Histórico de Versões e Alterações				
Versão	Data	Responsável	Tipo de Alteração	Revisor/Aprovador
1	17/11/2025	Samuel	Criação da Política	Igo

Sumário

1. Objetivo

O objetivo deste Plano de Resposta a Incidentes (PRI) é orientar o Hospital LISA a responder a eventos adversos e incidentes de segurança de forma documentada, ágil e confiável. Este plano visa minimizar o impacto operacional, financeiro e reputacional de um incidente, com foco primordial na segurança do paciente e na proteção de Dados Pessoais Sensíveis, assegurando o cumprimento das exigências legais, como a Lei Geral de Proteção de Dados (LGPD).

2. Escopo

Este plano se aplica a qualquer evento adverso, suspeita ou incidente confirmado que envolva a segurança dos ativos de informação ou o tratamento de Dados Pessoais sob a responsabilidade do Hospital LISA.

Sua observância é obrigatória para todos os indivíduos abrangidos pelo escopo da Política de Segurança da Informação (PSI), incluindo colaboradores, funcionários, terceiros, prestadores de serviços, estagiários, pesquisadores e membros da diretoria.

3. Glossário

Os termos e definições utilizados neste plano aderem ao glossário estabelecido na Política de Segurança da Informação e no Plano de Continuidade de Negócios. Termos adicionais relevantes para este plano incluem:

Incidente de Segurança: Qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais ou ativos de informação , como acesso não autorizado, destruição, perda, alteração ou vazamento.

Time de Resposta a Incidentes (TRI): Equipe central responsável pela coordenação das ações de resposta. No Hospital LISA, este time é composto, no mínimo, por membros da área da segurança da informação e pelo encarregado.

Vazamento de Dados: Qualquer quebra de sigilo ou disseminação não autorizada de dados.

4. Atores e Responsabilidades

O sucesso da resposta a um incidente depende da clara definição de papéis, adaptada ao LISA:

a. **Notificador (Qualquer Profissional do Hospital LISA):** Qualquer pessoa que identifique uma suspeita ou um incidente de segurança. Tem a responsabilidade de relatar o fato imediatamente.
b. **Acionador (Encarregado pelo Tratamento de Dados Pessoais - DPO):** É o ponto focal que recebe as notificações de incidentes. É responsável por acionar o TRI e comunicar o incidente à Diretoria Executiva.
c. **Time de Resposta a Incidentes (TRI):** Composto pela área da segurança da informação e pelo encarregado. Responsável pela triagem, análise, coordenação da contenção e documentação do incidente.
d. **Gestores da Informação (Data Owners):** Gestores das áreas de negócio (ex: Diretor Clínico, Gerente Financeiro). Atuam como responsáveis pelos processos afetados, apoiando o TRI na avaliação do impacto e na tomada de decisão.
e. **Diretoria Executiva:** Autoridade máxima, responsável pela tomada de decisão estratégica, alocação de recursos e aprovação de comunicações externas.

5. Macro Etapas do Processo

Este plano está estruturado conforme as macros etapas descritas a seguir, em ordem:

a. **Identificação**: A identificação de um incidente é um aspecto-chave. Ela depende das medidas de detecção (monitoramento, eventos de log, firewalls) gerenciadas pela Área de Segurança da Informação e do trabalho de conscientização e capacitação dos Profissionais do

Hospital LISA. Todos os profissionais devem ser capazes de identificar e informar imediatamente qualquer suspeita de vazamento de dados.

