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

PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
05/01/2024	1	Elaboração do processo gestão de incidentes de segurança da informação.

1. INTRODUÇÃO

Incidente de segurança é qualquer evento adverso, confirmado ou sob suspeita relacionado à segurança dos sistemas de computação ou das redes de computadores como por exemplo: ataques cibernéticos, invasão de servidores, roubo de informações, perda de dados, indisponibilidade do ambiente tecnológico, violação da política de segurança da informação, compartilhamento de senhas etc. O processo de gerenciamento de incidentes de segurança da informação é uma abordagem estruturada para lidar com eventos de segurança da informação, como violações de dados, ataques cibernéticos e outras ameaças à privacidade da informação.

Este processo é essencial para proteger os ativos digitais de uma organização, mitigar riscos, garantir conformidade, aprender com incidentes passados e manter a confiança dos clientes e partes interessadas. Ele geralmente inclui a detecção de incidentes de segurança, avaliação da gravidade do incidente, contenção do incidente, investigação da causa raiz do incidente, recuperação e restauração dos sistemas afetados, além de monitoramento e revisão para evitar futuros incidentes semelhantes.

O processo de gestão de incidentes de segurança da informação visa a garantir uma resposta eficaz e coordenada a eventos adversos, minimizando danos e interrupções nos negócios, além de fortalecer a resiliência do IFTO diante de ameaças cibernéticas. Para ter um controle maior sobre os incidentes de segurança este documento está estruturado em uma breve introdução, definições, gestão de incidentes de segurança da informação, papéis e responsabilidades, matriz RACI, indicador de desempenho, processos relacionados, práticas recomendadas e referências.

1.1. Escopo

O escopo do processo de gestão de incidentes de segurança da informação abrange todas as atividades necessárias para responder a um incidente de segurança, desde a detecção inicial até a resolução e recuperação, tais como: detecção de incidentes, classificação

e triagem, resposta imediata, investigação e análise, notificação e reporte, recuperação e remediação, análise pós-incidente e aprendizado e melhoria contínua.

1.2. Objetivos

O objetivo geral do processo é assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil. Para isso foram definidos os seguintes objetivos específicos:

a) identificação precoce de incidentes: detectar e identificar rapidamente possíveis incidentes de segurança para mitigar seu impacto e evitar danos maiores;

b) resposta eficiente e coordenada: responder de maneira rápida e eficaz aos incidentes, minimizando a propagação do ataque e reduzindo o tempo de inatividade dos sistemas;

c) contenção e redução de danos: isolar e conter incidentes para limitar o alcance do impacto nos sistemas, dados e operações da organização;

d) preservação de evidências: coletar e preservar evidências relevantes para análise forense, investigação de incidentes e suporte a possíveis processos legais;

e) análise e investigação detalhadas: compreender a natureza do incidente, suas causas, métodos utilizados pelos invasores e o impacto nos sistemas e na informação;

f) notificação e conformidade: cumprir com os requisitos legais e regulatórios para notificação de incidentes de segurança, quando necessário, além de manter registros precisos e relatórios adequados;

g) recuperação e restauração: restaurar a funcionalidade normal dos sistemas afetados, corrigindo as vulnerabilidades exploradas e aplicando medidas de segurança adicionais para prevenir futuros incidentes semelhantes;

h) aprendizado e melhoria contínua: analisar os incidentes passados para identificar lacunas nos controles de segurança, aprimorar políticas, procedimentos e treinamentos, visando fortalecer a postura de segurança da organização;

i) minimização de prejuízos financeiros e reputacionais: reduzir os impactos financeiros e proteger a reputação da empresa, mantendo a confiança dos clientes, parceiros e partes interessadas;

j) fortalecimento da resiliência: desenvolver e aprimorar a capacidade da organização de lidar com incidentes de segurança, garantindo sua capacidade de recuperação e continuidade de negócios.

