Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Centro Federal de Educação Tecnológica Celso Suckow da Fonseca
Diretoria de Gestão Estratégica

PLANO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO (PGISI)

1. Introdução

Incidentes de segurança da informação são eventos adversos que comprometem a confidencialidade, a integridade ou a disponibilidade de informações institucionais. No contexto do CEFET/RJ, tais eventos podem ter impacto significativo sobre os serviços prestados à sociedade e o cumprimento da legislação vigente, em especial a Lei Geral de Proteção de Dados Pessoais (LGPD).

Este plano tem como objetivo estabelecer um processo estruturado para a identificação, resposta, comunicação e ações de aprendizado de incidentes de segurança da informação e privacidade, garantindo a continuidade das atividades institucionais e o atendimento às normas legais.

A execução das diretrizes e procedimentos estabelecidos neste plano é operacionalizada por meio do **Plano de Ação para Implantação da Segurança Cibernética e Resposta a Incidentes** do CEFET/RJ, que detalha ações, responsáveis, prazos e indicadores para sua implementação, acompanhamento e aprimoramento contínuo.

1.1 Objetivos

Geral: Assegurar que os incidentes de segurança da informação sejam comunicados, analisados, tratados e resolvidos com eficiência, minimizando danos institucionais e riscos aos titulares de dados.

Específicos:

A) Detectar e responder a incidentes de forma tempestiva e coordenada, assegurando a notificação adequada aos envolvidos e órgãos competentes, em conformidade com a legislação vigente;
B) Proteger os ativos de informação e preservar evidências, garantindo a integridade dos dados e o suporte às ações legais e disciplinares, conforme requisitos da LGPD e demais normativos;
C) Cumprir requisitos legais e regulatórios, com ênfase na Lei Geral de Proteção de Dados Pessoais (LGPD), assegurando a conformidade nas ações de prevenção, resposta e comunicação de incidentes;

D) Realizar análise de causa raiz dos incidentes e implementar ações para prevenir reincidências, promovendo o aprendizado organizacional e a evolução das práticas de segurança;
E) Aprimorar continuamente os controles de segurança da informação, com base nas lições aprendidas, nas tendências de ameaças e boas práticas do setor;
F) Assegurar a recuperação e restauração dos ativos afetados, de modo a restabelecer os serviços críticos com o menor impacto possível, respeitando os planos de continuidade e recuperação;
G) Promover a notificação, a conformidade e a melhoria contínua, integrando as etapas de resposta, aprendizado e adaptação dos controles, com foco na resiliência organizacional.

1.2 Abrangência

Este plano aplica-se a todos os incidentes que envolvam ativos de informação sob responsabilidade do CEFET/RJ, incluindo equipamentos, redes, sistemas e dados, bem como incidentes que envolvam dados pessoais tratados pela instituição.

2. Definições

Ativo de informação: Qualquer recurso que contenha ou processe informação, como documentos, sistemas, equipamentos, redes, pessoas ou instalações.

Alta Administração: Representa o mais alto nível estratégico e decisório da organização.

Ataque: Evento de exploração de vulnerabilidades com o objetivo de obter acesso indevido, causar indisponibilidade ou danificar sistemas e dados.

Confidencialidade: Garantia de que a informação esteja acessível apenas a pessoas autorizadas.

Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (LGPD, Art. 5º, VI).

Dados pessoais: Informação relacionada a pessoa natural identificada ou identificável (LGPD, Art. 5º, I).

Dados pessoais sensíveis: Dado pessoal sobre origem racial, convicção religiosa, opinião política, saúde, vida sexual, dado genético ou biométrico (LGPD, Art. 5º, II).

Disponibilidade: Garantia de que os usuários autorizados tenham acesso à informação e aos ativos correspondentes sempre que necessário.

DPO (Data Protection Officer) / Encarregado: Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

Evento de segurança: Qualquer ocorrência identificada em um sistema, serviço ou rede que possa indicar uma falha de segurança.

Incidente de segurança da informação: Ocorrência confirmada ou suspeita de comprometer a confidencialidade, a integridade ou a disponibilidade da informação.