b. **Preparação**: A resposta a um incidente deve ser decisiva e executada prontamente. É essencial que as práticas de emergência sejam exercitadas e os tempos de resposta medidos, conforme definido nos requisitos de teste do Plano de Continuidade de Negócios. Esta preparação minimiza o impacto da indisponibilidade de recursos e os potenciais danos causados pelo comprometimento dos processos.
c. **Contenção**: Após a identificação, o incidente deve ser contido e, se for o caso, isolado, para que outros sistemas ou processos não sejam afetados. Essa etapa inclui a contenção de curto prazo (ex: isolar um servidor da rede), e deve ser seguida da adoção de medidas para garantir a preservação de dados, conforme a Norma de Backup. Durante a contenção, é crucial adotar medidas que permitam a documentação e o registro do incidente, evitando que evidências (logs) sejam destruídas.
d. **Erradicação**: Após a contenção da ameaça, a próxima etapa consiste na remoção da causa raiz do incidente (ex: eliminar um malware, corrigir uma vulnerabilidade explorada, reconfigurar um ativo) e na preparação dos sistemas afetados para que retornem ao seu estado seguro e original.
e. **Recuperação**: Nesta etapa, os sistemas e processos afetados retornarão ao ambiente de produção. A recuperação seguirá as prioridades e os Objetivos de Tempo de Recuperação (RTO) definidos na Análise de Impacto no Negócio (BIA) do Plano de Continuidade de Negócios. Os testes de validação são obrigatórios para garantir que nenhuma ameaça permaneça.
f. **Lições Aprendidas (Pós-Incidente)**: Esta última etapa visa revisar todo o processo de tratamento do incidente, contribuindo para o aprendizado da equipe e atualizando o Plano de Resposta a Incidentes. O Time de Resposta a Incidentes (TRI) usará essa análise para propor melhorias contínuas, conforme previsto na PSI.

g. **Documentação do Incidente**: O incidente deve ser documentado de forma detalhada pelo TRI, incluindo todas as ações implementadas nas etapas anteriores, os impactos analisados e as lições aprendidas.
h. **Comunicações**: A ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (pacientes, colaboradores) deve ser comunicada à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular afetado. Esta comunicação é uma responsabilidade legal e será coordenada pelo Encarregado (DPO) em conjunto com a Área de Segurança da Informação e aprovada pela Diretoria Executiva.

6. Descrição do Processo

6.1. Início/Detecção

Qualquer profissional do Hospital LISA que identifique um incidente ou suspeita deve reportá-lo imediatamente ao encarregado através do canal oficial como: e-mail hospitallisa@gmail.com ou chamado de suporte técnico.

O Notificador deve, ao reportar, fornecer o máximo de detalhes possível, incluindo:

a. Descrição do ocorrido.
b. Data e hora da ocorrência ou descoberta.
c. Tipo de dados envolvidos (especialmente se forem dados de saúde).
d. Sistemas ou ativos afetados

6.2. Triagem

Ao receber a notificação, o encarregado deve:

a. Comunicar imediatamente a Área de Segurança da Informação para iniciar a avaliação preliminar.

b. A Diretoria Executiva somente será acionada após a confirmação do incidente e somente se a criticidade for classificada como Média ou Alta, conforme matriz definida na seção 6.3.
c. O TRI realiza uma avaliação preliminar (triagem) para confirmar se o evento é um incidente de segurança.
d. Se não for um incidente, o DPO informa o Notificador e a Diretoria, registrando o fato.
e. Se for incidente confirmado, inicia-se a etapa de Avaliação (6.3).

6.3. Avaliação

Antes de iniciar a avaliação detalhada, o TRI deve classificar o evento como um dos seguintes itens:

a. Incidente Operacional: falhas que afetam serviços ou disponibilidade, sem evidência de impacto em dados pessoais.
b. Incidente de Dados Pessoais: eventos que envolvem acesso indevido, exposição, perda ou vazamento de dados pessoais ou dados pessoais sensíveis.

Essa distinção é necessária porque somente incidentes que envolvam dados pessoais podem exigir comunicação à ANPD e aos titulares. Após essa classificação inicial, o processo segue normalmente.

O TRI, com apoio do Gestor da Informação da área afetada, deve avaliar o incidente:

a. Preservar Evidências: Todas as evidências (logs, arquivos) devem ser preservadas.
b. Analisar Impacto: Identificar a fonte, os dados afetados (com foco em Dados Pessoais Sensíveis) e as possíveis consequências.

c. **Definir Criticidade:** A criticidade do incidente será definida com base na matriz de classificação de gravidade do Hospital LISA:

Volume de Dados Expostos	Sensibilidade dos Dados Afetados: Baixa (Anonimizados)	Sensibilidade: Média (Identificáveis, ex: CPF, Nome)	Sensibilidade: Alta (Dados de Saúde, Biometria, Crianças)
Alto (>10% da base)	Baixa Gravidade	Alta Gravidade	Alta Gravidade
Médio (2% a 10% da base)	Baixa Gravidade	Média Gravidade	Alta Gravidade
Baixo (<2% da base)	Baixa Gravidade	Média Gravidade	Média Gravidade

Nota: No contexto do Hospital LISA, a maioria dos incidentes que envolvem prontuários ou dados de pacientes será classificada automaticamente como "Sensibilidade Alta".

d. **Documentar Avaliação:** A avaliação deve ser registrada em um formulário próprio do incidente.