1.3. Abrangência

O processo de gestão de incidentes de segurança da informação abrange uma série de série de atividades para garantir a detecção, resposta, mitigação e aprendizado contínuo a partir de incidentes de segurança. Esta abordagem abrange os seguintes aspectos:

a) preparação: inclui a definição de políticas, procedimentos e planos de resposta a incidentes, alocando recursos adequados e treinando equipe para lidar com eventos de segurança;

b) detecção e identificação: consiste em identificar eventos ou atividades anômalas nos sistemas de informação que possam indicar um incidente de segurança em andamento ou

iminente;

c) classificação e avaliação: uma vez detectado, é importante classificar o incidente de acordo com sua gravidade, impacto potencial e categorização (ataque de *malware*, violação de dados, etc.) para priorizar a resposta;

d) resposta e contenção: Isso envolve responder imediatamente para conter o incidente, minimizar danos, isolar sistemas afetados e interromper a progressão do ataque;

e) investigação e análise: após a contenção, é essencial investigar a fundo o incidente para entender como ocorreu, identificar suas origens, o que foi afetado e as falhas que permitiram o incidente;

f) recuperação e restauração: uma vez que o incidente é compreendido, é hora de recuperar os sistemas afetados, restaurar os serviços e dados comprometidos para um estado seguro e funcional;

g) comunicação e notificação: dependendo da gravidade do incidente, é necessário comunicar interna e externamente, seja para informar sobre a situação, notificar partes interessadas afetadas ou seguir requisitos regulatórios;

h) aprendizado e melhoria contínua: uma parte crucial é aprender com o incidente. Isso envolve analisar o que foi feito, identificar oportunidades de melhoria nos processos, políticas e sistemas de segurança para evitar futuros incidentes similares;

i) documentação e relatórios: Registrar detalhes do incidente, ações tomadas, lições aprendidas e recomendações para futuras referências, relatórios regulatórios ou análises pós-incidente; e

j) monitoramento e revisão: implementar um processo contínuo de monitoramento de ameaças e sistemas para detectar atividades suspeitas, revisar regularmente políticas e procedimentos de resposta e adaptar estratégias de segurança conforme necessário.

1.4. Benefícios esperados

A execução do processo de gestão de incidentes de segurança da informação traz os seguintes benefícios:

a) resposta rápida a incidentes: permite que a organização responda rapidamente a eventos de segurança, minimizando danos potenciais;

b) redução de impactos financeiros e operacionais: ao identificar e responder prontamente a incidentes, a organização pode reduzir os custos associados a interrupções de operações, perda de dados ou danos à reputação;

c) proteção dos ativos de informação: a rápida detecção e resposta a incidentes de segurança ajuda a proteger os ativos críticos de informação da organização contra acesso não autorizado, alteração ou destruição;

d) conformidade: a gestão adequada de incidentes é muitas vezes um requisito para estar em conformidade com regulamentações e leis de proteção de dados, demonstrando que medidas foram tomadas para proteger informações sensíveis;

e) identificação de ameaças emergentes: ao analisar incidentes passados, é possível identificar tendências e novos métodos utilizados por hackers ou ameaças emergentes, ajudando na preparação para futuros ataques;

f) aprendizado e melhoria contínua: a gestão de incidentes permite que a organização aprenda com cada evento, refinando suas políticas, procedimentos e sistemas de segurança para se

tornar mais resiliente e preventiva;

g) preservação da reputação da organização: uma resposta rápida e eficaz a incidentes de segurança pode mitigar danos à reputação da organização, mostrando responsabilidade e compromisso com a proteção de dados dos clientes e parceiros;

h) detecção de vulnerabilidades e fraquezas: ao investigar incidentes, a organização pode identificar vulnerabilidades e fraquezas em seus sistemas, permitindo a implementação de medidas preventivas para mitigar futuros ataques; e

i) compartilhamento de informações: a participação em programas de compartilhamento de informações sobre ameaças permite que organizações aprendam com outras experiências e melhorem suas defesas cibernéticas.

2. **DEFINIÇÕES**

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

a) ameaça: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

b) alta administração: representa o mais alto nível estratégico e decisório de um órgão ou entidade, seja ela parte da Administração Pública Federal Direta ou Indireta.

c) 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;

d) comitê de segurança da informação (CSI): grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal;

e) equipe de tratamento e resposta a incidentes cibernéticos (ETIR): grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade;

f) evento: qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação. Em outras palavras, qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao cliente;

g) evento de segurança: qualquer ocorrência identificada em um sistema, serviço ou rede, que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança;

h) incidente: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

i) incidente cibernético: ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema;

j) incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

k) informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

l) 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; e

m) usuário: pessoa física ou jurídica, seja servidor público, estudante ou prestador de serviços, voluntário habilitado pela administração para acessar os ativos de informação do IFTO.

3. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O processo de gestão de incidentes de segurança da informação consiste em um conjunto de práticas e procedimentos adotados pelas organizações para lidar com possíveis ataques ou violações que envolvem seus sistemas, redes e dados. O objetivo do processo é prevenir, detectar e responder a incidentes de segurança de forma rápida e eficiente, minimizando os danos e protegendo as informações da empresa. A figura 1 apresenta de forma resumida o processo de gestão de incidentes de segurança da informação utilizado pelo IFTO.

Figura 1 - Processo de Gestão de incidentes de segurança da informação

O processo de gestão de incidentes em segurança da informação apresentado na figura 1 refere-se ao processo de identificar, avaliar, responder e mitigar incidentes de segurança que possam afetar a confidencialidade, integridade e disponibilidade das informações em uma organização. As atividades incluem a criação de planos de contingência e recuperação para tratar incidentes de segurança, implementação de medidas preventivas para minimizar o risco de ocorrência de futuros incidentes, monitoramento contínuo de ameaças e vulnerabilidades, análise forense, comunicação com as partes

interessadas e treinamento dos colaboradores para reduzir riscos e garantir que os sistemas, dados e informações sejam protegidos contra ameaças internas e externas.

3.1. Processo de gestão de incidentes de segurança da informação

O processo de gestão de incidentes de segurança da informação é uma abordagem sistemática e estruturada para lidar com eventos de segurança que afetam a integridade, confidencialidade e disponibilidade das informações. Ele abrange atividades de registro de eventos, coleta e preservação de evidências de incidentes de segurança em redes computacionais, o qual inclui a identificação das causas e o tratamento de incidentes (BRASIL, 2014).

Esse processo envolve a identificação do incidente, avaliação de seu impacto, investigação das causas, contenção do incidente e recuperação das informações afetadas, além da implementação de medidas para evitar que o incidente se repita. Geralmente este processo é conduzido por uma equipe designada de profissionais de segurança da informação que são responsáveis por identificar e responder a incidentes de segurança em toda a organização. No IFTO esta equipe foi estabelecida através de portaria. Esta equipe trabalha para estabelecer políticas, processos, procedimentos, ferramentas e técnicas para garantir uma resposta rápida e eficaz aos incidentes envolvendo a segurança da informação.

Para que o processo seja eficiente é importante que o processo de gestão de incidentes seja parte integrante de uma política de segurança da informação, para que a organização possa atuar proativamente na prevenção e resposta a incidentes. A tabela 1 apresenta as 6 (seis) fases que compõem o processo de gestão de incidentes de segurança da informação.

Tabela 1 - Detalhamento do processo de gerenciamento de incidentes de segurança da Informação

Processo de gerenciamento incidentes de segurança da Informação	
Entrada	- Incidentes registrados na central de serviços (SUAP).
Fases	1. Identificação. 2. Análise. 3. Contenção, erradicação, recuperação e resolução. 4. Avaliação Pós Incidente. 5. Comunicação. 6. Documentação.
Saída	- Relatórios de incidentes de segurança da informação.

3.1.1. Identificação

Fase responsável pela identificação e o registro dos incidentes de segurança da informação. Todos os incidentes notificados ou detectados devem ser registrados, com a finalidade de assegurar registro histórico das atividades da ETIR (BRASIL, 2010).

Esta fase começa com a identificação de potenciais incidentes de segurança por meio de sistemas de detecção, alertas de segurança, monitoramento de redes, análise de *logs* e outras ferramentas. Nesta fase, qualquer atividade suspeita é detectada e avaliada. A central de serviços no SUAP é o canal para relato de incidentes.

