Centro Universitário Euroamericano

Samuel Gonçalves de Araujo
Larissa Batista Maciel
Ageu Rocha Magalhães
Igo Cecílio Lobato de Carvalho

Dossiê de Segurança da Informação para o Setor de Saúde

Estudo de Caso Aplicado ao Hospital Fictício "LISA"

Brasília, DF
2025

Sumário de Documentos

Histórico de Versões e Alterações				
Versão	Data	Responsável	Tipo de Alteração	Revisor/Aprovador
1	01/10/2025	Larissa	Criação da Política	Ageu
2	08/10/2025	Igo	Revisão de Responsabilidades e Atribuições	Ageu

Sumário

1. Objetivo

A Política de Segurança de Informação da LISA (Larissa Igo Samuel Ageu) tem como objetivo estabelecer regras e diretrizes a serem seguidas em toda a instituição, de forma a proteger os seus ativos em todos os formatos, sejam físicos ou digitais, e em todos os processos, englobando a entrada, uso, processamento, tratamento, armazenamento e descarte dos dados em posse da instituição. Este documento visa garantir a confidencialidade, integridade e disponibilidade dos dados em conformidade com a Lei Geral de Proteção de Dados (LGPD), especialmente em casos dados pessoais sensíveis em relação ao contexto da saúde, de forma a reforçar compromisso com os princípios do Hospital LISA como instituição centrada no bem-estar e privacidade de seus pacientes e partes relacionadas, tanto interna como externamente.

2. Escopo

As diretrizes estabelecidas nesta Política de Segurança da Informação (PSI) são de aplicação obrigatória e se aplicam a todo e qualquer indivíduo que, de alguma forma, tenha acesso ou manipule os ativos de informação do Hospital LISA, incluindo, mas não se limitando, a colaboradores e funcionários de todos os níveis e áreas, terceiros e prestadores de serviços que atuem nas dependências da instituição ou remotamente em seu nome, estagiários, pesquisadores, voluntários, membros da diretoria, conselho e comitês. As mesmas diretrizes são aplicadas também a todos os ativos de informação e sistemas utilizados pela instituição, independentemente da sua forma, tipo, formato ou localização.

3. Glossário

AMEAÇA – Qualquer evento ou fator, interno ou externo, com potencial para causar dano aos ativos de informação de um sistema ou organização.

ATIVOS DE INFORMAÇÃO – O conjunto de informações, dados e os meios de armazenamento, transmissão e processamento, bem como os sistemas, locais e recursos humanos que têm acesso a eles e que possuem valor para a organização.

AUTENTICAÇÃO – Processo que busca verificar a identidade digital de um usuário ou sistema no momento em que requisita acesso, geralmente pela comparação de credenciais (como senha ou biometria) com as que estão pré-definidas no sistema.

CONFIDENCIALIDADE – Propriedade que garante que a informação não seja revelada ou disponibilizada a pessoas, sistemas ou entidades não autorizadas.

CONTROLE DE ACESSO – Conjunto de procedimentos, recursos e meios (físicos ou lógicos) utilizados para conceder ou bloquear o acesso a determinados recursos, geralmente exigindo autenticação prévia.

CONTROLES DE SEGURANÇA – Medidas e salvaguardas (sejam elas administrativas, técnicas ou físicas) utilizadas para proteger a confidencialidade, integridade e disponibilidade dos ativos de informação e mitigar riscos.

DADO PESSOAL SENSÍVEL – Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

DISPONIBILIDADE – Propriedade que garante que a informação esteja acessível e utilizável sob demanda por uma pessoa ou sistema autorizado.

ENCARREGADO – Pessoa indicada pelo controlador para atuar como canal de comunicação entre a organização, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

INFORMAÇÃO – Dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INTEGRIDADE – Propriedade que garante que a informação não foi modificada ou destruída de maneira não autorizada ou acidental, mantendo sua exatidão e completude.

LGPD – Sigla para a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), legislação brasileira que regula as atividades de tratamento de dados pessoais.

TITULAR DE DADOS – Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

VULNERABILIDADE – Uma fraqueza em um ativo ou controle que pode ser explorada por uma ou mais ameaças, resultando em uma violação de segurança.

4. Descrição

4.1. Princípios da Segurança da Informação

Todas as ações relacionadas à Segurança da Informação deverão ser norteadas pelos seguintes princípios:

Propriedade: A Informação, em qualquer forma ou suporte que se apresente (verbal, escrita, físico ou digital), e os Recursos Tecnológicos disponibilizados aos Profissionais do hospital LISA são de propriedade da Instituição, tendo natureza exclusiva de ferramentas de trabalho.

Garantia da Privacidade e da Proteção dos Dados de Pacientes e de Titulares de Dados Pessoais: A Instituição e os Profissionais do Hospital LISA são responsáveis pela segurança de quaisquer Informações e dados por ele administrados, devendo garantir a confidencialidade, integridade e disponibilidade destas Informações, prevenindo assim Incidentes de Segurança de Informação de qualquer natureza envolvendo o tratamento e a proteção de dados, em especial dados relacionados à saúde de pacientes, considerados Dados Pessoais Sensíveis nos termos da legislação vigente. Da mesma forma, projetos de pesquisa devem garantir a privacidade e a proteção dos dados de pacientes, incluindo, mas não se limitando a dados cadastrais, clínicos, biomoleculares e laudos.

Acesso e Guarda de Prontuários: Os prontuários pertencem exclusivamente aos pacientes. À Instituição, como depositária deste documento, cabe o dever de zelar por sua integridade, confidencialidade, disponibilidade e

guarda seguros, gerenciando-os de forma a atender integralmente os requisitos da legislação vigente. Os prontuários, sejam eles em versão física ou eletrônica, somente deverão ser disponibilizados aos Profissionais do Hospital que necessitarem acessar aquelas informações, para finalidades determinadas e justificadas. Sempre que possível, o acesso deve ser modulado, concedendo ao usuário acesso restrito exclusivamente às informações necessárias. Os prontuários devem ser guardados de forma segura, resguardando a integridade física dos documentos, e sistematizada, possibilitando a localização, armazenamento e recuperação dos documentos; e pelo tempo que determinar a legislação aplicável.

Propriedade Intelectual: A propriedade sobre o conhecimento, processos, informações, dados, produtos, documentos, livros, relatórios, resultados tangíveis e intangíveis, sistemas, ferramentas, plataformas e tecnologias geradas em projetos de pesquisas será regulamentada por padrões institucionais específicos sobre propriedade intelectual, os quais deverão ser integralmente observados por todos os Profissionais do Hospital LISA.

4.2. Diretrizes de Segurança da Informação

O objetivo da gestão de Segurança da Informação da Instituição é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à Segurança da Informação, provendo suporte às operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos na Instituição. A Instituição está comprometida com uma gestão efetiva de Segurança da Informação, adotando todas as medidas cabíveis para garantir que esta Política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades da Instituição.

4.3. Responsabilidades e Atribuições

Para esta política, devem-se considerar as atribuições e responsabilidades descritas a seguir:

4.3.1. Diretoria Executiva

a) aprovar o plano geral de implementação e as ações estratégicas e operacionais de Segurança da Informação e as iniciativas em suas diferentes etapas;

b) assegurar a implementação de medidas técnicas de segurança da informação e de proteção de dados, em conformidade com os requisitos de sistemas padrão de boas práticas e de governança, em alinhamento com os termos desta Política, da Política de Privacidade, das normatizações internas de segurança e tecnologia da informação e com os princípios gerais estipulados na Legislação de Proteção de Dados;

c) assegurar a provisão orçamentária de recursos suficientes para o adequado funcionamento do Sistema de Gerenciamento de Segurança da Informação;

d) providenciar a instalação e a manutenção de uma estrutura de pessoal para a gestão e coordenação das atividades de Segurança da Informação.

4.3.2. Área da segurança da informação

a) aplicar a presente Política de forma que a proteção da Informação esteja alinhada com a proteção dos processos estratégicos do negócio;

b) estabelecer, implantar e monitorar o Sistema de Gerenciamento de Segurança da Informação, de acordo com os requisitos da legislação, das normas técnicas aplicáveis e as melhores práticas internacionais;

c) identificar os riscos inerentes à Segurança da Informação da Instituição através do mapeamento das vulnerabilidades, ameaças, impacto e probabilidade de ocorrência, e classificá-los, conforme metodologia institucional de gerenciamento de riscos e com o apoio da área de Gerenciamento de Riscos Corporativos;

d) recomendar e/ou adotar controles que mitigam os riscos mapeados, inerentes à Segurança da Informação;

e) recomendar e/ou adotar mecanismos automatizados para o gerenciamento, prevenção e detecção de eventos de Segurança da Informação;

f) recomendar e/ou implementar processos de autenticação e controle de acesso seguros para os Recursos Tecnológicos;

g) analisar criticamente as ocorrências de Segurança da Informação, considerando a efetividade desta Política frente ao volume e impactos dos eventos, Incidentes de Segurança da Informação detectados e mudanças de tecnologias;

h) estabelecer e divulgar as responsabilidades pelo cumprimento desta Política;

i) informar e orientar os Profissionais do Hospital LISA sobre a importância da Segurança da Informação e a obrigatoriedade de cumprimento desta Política;

j) desenvolver programas de treinamento e conscientização para os profissionais do Hospital LISA. Tais treinamentos devem ocorrer com frequência mínima anual e sempre que houver mudanças significativas nas políticas, abordando obrigatoriamente os temas: Lei Geral de Proteção de Dados (LGPD) e suas implicações na saúde, identificação e prevenção contra phishing e engenharia social, uso ético de dados clínicos e confidencialidade médica, além das próprias políticas internas de Segurança da Informação.

k) realizar auditorias e inspeções periódicas, com o objetivo de avaliar a conformidade com as definições desta Política;

l) manter atualizado o inventário de Recursos de Tecnologia, com todos os sistemas, aplicativos, softwares, ferramentas de gerenciamento de informações e dados da Instituição;

m) definir, implementar e testar planos de continuidade de negócios para garantir a disponibilidade dos recursos tecnológicos estratégicos em casos de Incidentes de Segurança da Informação;

n) em conjunto com o Encarregado e com a área de Privacidade e Proteção de Dados, gerir, analisar e acompanhar os Incidentes de Segurança da Informação e as suspeitas ou casos de violações dessa Política, definindo as ações de remediação conforme as diretrizes e procedimentos estabelecidos pela Instituição e acompanhando sua implementação pelas áreas responsáveis.

o) definir e monitorar um conjunto de Indicadores Chave de Desempenho (KPIs) para avaliar a eficácia desta Política e do Sistema de Gerenciamento de Segurança da Informação. Estes indicadores devem incluir, mas não se limitar a: número de incidentes de segurança, taxa de adesão aos treinamentos obrigatórios e tempo médio para resposta e remediação de incidentes.

