de *logs* de auditoria;

c) constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre registro de *logs* de auditoria;

d) participar da elaboração da política de gestão registro de *logs* de auditoria e norma interna complementar;

e) propor alterações à Política de gestão de registro de *logs* de auditoria e normas internas complementares;

f) deliberar sobre normas internas complementares de registro de *logs* de auditoria; e

g) avaliar e aprovar o processo de registro de logs de auditoria.

4.3. Equipe de Tratamento e Resposta à Incidentes Cibernéticos - ETIR

Grupo de pessoas composto por servidores públicos civis ocupantes de cargo efetivo, com capacitação técnica compatível com as atividades dessa equipe. Compete à estas pessoas a seguinte responsabilidade:

a) avaliar o processo de gestão de registro de *logs* de auditoria; e

b) deliberar sobre procedimentos internos para registro de *logs* de auditoria.

4.4. Gestor de Tecnologia da Informação

Servidor designado para gerir os recursos, sistemas, softwares, aplicativos, sistemas de informação e serviços de TI. Compete à esta pessoa a seguinte responsabilidade:

a) planejar, implementar e melhorar continuamente os controles de registro de *logs* de auditoria em soluções de tecnologia da informação e comunicações, nos termos da legislação vigente na administração pública federal.

4.5. Gestor de Segurança da Informação

Servidor designado para gerir a segurança da informação. Compete à esta pessoa as seguintes responsabilidades:

a) coordenar a elaboração da política e processo de Gestão de Registros (*logs*) de Auditoria e das normas internas complementares, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

b) assessorar a alta administração na implantação da Política de Gestão de Registros (*logs*) de Auditoria e das normas internas de segurança da informação do IFTO;

c) incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à registros de *logs* de auditoria;

d) propor recursos necessários às ações de registros de *logs* de auditoria;

e) verificar os resultados dos trabalhos de auditoria sobre a gestão de registros de *logs* de auditoria;

f) acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos relacionados à gestão de registros de *logs* de auditoria; e

g) designar um agente responsável pela execução das atividades inerentes à gestão de registro de *logs* de auditoria, dentre os servidores efetivos do IFTO.

4.6. Setor de TI (Diretoria de Tecnologia da Informação e demais Setores de TI das unidades do IFTO)

Agente responsável pela gestão de *logs* de auditoria. Compete ao setor as seguintes responsabilidades:

a) identificar os recursos, sistemas e serviços de TI que terão logs de auditoria gerenciados de acordo com a sua criticidade;

b) pesquisar, implantar e manter soluções para gestão de registro de *logs* de auditoria no âmbito do IFTO;

c) propor e gerenciar procedimentos de gestão de registro de *logs* de auditoria para a rede de comunicação de dados do IFTO;

d) implantar, configurar, gerenciar e monitorar a estrutura de registro de *logs* de auditoria; e

e) implementar rotinas para gestão de *logs* de auditoria.

4.7. Usuários

Pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da administração pública federal. Compete aos usuários as seguintes responsabilidades:

a) atender aos princípios e diretrizes contidos nesta política, incluindo normas e procedimentos complementares destinados à segurança da informação e comunicação; e

b) guiar-se pelos princípios de confidencialidade, autenticidade, integridade, não repúdio, conformidade, controle de acesso e disponibilidade no decorrer de suas atividades.

5. MATRIZ RACI

A matriz RACI apresentada na tabela 2 é utilizada para definir com clareza as atribuições, papéis e responsabilidades de cada colaborador nas atividades do processo. A sigla RACI significa, em inglês: *responsible, accountable, consulted e informed*.

a) responsible (responsável): pessoa, função ou unidade organizacional responsável pela execução de uma atividade no âmbito de um processo; representa quem irá, de fato executar a tarefa; deve haver ao menos um por tarefa;

b) accountable (responsabilizado): dono da atividade, deverá fornecer os meios para que a atividade possa ser executada, e será responsabilizado caso a atividade não alcance os seus objetivos; cada atividade só pode possuir um *Accountable*; define quem será responsável pelo sucesso da atividade; fica encarregado de verificar se a atividade foi realizada com sucesso e dentro do prazo; deve haver um, e apenas um, por atividade;

c) consulted (consultado): pessoa que deve ser consultada durante a execução da atividade; As informações levantadas junto a essas pessoas tornam-se entradas para a execução da atividade; geralmente exercem papel de conselho na tomada de decisões; e

d) ***informed (informado):*** pessoa que será informada acerca do progresso da execução da atividade.

