# Plano de Resposta a Incidentes de Segurança

Este documento tem como objetivo preparar a Instituição para lidar com a ocorrência de um incidente de segurança garantindo que responda de forma mais rápida, organizada e eficiente ao evento, minimizando suas consequências para todos os envolvidos. Antes de mais nada, é necessário definir o que é um incidente. De maneira geral, um incidente é uma situação inesperada, capaz de alterar a ordem normal das coisas e, no caso da proteção de dados, colocar em risco dados pessoais dos indivíduos que se relacionam com nossa Instituição. De acordo com o **Artigo 50 da Lei Geral de Proteção de Dados (LGPD)**, parágrafo 2º, inciso I, o controlador de dados poderá implementar um programa de governança em privacidade que conte, entre outras medidas e políticas, com um plano de resposta a incidentes e remediação.

Baseado no exposto, a Univille seguirá os procedimentos aqui descritos frente a um incidente de segurança da informação que possa causar a violação de dados pessoais ou de informações críticas institucionais. O plano de resposta a incidentes de segurança é dividido em 4 etapas, sendo elas: Identificação, Planejamento, Tratamento e Lições Aprendidas.

## 1. IDENTIFICAÇÃO:

É responsabilidade de toda a comunidade acadêmica que utiliza ou tem acesso às informações tratadas pela **Fundação Educacional da Região de Joinville (FURJ)** e suas mantidas, reportar à gerência de Tecnologia da Informação (GTI) **incidentes** que possam violar a segurança e a proteção de dados, pessoais ou institucionais, que são tratados em seus sistemas ou procedimentos. Entende-se por segurança, no mínimo, ameaças à Confidencialidade, Integridade e Disponibilidade (CID) de dados e informações.

Um incidente de segurança também pode ser detectado através de monitoramento, como análise dos *logs* dos servidores institucionais, sistema de inventário, comportamento inadequado dos ativos de tecnologia, tráfego de rede incomum e alertas emitidos pelo firewall corporativo e de software antivírus das estações e servidores. Procedimentos internos também podem levar à violação de dados e informações e por este motivo também devem ser monitorados e revistos pelo gerente ou coordenador responsável, sempre com o apoio da Gerência de Tecnologia da Informação.

Em resumo, para a confirmação de um incidente de segurança, é necessário que o evento que o gerou esteja relacionado com:

- Violação da confidencialidade, integridade e disponibilidade da informação ou dado pessoal tratado, independentemente do ativo de tecnologia;
- Processos e procedimentos que estejam em inconformidade com a Instrução Normativa e com o Manual de Segurança da Informação e Proteção de Dados;
- Funcionamento errôneo de software e hardware em ativos de tecnologia.

Uma vez confirmada a ocorrência de um incidente, então a análise do escopo do incidente deverá ser executada. Essa análise deve prover informações suficientes que permitam identificar e priorizar as atividades subsequentes.

**2. PLANEJAMENTO:**

Nesta fase, se aplicam as ações previamente desenvolvidas que devem ser tomadas frente a detecção ou conhecimento de um incidente que possa levar à uma violação de dados pessoais ou de informações institucionais críticas. Estas ações são descritas em documentos chamados de Planos de Recuperação e levam em consideração:

- Nome e consequência do incidente em relação à Confidencialidade, Integridade, Disponibilidade (CID)
- Ativo: listar os ativos envolvidos no incidente
- Características do incidente
- Responsabilidade – gestor responsável pelo ativo envolvido
- Ações imediatas – os passos que devem ser executados imediatamente após o conhecimento do incidente pela equipe interna da TI.
- A criticidade do incidente.

Exemplo de um plano de recuperação para sequestro de dados:

1. **Sequestro de dados | CID:**
   i. **Ativos:** Estações de trabalho da TI.
   ii. **Características do incidente:** uso de criptografia que torna os dados ininteligíveis, impossibilitando o uso dos ativos, seus arquivos, sistemas ou banco de dados.
   iii. **Responsabilidade:** Gerência de Tecnologia da Informação
   iv. **Ações imediatas:** 1. Não reiniciar os ativos; 2. Desabilitar a rede de comunicação de dados dos ativos; 3. Identificar o *Ransomware*; 4. Formatar os equipamentos envolvidos somente após a comunicação e autorização do responsável; 5. Restaurar os arquivos sequestrados através das cópias de segurança, quando for o caso.
   v. **Criticidade:** Alta.

Os Planos de Recuperação devem ser elaborados pela **Gerência de Tecnologia da Informação**, em conjunto com uma equipe de resposta à incidentes de segurança (ERIS). Cabe a ERIS, atuar antes, durante e após a ocorrência de um incidente de segurança, auxiliando na elaboração de normativas, manuais, planejamento e suporte jurídico. A ERIS deve ser acionada sempre que houver um incidente de segurança da informação que gere violação de dados pessoais, mesmo que a TI tenha sido capaz de solucionar o problema através dos Planos de Recuperação.

A ERIS é composta por:

Pró-Reitor de Infraestrutura: Professor Gean Cardoso de Medeiros;

Procuradora Jurídica: Dra. Ana Carolina Amorim;

Procurador Jurídico: Dr. Gilson Semer Guimarães;

Gerente da Tecnologia da Informação: Juarez William Vicenzi Bartuscheck;

Analista de Segurança da Informação/Encarregado de Dados: Marcelo Pereira da Silva.

## 3. TRATAMENTO:

A partir da confirmação de um incidente de segurança, é preciso avaliar rapidamente o risco de propagação da ameaça que o causou. Por exemplo, estações de trabalho contaminadas por **malwares**, como vírus ou ***ransomwares***, podem se espalhar rapidamente por toda a rede de dados, causando um incidente de maiores proporções.

