

POLÍTICA INSTITUCIONAL DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS

INSTITUTO DE CIÊNCIAS MÉDICAS CANAÃ

1. Apresentação e Escopo

Esta Política estabelece as diretrizes de Segurança da Informação e de Proteção de Dados Pessoais do Instituto de Ciências Médicas Canaã (Instituto Canaã), organização privada sem fins lucrativos qualificada como Organização Social (OS) nos termos da Lei nº 9.637/1998, dedicada à gestão de serviços públicos de saúde.

As normas aqui descritas aplicam-se a todas as unidades, departamentos, projetos, colaboradores, prestadores de serviços, fornecedores e parceiros que tenham acesso aos ativos de informação da instituição. Isso engloba hospitais, unidades de pronto atendimento (UPAs), unidades básicas de saúde (UBSs), centros de especialidades, centrais de regulação, farmácias públicas, áreas administrativas e todos os ambientes físicos e tecnológicos sob gestão do Instituto.

O escopo abrange qualquer formato ou suporte de informação — seja físico, digital, eletrônico ou em nuvem —, incluindo prontuários eletrônicos, registros clínicos, dados cadastrais e informações financeiras ou estratégicas.

2. Nosso Compromisso Institucional

O Instituto Canaã reconhece a informação como um ativo fundamental para prestar serviços de saúde com qualidade, segurança, eficiência e total respeito aos direitos dos cidadãos. A instituição compromete-se a zelar pelas seguintes propriedades de segurança:

- **Confidencialidade:** garantia de acesso restrito apenas a pessoas autorizadas;
- **Integridade:** proteção da exatidão e completude dos dados e métodos de processamento;
- **Disponibilidade:** assegurar que usuários autorizados acessem a informação sempre que necessário;
- **Autenticidade:** garantia de que a informação provém de fonte legítima;
- **Rastreabilidade:** capacidade de acompanhar a origem, as modificações e o ciclo de vida dos dados.

3. Fundamento Legal e Normativo

Esta Política fundamenta-se nas leis brasileiras e em normas técnicas aplicáveis, destacando-se a Constituição Federal de 1988, a Lei das Organizações Sociais (Lei nº 9.637/1998), a Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/2018), a Lei de Acesso à Informação - LAI (Lei nº 12.527/2011), a Lei Orgânica da Saúde (Lei nº 8.080/1990), além de resoluções do Conselho Federal de Medicina (CFM), normas ISO/IEC 27001 e 27002, e

diretrizes do SUS e da ANVISA.

4. Conceitos Básicos

Para facilitar a compreensão desta Política, consideram-se os seguintes conceitos:

- **Ativo de Informação:** qualquer recurso de valor para a instituição que armazene, processe ou transmita dados.
- **Dado Pessoal:** informação relacionada a uma pessoa natural identificada ou identificável.
- **Dado Pessoal Sensível:** dado sobre origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, genética ou biometria.
- **DPO (Data Protection Officer):** o encarregado pelo tratamento de dados pessoais, responsável pela comunicação entre a instituição, os titulares e a ANPD.
- **Incidente de Segurança:** evento adverso que comprometa a confidencialidade, a integridade ou a disponibilidade das informações.
- **Prontuário Eletrônico do Paciente (PEP):** sistema informatizado para registro de informações clínicas e administrativas do paciente.
- **Tratamento de Dados:** qualquer operação realizada com dados pessoais, como coleta, uso, armazenamento, transmissão ou eliminação.

5. Governança da Segurança da Informação

A gestão da segurança da informação integra a governança corporativa do Instituto Canaã, sendo liderada pela Diretoria Executiva em conjunto com a área de Tecnologia da Informação (TI), o Encarregado de Dados (DPO) e a Auditoria Interna. O DPO atua com independência funcional para orientar colaboradores, atender solicitações de titulares e manter o diálogo com a Autoridade Nacional de Proteção de Dados (ANPD).