4.3.3. Área de privacidade e proteção de dados

a) avaliar os impactos da legislação e da regulamentação relacionada à privacidade e à proteção de dados pessoais às disposições desta Política e trabalhar em conjunto com as áreas de Tecnologia e Segurança da Informação para garantir o cumprimento das normas aplicáveis e implementar melhorias nos procedimentos, controles e medidas de segurança, visando à mitigação de riscos decorrentes do tratamento de Dados Pessoais.

4.3.4. Área dos recursos humanos

a) garantir que, no momento da contratação, o Profissional do Hospital LISA tenha ciência desta Política e assine os termos de ciência e responsabilidade definidos pela área de Segurança da Informação;

b) implementar os programas de treinamento para os Profissionais do Hospital LISA, de forma a conscientizá-los sobre as responsabilidades de todos em relação à Segurança da Informação;

c) informar imediatamente para a área de Tecnologia da Informação todas as contratações, transferências, afastamentos, desligamentos, mudanças de funções, licenças e modificações no quadro de colaboradores sob a sua supervisão.

4.3.5. Gestores da informação

a) gerenciar as Informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu Ciclo de Vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pela Instituição;

b) identificar, classificar e rotular as Informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pela Instituição;

c) revisar periodicamente as Informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem das mesmas conforme necessário;

d) autorizar e revisar os acessos à Informação e sistemas de Informação sob sua responsabilidade;

e) aprovar a concessão ou solicitar a revogação de acesso à Informação ou sistemas de informação de acordo com os procedimentos adotados pela Instituição.

4.3.6. Profissionais do Hospital LISA

a) conhecer e cumprir todas as regras definidas nesta Política;

b) adotar a conduta e todos os procedimentos necessários para proteger as Informações da Instituição;

c) evitar discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, entre outros), buscando sempre fazê-lo em ambientes adequados e somente com as pessoas que realmente precisam ser envolvidas;

d) utilizar as Informações e os Recursos Tecnológicos da Instituição exclusivamente para os objetivos da Instituição e para o cumprimento de suas funções, sendo vedado o uso para fins pessoais ou de terceiros;

e) solicitar esclarecimentos à Instituição para qualquer dúvida que possa vir a ter quanto ao disposto nesta Política, para que possa cumpri-la, não podendo, em nenhuma hipótese, alegar desconhecimento;

f) relatar para a área de Segurança da Informação eventuais Incidentes de Segurança da Informação ou suspeitas ou violações desta Política das quais venha a tomar conhecimento.

5. Disposições Gerais

5.1. Descumprimento dos padrões institucionais de Segurança da Informação

O não cumprimento desta Política ou de qualquer dos demais padrões institucionais de Segurança de Informação, comprovado após a devida apuração, serão passíveis de penalidades, tanto na esfera administrativa (advertências, punições administrativas, demissão ou rescisão contratual, entre outras) quanto na esfera legal (reparação dos danos causados à Instituição e às demais pessoas prejudicadas), conforme a gravidade do ato.

5.2. Atualização desta política

Este documento poderá sofrer alterações em caso de mudanças de processo e/ou alteração de tecnologia, mudanças de diretrizes institucionais ou da legislação vigente, ou ainda por determinação da Instituição.

Histórico de Versões e Alterações				
Versão	Data	Responsável	Tipo de Alteração	Revisor/Aprovador
1	08/10/2025	Ageu	Criação da Política	Samuel
2	22/10/2025	Larissa	Aumento do número de caracteres na senha	Igo

Sumário

1. Objetivo

O objetivo desta política é estabelecer regras e diretrizes para o uso adequado e seguro de todos os recursos de Tecnologia da Informação do Hospital, visando proteger a infraestrutura, a informação (especialmente Dados Pessoais Sensíveis de pacientes e colaboradores) e garantir a conformidade legal.

2. Regras Gerais para uso da Rede Corporativa e Equipamentos

Esta seção estabelece as diretrizes fundamentais para acesso e segurança geral na infraestrutura de TI do Hospital.

2.1. Acesso e Contas de Usuário

a) **Restrição de Acesso:** O acesso à rede é permitido exclusivamente a pessoas explicitamente autorizadas e limitado ao mínimo necessário para o desempenho de suas funções (Princípio do Mínimo Acesso).
b) **Identificação Pessoal:** Cada usuário deve possuir uma identificação (login) exclusiva, sendo seu uso pessoal e intransferível. O empréstimo de credenciais é considerado infração disciplinar grave.
c) **Gestão de Contas:**
    i) Contas ativas e sem atividade por mais de 45 dias, não havendo justificativa válida, serão automaticamente bloqueadas sem aviso prévio.
    ii) Em casos de desligamento, mudança de função ou fim de contrato, o RH deve registrar um chamado para que a TI realize os ajustes ou a desativação do perfil de acesso em até 2 horas após o registro.

2.2. Política de Senha Obrigatória

a) **Sigilo:** A senha é pessoal e intransferível, devendo ser mantida em total sigilo.
b) **Criação:** A senha inicial é temporária e deve ser alterada obrigatoriamente no primeiro acesso.

c) **Requisitos Mínimos:** A senha deve ter um tamanho mínimo de 12
d) caracteres, composta por letras (maiúsculas e minúsculas), números e caracteres especiais (ex: !, $, #, %).
e) **Atualização:** Será solicitada automaticamente a alteração da senha a cada 60 dias.
f) **Histórico:** Não é permitido o uso das últimas 3 (três) senhas utilizadas.
g) **Bloqueio:** A conta de acesso será bloqueada automaticamente após 5 tentativas inválidas. Caso o usuário não consiga acessar sua conta, deverá solicitar o desbloqueio ou redefinição de senha junto à equipe de suporte técnico, exclusivamente por meio dos canais autorizados. A identidade do solicitante será validada antes da liberação do acesso.
h) **Armazenamento:** É proibido manter senhas registradas em arquivos na rede, no computador, em anotações ou qualquer outro meio que comprometa o sigilo.

2.3. Monitoramento, Uso e Responsabilidade

a) **Monitoramento:** A Instituição e/ou o Setor de TI se reservam o direito de monitorar e gravar todo o uso da rede corporativa, Internet, e-mail e estações de trabalho. Os dados de uso podem ser auditados via logs de sistemas.
b) **Uso Profissional:** Os recursos computacionais são propriedade do Hospital LISA e devem ser utilizados exclusivamente para a atividade profissional e para os objetivos da Instituição.
c) **Bloqueio de Inatividade:** Após 15 minutos de inatividade, a tela do equipamento será bloqueada, exigindo nova autenticação para evitar acesso de terceiros a dados confidenciais ou sensíveis.
d) **Responsabilidade por Danos:** Qualquer dano ou prejuízo material ou informacional causado por mau uso ou negligência na guarda dos equipamentos e credenciais será de inteira responsabilidade do colaborador.

2.4. Uso de Impressoras e Scanners

a) **Finalidade:** Devem ser utilizados única e exclusivamente para atender às necessidades do Hospital LISA.
b) **Proibições:** É proibida a impressão de documentos particulares ou a utilização das funcionalidades de scan/cópia para materiais que violem Direitos Autorais.
c) **Segurança da Informação:** O colaborador deve certificar-se de que a impressão esteja segura e seja imediatamente recolhida para evitar o vazamento de informações e dados confidenciais ou sensíveis.
d) **Auditoria:** O conteúdo impresso e escaneado poderá ser monitorado.

3. Regras para uso de e-mail Corporativo

O e-mail é uma ferramenta corporativa e seu uso deve refletir o profissionalismo e as normas de segurança da informação da Instituição.

3.1. Uso e Conduta Profissional

a) **Exclusividade:** O e-mail deve ser utilizado única e exclusivamente para o trato de questões de interesse da Instituição.
b) **Proibição de Uso Pessoal:** Não pode ser utilizado para fins pessoais ou que infrinjam o Código de Ética da Instituição.
c) **Individualidade:** A conta é individual, e o colaborador é responsável por toda mensagem enviada a partir de seu endereço, devendo zelar pela imagem da organização e utilizar linguagem profissional.
d) **Transferência:** A conta de e-mail não pode ser transferida ou cedida a terceiros.

3.2. Segurança e Conteúdo Proibido

a) **Conteúdo Ofensivo/Ilegal:** É proibido o uso para transmitir/divulgar material ilegal, difamatório, abusivo, ameaçador, obsceno, ou que viole a privacidade de terceiros.
b) **Imagens Corporativas/Éticas:** É proibido o uso de e-mail que contenha declarações com ideologias políticas, religiosas, raciais, pornografia, apologia às drogas ou que possam prejudicar a imagem da organização, pacientes, concorrentes ou fornecedores.
c) **Compartilhamento de Dados:**
    i) Não compartilhar Dados Pessoais e Dados Pessoais Sensíveis (exames, laudos, histórico de saúde) via e-mail.
    ii) Caso estritamente necessário e autorizado, o usuário deve certificar-se de que os destinatários seguem a Política de Privacidade de Dados, atendendo à LGPD.

3.3. Propriedade e Auditoria de E-mail

a) **Propriedade Institucional:** Todos os e-mails recebidos ou enviados através da conta corporativa são de propriedade do Hospital LISA.
b) **Monitoramento:** Todos os e-mails estão sujeitos ao monitoramento integral de seu conteúdo, a qualquer momento e sem notificação prévia.
c) **Gestão de Conteúdo:** O usuário não deve esvaziar a caixa de e-mail ou eliminar arquivos em caso de afastamento ou desligamento, visto que o conteúdo pertence à instituição.
d) **Acesso Restrito:** O acesso a e-mails de colaboradores desligados ou afastados é restrito, exigindo aprovação formal da gerência.

4. Regras Para Uso de Internet

O acesso à Internet é um recurso profissional e deve ser gerido para manter a produtividade e a segurança da rede.