Incidente cibernético: Evento adverso relacionado à infraestrutura tecnológica (redes, sistemas e dispositivos) que possa comprometer a confidencialidade, a integridade ou a disponibilidade dos ativos digitais da organização.

Integridade: Garantia de que a informação está completa e não foi modificada indevidamente.

LGPD: Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018.

Operador: Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador (LGPD, Art. 5º, VII).

Política de Segurança da Informação (PSI): Documento que estabelece diretrizes, responsabilidades e práticas para proteger os ativos de informação da instituição.

Privacidade: Direito fundamental à proteção dos dados pessoais e à inviolabilidade da intimidade e da vida privada.

Responsável pelo sistema/processo: Pessoa designada como gestora de um sistema de informação ou processo institucional, com autoridade sobre ações de resposta em incidentes.

Tratamento de dados pessoais: Toda operação realizada com dados pessoais, como coleta, armazenamento, uso, transmissão, exclusão, entre outros (LGPD, Art. 5º, X).

Vazamento de dados: Divulgação, acesso ou transmissão não autorizada de dados pessoais ou corporativos, seja por falha técnica, erro humano ou ataque externo.

3. Fases do Processo de Gestão de Incidentes

O processo de gestão de incidentes é composto por etapas sequenciais que visam garantir a resposta eficaz, o aprendizado organizacional e a melhoria contínua da segurança da informação. As fases são:

3.1 Identificação

Detecção e registro de eventos que indiquem a ocorrência de um incidente de segurança da informação, por meio do sistema de chamados institucional, do Sistema de Gestão de Incidentes de Segurança (SGIS/CAIS), do SOC da RNP, de ferramentas de

monitoramento, da comunicação com usuários e da análise de eventos anômalos provenientes de áreas parceiras.

Essa etapa envolve a triagem, classificação e definição de prioridade dos incidentes de segurança da informação.

Inicialmente, são recebidas e analisadas as notificações ou alertas que indicam a ocorrência de um possível incidente.
Em seguida, o incidente é classificado conforme seu tipo, como por exemplo: ataque por malware, tentativa de acesso não autorizado ou indisponibilidade de serviços. Com base nessa classificação, realiza-se a avaliação da gravidade do incidente, considerando o impacto potencial, os riscos envolvidos e o nível de urgência para tratá-lo. Isso permite estabelecer uma ordem de resposta adequada, priorizando os casos mais críticos.

Durante essa fase, também são definidas categorias para padronizar o registro dos incidentes; são identificados os sistemas e serviços impactados; é feita a análise do impacto sobre dados sensíveis, processos internos e parceiros externos; além da verificação de alertas relacionados, da identificação das informações comprometidas e dos responsáveis pelos sistemas afetados, incluindo equipes técnicas e gestores das informações.

As atividades a seguir podem ser conduzidas nesta fase, de acordo com a situação identificada:

Estabelecer categorias para os tipos de incidentes:

A) Criar uma estrutura para organizar os incidentes em grupos, como, por exemplo: ataques de malware, tentativas de phishing, vazamento de dados, ataques de negação de serviço, entre outros.
B) Registrar o incidente, classificá-lo e definir a prioridade:
    a. Anotar todas as informações do incidente em um sistema de controle.
    b. Avaliar o nível de severidade, o impacto potencial e a urgência do caso.
    c. Organizar a ordem de atendimento com base nesses critérios.
C) Mapear quais sistemas e serviços estão sendo afetados:
    a. Identificar os sistemas, aplicações e serviços envolvidos ou comprometidos.
D) Analisar os impactos e riscos associados:
    a. Verificar quais danos o incidente pode causar, incluindo vazamento de informações confidenciais, efeitos sobre os parceiros, prejuízos à instituição e possíveis danos à imagem.
E) Checar se há outros eventos ou alertas relacionados:

   a. Investigar se há outros sinais ou avisos que possam estar relacionados ao incidente, para entender melhor o contexto.

F) Determinar quais dados e processos podem estar comprometidos:
   a. Identificar quais informações e quais atividades operacionais podem ter sido afetadas pelo incidente.