Tabela 2 - Matriz de responsabilidades

Fase	AA	CSI	GSI	ETIR	STI	U
Coleta	A	C	C	C	R	I
Armazenamento	A	C	C	C	R	I
Uso	A	C	C	C	R	I
Exclusão	A	C	C	C	R	I

Legenda:

AA: Alta Administração

CSI: Comitê de Segurança da Informação.

GSI: Gestor de Segurança da Informação.

ETIR: Equipe de Tratamento e Resposta à Incidentes Cibernéticos.

STI: Setor de Tecnologia da Informação (Diretoria de Tecnologia da Informação e demais unidades do IFTO)

U: Usuários

6. INDICADOR DE DESEMPENHO

O processo de gerenciamento de registro de (*logs*) de auditoria deve ser monitorado e avaliado periodicamente através de indicador de desempenho de forma a realizar eventuais ajustes necessários. Esse monitoramento tem como objetivo acompanhar a eficácia do processo, identificando tendências, falhas e oportunidades de correções, promovendo sempre a melhoria contínua. A tabela 3 apresenta o indicador de desempenho do processo.

Tabela 3 - Indicador de Desempenho

Indicador	Número de sistemas com registro de *logs* de auditoria configurados de forma centralizada.
Descrição	Quantidade de sistemas com registro de *logs* de auditoria configurados de forma centralizada.
Objetivo	Aumentar o número de sistemas com registro de *logs* de auditoria configurados de forma centralizada.
Periodicidade	Anual
Fonte	DTI
Fórmula	Soma de sistemas com registro de *logs* de auditoria configurados de forma centralizada.
Meta	Aumentar o número de sistemas com registro de *logs* de auditoria configurados de forma centralizada.

7. PROCESSOS RELACIONADOS

Para que a abordagem de segurança da informação seja efetiva, a gestão de registros (*logs*) de auditoria está interligada à outros processos de privacidade e segurança da informação. A figura 2 apresenta os processos que compõem o SGSI-IFTO.

Figura 2 - Processos que compõem o SGSI-IFTO

8. PRÁTICAS RECOMENDADAS

As práticas recomendadas nas referências utilizadas para a elaboração deste documento incluem:

1. Regras para registro (*logs*) de auditoria devem ser estabelecidas, documentadas e atualizadas continuamente de forma a produzir inteligência contra ameaças cibernéticas.

2. Um processo de gestão de registros (*logs*) de auditoria deve ser estabelecido, executado, documentado e atualizado continuamente, contendo minimamente as fases coleta, armazenamento, uso e exclusão de eventos relacionados à recursos, redes, sistemas operacionais, *softwares*, aplicativos, sistemas de informação e serviços de TI.

3. Registros (*logs*) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação devem ser produzidos e mantidos por um período de tempo conforme disponibilidade de recursos tecnológicos para futuras investigações e monitoramento de controle de acesso.

4. O IFTO deve manter, monitorar e analisar logs de auditoria dos ativos de *software*, *hardware* e de rede críticos para o negócio.

5. Serviços de TI disponibilizados por terceiros devem ter *logs* analisados criticamente e auditorias devem ser executadas regularmente.

6. O IFTO deve quando possível garantir o armazenamento adequado do registro de auditoria, ou seja, certificar de que os destinos dos logs mantenham armazenamento adequado para cumprir o processo de gestão de log de auditoria da organização.

7. O IFTO deve padronizar a sincronização de tempo, ou seja padronizar a sincronização de tempo, ou seja configurar pelo menos duas fontes de tempo sincronizadas nos ativos institucionais.

8. Quando possível o IFTO deve reter os *logs* de auditoria em ativos institucionais por no mínimo 90 dias.

9. Quando possível o IFTO deve coletar *logs* de auditoria e certificar de que a coleta esteja sendo realizada de acordo como o processo de gestão de *logs* de auditoria.

10. Quando possível o IFTO deve configurar o *logs* e auditoria detalhado para ativos institucionais contendo dados sensíveis, incluir a origem do evento, data, nome de usuário, data e hora, endereços de origem, endereços de destino e outros elementos úteis que podem ajudar em uma investigação forense.