4.1. Finalidade e Controle de Acesso

a) **Aderência:** O acesso à Internet é permitido se for aderente aos objetivos e atividades fins desempenhadas pelo usuário (uso profissional).
b) **Sites Proibidos:** Sites com conteúdo pornográfico, de apologia ao racismo/discriminação, de jogos online, ou de relacionamento não devem ser acessados. A TI utilizará filtros de acesso para bloquear esta navegação.
c) **Exceções:** Se for necessário o acesso a sites bloqueados por motivos estritamente profissionais, o usuário deverá solicitar a liberação via chamado, que será analisado pela TI e aprovado formalmente pela gerência.
d) **Relatórios:** O sistema de filtros de acesso pode gerar relatórios periódicos para auditoria do uso.

4.2. Conteúdo e Software

a) **Download Proibido:** É estritamente proibido fazer download de software comercial ou material protegido por Direitos Autorais (copyright) sem um contrato de licenciamento válido. É proibido baixar programas de entretenimento ou jogos.
b) **Vírus e Malware:** Nenhum usuário pode utilizar os recursos para deliberadamente propagar qualquer tipo de vírus ou programas de controle de outros computadores.
c) **Instalação de Programas:** É proibido instalar programas provenientes da Internet ou de qualquer outra fonte sem expressa autorização do Departamento de TI.

d) **Redes P2P e Mensageiros:** É proibido o uso de ferramentas P2P, P2M e de Redes Sociais ou Instant Messenger (IM) não autorizados para fins profissionais ou pessoais.

5. Regras Para Dispositivos Móveis e Mídias Removíveis

Esta seção trata do risco de vazamento de dados via dispositivos não corporativos e mídias físicas.

5.1. Uso de Mídias Removíveis (USB, Pen Drive, etc.)

a) **Bloqueio Padrão:** O uso de mídias removíveis é considerado uma fonte de infecção por malwares e um risco de evasão de dados. As portas de comunicação USB e barramentos similares (bluetooth) são automaticamente bloqueadas por software de gerenciamento central.
b) **Concessão Excepcional:** Para concessão de acesso (excepcional), é necessário registrar um chamado, anexar um termo de autorização específico e ter aprovação formal do gestor.
c) **Termo de Responsabilidade:** O usuário e o gestor assinam um termo de responsabilidade, assumindo a inteira e exclusiva responsabilidade por manter a integridade, confidencialidade e disponibilidade dos dados do Hospital.

5.2. Dispositivos Móveis (Smartphones e Tablets Corporativos/Pessoais)

a) **Equipamentos Corporativos:** Usuários que utilizam smartphones/tablets fornecidos pelo Hospital devem assinar o respectivo termo de responsabilidade. É vedado o uso do equipamento para qualquer finalidade que não seja ligada diretamente às atividades de sua área.
b) **Perda ou Roubo:** Em caso de perda ou roubo de equipamentos corporativos, o usuário deve formalizar imediatamente um Boletim de Ocorrência (BO) e comunicar o suporte da TI.

c) **Dispositivos Pessoais (BYOD - Bring Your Own Device):** O uso de dispositivos móveis pessoais não é autorizado para tratar de temas corporativos, especialmente Dados Pessoais e Dados Pessoais Sensíveis.

5.3. Uso de Aplicativos de Comunicação para Fins Profissionais

Se o uso for autorizado ou necessário:

a) **Prevenção de Vazamento:** O usuário deve evitar compartilhar Dados Pessoais/Sensíveis (exames, laudos, imagens) por esses meios.
b) **Minimização de Risco:** Caso estritamente necessário, deve-se adotar o envio de mensagens temporárias ou eliminar o conteúdo o mais breve possível do dispositivo após a inserção nos sistemas de gestão da organização (preferencialmente em até 24h).
c) **Corresponsabilidade:** O usuário está ciente de que o compartilhamento de Dados Pessoais/Sensíveis referente ao Hospital implica em corresponsabilidade jurídica sobre o dado.

5.4. Boas Práticas de Segurança

Recomenda-se que todos os dispositivos (corporativos ou pessoais autorizados) utilizem:

a) Software antivírus licenciado e atualizado.
b) Sistemas operacionais atualizados.
c) Senhas seguras (12 caracteres alfanuméricos) e bloqueio de tela automático.
d) Autenticação de dois fatores ativada (se suportado).
e) Criptografia de disco/dados.
f) Proibição de uso de Wi-Fi aberto (público) ou carregadores USB públicos para acessar dados hospitalares.

6. Conclusões e Penalidades

O não cumprimento de qualquer diretriz estabelecida nesta Política será considerado uma infração e estará sujeito a medidas disciplinares, que podem variar desde uma advertência até a rescisão do contrato de trabalho por justa causa, além de responsabilização civil e criminal, conforme a legislação vigente (incluindo a LGPD).

Histórico de Versões e Alterações				
Versão	Data	Responsável	Tipo de Alteração	Revisor/Aprovador
1	20/10/2025	Samuel	Criação da Política	Igo
2	22/10/2025	Ageu	Padronização de termos	Larissa
3	24/10/2025	Samuel	Adição de tópicos	Larissa

Sumário

1. Objetivo e Diretrizes Gerais

O objetivo principal desta política é assegurar que as informações recebam classificação apropriada de confidencialidade, integridade, disponibilidade, autenticidade e privacidade (CIDAP), de acordo com sua sensibilidade e criticidade para o hospital e para os titulares dos dados.

As diretrizes essenciais para o ambiente hospitalar são:

a. **Proteção Mandatória de Dados Sensíveis:** O tratamento de informações deve respeitar a privacidade e a proteção de dados pessoais, especialmente aqueles definidos pela Lei nº 13.709/18 (LGPD), como dados de saúde ou biometria.
b. **Classificação no Ciclo de Vida:** Todas as informações e ativos (documentos digitais, físicos e sistemas) devem ser classificados na sua emissão ou recepção, e revisadas periodicamente para garantir que a classificação permaneça adequada.
c. **Princípio da Necessidade de Conhecimento (Need-to-Know):** O acesso deve ser limitado a pessoas especificamente autorizadas que necessitem da informação para o desempenho de suas tarefas profissionais.

2. Escopo e Responsabilidades

2.1. Abrangência da Política

Esta política é aplicável a todos os ativos de informação (documentos digitais, físicos e sistemas) e a todas as pessoas que, direta ou indiretamente, acessem, tratem ou suportem as informações do hospital. Isto inclui, mas não se limita a: colaboradores (funcionários, médicos, estagiários), gestores e diretores, consultores, fornecedores e terceiros que realizem qualquer tratamento de informações em nome do hospital.

2.2. Papéis e Responsabilidades

A responsabilidade pela classificação correta, manuseio e proteção das informações deve ser atribuída para garantir a rastreabilidade e a conformidade.

a) **Proprietário da Informação (Data Owner):** Normalmente o gestor da área de negócio (ex: Diretor Clínico, Gerente Financeiro) que cria, utiliza ou é responsável pelas informações. É o responsável final pela classificação correta, pela aplicação desta política em suas equipes, e pelo estabelecimento dos critérios de tratamento da informação. O Proprietário da Informação deve garantir que as informações sejam corretamente classificadas e rotuladas.
b) **Custodiante da Informação (Data Custodian/TI):** A equipe responsável pela segurança tecnológica, armazenamento, processamento e manutenção dos sistemas e infraestrutura que suportam a informação. Deve assegurar os recursos tecnológicos e sistemas para o tratamento seguro da informação.
c) **Usuário da Informação (Colaborador):** Qualquer pessoa que acesse ou utilize a informação para o desempenho de suas tarefas profissionais. Deve cumprir rigorosamente as diretrizes de classificação e proteção, e reportar imediatamente quaisquer não conformidades ou eventos de segurança.
d) **Encarregado de Dados (DPO):** Responsável por atuar como canal de comunicação com os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), garantindo que o tratamento dos Dados Pessoais Sensíveis (como prontuários médicos) siga os requisitos legais da Lei Geral de Proteção de Dados (LGPD).

3. Definição dos Níveis de Classificação

A classificação da informação no hospital deve ser realizada de acordo com o nível de impacto potencial em caso de divulgação, modificação ou destruição não autorizada.

Nível de Classificação	Impacto Potencial (Confidencialidade)	Descrição e Critérios de Acesso	Exemplos
PÚBLICA	Muito Baixo	Informação oficialmente liberada para divulgação ampla, sem causar danos ou prejuízos ao hospital. Acesso irrestrito.	Horário de atendimento, lista de especialidades médicas, políticas, relatórios anuais de gestão sem dados sensíveis e campanhas públicas de saúde.
INTERNA	Baixo	Informação destinada ao uso interno do hospital, para usuários e departamentos específicos. Sua divulgação ao público em geral requer autorização expressa e não deve causar problemas significativos.	Manuais de procedimentos operacionais, relatórios gerenciais internos (sem dados de pacientes), lista de ramais, e-mails corporativos, comunicados internos e avisos gerais.
RESTRITA	Moderado	Informação cujo acesso é limitado a grupos específicos de colaboradores. A divulgação não autorizada pode prejudicar investigações em	Documentos internos de tomada de decisão, relatórios de auditoria interna (não sensíveis), relatórios

		andamento ou comprometer atividades administrativas sensíveis.	financeiros internos e planejamentos administrativos.
CONFIDENCIAL	Alto/Muito Alto	Informação de caráter sigiloso, cuja divulgação ou alteração não autorizada pode causar graves danos, prejuízos irreversíveis ou violação da lei para o hospital e/ou terceiros. Este nível é obrigatório para Dados Pessoais Sensíveis.	Prontuários médicos de pacientes, resultados de exames, histórico de internações, dados biométricos, informações salariais e contratuais de colaboradores, segredos comerciais ou propriedade intelectual (ex: pesquisa clínica confidencial).

3.1. Classificação Padrão (Omissão de Rótulo)

Caso um documento ou ativo de informação não contenha um rótulo de classificação visível ou a rotulagem não seja tecnicamente possível (restrições de sistema), a informação deve ser tratada por padrão como INTERNA. Se houver qualquer dúvida quanto à presença de Dados Pessoais Sensíveis ou criticidade moderada, o tratamento deverá ser o mais restritivo possível, sendo elevada para, no mínimo, RESTRITA até que o Proprietário da Informação defina o nível correto.