G) Reconhecer os responsáveis e as equipes envolvidas:
   a. Apontar os responsáveis pelos sistemas afetados, as equipes de suporte técnico e os titulares das informações afetadas.

3.2 Análise

Verificação e categorização do incidente, com a avaliação de seu impacto, escopo e criticidade, bem como a identificação dos sistemas, ativos e dados afetados.
As atividades a seguir podem ser conduzidas nesta fase, de acordo com a situação identificada:

A) Avaliar a importância e os impactos do incidente para determinar sua gravidade e definir quais ações devem ser adotadas em seguida.
B) Coletar e examinar as informações disponíveis, como registros de log, alertas de segurança, dados de monitoramento e outros elementos que possam fornecer pistas sobre o ocorrido.
C) Determinar o tipo de incidente e classificá-lo conforme seu nível de severidade e os efeitos no ambiente de segurança da informação.
D) Investigar as possíveis causas, o alcance e impactos do incidente, buscando entender como ele ocorreu, quais sistemas foram afetados e quais são os riscos decorrentes, a fim de subsidiar as decisões para conter e tratar o problema adequadamente.

3.3 Contenção, Erradicação e Repercussão

Adoção de medidas para conter o incidente, eliminar sua causa, restaurar os serviços afetados e evitar recorrências.

As atividades a seguir podem ser conduzidas na fase de **Contenção**:

A) Executar ações imediatas para isolar o incidente, evitando que se espalhe para outros sistemas, serviços ou redes.
B) Implementar medidas temporárias de controle, como o bloqueio de acesso, a quarentena de dispositivos afetados ou a desativação de contas comprometidas.

C) Garantir que a contenção não afete serviços essenciais, buscando equilibrar a resposta ao incidente com a continuidade das operações críticas da instituição.
D) Documentar todas as medidas aplicadas, registrando quem as executou, quando e quais foram os resultados, para rastreabilidade e auditoria.

As atividades a seguir podem ser conduzidas na fase de **Erradicação**:

A) Remover as causas do incidente, eliminando arquivos maliciosos, corrigindo vulnerabilidades, desinstalando softwares comprometidos ou atualizando os sistemas.
B) Verificar se não há resquícios do incidente, realizando varreduras completas nos sistemas e redes para garantir que o ambiente esteja limpo.
C) Aplicar correções e reforçar a segurança, como a atualização de patches, a reconfiguração de permissões e a mudança de senhas, para evitar que o incidente se repita.
D) Confirmar com evidências técnicas que a ameaça foi completamente eliminada, antes de seguir para a recuperação.

As atividades a seguir podem ser conduzidas na fase de **Recuperação**:

A) Restabelecer os serviços e sistemas afetados, garantindo que voltem a operar com segurança e estabilidade.
B) Monitorar os ativos restaurados, por meio de ferramentas de segurança, para detectar qualquer sinal de recorrência do incidente.
C) Validar a integridade e funcionalidade dos sistemas, testando se os dados, aplicações e serviços estão íntegros e operacionais após a restauração.
D) Comunicar a normalização aos responsáveis e usuários afetados, de forma clara e transparente, informando que os ambientes foram recuperados com segurança.

3.4 Lições Aprendidas

Revisão do incidente para identificar lições aprendidas, falhas nos controles e oportunidades de melhoria.

As atividades a seguir podem ser conduzidas nesta fase, de acordo com a situação identificada:

A) Revisar todo o processo de resposta ao incidente, identificando o que funcionou bem e o que pode ser melhorado.

B) Analisar as causas raiz do incidente, para entender como ele ocorreu e evitar que aconteça novamente.
C) Avaliar os impactos reais causados pelo incidente, incluindo aspectos técnicos, operacionais, financeiros e reputacionais.
D) Documentar lições aprendidas e atualizar políticas, procedimentos e planos de resposta com base nos conhecimentos adquiridos.
E) Compartilhar os resultados com as equipes envolvidas e a alta gestão, promovendo o aprendizado organizacional.
F) Planejar e implementar melhorias contínuas, fortalecendo a postura de segurança da instituição.