6.4. Métricas e Indicadores de Desempenho

Para garantir eficiência, rastreabilidade e conformidade legal, o processo de Resposta a Incidentes do Hospital LISA adota os seguintes indicadores e prazos (SLA):

a) **Indicadores Operacionais**
   i) **Tempo de Resposta Inicial (SLA):** prazo máximo de 1 hora para o DPO ou TRI responder à notificação inicial do incidente.
   ii) **Tempo para Triagem:** prazo máximo de 4 horas para confirmar se o evento é ou não um incidente.

b) **Indicadores Regulatórios**
   i) **Tempo Máximo para Comunicação à ANPD:** Em incidentes de segurança com risco ou dano relevante ao

titular, a comunicação deve ocorrer em até 3 dias úteis, conforme recomendação e prática do mercado.

ii) **Tempo para Comunicação aos Titulares:** alinhado com o prazo da ANPD, respeitando o princípio da transparência.

c) **Indicadores Pós-Incidente**

i) **Tempo para Concluir a Análise Pós-Incidente:** prazo de até 10 dias úteis para elaboração do Relatório Final (seção 6.7).

ii) **Tempo para Implementação das Ações Corretivas:** definido pelo TRI conforme criticidade, mas deve ser acompanhado mensalmente pela Área de Segurança da Informação.

Esses indicadores devem ser revisados anualmente no processo de melhoria contínua.

6.5. Contenção, Erradicação e Manutenção

a. **Contenção:** O TRI implementa ações imediatas para limitar o dano, como isolar sistemas da rede, bloquear contas de usuário comprometidas (conforme PGA) ou desligar serviços.
b. **Erradicação:** O TRI investiga a causa raiz e a elimina (ex: removendo malware, corrigindo vulnerabilidades).
c. **Recuperação:** A restauração dos serviços deve seguir a ordem de prioridade definida na Análise de Impacto no Negócio (BIA) do Plano de Continuidade de Negócios (PCN/DRP). A recuperação dos sistemas (DRP) será feita a partir dos backups gerenciados pela Norma de Backup (NBRD), garantindo a integridade dos dados.

Todas as medidas de contenção e recuperação devem ser registradas.

6.6. Comunicações

A gestão da comunicação é crítica e segmentada, conforme definido também no PCN/DRP do Hospital LISA:

a. **Comunicação Regulatória (ANPD) e aos Titulares:** Se a Avaliação (6.3) determinar que o incidente acarreta "risco ou dano relevante", o encarregado, em conjunto com a Diretoria Executiva, realizará as comunicações obrigatórias à ANPD e aos titulares dos dados.
b. **Comunicação Interna:** A Área de Recursos Humanos será responsável por manter os colaboradores informados sobre o status da crise e instruções de trabalho.
c. **Comunicação Externa (Imprensa, Pacientes):** A Diretoria Executiva (liderando o Comitê de Gerenciamento de Crise) definirá a comunicação oficial.