3.2. Revisão e Análise Crítica das Classificações

Todas as informações e ativos devem ter sua classificação revisada periodicamente para garantir que o nível atribuído permaneça adequado. O

processo de análise crítica da classificação deve ser realizado a cada 12 meses (anualmente), ou sempre que ocorrerem mudanças relevantes, como:

a) Mudanças nos critérios de classificação ou na legislação (ex: LGPD).
b) Mudanças nas necessidades do negócio ou na sensibilidade da informação.
c) Ocorrência de eventos ou incidentes de segurança.
d) Ao longo do ciclo de vida da informação.

4. Critérios de Tratamento e Manuseio Específicos

O tratamento da informação é o conjunto de ações (produção, classificação, utilização, acesso, armazenamento, eliminação, etc.). Para o hospital, o tratamento deve ser rigorosamente controlado para garantir os princípios de CIDAP.

4.1. Tratamento de Dados Pessoais Sensíveis (Confidencial)

a) **Fundamento Legal:** O tratamento de dados de saúde deve seguir os requisitos legais da LGPD, sendo os dados de saúde classificados como Confidenciais.
b) **Anonimização/Pseudonimização:** Sempre que possível e aplicável à finalidade, as informações devem ser anonimizadas ou pseudonimizadas, reduzindo o impacto em caso de vazamento.
c) **Registro e Rastreabilidade:** Deve-se manter uma cadeia de custódia e registros claros de quem acessou, modificou ou transferiu prontuários e dados de pacientes.

4.2. Diretrizes de Rotulagem

A rotulagem visa comunicar o nível de classificação da informação contida no documento, facilitando seu manuseio e proteção.

a) **Formatos:** Os procedimentos de rotulagem devem abranger todos os formatos: documentos físicos (prontuários, radiografias), documentos digitais (e-mails, sistemas) e informações verbais.
b) **Técnicas Recomendadas:** Para documentos digitais de nível RESTRITA ou CONFIDENCIAL, recomenda-se o uso de cabeçalhos, rodapés ou marcas d'água que indiquem claramente o nível de classificação (Ex: "CONFIDENCIAL – DADOS DE PACIENTE").
c) **Omissão:** Se a rotulagem não for tecnicamente possível (restrições de sistema), o tratamento deve ser o mais restritivo, conforme o nível de classificação presumido.

4.3. Diretrizes para Transferência de Informações

A transferência de informações (entre áreas internas ou com terceiros, como laboratórios externos ou operadoras de saúde) deve ser definida por regras, procedimentos e acordos, alinhados à classificação.

Tipo de Transferência	Requisitos de Controle
Verbal	Não realizar conversas envolvendo dados do tipo CONFIDENCIAL em locais públicos (corredores, elevadores, refeitórios) ou por canais de comunicação inseguros. Em reuniões internas sensíveis, o nível de classificação do assunto deve ser avisado para que todos os presentes observem os controles.
Mídia Física (Prontuários)	As informações do tipo CONFIDENCIAL devem ser transportadas de forma segura. Controles devem proteger contra danos físicos (ex: derramamento de líquidos) e garantir o endereçamento e transporte corretos. Deve-se manter um registro (cadeia de custódia) de quem enviou e recebeu a mídia.
Eletrônica	Informações do tipo CONFIDENCIAL (ex: resultados de exames via e-mail) devem ser

	protegidas contra malware e enviadas com prevenção contra destinos incorretos. Deve-se utilizar criptografia ou canais seguros para transferência de dados sensíveis e autenticação rigorosa ao acessar sistemas remotamente.

4.4. Diretrizes de Retenção e Descarte

O tratamento da informação inclui o conjunto de ações de eliminação, arquivamento e destinação. Devem ser definidas diretrizes de retenção e descarte para todos os registros, em alinhamento com a classificação, a sensibilidade e os requisitos legais (como a LGPD).

O tempo de retenção das informações deve ser baseado em requisitos legais, regulamentares (ex: normas do Conselho Federal de Medicina sobre guarda de prontuários) e contratuais.

O método de descarte deve ser proporcional ao nível de classificação e ao impacto potencial de vazamento.

Nível de Classificação	Requisito de Retenção e Descarte	Método de Descarte
PÚBLICA	Descarte quando não houver valor histórico ou legal.	Eliminação Lógica Padrão (para mídias digitais); Reciclagem (para mídias físicas).
INTERNA	Definido pelo Proprietário da Informação, respeitando o ciclo de vida da informação.	Eliminação Lógica Padrão (para mídias digitais); Descarte seguro que impeça leitura superficial (mídias físicas).
RESTRITA	Retenção conforme determinação legal ou regulatória específica (ex: 5 anos, se	Descarte deve ser rastreável e controlado. Recomenda-se trituração ou

	aplicável a contextos de sigilo legal).	incineração (físico); Eliminação Lógica com verificação de não recuperabilidade (digital).
CONFIDENCIAL	Período de retenção rigoroso, determinado pela legislação de saúde e LGPD.	Deve ser utilizado o método de descarte mais seguro: Trituração física segura (para prontuários e exames impressos) ou Wipe Criptográfico/Sanitização de Mídia (para mídias digitais e discos) que impossibilite a recuperação dos dados, devendo haver registro (log) e cadeia de custódia do processo de descarte.

5. Auditoria e Conformidade

A Equipe de Segurança da Informação do hospital é responsável por monitorar e auditar o cumprimento desta Política, visando avaliar a eficácia e a eficiência dos controles de segurança.

5.1. Manutenção de Evidências

a) A equipe de segurança deve manter registros (logs) e evidências que assegurem a rastreabilidade e não repúdio das ações realizadas sobre informações classificadas.

b) As evidências incluem a manutenção de uma cadeia de custódia de prontuários e dados de pacientes, registros de acesso e modificação, e registros de auditoria e logs de segurança.

c) Devem ser realizadas amostragens periódicas de documentos, mídias e sistemas para verificar a rotulagem e o tratamento.

5.2. Indicadores de Conformidade

O gestor de segurança e o comitê de segurança da informação devem acompanhar indicadores simples para avaliar a eficácia dos controles, como:

a) Percentual de informações/ativos corretamente classificados e rotulados.
b) Número de incidentes de segurança ou vazamentos relacionados à classificação ou rotulagem.
c) Conformidade da retenção e eliminação dos dados CONFIDENCIAIS.
d) Percentual de colaboradores treinados sobre as diretrizes de classificação.

6. Responsabilidades e Penalidades

a) **Proprietários da Informação:** Os gestores de áreas e proprietários de ativos são responsáveis pela correta classificação e garantia da aplicação desta política em suas equipes.
b) **Colaboradores:** Devem seguir as diretrizes de classificação e proteção, reportando imediatamente quaisquer não conformidades ou eventos de segurança.

O não cumprimento desta Política implica em falta grave, podendo resultar em ações disciplinares (advertência, suspensão, rescisão) e/ou processos civis ou criminais, dependendo da natureza e gravidade do vazamento/dano. Para o hospital, a violação de dados do tipo CONFIDENCIAL de pacientes acarreta responsabilidade legal conforme a LGPD.

Histórico de Versões e Alterações				
Versão	Data	Responsável	Tipo de Alteração	Revisor/Aprovador
1	20/10/2025	Igo	Criação da Política	Ageu

Sumário

1. Propósito e Escopo

Esta Política de Gestão de Acessos (PGA) tem como propósito complementar as diretrizes de Segurança da Informação, estabelecendo os mecanismos de controle de identificação, autenticação e autorização para salvaguardar as informações e ativos do Hospital, com o objetivo de proteger os Dados Pessoais Sensíveis e evitar acessos não autorizados que impliquem em risco de perda, destruição ou divulgação indevida.

Esta PGA abrange a gestão de acessos lógicos (sistemas, redes, recursos de TI) e físicos (instalações, salas críticas).

2. Princípios e Modelos de Acesso

O controle de acesso no Hospital será orientado por dois princípios primários e um modelo de gestão:

a) **Princípio do Menor Privilégio (Privilégio Mínimo):** Os usuários terão acesso apenas aos recursos e informações estritamente necessários para o desempenho de suas funções.
b) **Princípio da Necessidade de Conhecimento (Need-to-Know):** O acesso a informações confidenciais e restritas, como prontuários, deve ser configurado apenas quando houver uma necessidade de trabalho identificada e o acesso for aprovado pelo Proprietário da Informação.
c) **Modelo de Acesso Baseado em Funções (RBAC):** O controle de acesso será implementado e mantido com base nas funções/papéis (ou perfis) dos colaboradores.

3. Identificação e Autorização

3.1. Definição de Privilégios

A Equipe de Segurança da Informação, em conjunto com os Proprietários da Informação (Gestores das áreas), é responsável por:

a) Definir os perfis de acesso (privilégios) com base nas tarefas, alinhando-os ao nível de classificação da informação (PÚBLICA, INTERNA, RESTRITA, CONFIDENCIAL) definido na Política de Classificação da Informação (PCI).

b) Elaborar e manter a documentação dos direitos de acesso para cada função dentro do Hospital.

c) Ao conceder acesso a usuários que lidam com Dados Pessoais Sensíveis, limitar estritamente o acesso ao mínimo necessário para cumprir os objetivos essenciais do processamento (Minimização de Dados).

3.2. Contas de Acesso e Provisionamento

A gestão adequada das contas de acesso é fundamental para mitigar riscos e assegurar que apenas usuários autorizados acessem os sistemas. Para isso, aplicam-se as seguintes regras:

a) **Identificador Único:** Cada usuário deve possuir uma identificação (login) exclusiva e única.

b) **Contas de Serviço:** Contas de serviço (necessárias a um procedimento automático) devem ser inventariadas e gerenciadas, sendo utilizada uma credencial específica para este propósito.

c) **Contas Privilegiadas (Administradores):** Usuários com privilégios administrativos devem possuir uma credencial específica e dedicada exclusivamente para a execução de atividades administrativas. Esta credencial privilegiada não deve ser utilizada para atividades gerais como navegação na internet ou e-mail.

d) **Inventário e Revisão:** Um inventário centralizado de todas as contas (usuário, administrativas, de serviço) deve ser estabelecido e mantido atualizado. As contas ativas devem ser validadas periodicamente (ex: a cada 90 dias, conforme sugerido em modelos de boas práticas).

4. Gestão de Credenciais e Autenticação

Esta seção estabelece as diretrizes para a criação, uso e gestão das credenciais de acesso lógico, visando garantir a autenticidade dos usuários e proteger os ativos de informação.