Esta fase detecta o incidente, determina o escopo e as partes envolvidas com o incidente. Ela é responsável por identificar incidentes por meio de monitoração, relatórios, denúncias, informações obtidas de áreas parceiras ou qualquer outra análise de eventos adversos. Nesta fase são podem ser realizadas as seguintes atividades:

a) definir esquemas de classificação de incidentes de segurança da informação;

b) registrar, classificar e priorizar incidentes de segurança da informação de acordo com sua gravidade, impacto potencial e urgência, priorizando a resposta com base nesses critérios;

c) identificar todos os sistemas e serviços afetados relacionados com o incidente;

d) avaliar o impacto do incidente e os potenciais riscos dos sistemas afetados (dados vazados, informações de instituições parceiras, impacto na própria organização e impacto na reputação);

e) identificar a existência de outros eventos e alertas relacionados com o incidente em questão;

f) identificar que tipo de informação e processos podem ter sido afetados; e

g) identificar os responsáveis pelo sistema comprometido, equipes de suporte e donos das informações.

O incidente deve ser registrado, catalogado e documentado em base de conhecimento apropriada com detalhes sobre linha do tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações tomadas, inclusive as lições aprendidas. Nesta fase é realizada a triagem, classificação e priorização do incidente de acordo com o seu nível de criticidade.

3.1.2. Análise

Fase responsável por realizar análise detalhada do incidente de segurança da informação de forma a compreender a sua natureza, causas, extensão, métodos utilizados pelos invasores (se houver) e o impacto nos sistemas e dados. Nesta fase podem ser realizadas as seguintes atividades:

a) avaliar a relevância e o impacto do incidente, a fim de definir quais medidas devem ser tomadas em seguida;

b) coletar e analisar as informações disponíveis sobre o incidente, incluindo *logs* e outros registros gerados pelo sistema;

c) identificar o tipo de incidente, a categorização de acordo com sua gravidade e seu impacto no ambiente de segurança; e

d) investigar as possíveis causas, extensão e impacto do incidente, a fim de subsidiar as decisões e ações para sua contenção ou para o seu encaminhamento.

3.1.3. Contenção, erradicação, recuperação e resolução

Esta fase é responsável por conter o incidente de maneira a atenuar os danos e evitar que demais recursos sejam comprometidos. Após conter o incidente e investigá-lo são tomadas medidas para restaurar sistemas afetados, corrigir falhas de segurança, aplicar *patches* e implementar medidas para prevenir recorrências.

Esta fase deve limitar o impacto do incidente, isolando sistemas comprometidos, interrompendo atividades maliciosas ou bloqueando acessos não autorizados. Nesta fase podem ser realizadas as seguintes atividades:

a) iniciar a execução do plano de continuidade de serviços de TI;

b) desconectar o sistema comprometido ou isolar a rede afetada;

c) desativar o sistema para evitar maiores perdas quando há perda ou roubo de informações durante o ataque;

d) alterar políticas de roteamento dos equipamentos de rede ou bloquear padrões de tráfego, interrompendo o fluxo malicioso, desabilitar serviços vulneráveis, inibindo comprometimento de outros sistemas;

e) restaurar a integridade do sistema;

f) garantir que o sistema foi recuperado corretamente e que as funcionalidades estejam ativas;

g) implementar medidas de segurança para evitar novos comprometimentos;

h) restaurar o último e íntegro backup completo armazenado;

i) eliminar as causas do incidente, removendo todos os eventos relacionados de forma que o incidente não volte a ocorrer;

j) garantir que as causas do incidente foram removidas, assim como todas as atividades e arquivos associados ao incidente;

k) assegurar a remoção de todos os métodos de acesso utilizados pelo atacante: novas contas de acessos; *backdoors* e, se aplicável, acesso físico ao sistema comprometido, etc;

l) implementação de medidas adicionais de proteção da informação; e

m) executar ações para resolução de contorno ou de resolução do problema.

3.1.4. Avaliação Pós Incidente

Uma análise detalhada do incidente deve ser realizada para identificar lições aprendidas, pontos de melhoria nos processos e segurança e recomendações para prevenir futuros incidentes similares. Esta fase investiga as causas do incidente, a extensão do dano e o que foi comprometido.