Entende-se por tratamento a execução das tarefas necessárias para disponibilização dos serviços afetados, análise de questões legais, contenção do incidente e recuperação de dados. Neste sentido, o tratamento deverá ser realizado observando os seguintes itens:

i. Preservar, na medida do possível, todas as evidências do incidente, para que seja possível rastrear e identificar suas causas posteriormente;
ii. Verificar se existe um Plano de Recuperação para o incidente;
iii. Agir para que os serviços afetados sejam disponibilizados no menor tempo possível;
iv. Utilizar todos os recursos necessários para a contenção do incidente;
v. Utilizar todos os recursos existentes para recuperação de dados e sistemas, como restauração através *backups*;
vi. Avaliar o risco aos titulares de dados pessoais e, se necessário, comunicar o incidente à Autoridade Nacional de Proteção de Dados (ANPD) e aos próprios titulares que tiveram seus dados violados.

O fluxograma presente no “Anexo A” ilustra os passos que devem ser seguidos após a confirmação de um incidente de segurança que possa levar à violação de dados pessoais ou críticos para a FURJ e suas mantidas.

## 4. LIÇÕES APRENDIDAS:

Para que o mesmo incidente não volte a ocorrer, todas as características do evento, incluindo as ameaças, o impacto e probabilidade, deverão ser documentados nos Planos de Recuperação. Um Plano de Recuperação deverá ser criado para o incidente após o restabelecimento normal dos serviços, caso ainda não tenha um elaborado.

**ANEXO A:**

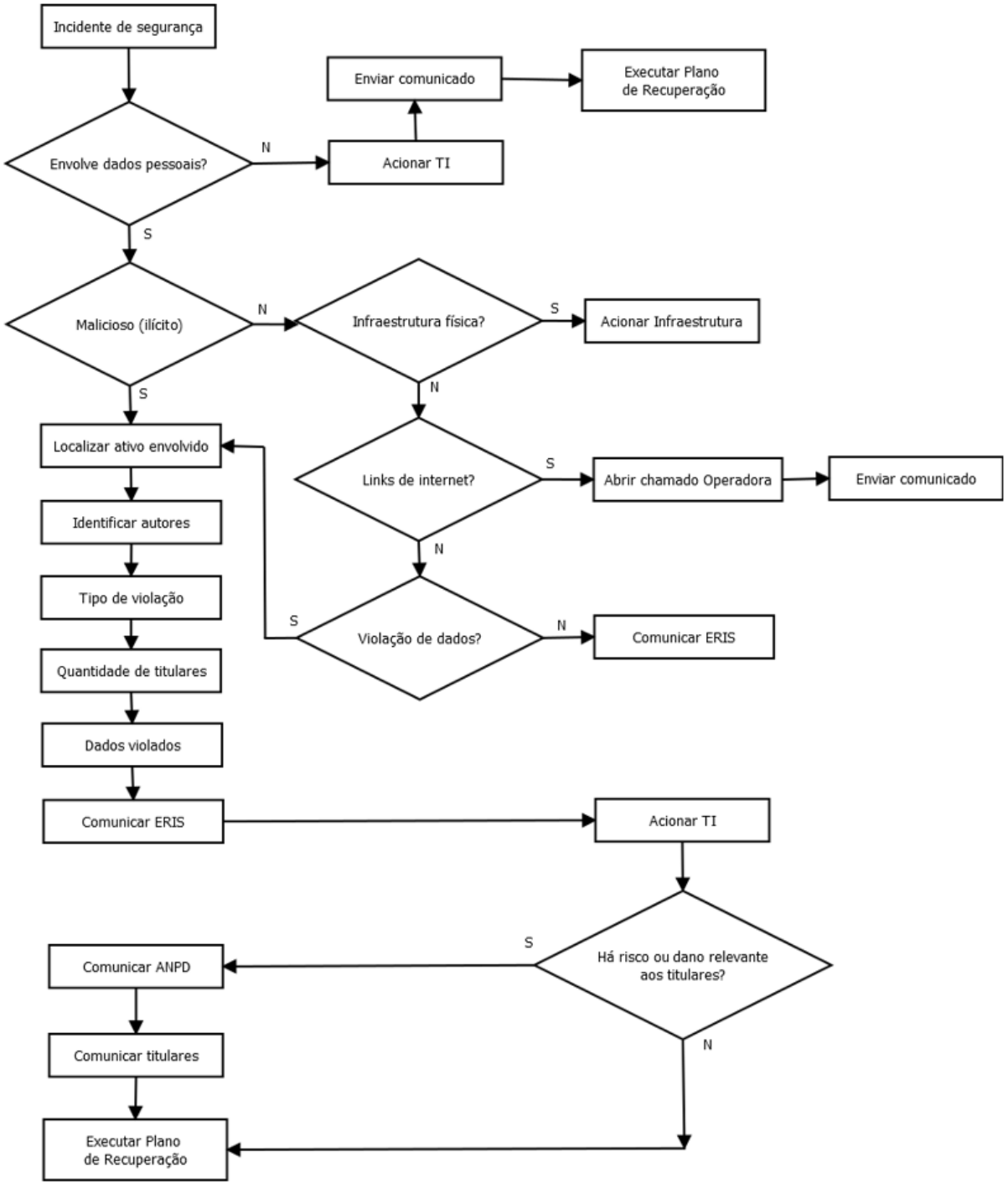


***Figura 1. Fluxograma de resposta a incidentes de segurança da informação.***