4.1. Controle de Senhas

As diretrizes para senhas devem ser rigorosamente seguidas para minimizar pontos de vulnerabilidade, sendo que as vulnerabilidades de senha são consideradas as principais causadoras de ataques cibernéticos. Sendo assim, ficam estabelecidos os seguintes critérios técnicos e comportamentais para todas as senhas de acesso utilizadas no ambiente corporativo:

a) **Requisitos Mínimos de Força:** A senha de acesso deve ter um tamanho mínimo de 12 (doze) caracteres, composta obrigatoriamente por uma combinação de:
   i) Letras maiúsculas e minúsculas.
   ii) Números.
   iii) Caracteres especiais (ex: !, $, #, %).

b) **Inicialização:** A senha inicial é temporária e deve ser obrigatoriamente alterada no primeiro acesso.

c) **Histórico de Reutilização:** Não é permitido o uso das últimas 3 (três) senhas utilizadas.

d) **Proibições:** É proibido o uso de informações pessoais óbvias (como nomes, datas de nascimento ou informações facilmente acessíveis) na criação de senha. Também não devem ser utilizados termos óbvios como "senha", "usuário", "password" ou "system".

e) **Bloqueio por Tentativas:** A conta de acesso será bloqueada automaticamente após 5 (cinco) tentativas consecutivas de acesso inválido.

f) **Sigilo e Compartilhamento:** O login e a senha são de uso pessoal e intransferível. É proibida sua divulgação ou compartilhamento, sendo o empréstimo de credenciais considerado infração disciplinar grave.

g) **Armazenamento Seguro:** É estritamente proibido manter senhas registradas em arquivos na rede, no computador, em anotações ou qualquer outro meio que comprometa o sigilo.

4.2. Autenticação Multifator (MFA)

O MFA (Autenticação de Multifatores) deve ser implementado para reforçar a autenticação de identidade.

a) **Obrigatoriedade de Uso:** A Autenticação de Multifatores (MFA) deve ser utilizada sempre que possível, sendo obrigatória para:
   i. Acesso remoto via VPN (Rede Virtual Privada). O acesso remoto deve ser controlado por autenticação forte, de preferência com MFA.
   ii. Todas as contas com privilégio administrativo.
   iii. Acesso a todas as aplicações corporativas ou de terceiros hospedadas em fornecedores.

b) **Biometria:** Quando implementada, a conta de acesso biométrico deve ser vinculada a uma conta de acesso lógico (login/senha) para atender os conceitos da MFA. Os dados biométricos devem ser tratados como sigilosos, utilizando preferencialmente criptografia.

5. Desprovisionamento e Revogação (Gestão do Ciclo de Vida do Acesso)

A revogação de acessos deve ser imediata em caso de encerramento de vínculo, para mitigar o risco de acessos indevidos por ex-colaboradores.

Este princípio de remoção imediata se aplica não apenas a desligamentos, mas também a mudanças de função e períodos de inatividade. Sendo assim, o processo de desprovisionamento e revogação seguirá as seguintes regras:

a) **Desligamento e Revogação Imediata:** Os direitos de acesso (lógicos e crachás) devem ser imediatamente removidos ou desabilitados após

o encerramento das atividades, contratos ou desligamento do usuário. O acesso de ex-servidores ou ex-contratados aos sistemas de informação deve ser proibido.

b) **Comunicação Imediata (RH):** A área de Recursos Humanos (RH) é responsável por comunicar imediatamente à área de TI sobre desligamentos, férias, licenças, transferências e modificações no quadro de colaboradores. A TI deve realizar os ajustes ou a desativação do perfil de acesso em até 2 horas após o registro do chamado de desligamento pelo RH.
c) **Movimentação Interna:** Em caso de mudança de função ou setor, os direitos de acesso antigos devem ser imediatamente revogados, e novos acessos concedidos conforme a nova função.
d) **Inatividade:** Contas ativas e sem atividade por mais de 45 (quarenta e cinco) dias poderão ser automaticamente bloqueadas sem aviso prévio. Contas não utilizadas há mais de 180 (cento e oitenta) dias poderão ser canceladas.
e) **Bloqueio de Sessão:** O bloqueio automático de sessão nos ativos de TI deve ser configurado após um período de inatividade preestabelecido (ex: 15 minutos), exigindo nova autenticação para evitar acesso de terceiros a dados confidenciais.
f) **Priorização:** A TI deve priorizar a revogação/desativação de contas com o objetivo de manter dados e logs para possíveis auditorias.

6. Controle de Acesso Físico

A segurança da informação não se limita ao ambiente digital. A proteção dos ativos de informação e da infraestrutura de TI depende diretamente da implementação de controles de acesso físico para proteger os locais onde os dados são armazenados, processados ou acessados.

Para mitigar riscos de intrusão, danos ou acesso indevido a Dados Pessoas Sensíveis (como prontuários em arquivos físicos ou servidores), aplicam-se os seguintes controles:

a) **Perímetros de Segurança:** O Hospital deve definir perímetros de segurança para proteger ambientes e ativos contra acesso físico não autorizado, danos e interferências.
b) **Ambientes Seguros:** Áreas críticas (como Salas de Servidores/CTI, Salas de Arquivo Médico, Farmácia Hospitalar) devem ser protegidas por mecanismos de controle de acesso (fechaduras digitais, biometria, cartões de acesso).
c) **Monitoramento:** Os mecanismos de controle de acesso devem ser monitorados pelo Setor de Segurança.
d) **Acesso de Terceiros:** O acesso a ambientes seguros por fornecedores ou prestadores de serviços será concedido somente para fins específicos e autorizados, devendo ser supervisionado e monitorado.
e) **Logs de Acesso:** O Hospital deve manter um log ou registro físico seguro de todos os acessos aos ativos de informação.

7. Monitoramento, Treinamento e Conformidade

7.1. Monitoramento e Auditoria

A simples implementação de controles de acesso não garante a segurança. É essencial verificar ativamente se esses controles estão sendo utilizados corretamente e se há tentativas de burlá-los. Para isso, o Hospital manterá um processo contínuo de monitoramento e auditoria focado na detecção e resposta a anomalias, com base nas seguintes ações:

a) **Registro de Atividades:** As atividades de acesso dos usuários (lógico e físico) devem ser registradas e monitoradas continuamente para detectar atividades suspeitas ou não autorizadas.

b) **Análise de Logs:** Devem ser realizadas análises dos registros de atividades para identificar padrões incomuns ou atividades suspeitas.
c) **Integração de Sistemas:** Assegurar a integração entre controle de acesso, CFTV (vídeo monitoramento) e sistemas de gestão de RH para uma resposta coordenada a incidentes.

7.2. Treinamento

O fator humano é uma prioridade, visto que muitas falhas ocorrem por descuidos humanos.

a) **Capacitação:** Programas de treinamento e conscientização regulares são obrigatórios, abordando temas como a LGPD, o uso ético de dados clínicos e a confidencialidade.
b) **Engajamento:** O treinamento deve focar na conscientização contínua sobre a importância da segurança, incluindo os riscos e consequências do não cumprimento das políticas de acesso.

8. Responsabilidades e Penalidades

A eficácia dos controles de acesso depende do correto cumprimento desta política por todos os usuários. Sendo assim, ficam estabelecidas as responsabilidades individuais e as consequências administrativas, civis e criminais aplicáveis em caso de descumprimento:

a) **Responsabilidade do Usuário:** O usuário é responsável por todos os acessos realizados através de sua conta, devendo interromper a conexão ou bloquear o equipamento ao se ausentar do local de trabalho.
b) **Incidentes:** Qualquer utilização não autorizada ou tentativa de utilização de credenciais será tratada como um incidente de segurança da informação.

c) **Sanções:** O não cumprimento desta Política implica em falta grave, sendo passível de penalidades (advertências, rescisão contratual) e/ou responsabilidade civil e criminal, conforme a legislação vigente (LGPD).

d) **Suspensão de Serviço:** Em caso de suspeita de quebra da segurança da informação, a Equipe de Segurança da Informação conduzirá a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

Histórico de Versões e Alterações				
Versão	Data	Responsável	Tipo de Alteração	Revisor/Aprovador
1	03/11/2025	Ageu	Criação da Norma	Larissa
2	16/11/2025	Samuel	Detalhamento de procedimentos	Larissa

Sumário

1. Objetivo

Esta Norma tem como objetivo definir as diretrizes, responsabilidades e procedimentos para a execução de backups e a determinação de prazos para a retenção e o descarte seguro dos dados corporativos do Hospital LISA. O cumprimento desta norma busca assegurar a capacidade de recuperação de informações críticas em caso de incidentes, falhas ou desastres, além de garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD), especialmente no tratamento de Dados Pessoais Sensíveis de pacientes.

2. Escopo

Esta norma é aplicável a todos os dados e informações de propriedade do Hospital LISA ou sob sua custódia, em todos os formatos (digitais ou físicos), como por exemplo:

- **a.** Bancos de dados de sistemas de gestão hospitalar (prontuários eletrônicos, agendamentos, faturamento);
- **b.** Servidores de arquivos, aplicações e e-mail;
- **c.** Resultados de exames, laudos e imagens médicas;
- **d.** Configurações de ativos de rede e sistemas.

3. Responsabilidades

- **a.** Área de Tecnologia da Informação (TI):
  - **i.** Elaborar, documentar (o "Plano de Backup"), implementar e gerenciar as rotinas de backup (diárias, semanais, mensais) conforme o definido nesta norma. Este plano deve ser formalmente aprovado pelo Gestor de TI e validado pela Diretoria Executiva.
  - **ii.** Monitorar a execução dos backups, garantindo sua conclusão com sucesso;

iii. Garantir a segurança das mídias de backup, incluindo o armazenamento em local externo (off-site) e o uso de criptografia;
iv. Realizar e documentar testes periódicos de restauração para comprovar a integridade dos dados;
v. Executar o descarte seguro dos dados após o término do período de retenção, conforme autorização.

b. Proprietários da Informação (Gestores de Áreas):
i. Definir, em conjunto com a área de TI e o Encarregado de Dados, os prazos de retenção das informações de sua área, respeitando os requisitos legais, regulatórios e contratuais;
ii. Solicitar formalmente à TI a restauração de dados quando necessário;
iii. Autorizar o descarte de informações que chegaram ao fim de seu ciclo de vida.

c. Todos os Profissionais do Hospital LISA:
i. Assegurar que todos os dados corporativos críticos sejam armazenados nos servidores de rede oficiais (e não em estações de trabalho locais ou dispositivos pessoais), assegurando sua inclusão nas rotinas de backup.