Com base na análise pós-incidente são implementadas melhorias nos controles de segurança, treinamentos para a equipe, revisão de políticas e procedimentos para fortalecer a postura de segurança da informação. Nesta fase podem ser realizadas as seguintes atividades:

a) coletar informações, a análise dos dados e a identificação da causa raiz do incidente;

b) documentar todos os passos da investigação, desde a detecção do incidente até a resolução e ação corretiva;

c) garantir que as medidas de segurança apropriadas sejam implementadas e que riscos similares sejam prevenidos no futuro; e

d) seguir os procedimentos de gestão de incidentes de segurança da informação definidos pela organização.

3.1.5. Comunicação

Fase responsável por avaliar as ações realizadas para resolver o incidente, documentando detalhes, e discutir lições aprendidas. Após a conclusão do processo de coleta e preservação das evidências do incidente, a ETIR deverá elaborar relatório de comunicação de incidente de segurança em redes computacionais, descrevendo detalhadamente os eventos verificados (BRASIL, 2014).

Dependendo da natureza do incidente e das regulamentações vigentes, pode ser necessário notificar autoridades, parceiros de negócios ou indivíduos afetados, além de relatar o incidente para registro e análise futura. Nesta fase deve ser elaborado o relatório de comunicação de incidente de segurança da informação, contendo minimamente as seguintes informações:

a) nome do responsável pela preservação dos dados do incidente, com informações de contato;

b) nome do agente responsável pela ETIR, e informações de contato;

c) órgão comunicante com sua localização e informações de contato;

d) número de controle da ocorrência;

e) relato sobre o incidente, descrevendo como ocorreu o fato, como foi detectado, os dados coletados e preservados, bem como outros dados considerados relevantes; e

f) descrição das atividades de tratamento e resposta ao incidente, bem como outras providências tomadas pela ETIR incluindo as ações de preservação, registrando-se a metodologia, caso aplicada, as ferramentas utilizadas e o local de armazenamento das informações preservadas.

3.1.5. Documentação

Nesta fase é feito o encerramento formal e análise para identificação de possíveis melhorias em processos, controles e na gestão de incidentes de segurança da informação. Deve ser verificada a existência de providências ou determinações pendentes e providenciar sua execução. Em seguida, o incidente de segurança da informação é considerado encerrado. Nesta fase podem ser realizadas as seguintes atividades:

a) caracterizar o conjunto de lições aprendidas de modo a aprimorar os procedimentos e processos existentes;

b) prover estatísticas e métricas relativas ao processo de resposta a incidentes;

c) obter informações que podem ser utilizadas em processos legais;

d) confirmar o restabelecimento da normalidade dos recursos computacionais;

e) registrar lições aprendidas e *feedback* com usuário; e

f) atualizar políticas e procedimentos.

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 incidentes de segurança da informação 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 Direta ou Indireta. Cabe ao representante deste nível as seguintes responsabilidades:

a) prover a orientação e o apoio necessário às ações de gestão de incidentes de segurança da informação, de acordo com os objetivos estratégicos, planos institucionais e com as leis e regulamentos pertinentes à Administração Pública Federal; e

b) disponibilizar os recursos (humanos, tecnológicos e financeiros) necessários para a execução das ações relacionadas à gestão de incidentes de segurança da informação no âmbito do IFTO.

4.2. Comitê de Segurança da Informação

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

a) avaliar e aprovar diretrizes e responsabilidades para a gestão de incidentes de segurança da informação; e

b) propor melhorias para a gestão de incidentes de segurança da informação.

4.3. Gestor de Segurança da Informação

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

a) propor diretrizes e responsabilidades para a gestão de incidentes de segurança da informação;

b) coordenar o processo de gestão de incidentes de segurança da informação; e

b) designar um agente responsável pela gestão de incidentes de segurança da informação, dentre os servidores efetivos do IFTO.

4.4. 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) definir procedimentos e controles sobre gestão de incidentes de segurança da informação; e

b) assessorar o Comitê de Segurança da Informação e a DTI na análise e tomada de decisões a respeito de situações resultantes de incidentes de segurança da informação.