3.5 Comunicação

Elaboração de comunicados oficiais, conforme as diretrizes institucionais, para informar, quando necessário, órgãos reguladores, parceiros e, em casos críticos, o público externo. Caso seja constatado risco ou dano relevante aos titulares de dados pessoais, o Encarregado de Proteção de Dados (DPO) deverá proceder às comunicações obrigatórias previstas na legislação vigente, incluindo a notificação aos titulares dos dados e à Autoridade Nacional de Proteção de Dados (ANPD), observadas as diretrizes institucionais de comunicação.

3.6 Documentação

Registro detalhado de todas as etapas do incidente, decisões tomadas e ações realizadas, visando ao histórico, à auditoria e à melhoria contínua.

As atividades a seguir podem ser conduzidas nesta fase, de acordo com a situação identificada:

A) Registrar detalhadamente todas as informações relacionadas ao incidente, incluindo data, hora, meio de detecção, sistemas afetados e descrição dos eventos.
B) Documentar as ações realizadas em cada etapa do tratamento do incidente, identificando os responsáveis, as decisões tomadas e os prazos cumpridos.
C) Armazenar evidências técnicas, como logs, prints de tela, backups e relatórios gerados durante a investigação e resposta.
D) Assegurar a proteção e confidencialidade dos registros, controlando o acesso e prevenindo alterações indevidas.
E) Registrar as lições aprendidas, revisar e atualizar as políticas e procedimentos com base nas experiências adquiridas durante o atendimento ao incidente.

4. Papéis e Responsabilidades

4.1 Alta administração

Refere-se à instância máxima de direção e tomada de decisões dentro do órgão ou entidade. Garantir apoio estratégico e disponibilização de recursos necessários para a gestão de incidentes de segurança da informação.

4.2 Comitê Gestão e Segurança da Informação (CSI)

Grupo formado por representantes das áreas finalísticas do CEFET/RJ, responsável por apoiar as diretrizes e decisões estratégicas relacionadas à segurança da informação. Avaliar e aprovar diretrizes, bem como propor melhorias para a gestão de incidentes.

4.3 Gestor de Segurança da Informação

Servidor formalmente designado para planejar, coordenar e supervisionar as ações relacionadas à gestão da segurança da informação no âmbito institucional. Propor diretrizes, coordenar o processo e designar responsável pela gestão de incidentes.

4.4 Equipe de prevenção, tratamento e resposta a incidentes cibernéticos (ETIR)

Grupo formado por servidores públicos efetivos com capacitação técnica compatível, responsável por atuar na identificação, análise, contenção, erradicação, recuperação e resposta a incidentes de segurança da informação. Definir procedimentos e controles, executar e documentar o processo de gestão de incidentes, além de assessorar o comitê e a diretoria de TI nas decisões.

4.5 Departamento de TI (DTINF)

Departamento de Tecnologia da Informação, em conjunto com os demais setores de TI, atua como principal responsável pela gestão da infraestrutura tecnológica e pelo apoio técnico na prevenção, detecção e tratamento de incidentes de segurança da informação no âmbito institucional. Monitorar o ambiente de TI, investigar e analisar incidentes, apoiar na contenção e correção, e manter comunicação, quando aplicável, com o CTIR.BR e demais entidades de coordenação de incidentes.

4.6 Encarregado de Proteção de Dados (DPO)

Pessoa indicada institucionalmente para atuar como canal de comunicação entre o CEFET/RJ, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD), com responsabilidades relacionadas à proteção de dados pessoais e à conformidade com a LGPD. Avaliar comunicação de incidentes com dados pessoais, atuar como canal de comunicação com os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

4.7 Usuários

Todos que utilizam os recursos tecnológicos da instituição e que devem zelar pelo uso responsável das informações, além de comunicar prontamente quaisquer suspeitas de incidentes. Utilizar informações com responsabilidade, notificar incidentes e adotar condutas que evitem incidentes.

5. Matriz de Responsabilidades

Define e esclarece os papéis e responsabilidades de cada membro nas atividades do plano. Também conhecida como matriz RACI.