4. Diretrizes de Backup

4.1. Frequência e Tipos de Backup

As rotinas de backup devem seguir uma estratégia que reduza ao mínimo a perda de dados.

a. **Backups Diários:** Devem ser realizados backups de todos os dados críticos e transacionais, como bancos de dados de prontuários eletrônicos.

b. **Backups Semanais:** Devem ser realizadas cópias de segurança completas de todos os servidores e sistemas críticos.
c. **Backups Mensais e Anuais:** Cópias completas devem ser geradas para arquivamento de longo prazo.

4.2. Armazenamento, Mídia e Criptografia

a. **Regra 3-2-1:** A estratégia de backup deve contemplar, no mínimo, 3 (três) cópias dos dados, em 2 (duas) mídias diferentes, e 1 (uma) cópia precisa estar em local externo (off-site). Para o Hospital LISA, este local será um ambiente em nuvem (pública ou privada) que atenda aos seguintes requisitos mínimos de segurança:
    i. O provedor deve possuir contrato que assegure a conformidade com a LGPD.
    ii. O provedor deve possuir certificações de segurança auditáveis, como ISO 27001 e, preferencialmente, conformidade com a HIPAA (padrão de segurança para saúde).
b. **Segurança da Mídia:** O acesso às mídias de backup (fitas, discos ou nuvem) deve ser restrito e controlado pela Área de TI.
c. **Criptografia:** Todas as cópias de backup que contenham Dados Pessoais Sensíveis (dados de pacientes ou colaboradores) devem ser obrigatoriamente criptografadas.

4.3. Testes de Restauração

A efetividade dos backups deve ser comprovada por meio de testes de restauração.

a. **Frequência:** Os testes devem ser realizados em intervalos regulares (no mínimo, semestralmente) e sempre que houver mudanças significativas na infraestrutura.
b. **Documentação:** Todos os testes de restauração devem ser documentados com o detalhamento dos dados restaurados e o tempo de recuperação e os resultados obtidos.

4.4. Monitoramento e Tratamento de Falhas

a. Todas as rotinas de backup, sejam elas bem-sucedidas ou falhas, devem gerar logs automatizados e centralizados, que serão retidos por no mínimo 30 dias.
b. A Área de TI deve analisar ativamente os logs de falhas de backup diariamente.
c. Qualquer falha em um backup de dados críticos (ex: prontuários) deve ser tratada como um incidente de prioridade alta, e a rotina deve ser re-executada manualmente no menor tempo possível.

4.5. Indicadores de Desempenho (KPIs)

Para garantir a eficácia desta norma e facilitar auditorias, a Área de TI manterá os seguintes indicadores de desempenho (KPIs):

a. **Taxa de Sucesso de Backup:** Meta de > 99% dos jobs de backup concluídos com sucesso mensalmente.
b. **Taxa de Sucesso de Restore:** Meta de 100% de sucesso nos testes de restauração (restore) semestrais.
c. **Tempo Objetivo de Recuperação (RTO):** O tempo máximo aceitável para restauração será definido no Plano de Continuidade de Negócios (PCN).

5. Diretrizes de Retenção e Descarte

5.1. Prazos de Retenção

a. **Princípio da Necessidade (LGPD):** Os dados pessoais serão mantidos armazenados apenas pelo período necessário para cumprir as finalidades para as quais foram coletados.
b. **Obrigações Legais:** Os prazos de retenção devem seguir estritamente os requisitos legais e regulatórios do setor de saúde (ex:

normas do Conselho Federal de Medicina, Ministério da Saúde) e outras legislações (tributária, trabalhista).

c. **Tabela de Temporalidade:** O Hospital LISA manterá uma Tabela de Temporalidade que especifica os prazos exatos para cada tipo de dado. A título de exemplo, seguem as diretrizes gerais:
   i. **Prontuários de Pacientes:** Mínimo de 20 (vinte) anos após o último registro
   ii. **Exames (Laudos e Imagens):** Mínimo de 20 (vinte) anos (integrados ao prontuário)
   iii. **Dados Financeiros (Faturamento):** Mínimo de 5 (cinco) anos (Legislação Tributária)
   iv. **Logs de Acesso a Aplicações:** Mínimo de 6 (seis) meses (Marco Civil/LGPD)
   v. **Dados de Colaboradores (RH):** Período definido por legislação trabalhista]

5.2. Descarte Seguro

a. Expirado o período de retenção definido, ou mediante solicitação de eliminação de dados por um titular (conforme Art. 18 da LGPD) os dados devem ser descartados mediante uma solicitação formal de descarte.
b. O descarte deve ser feito por métodos que assegurem a eliminação permanente e irreversível dos dados, impedindo sua recuperação.
c. Rastreabilidade e Evidência de Descarte:
   i. A solicitação de descarte do Proprietário da Informação deve ser formalizada via sistema de chamados (ticket) ou formulário eletrônico com assinatura, servindo como autorização formal.
   ii. A Área de TI deve, após a eliminação segura, anexar ao ticket as evidências do descarte (ex: logs de exclusão do sistema, relatório de wipe da mídia).

iii. Este registro completo (autorização + evidência) deve ser arquivado por, no mínimo, 5 (cinco) anos para fins de auditoria.

6. Disposições Gerais

6.1. Penalidades

O descumprimento desta Norma ou de qualquer dos demais padrões institucionais de Segurança de Informação poderá ser passível de penalidades, tanto na esfera administrativa (advertências, punições administrativas, afastamento) quanto na esfera legal (reparação dos danos), de acordo com a gravidade do ato.

6.2. Revisão da Norma

Este documento será revisado e poderá ser alterado em caso de mudanças de processo, tecnologia, diretrizes institucionais ou da legislação vigente. A revisão deve ocorrer com frequência mínima anual.

Histórico de Versões e Alterações				
Versão	Data	Responsável	Tipo de Alteração	Revisor/Aprovador
1	09/11/2025	Igo	Criação da Política	Samuel

Sumário

1. Objetivo

O objetivo central deste Plano de Continuidade de Negócios (PCN) e Recuperação de Desastres (DRP) é detalhar como o Hospital LISA irá agir em incidentes críticos. Ele fornece as diretrizes e os procedimentos para garantir a continuidade das operações essenciais, colocando em primeiro lugar a segurança do paciente e a proteção dos Dados Pessoais Sensíveis. Nosso propósito é minimizar o impacto de qualquer desastre, assegurando que os processos e sistemas críticos sejam retomados rapidamente e dentro dos prazos aceitáveis.

2. Escopo

Este plano aplica-se a todos os processos, sistemas de informação, dados e infraestruturas (físicas e lógicas) que suportam as operações críticas do Hospital LISA, definidos na Política de Gestão de Acessos (PGA) e na Política de Classificação da Informação (PCI).

Abrange cenários de desastre que incluem, mas não se limitam a:

a. Falhas de infraestrutura (energia, rede, servidores);
b. Ataques cibernéticos (Ransomware, negação de serviço);
c. Desastres naturais ou incidentes físicos (incêndio, inundação);
d. Indisponibilidade de pessoal-chave ou pandemias.

3. Glossário

Para padronizar e facilitar o entendimento dos termos utilizados neste documento, abaixo estão os conceitos relacionados:

Análise de Impacto no Negócio (BIA): Processo que identifica os processos de negócio críticos e os recursos necessários para sua operação, bem como o impacto de uma interrupção.

Plano de Continuidade de Negócios (PCN): Estratégia focada na continuidade dos processos de negócio (incluindo procedimentos manuais) durante uma crise.

Plano de Recuperação de Desastres (DRP): Subconjunto do PCN, focado especificamente na recuperação da infraestrutura e sistemas de Tecnologia da Informação (TI).

Objetivo de Tempo de Recuperação (RTO): O tempo máximo aceitável que um processo ou sistema pode ficar indisponível após um desastre.

Objetivo de Ponto de Recuperação (RPO): A quantidade máxima aceitável de perda de dados medida em tempo (ex: "dados das últimas 4 horas").

Incidente Crítico: Um evento que excede a capacidade de resposta a incidentes padrão e requer a ativação deste plano.

4. Análise de Impacto no Negócio (BIA)

A priorização da recuperação baseia-se na criticidade do processo para a vida do paciente e para a operação do hospital, conforme a classificação de dados "CONFIDENCIAL" e as áreas seguras "críticas".

4.1. Processos Críticos

Os processos são classificados em níveis de prioridade para recuperação:

a. **Prioridade 0 (Crítico - RTO < 1 hora):**
   i. Sistemas de suporte à vida (ex: monitores em CTI e Centro Cirúrgico).
   ii. Sistemas de admissão de emergência (Pronto-Socorro).
   iii. Acesso imediato a Prontuários Eletrônicos para pacientes em atendimento.
   iv. Sistemas da Farmácia Hospitalar (para dispensação de emergência).
b. **Prioridade 1 (Alta - RTO < 4 horas):**

i. Sistemas de Prontuário Eletrônico - funcionalidade completa.
ii. Sistemas de Laudos e Imagens Médicas.
iii. Sistemas de agendamento cirúrgico.
iv. Infraestrutura de rede e servidores principais.

c. **Prioridade 2 (Média - RTO < 24 horas):**
   i. Sistemas de Faturamento e Contas.
   ii. Sistemas de agendamento de consultas.
   iii. Servidores de arquivos e e-mail corporativo.
d. **Prioridade 3 (Baixa - RTO < 72 horas):**
   i. Sistemas de Recursos Humanos (RH).
   ii. Sistemas administrativos não assistenciais.

4.2. Aceitação de Riscos Residuais

A aceitação de riscos residuais poderá ocorrer quando a recuperação dentro do RTO não for possível ou viável. Toda exceção deve ser formalizada com justificativa, impacto e período de validade, e aprovada conforme a autoridade definida no item 4.3.

4.3. Autoridade de Aprovação

a. **Prioridade 0 e 1:** Somente a Diretoria Executiva, após parecer técnico da Área de TI e Segurança da Informação.
b. **Prioridade 2:** Aprovação da Diretoria Administrativa, com análise técnica da Área de TI.
c. **Prioridade 3:** A aceitação poderá ser aprovada pela Gestão de TI, com ciência da Diretoria Administrativa, dada a menor criticidade e tolerância ampliada à indisponibilidade.