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

Agente responsável pela gestão de incidentes de segurança da informação. Cabe a este setor as seguintes responsabilidades:

a) monitorar o ambiente e recursos de TI a fim de identificar possíveis incidentes de segurança da informação;

b) realizar a investigação do incidente de segurança da informação, propondo medidas de contenção;

c) realizar a análise do incidente de segurança da informação, de forma a propor medidas para eliminar ou solucionar problemas que causaram o incidente; e

d) realizar a comunicação com o CTIR.BR.

4.6. Usuários

Pessoas que utilizam os dados e informações processados pelo IFTO. Cabe aos usuários as seguintes responsabilidades:

a) utilizar os dados e informações no IFTO prioritariamente para a realização das atividades desempenhadas nos limites da ética, razoabilidade e legalidade;

b) notificar incidentes de segurança da informação; e

c) evitar na medida do possível se envolver em incidentes de segurança da informação.

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;

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
Identificação	A	C	I	C	R	I
Análise	A	C	C/I	R	C	I
Contenção, Erradicação, Recuperação e Resolução	A	C	C	C	R	I
Avaliação Pós Incidente	A	C	C	R	C	I
Comunicação	A	C	C	C/I	R	I
Documentação	A	C	C	C/I	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 setores de TI das unidades do IFTO).

6. INDICADOR DE DESEMPENHO

O processo de gerenciamento de incidentes de segurança da informação 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	Incidentes de segurança da informação resolvidos durante o ano.
Descrição	Número de incidentes de segurança da informação solucionados durante o ano.
Objetivo	Medir o percentual de incidentes de segurança da informação solucionados durante o ano.
Periodicidade	Anual
Fonte	Sistema de Gestão de Incidentes de Segurança da Informação.
Fórmula	Total de incidentes de segurança da informação resolvidos durante o ano.
Meta	Monitorar a quantidade de incidentes de segurança da informação solucionados a cada ano.

7. PROCESSOS RELACIONADOS

Para que a abordagem de segurança da informação seja efetiva, o gerenciamento de incidentes de segurança da informação está interligado à outros processos

que compõem o Sistema de Gestão de Segurança da Informação (SGSI-IFTO). A figura 2 apresenta estes processos.

Figura 2 - Processos que compõem o SGSI-IFTO

8. PRÁTICAS RECOMENDADAS

As práticas recomendadas para o processo de gestão de incidentes de segurança da informação incluem:

1. **Identificação**: implementar sistemas e ferramentas de monitoramento de segurança é essencial para identificar rapidamente os incidentes de segurança e minimizar o tempo de resposta.

2. **Análise:** a equipe de gestão de incidentes deve coletar informações sobre o incidente, analisá-las e determinar sua gravidade, impacto e causa raiz.

3. **Contenção, Erradicação, Recuperação e Resolução:** a equipe deve agir rapidamente para conter o incidente, interrompendo sua propagação e minimizando os danos. É importante restaurar os sistemas afetados e retorná-los ao funcionamento normal o mais breve possível.

4. **Avaliação Pós Incidente:** uma investigação completa do incidente deve ser realizada para determinar a origem e a extensão do evento.

5. **Comunicação:** a equipe deve comunicar as partes interessadas sobre o incidente ocorrido.

6. **Documentação:** a equipe deve revisar os incidentes após a resolução para identificar padrões e tendências e documentar essas informações para melhorar o processo de gestão de incidentes de segurança da informação.

7. **Plano de Resposta a Incidentes (PRI):** desenvolver um PRI detalhado que inclua procedimentos claros e estruturados para lidar com diferentes tipos de incidentes. Esse plano

deve ser revisado e testado regularmente.

8. **Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR):** formar uma equipe dedicada ou designe responsabilidades específicas para responder a incidentes de segurança. Defina papéis e responsabilidades com antecedência.

9. **Identificação e Classificação de Incidentes:** estabelecer critérios claros para identificar, classificar e priorizar incidentes. Isso ajuda a responder de forma adequada, dando atenção aos incidentes mais críticos primeiro.

10. **Coleta de Evidências:** implementar processos para coletar e preservar evidências de incidentes de segurança. Isso é fundamental para investigações forenses e análises pós-incidentes.

11. **Notificação e Comunicação:** definir procedimentos para notificar as partes interessadas internas e externas sobre incidentes de segurança, incluindo a comunicação com clientes, autoridades regulatórias e parceiros.