6.7. Lições Aprendidas

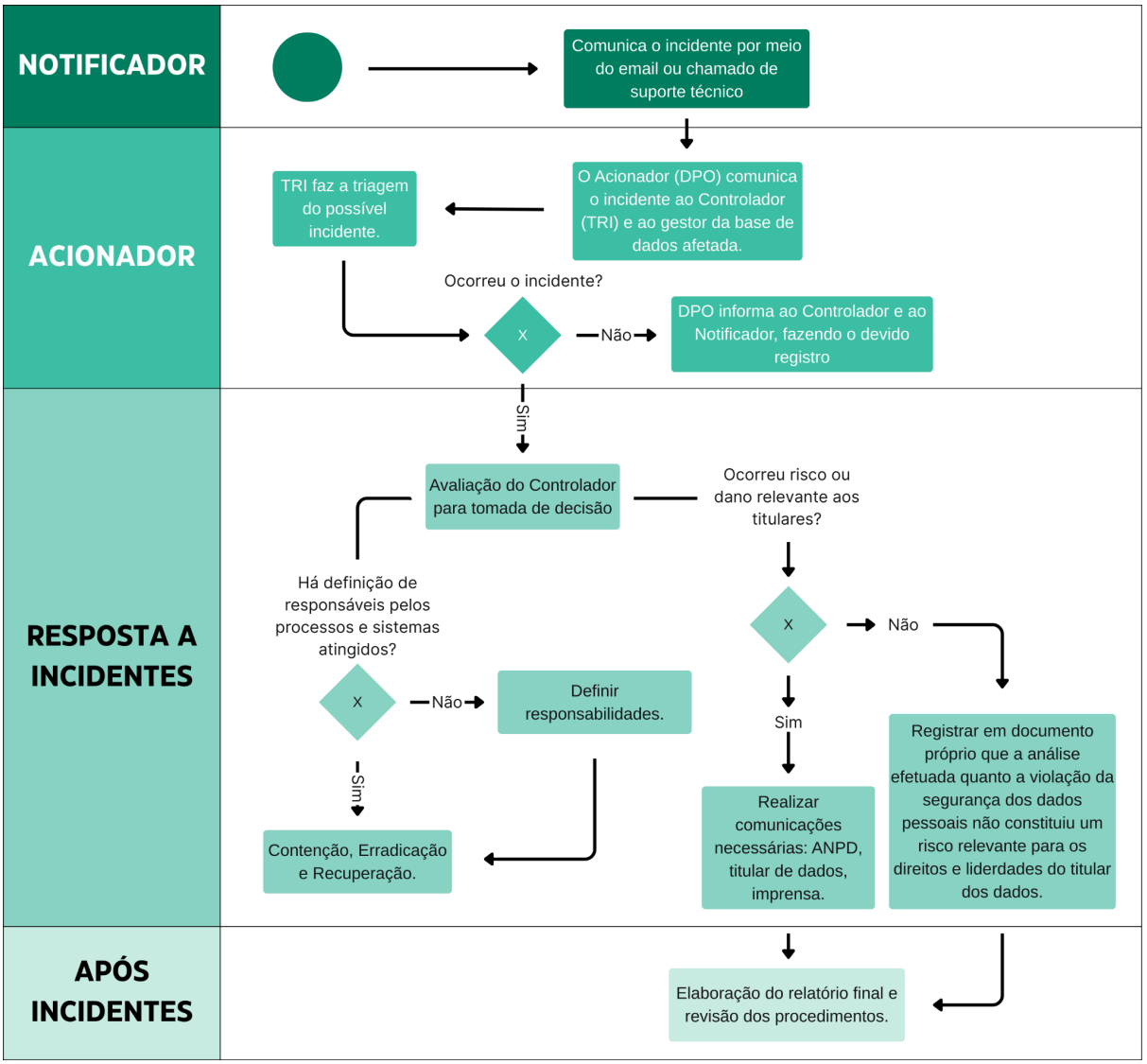
Após a normalização dos serviços, o TRI deve conduzir uma reunião de "Lições Aprendidas" com os Gestores da Informação envolvidos. O objetivo é discutir o que funcionou, o que falhou e propor melhorias para este Plano de Resposta a Incidentes e para as demais políticas de segurança.

6.8. Documentação

O TRI deve elaborar um relatório final circunstanciado sobre o incidente. Este documento deve conter a linha do tempo, evidências, ações de contenção, impacto, decisões tomadas e as lições aprendidas. Este relatório é fundamental para a prestação de contas à Diretoria Executiva e como evidência de conformidade à LGPD.

7. Fluxo do Processo

O processo de resposta a incidentes do Hospital LISA segue o seguinte fluxo:


NOTIFICADOR
Comunica o incidente por meio do email ou chamado de suporte técnico
ACIONADOR
O Acionador (DPO) comunica o incidente ao Controlador (TRI) e ao gestor da base de dados afetada.
TRI faz a triagem do possível incidente.
Ocorreu o incidente?
X
Não
DPO informa ao Controlador e ao Notificador, fazendo o devido registro
Sim
RESPOSTA A INCIDENTES
Avaliação do Controlador para tomada de decisão
Ocorreu risco ou dano relevante aos titulares?
Há definição de responsáveis pelos processos e sistemas atingidos?
X
Não
Definir responsabilidades.
Sim
Contenção, Erradicação e Recuperação.
X
Não
Sim
Realizar comunicações necessárias: ANPD, titular de dados, imprensa.
Registrar em documento próprio que a análise efetuada quanto a violação da segurança dos dados pessoais não constituiu um risco relevante para os direitos e liberdades do titular dos dados.
APÓS INCIDENTES
Elaboração do relatório final e revisão dos procedimentos.