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....2
2. Escopo....2
3. Glossário....2
4. Descrição....4
4.1. Princípios de Segurança da Informação....4
4.2. Diretrizes de Segurança da Informação....5
4.3. Responsabilidades e Atribuições....5
4.3.1. Diretoria Executiva....6
4.3.2. Área da segurança da informação....6
4.3.3. Área de privacidade e proteção de dados....8
4.3.4. Área dos recursos humanos....9
4.3.5. Gestores da informação....9
4.3.6. Profissionais do Hospital LISA....10
5. Disposições Gerais....10
5.1. Descumprimento dos padrões institucionais de Segurança da Informação....10
5.2. Atualização desta política....11

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.