12. **Isolamento e Mitigação:** implementar medidas para isolar o incidente, minimizando seu impacto. Isso pode incluir a desconexão de sistemas afetados ou a interrupção de serviços comprometidos.

13. **Análise e Investigação:** realizar uma análise detalhada para entender a origem e a natureza do incidente. Isso envolve investigação forense para determinar a extensão do dano e como o incidente ocorreu.

14. **Recuperação e Restauração:** executar procedimentos para restaurar os sistemas afetados para um estado seguro e funcional. Isso pode incluir a restauração a partir de backups ou aplicação de *patches* de segurança.

15. **Análise Pós-Incidente:** realizar uma análise pós-incidente para identificar lições aprendidas e melhorias no PRI. Isso ajuda a fortalecer a postura de segurança e a prevenir futuros incidentes.

16. **Treinamento e Simulações:** realizar exercícios de simulação e treinamentos regulares para a equipe de resposta a incidentes. Isso garante que todos estejam preparados e familiarizados com os procedimentos de resposta.

9. REFERÊNCIAS

Brasil. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Norma Complementar Nº 8, de 19 de agosto de 2010: Gestão de ETIR: diretrizes para 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: 5 dez. 2023.

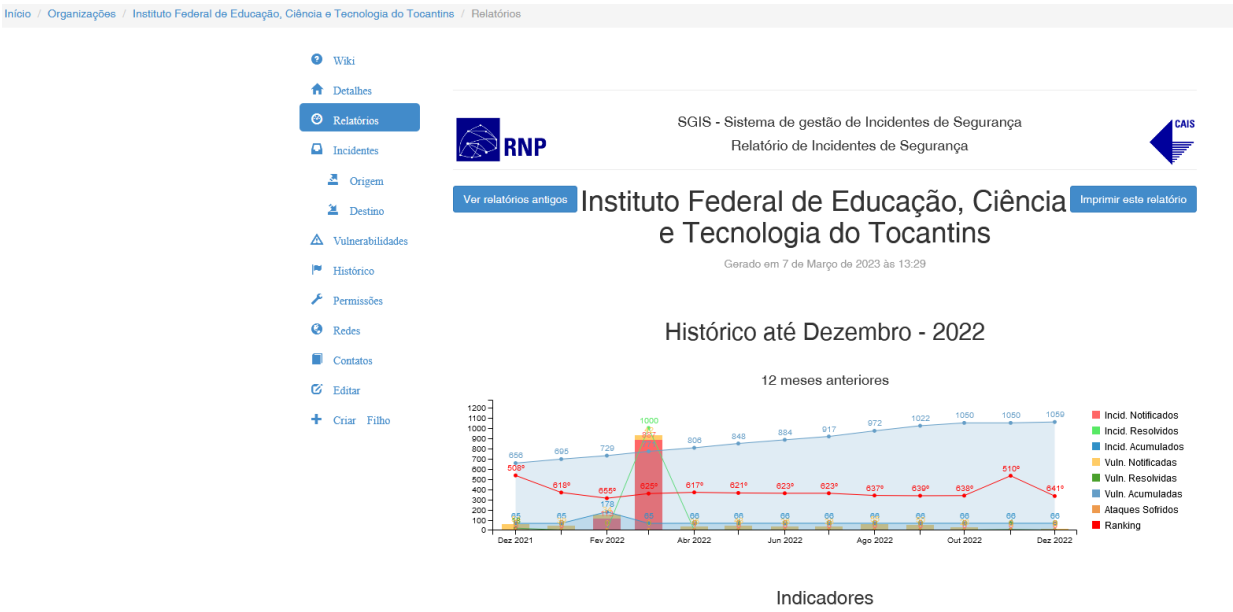
Brasil. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Norma Complementar Nº 21, de 8 de outubro de 2014. Diretrizes para registro de eventos, coleta e preservação de evidências de incidentes de segurança em redes.** Disponível em: https://datasus.saude.gov.br/wp-content/uploads/2019/08/Norma-Complementar-n%C2%BA-21IN01DSICGSIPR.pdf. Acesso em: 7 de dezembro de 2023.