Prioridade	RTO (Tempo de Recuperação)	RPO (Perda de Dados)
Prioridade 0	< 1 Hora	< 15 Minutos (Replicado)
Prioridade 1	< 4 Horas	< 24 Horas (Backup Diário)
Prioridade 2	< 24 Horas	< 24 Horas (Backup Diário)
Prioridade 3	< 72 Horas	< 48 Horas

5. Estratégias de Continuidade e Recuperação

5.1. Continuidade de Processos

Caso os sistemas de TI (Prioridade 0 e 1) fiquem indisponíveis, os seguintes procedimentos manuais de contingência devem ser adotados pelos Gestores da Informação:

a. **Prontuários e Atendimento:** Utilização de formulários de contingência (papel) pré-impressos e armazenados nas áreas de atendimento (Enfermarias, CTI, Pronto-Socorro). Os registros deverão ser inseridos no sistema assim que este for restabelecido.
b. **Dispensação de Medicamentos:** A Farmácia Hospitalar utilizará controles manuais (livro de atas ou formulários) para registro de entrada e saída de medicamentos, com base em prescrições físicas assinadas.
c. **Laudos e Exames:** Os equipamentos de diagnóstico (ex: Tomografia, Raio-X) que funcionam de forma independente do sistema central devem salvar os exames localmente. Os laudos serão emitidos em formulários de contingência.

d. **Infraestrutura Física:** Em caso de falha no Data Center principal, os serviços essenciais serão migrados para o local de recuperação.

5.2. Recuperação de Desastres de TI (DRP)

A recuperação da infraestrutura de TI seguirá a estratégia definida na Norma D.NBRD.TI.01:

a. **Declaração de Desastre:** A Área de Segurança da Informação, após aprovação da Diretoria Executiva, declara o desastre de TI.
b. **Ativação do Ambiente de DR:** A recuperação dos sistemas será priorizada no "ambiente em nuvem seguro" (local externo), conforme a estratégia 3-2-1 de backup.
c. **Restauração:** A Área de TI iniciará a restauração dos sistemas a partir das cópias de backup (diárias, semanais), seguindo a ordem de prioridade definida na BIA.
d. **Segurança:** Todas as cópias de backup de dados sensíveis de pacientes são criptografadas, garantindo a confidencialidade durante a restauração.
e. **Validação:** A Área de TI e os Gestores da Informação (Proprietários) validarão a integridade dos dados e o funcionamento dos sistemas restaurados antes de liberar o acesso aos usuários.

6. Ativação do Plano e Gerenciamento de Crise

A eficácia do plano depende de uma estrutura de resposta clara, sabendo quando ativar o plano e quem é responsável por cada ação.

6.1. Critérios de Ativação

Este plano deve ser ativado pela Diretoria Executiva ou pela Área de Segurança da Informação quando um incidente crítico:

a. Ameaçar a segurança ou a vida de pacientes e colaboradores;
b. Causar a indisponibilidade dos processos de Prioridade 0 ou 1 por um tempo superior a 30 minutos;
c. Resultar na perda ou inacessibilidade do Data Center principal ou da Sala de Arquivos Médicos.

6.2. Estrutura de Resposta (Equipes)

Uma vez que o plano é ativado, a seguinte estrutura de comando e controle é estabelecida:

a. **Comitê de Gerenciamento de Crise:**
    i. **Líder:** Membro da Diretoria Executiva.
    ii. **Membros:** Líderes da Área de Segurança da Informação, TI, Encarregado de Dados (DPO), RH e Gestores das áreas de negócio afetadas.
    iii. **Responsabilidade:** Tomada de decisão estratégica, alocação de recursos e comunicação externa.
b. **Equipe de Recuperação de TI (DRP):**
    i. **Líder:** Gestor da Área de TI / Segurança da Informação.
    ii. **Responsabilidade:** Executar os procedimentos técnicos de restauração (Seção 5.2), gerenciar o ambiente de DR e restaurar a conectividade.
c. **Equipes de Continuidade Operacional:**
    i. **Líder:** Gestores de cada área de negócio (ex: Diretor Clínico, Gerente de Enfermagem).
    ii. **Responsabilidade:** Implementar os procedimentos manuais de contingência (Seção 5.1), gerenciar a equipe da área e garantir o atendimento mínimo ao paciente.

6.3. Comunicação de Crise

A gestão da informação durante a crise é fundamental para manter a ordem e a confiança. A comunicação será segmentada da seguinte forma:

a. **Comunicação Interna:** A Área de Recursos Humanos será responsável por manter os colaboradores informados sobre o status da crise, locais seguros e instruções de trabalho.
b. **Comunicação Externa (Pacientes e Imprensa):** O Comitê de Gerenciamento de Crise definirá a comunicação oficial, visando a transparência e a calma.
c. **Comunicação Regulatória:** Em caso de incidente de segurança que afete Dados Pessoais Sensíveis, o Encarregado (DPO), em conjunto com a área de Segurança da Informação, avaliará a necessidade e realizará a comunicação à Autoridade Nacional de Proteção de Dados.

7. Testes e Manutenção do Plano

Para garantir a eficácia deste plano, conforme exigido pela PSI e pela NBRD, serão realizados:

a. **Testes de Recuperação de Desastres (DRP):** A Área de TI deve realizar testes de restauração de dados com frequência mínima semestral, para validar os backups e o tempo de recuperação (RTO). Todos os testes devem ser documentados.
b. **Testes de Continuidade de Negócios:** O Comitê de Gerenciamento de Crise deve coordenar, no mínimo anualmente, um exercício simulado ("Tabletop" ou "Walk-through") envolvendo os Gestores de Área para validar os procedimentos manuais.
c. **Revisão do Plano:** Este documento deve ser revisado anualmente ou sempre que ocorrerem mudanças significativas na infraestrutura, processos ou após um incidente real.

8. Disposições Gerais

O não cumprimento das diretrizes estabelecidas neste Plano por parte dos colaboradores, especialmente das Equipes de Resposta designadas, será considerado uma falha grave de segurança.

Após a devida apuração, o descumprimento estará sujeito às penalidades administrativas e legais cabíveis, conforme a gravidade do ato e o impacto gerado à segurança dos pacientes ou à integridade dos dados do Hospital LISA.

Este plano considera as diretrizes das normas ISO 22301:2019 e ISO/IEC 27031:2011 como referência técnica para estruturação das estratégias de continuidade e recuperação.

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

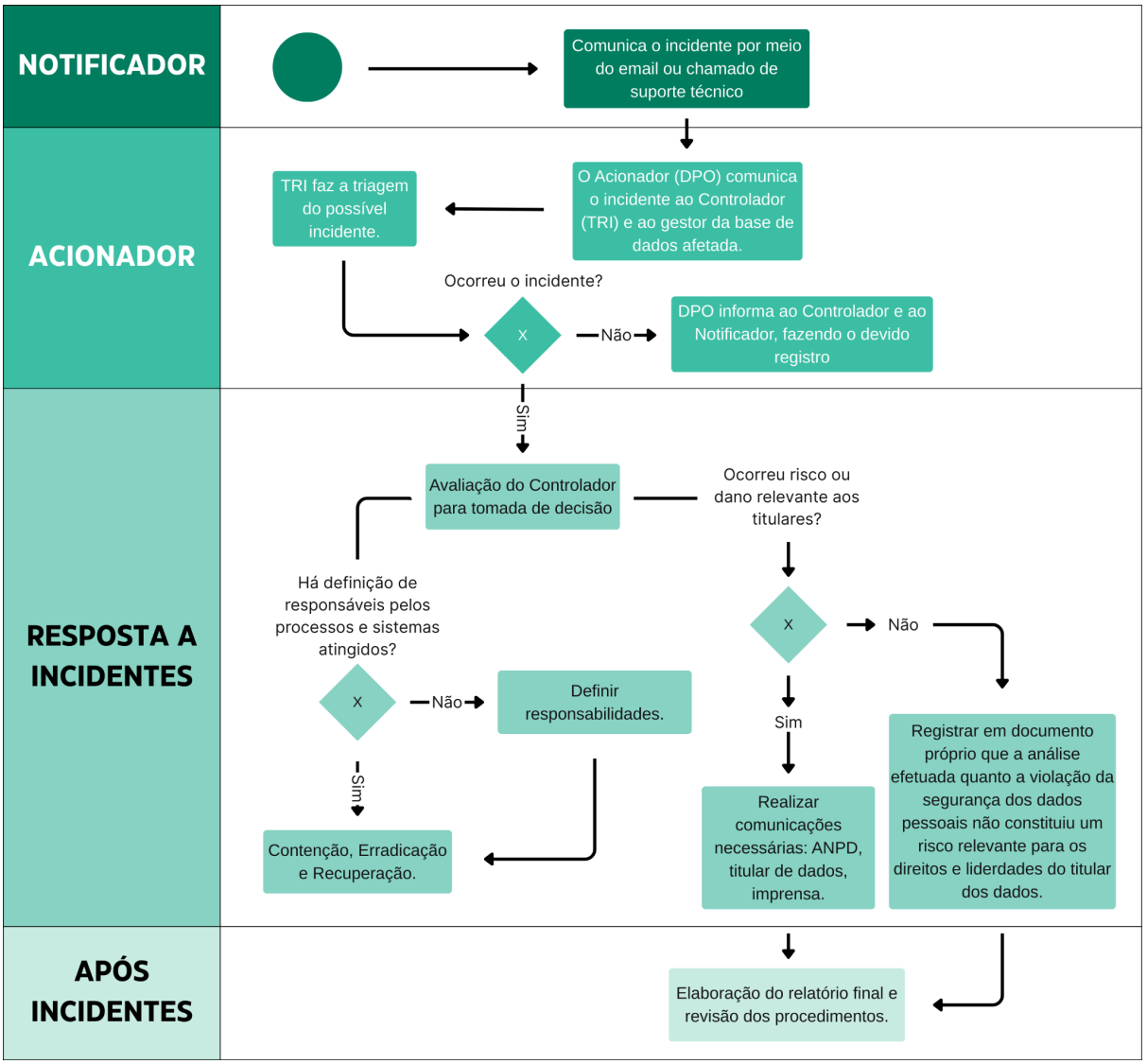
Após a normalização dos serviços, o TRI deve conduzir uma reunião de "Lições Aprendidas" com os Gestores da Informação envolvidos. O objetivo é discutir o que funcionou, o que falhou e propor melhorias para este Plano de Resposta a Incidentes e para as demais políticas de segurança.

