INPA INSTITUTO NACIONAL DE PESQUISAS DA AMAZÔNIA | COTIN COORDENAÇÃO DE TECNOLOGIA DA INFORMAÇÃO	**Fluxo de Gestão de Incidentes de Segurança da Informação COTIN/ INPA**	**POP: 006/COTIN/INPA**
Elaboração: Clausewykson Cunha Jorge Charles C. da Silva Roberto O. dos Santos	Versão: 01.00	Data de criação: 04/08/2025

1. Objetivo

Definir as etapas e responsabilidades no tratamento de incidentes de segurança da informação no INPA, garantindo a **detecção, resposta, contenção, análise e lições aprendidas** de forma eficiente, alinhada às diretrizes da Administração Pública Federal.

2. Abrangência

Aplica-se a todos os **usuários, sistemas, redes, serviços e dados** sob responsabilidade da COTIN/INPA, incluindo servidores, colaboradores, bolsistas, estagiários, terceiros e fornecedores.

3. Conceito

Incidente de Segurança da Informação é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas ou dados, que possa comprometer a **confidencialidade, integridade, disponibilidade ou autenticidade** das informações institucionais.

4. Fluxo de Gestão de Incidentes

Etapas:

1. **Identificação e Notificação**

    - O usuário que identificar ou suspeitar de incidente deve comunicar imediatamente à COTIN/INPA por canal oficial (e-mail, telefone ou sistema de chamados).

    - Exemplos: phishing, acesso não autorizado, vazamento de dados, indisponibilidade de sistemas, malware, violação de políticas.

2. **Registro**
    - O incidente será registrado em sistema de chamados ou planilha controlada pela COTIN/INPA, com data, hora, descrição, origem e responsável pelo reporte.
3. **Classificação e Priorização**
    - O incidente será classificado quanto ao impacto e urgência:
        - **Alto:** vazamento de dados sensíveis, indisponibilidade crítica de serviços.
        - **Médio:** degradação de desempenho, tentativa de acesso não autorizado.
        - **Baixo:** falhas isoladas de usuário ou pequenas não conformidades.
4. **Análise e Diagnóstico**
    - A equipe técnica da COTIN investiga a causa do incidente, avalia o escopo e identifica vulnerabilidades exploradas.
5. **Contenção**
    - Ações imediatas para isolar o incidente e minimizar danos (ex.: bloquear usuário, desconectar máquina da rede, suspender serviço).
6. **Erradicação e Recuperação**
    - Eliminar a causa do incidente (ex.: remoção de malware, correção de vulnerabilidade, troca de credenciais).
    - Restaurar serviços afetados com apoio de **planos de backup e contingência**.
7. **Comunicação**
    - Incidentes relevantes devem ser reportados ao **Comitê de Segurança da Informação do INPA** e, quando aplicável, ao **CTIR Gov**.
    - Se envolver **dados pessoais**, comunicar ao **Encarregado de Dados (DPO/LGPD)**.
8. **Lições Aprendidas e Melhoria Contínua**

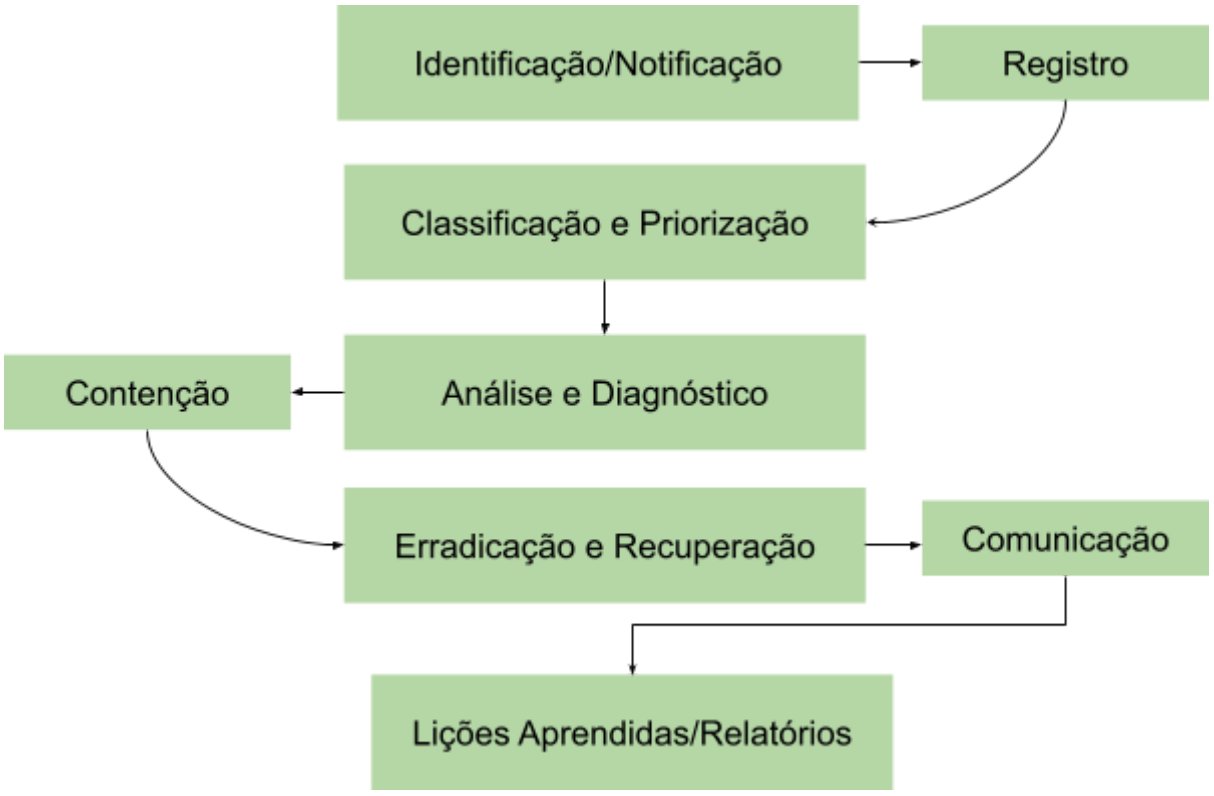
- Após a resolução, registrar um relatório contendo: causa raiz, impacto, medidas aplicadas, responsáveis e recomendações.

- Revisar controles e políticas para prevenir recorrência.

5. Responsabilidades

- **Usuários:** reportar imediatamente qualquer incidente.
- **COTIN/INPA:** registrar, analisar, tratar e monitorar incidentes, mantendo logs e relatórios.
- **Comitê de Segurança da Informação:** avaliar incidentes críticos e recomendar medidas estratégicas.
- **DPO (LGPD):** acompanhar incidentes que envolvam dados pessoais.

6. Representação Visual do Fluxo



7. Vigência e Atualização

Este fluxo entra em vigor na data de sua publicação e deverá ser revisado **anualmente** ou em caso de atualização normativa ou tecnológica relevante.

Coordenação de Tecnologia da Informação/INPA