ISACA. **COBIT 2019.** Disponível em: https://www.isaca.org/ Acesso em: 6 dez. 2023.

UNIVERSIDADE FEDERAL DE LAVRAS. **Plano de Gestão de Incidentes de Segurança da Informação e Privacidade.** UFLA, 2021. Disponível em: https://dgti.ufla.br/images/politicas-e-normas/Plano_Gestao_Incidentes_v12_assinado.pdf Acesso em: 21 dez. 2021.

ANEXO I

MONITORAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO



ANEXO II
PLANO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O Plano de Gestão de Incidentes da Segurança da Informação e estabelece princípios, conceitos, diretrizes e responsabilidades sobre a gestão de incidentes de segurança da informação no IFTO, orientando o funcionamento do processo, de forma que este seja tratado adequadamente, reduzindo ao máximo os impactos para o negócio.

Este plano abrange todos os recursos computacionais pertencentes, operados, mantidos e controlados pelo IFTO. A tabela 1 apresenta as atividades e tarefas que compõem o plano de ação de gestão de incidentes de segurança da informação.

Tabela 1 - Ações para resposta e tratamento de incidentes de segurança da informação

Fase	Atividade	Responsável
Identificação	Estabelecer sistemas e ferramentas de detecção de incidentes, como sistemas de detecção de intrusões (IDS) e sistemas de prevenção de intrusões (IPS).	CRSI
	Monitorar constantemente as atividades de rede e sistema em busca de indicadores de comprometimento (IOCs) e comportamentos suspeitos.	CRSI
Análise	Desenvolver critérios para classificar e priorizar os incidentes com base em sua gravidade, impacto e probabilidade.	CRSI

	Alocar recursos de forma eficiente para os incidentes mais críticos.	DTI
	Realizar uma análise detalhada do incidente para entender como ocorreu e quais sistemas foram afetados.	CRSI
	Determinar a extensão do comprometimento e identifique a origem do incidente.	CRSI
Contenção, Erradicação, Recuperação e Resolução	Isolar sistemas ou redes afetados para evitar a propagação do incidente.	CRSI
	Preservar e coletar evidências relevantes para a investigação posterior.	CRSI
	Desenvolver e implementar medidas para mitigar o impacto do incidente e restaurar a operação normal.	CRSI
Avaliação Pós Incidente	Certificar-se de que as vulnerabilidades exploradas foram corrigidas e de que as medidas de segurança foram reforçadas.	CRSI
	Após a resolução do incidente, realizar uma análise pós-incidente para identificar o que funcionou bem e o que pode ser melhorado no processo de resposta.	CRSI
Comunicação	Estabelecer um plano de comunicação interna e externa para manter as partes interessadas informadas sobre o incidente.	DTI
	Comunicar-se com as autoridades competentes, se necessário, dependendo da natureza do incidente.	DTI
	Treinar regularmente a equipe de resposta a incidentes e outros funcionários em como identificar e lidar com incidentes.	GSI
	Realizar simulações de incidentes para testar a eficácia do plano de resposta e identificar lacunas.	CRSI
Documentação	Manter registros detalhados de todos os incidentes, ações tomadas e resultados da investigação.	CRSI
	Documentar as lições aprendidas para atualizar o plano de resposta a incidentes e fortalecer a postura de segurança.	CRSI

ANEXO III
NOTIFICAÇÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1. Incidentes envolvendo recursos, sistemas operacionais, *softwares*, sistemas de informação e serviços de TI

Equipe de Tratamento e Resposta a Incidentes Cibernéticos
Telefone: (63) 2229-2200
E-mail: etir@ifto.edu.br
Endereço:
Prédio da Reitoria
Avenida Joaquim Teotônio Segurado

Palmas-Tocantins

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 05/01/2024, às 19:48, 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 **2218356** e o código CRC **16273FDF**.

Avenida Joaquim Teotônio Segurado, Quadra 202 Sul, ACSU-SE 20, Conjunto 1, Lote 8 - Plano Diretor Sul — CEP 77020-450 Palmas/TO — (63) 3229-2200
portal.ifto.edu.br — reitoria@ifto.edu.br

Referência: Processo nº 23235.015911/2021-16 SEI nº 2218356