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.

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

Sumário

1. Objetivo

O objetivo deste procedimento é estabelecer um processo técnico e operacional padrão para garantir o inventário, a instalação segura, a atualização (patching) e o descomissionamento de todos os dispositivos médicos conectados (IoMT) à rede do Hospital LISA.

Este processo visa proteger a segurança do paciente, a confidencialidade, integridade e disponibilidade dos dados, especialmente Dados Pessoais Sensíveis de saúde e a estabilidade da rede.

2. Escopo

Este procedimento se aplica a todos os dispositivos médicos que possuem capacidade de conexão de rede (com ou sem fio) e que interagem com pacientes ou Dados Pessoais Sensíveis de pacientes.

a. **Inclui:** Bombas de infusão, monitores de sinais vitais, ventiladores, máquinas de Raio-X digital, Tomografia, Ressonância Magnética e carrinhos de telemedicina.
b. **Exclui:** Estações de trabalho padrão ou dispositivos pessoais e ativos que não se conectam à rede.

3. Responsabilidades

A segurança do IoMT requer uma estrutura de responsabilidade compartilhada:

Área	Atribuição no Ciclo de Vida do IoMT
Engenharia Clínica	Proprietária do dispositivo (hardware). Lidera a aquisição, manutenção, calibração, contato com o fornecedor e o processo de descomissionamento.

Equipe de TI (Infraestrutura)	Custodiante da Informação. Gerencia a configuração da rede (VLAN, Wi-Fi, firewall) e o gerenciamento técnico do inventário (CMDB).
Equipe de Segurança da Informação (SI)	Define os requisitos de segurança, realiza a análise de risco, audita a configuração e lidera o monitoramento e a resposta a incidentes de segurança.
Equipe Clínica/Assistencial	Usuário Final. Responsável pelo uso correto do equipamento e por reportar imediatamente qualquer anomalia ou mau funcionamento à SI e à Engenharia Clínica.

4. Fases do Procedimento

4.1. Fase 1: Aquisição e Avaliação de Risco

Esta fase é crucial, pois define o risco que o hospital aceita gerenciar.

a. A Engenharia Clínica deve envolver a Equipe de SI no planejamento de qualquer nova aquisição de equipamento conectado.

b. A Equipe de SI deve solicitar e analisar um Questionário de Segurança do Fabricante. Este documento é usado para avaliar a capacidade do dispositivo de cumprir os requisitos de segurança do hospital.

c. A SI deve usar este questionário para verificar:

i. Se o dispositivo armazena Dados Pessoais Sensíveis, o que aumenta a criticidade da Fase 4 (Sanitização).

ii. A disponibilidade e o processo de atualizações de segurança (patches).

iii. O Sistema Operacional utilizado (para identificar o risco de se tornar legado ou sem suporte do fabricante).

d. É vedada a aquisição de dispositivos cuja senha de administrador ou serviço de fábrica não possa ser alterada.

e. Além do previamente citado, passam a ser requisitos mínimos no contrato de compra:

i. Garantia de suporte contínuo e atualizações de segurança durante todo o ciclo de vida útil do equipamento

ii. Definição de Acordo de Nível de Serviço (SLA) com prazos máximos para a disponibilização de correções (*patches*) após a identificação de uma vulnerabilidade;

iii. Obrigação de divulgação responsável e notificação proativa ao Hospital LISA sobre quaisquer vulnerabilidades identificadas no produto;

iv. Obrigatoriedade de fornecimento do questionário de segurança do fabricante devidamente preenchido antes da aquisição;

v. Existência de um plano formal de *recall* para recolhimento ou substituição do equipamento em casos de falhas críticas de segurança que não possam ser mitigadas remotamente;

vi. Garantia de que o dispositivo opera corretamente em conformidade com os controles de segurança da rede hospitalar (segmentação de VLANs, firewall, etc.).

vii. Exigência de apresentação de documentos técnicos que comprovem a segurança do produto, incluindo relatórios de testes de intrusão (*Pentest*), lista de componentes de software (*SBOM*) e política de ciclo de vida (*Lifecycle Policy*).

4.2. Fase 2: Instalação e Onboarding

a. **Inventário e Registro:** Nenhum dispositivo pode ser conectado à rede sem antes ser cadastrado no CMDB (inventário central) pela TI, conforme exigido pela PGA.
b. **Troca de Credenciais:** No momento da instalação, o técnico (Engenharia Clínica ou TI) deve alterar todas as senhas padrão de fábrica para credenciais complexas, conforme os Requisitos Mínimos de Força (mínimo de 12 caracteres, alfanuméricos e especiais) da PUA e PGA. As senhas devem ser gerenciadas em um cofre de senhas do hospital.
c. **Segmentação de Rede:** Esta é a ação mais importante para proteger os ativos.
    i. **VLAN Específica:** O dispositivo deve ser colocado em uma Rede Virtual (VLAN) específica: "VLAN_IOMT".
    ii. **Regras de Firewall Estritas:** O firewall deve impor as seguintes restrições, garantindo o Princípio do Menor Privilégio:
        - Proibido acesso direto de saída à Internet.
        - Proibido acesso à rede administrativa (RH, Financeiro) e à rede de visitantes (Wi-Fi de Pacientes).
        - Permitido acesso apenas aos servidores e portas específicos que o dispositivo precisa para operar.
d. **Desativação de Serviços:** O técnico de TI deve desabilitar quaisquer serviços de gerenciamento inseguros (ex: Telnet, FTP, SMBv1) no dispositivo.

4.3. Fase 3: Operação e Manutenção

a. **Monitoramento Ativo (Detecção):** A Equipe de SI deve monitorar o tráfego da "VLAN_IOMT" em busca de comportamento anômalo.
b. **Gerenciamento de *Patches* (Resposta):**
    i. **Monitoramento:** A Engenharia Clínica é responsável por monitorar os boletins de segurança dos fornecedores.

ii. **Homologação:** Nenhum *patch* pode ser aplicado diretamente em produção. Ele deve ser testado em um dispositivo de homologação (reserva) para garantir que a atualização não afete a funcionalidade clínica.

iii. **Janela de Manutenção:** A atualização de dispositivos em uso (Prioridade 0 e 1, conforme o PCNDRP) só pode ocorrer em janelas de manutenção programadas e aprovadas pela chefia do setor, garantindo a disponibilidade de um dispositivo de backup.

iv. **SLA de Correção:** A aplicação de patches deve respeitar a criticidade da vulnerabilidade, contada a partir da disponibilização pelo fabricante:

- **Crítica/Urgente** (Exploit público/Risco iminente): Aplicar em até 7 dias.
- **Alta:** Aplicar em até 30 dias.
- **Média/Baixa:** Aplicar em até 90 dias ou na próxima manutenção preventiva.

v. **Gestão de Exceção:** Caso não seja possível aplicar o patch no prazo (ex: risco operacional alto ou incompatibilidade), deve-se abrir um processo formal de Aceite de Risco, documentando os controles compensatórios adotados.

c. **Controle Compensatório para Legados:** Para dispositivos "incorrigíveis" (que rodam em SOs obsoletos ou sem *patch*), a SI deve implementar:

i. **Isolamento de Rede:** Garantir que o dispositivo permaneça na VLAN_IOMT com o mínimo de acesso possível.

ii. ***Virtual Patching*** **(Patch Virtual):** Aplicar políticas de segurança (regras/assinaturas) em um Sistema de Prevenção de Intrusão (IPS) ou Firewall. O IPS/Firewall intercepta o tráfego malicioso *antes* que ele chegue ao dispositivo vulnerável, mitigando o risco sem necessidade de aplicar o *patch* no dispositivo.

4.4. Fase 4: Descomissionamento

a. **Sanitização de Dados:** O dispositivo não pode sair do controle do hospital (para lixo, revenda ou devolução) antes que a TI realize a sanitização de todos os dados de paciente armazenados nele, conforme a LGPD.
b. **Padrão de Descarte:** A TI deve seguir métodos padronizados para garantir a eliminação dos dados, variando conforme o destino do ativo:
    i. **Reutilização Interna:** Método *Clear* (ex: redefinição de fábrica) é aceitável.
    ii. **Revenda ou Devolução:** Método *Purge* (ex: formatação de baixo nível ou *ATA Secure Erase*) é o mínimo obrigatório para garantir que a recuperação dos dados seja inviável.
    iii. **Descarte (Lixo):** Método *Destroy* (ex: trituração física ou incineração da mídia de armazenamento) é obrigatório.
c. **Registro:** Deve haver um registro (log) e cadeia de custódia do processo de sanitização e descarte para fins de auditoria.
d. **Remoção de Acesso:** A TI deve remover o dispositivo do inventário (CMDB), desativar sua porta de rede e revogar suas credenciais de acesso imediatamente.

5. Auditoria e Monitoramento

A Equipe de Segurança da Informação (SI) deve monitorar ativamente o cumprimento deste procedimento, focando especificamente nos riscos únicos dos dispositivos médicos conectados. As auditorias devem incluir:

a. **Auditoria de Rede (Trimestral):** Varreduras ativas da rede para confirmar que todos os dispositivos IoMT identificados estão corretamente isolados na "VLAN_IOMT" e procurar por dispositivos não catalogados conectados indevidamente.

b. **Auditoria de Credenciais (Contínua):** Monitoramento para identificar dispositivos IoMT que ainda utilizam senhas de fábrica ou serviços inseguros (ex: Telnet).
c. **Auditoria de Inventário (Semestral):** Cruzamento do inventário da Engenharia Clínica com o CMDB da TI para validar o status do ciclo de vida (em operação, em manutenção, descomissionado) de todos os ativos IoMT.
d. **Auditoria de Descarte (Por Demanda):** Verificação dos registros de sanitização sempre que um dispositivo médico for descomissionado, garantindo que nenhum dado de paciente saia do hospital.

6. Revisão e Manutenção

Este procedimento deve ser revisado anualmente ou sempre que:

a. Uma nova categoria de dispositivo médico (ex: novas bombas de infusão inteligentes, scanners portáteis) for adquirida pelo hospital.
b. Um incidente de segurança global relevante para IoMT (ex: uma nova vulnerabilidade em um sistema operacional embarcado) for divulgado.
c. Ocorrer uma mudança significativa na arquitetura da rede hospitalar.