O acrônimo RACI significa:

A) Responsável/Executor (Responsible): Responsável pela execução da atividade. Pode haver mais de um.
B) Aprovador/Responsabilizado (Accountable): Detém a autoridade sobre determinada atividade e que, portanto, é a principal responsável por seu êxito. Compete a essa pessoa assegurar a alocação adequada de recursos e condições necessárias para a execução da atividade. Será igualmente responsabilizada caso os objetivos não sejam alcançados. Cada atividade deve possuir exatamente um responsável principal, incumbido de verificar se a execução foi realizada de forma satisfatória e dentro do prazo estipulado.
C) Consultado (Consulted) - Pessoa que pode ser consultado antes ou durante a execução. Tem conhecimento ou autoridade técnica.
D) Informado (Informed) - Pessoa que será informada sobre o andamento ou resultado da atividade.

FASES	AA	CSI	GSI	ETIR	DTINF	DPO	USUARIO
Identificação	A	C	I	R	R	I	I
Análise	A	C	C	R	C	I	I
Contenção, Erradicação e Recuperação	A	C	C	R	R	I	I
Lições aprendidas	A	C	C/R	R	C	I	I
Comunicação	A	C	C	C/R	R	C	I
Documentação	A	C	C	R	C	I	I

Tabela 1 – Matriz RACI

Legenda:

AA: Alta Administração
CSI: Comitê de Segurança da Informação
GSI: Gestor de Segurança da Informação
ETIR: Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos
DTINF: Departamento de Tecnologia da Informação e os demais setores de TI
DPO: Encarregado de Proteção de Dados

6. Métrica de Avaliação de Eficiência

O processo de gestão de incidentes de segurança da informação deve ser acompanhado e analisado periodicamente por meio de uma métrica que permita aferir sua eficiência. Essa prática visa identificar a necessidade de ajustes no processo, de forma a garantir sua efetividade.

- **Nome da Métrica:** Quantidade anual de incidentes de segurança da informação tratados e encerrados.
- **Descrição:** Quantitativo de incidentes que foram devidamente tratados e encerrados no período anual.
- **Finalidade:** Mensurar o percentual de incidentes solucionados, possibilitando a análise do desempenho da gestão de incidentes.
- **Frequência de Verificação:** Anual
- **Origem dos Dados:** Sistema de chamados institucional, Sistema de Gestão de Incidentes de Segurança SGIS/CAIS da RNP, SOC intermediário RNP, plataformas Microsoft, e outros sistemas de apoio.
- **Método de Cálculo:** Contagem total de incidentes resolvidos dentro do ano de referência.
- **Meta Esperada:** Acompanhar o volume anual de incidentes solucionados, fornecendo subsídios para decisões estratégicas e aprimoramento contínuo do processo.

A imagem abaixo apresenta os incidentes de segurança da informação registrados no Sistema de Gestão de Incidentes de Segurança (SGIS/CAIS) ao longo do ano, permitindo acompanhar sua evolução e distribuição no período. Esses dados funcionam como métrica para avaliar a eficiência do processo de gestão de incidentes, possibilitando identificar padrões, pontos de atenção e a necessidade de ajustes para garantir a efetividade das ações de segurança da informação.

Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Centro Federal de Educação Tecnológica Celso Suckow da Fonseca
Diretoria de Gestão Estratégica