11. Quando possível o IFTO deve habilitar *logs* de auditoria de consulta DNS para detectar pesquisas de nome de host para domínios maliciosos conhecidos.

12. Quando possível o IFTO deve coletar *logs* de auditoria de linha de comando, tais como microsoft powershell e bash.

13. Quando possível o IFTO deve centralizar a coleta e retenção de *logs* de auditoria nos ativos institucionais.

14. Quando possível o IFTO deve realizar análises de *logs* de auditoria para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial.

15. Quando possível o IFTO deve coletar *logs* do provedor de serviços (coleta de eventos de autenticação e autorização, eventos de criação e de descarte de dados e eventos de gestão de usuários.

16. Ferramentas de agregação de *logs* devem ser utilizadas para simplificar a análise e pesquisa de eventos.

17. Análises regulares dos *logs* devem ser realizadas para identificar padrões, anomalias e atividades suspeitas.

18. Relatórios de auditoria devem ser criados para documentar a conformidade e as atividades relevantes.

19. *Backup*s regular dos *logs* para garantir que os dados estejam disponíveis em caso de falhas ou incidentes devem ser realizados.

20. Procedimentos de registro de *logs* devem ser revisados e reajustados com base nas mudanças nos requisitos de segurança e conformidade.

21. Auditorias periódicas nos registros de *logs* de auditoria devem ser realizadas para identificar possíveis melhorias no processo.

9. REFERÊNCIAS

BRASIL. Presidência da República. Gabinete de Segurança da Informação. **Norma Complementar Nº 8, de 19 de agosto de 2010: Gestão de ETIR: diretrizes para o gerenciamento de incidentes em redes computacionais nos órgãos e entidades da administração pública federal. Disponível em:** https://datasus.saude.gov.br/wp-content/uploads/2019/08/Norma-Complementar-n%C2%BA-08IN01DSICGSIPR.pdf Acesso em: 6 de dez. 2023.

BRASIL. Presidência da República. Gabinete de Segurança da Informação. **Norma Complementar Nº 21, de 8 de outubro de 2014. Disponível em:** https://datasus.saude.gov.br/wp-content/uploads/2019/08/Norma-Complementar-n%C2%BA-21IN01DSICGSIPR.pdf Acesso em: 6 de dez. 2023.

BRASIL. Presidência da República. Gabinete de Segurança da Informação. **Instrução Normativa Nº 1 de 27 de maio de 2020: dispõe sobre a estrutura de gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.** Disponível

em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215 Acesso em: 6 de dez. 2023.

BRASIL. Presidência da República. Gabinete de Segurança da Informação. **Instrução Normativa Nº 4 de 26 de março de 2020: dispõe sobre os requisitos mínimos de segurança cibernética que devem ser adotados no estabelecimento das redes 5G.** Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-4-de-26-de-marco-de-2020-250059468. Acesso em: 6 de dez. 2023.

BRASIL. Presidência da República. Gabinete de Segurança da Informação. **Instrução Normativa Nº 5, de 30 de agosto de 2021: dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.** Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684. Acesso em: 6 de dez. 2023

BRASIL. Presidência da República. Gabinete de Segurança da Informação. **Instrução Normativa Nº 3, de 28 de maio de 2021: dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.** Disponível em: https://www.gov.br/gsi/pt-br/ssic/legislacao/copy_of_IN03_consolidada.pdf. Acesso em: 6 dez. 2023.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Portaria nº 852, de 28 de março de 2023: dispõe sobre o programa de privacidade e segurança da informação** - PPSI. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908 Acesso em: 6 de dez. 2023.

UNIVERSIDADE DE CAMPINAS. **Instrução Normativa IN-CITIC-006/2020: gestão de registros (logs).** Disponível em: https://www.citic.unicamp.br/sites/default/files/normas/Instru%C3%A7%C3%A3o%20Normativa%20CITIC%20IN-006_2020%20-%20Gest%C3%A3o%20de%20registros%20(logs)%20de%20auditoria_1188504.pdf Acesso em: 5 dez. 2023.

CENTER FOR INTERNET SECURITY. **Controle 8: gestão de registro de auditoria.** Disponível em: https://www.cisecurity.org/ Acesso em: 5 dez. 2023.

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 05/01/2024, às 16:13, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ifto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2218366** e o código CRC **626F5FA5**.