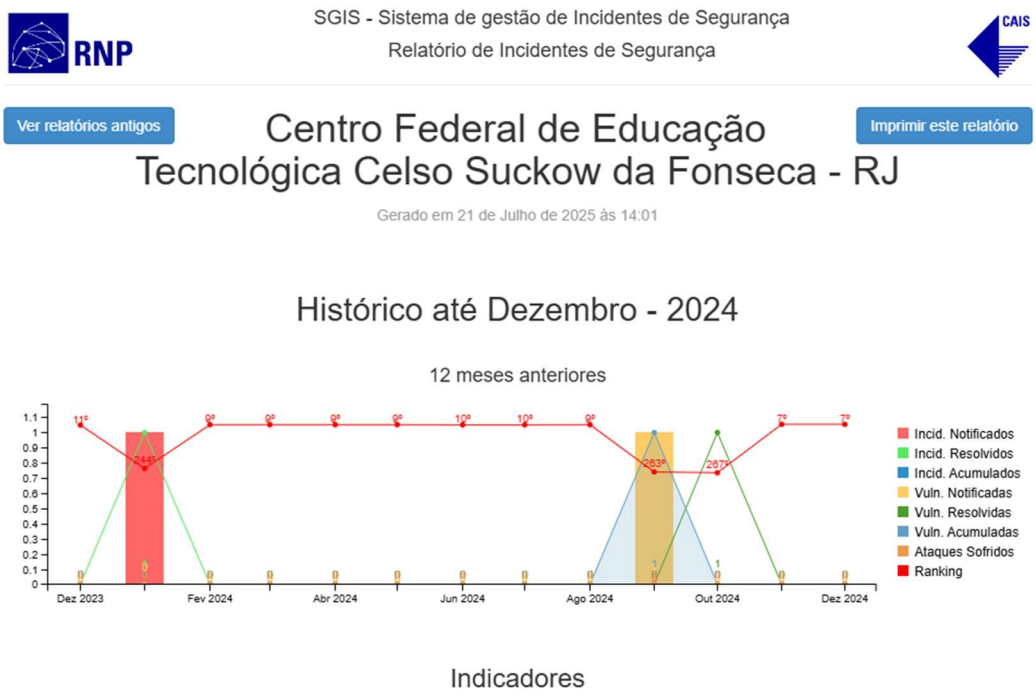

Figura 1 - Relatório de Incidentes de Segurança da Informação registrados no SGIS/CAIS (RNP)

7. Práticas Recomendadas

A) Adoção de tecnologias e recursos de monitoramento de segurança para garantir a identificação imediata de incidentes e agilizar a atuação corretiva;
B) Manutenção e aprimoramento contínuo do Plano de Gestão de Incidentes de Segurança da Informação (PGISI) e de seus instrumentos operacionais;
C) Realização de simulações anuais de incidentes;
D) Coleta e preservação de evidências digitais;
E) Treinamentos periódicos das equipes;
F) Atualização anual do plano;

8. Referências

GABINETE DE SEGURANÇA INSTITUCIONAL GSI/PR. Plano de Gestão de Incidentes Cibernéticos (PlanGIC). Disponível em: < https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/plano-de-gestao-de-incidentes-ciberneticos-plangic/plangic.pdf >

INSTITUTO FEDERAL DO TOCANTINS. Gestão de Incidentes de Segurança da Informação. Disponível em: < https://www.ifto.edu.br/acesso-a-informacao/seguranca-da-informacao/documentos-lgpd-ifto/PGISI.pdf >.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentosexternos/anpd_guia_agentes_de_tratamento.pdf >.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Glossário de Segurança da Informação, de 26 de novembro de 2021. Disponível em: < https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1 >.

BRASIL. Governo Digital. Ministério da Economia. Segurança e Proteção de Dados, Guia de Resposta a Incidentes de Segurança, de dezembro de 2021. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_resposta_incidentes.pdf >.

GOVERNO DO ESTADO DE RONDÔNIA. Secretaria De Finanças Do Estado De Rondônia. PRISIP – Plano de Resposta a Incidentes de Segurança da Informação e Privacidade. Disponível em: < https://www.sefin.ro.gov.br/portalsefin/userfiles/PRISIP.pdf >.
UNIVERSIDADE FEDERAL DE LAVRAS. Plano de Gestão de Incidentes de Segurança da Informação e Privacidade. Disponível em: < https://dgti.ufla.br/images/politicas-e-normas/Plano_Gestao_Incidentes_v12_assinado.pdf >.

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO. Plano de Gestão de Incidentes de Segurança da Informação. Disponível em: < https://seguranca.tic.ufrj.br/documentos/plano-de-gestao-de-incidentes-de-seguranca-da-informacao/ >.

HISTÓRICO DE VERSÕES

Data	Versão	Descrição das alterações
01/04/2026	**1.0**	**Aprovação do Plano no CSI**