6. Princípios e Diretrizes

As atividades do Instituto fundamentam-se na confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, transparência, responsabilização, gestão de riscos, melhoria contínua e conformidade legal. No tratamento de dados pessoais, observam-se estritamente os princípios da LGPD, como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, segurança, prevenção e não discriminação.

7. Classificação e Ciclo de Vida da Informação

As informações institucionais são classificadas em quatro níveis de sensibilidade: **Público** (livre acesso), **Interno** (uso exclusivo da instituição), **Confidencial** (cujo acesso não autorizado pode gerar danos) e **Restrito** (alta sensibilidade, como dados de saúde e prontuários). O ciclo de vida da informação compreende desde a sua criação até o descarte seguro, que deve impedir qualquer forma de recuperação indevida.

8. Proteção de Dados Pessoais e Dados Sensíveis

O tratamento de dados pessoais e de saúde ocorre de forma ética e lícita. O uso de dados sensíveis de saúde restringe-se às hipóteses legais da LGPD, tais como o consentimento específico do titular, tutela da saúde, execução de contratos, exercício regular de direitos ou proteção da vida. O Instituto mantém um Registro de Operações de Tratamento (ROT) para documentar essas atividades.

9. Direitos dos Titulares de Dados

Os titulares de dados possuem o direito de confirmar a existência de tratamento, acessar seus dados, solicitar correção de informações desatualizadas, requerer anonimização ou eliminação de dados desnecessários, portabilidade, revogação de consentimento e esclarecimentos sobre o compartilhamento. As solicitações são atendidas pelo DPO no prazo máximo de 15 dias.

10. Controles Técnicos e Administrativos

Para mitigar riscos, o Instituto adota rigorosos controles de acesso baseados no princípio do menor privilégio, senhas robustas e autenticação multifator (MFA). A infraestrutura conta com segmentação de redes, firewalls, criptografia de dados em trânsito e em repouso (especialmente nos prontuários eletrônicos), backups regulares, monitoramento de eventos de segurança e controles de segurança física nas instalações.

11. Gestão de Incidentes de Segurança

Qualquer anomalia ou suspeita de violação deve ser comunicada imediatamente à TI ou ao DPO. O Instituto adota um fluxo formal de resposta a incidentes que inclui contenção, erradicação, análise de causa e recuperação. Incidentes que envolvam riscos relevantes a dados pessoais serão comunicados à ANPD e aos titulares afetados nos prazos previstos em lei.

12. Transparência Ativa e Prestação de Contas

Em consonância com a Lei de Acesso à Informação (LAI) e o perfil de Organização Social, o Instituto disponibiliza em seu Portal da Transparency informações institucionais, relatórios de gestão, demonstrações contábeis auditadas e dados de desempenho em saúde, mantendo o equilíbrio necessário entre o controle social e o sigilo legal.

13. Conscientização e Cultura de Segurança

O Instituto promove treinamentos contínuos, simulações de segurança e campanhas educativas para engajar todos os colaboradores na preservação da privacidade e da segurança da informação, integrando essa cultura aos processos institucionais.

14. Responsabilidades e Sanções

A segurança da informação é uma responsabilidade compartilhada por toda a cadeia institucional. O descumprimento das normas desta Política sujeita os infratores a medidas

disciplinares, administrativas, civis e criminais, variando de advertências à rescisão contratual e responsabilização legal.

15. Disposições Finais e Vigência

Esta Política entra em vigor na data de sua aprovação. Regulamentos complementares serão detalhados em até 90 dias, e o documento passará por revisões periódicas anuais para garantir sua constante atualização frente às demandas legais e tecnológicas.

Mensagem Institucional

"Proteger a informação é proteger pessoas."

No **Instituto de Ciências Médicas Canaã**, a segurança da informação, a proteção de dados pessoais e a transparência são pilares da nossa governança e refletem o compromisso permanente com a excelência na gestão da saúde pública, a integridade institucional e o fortalecimento do Sistema Único de Saúde — o SUS.

São Paulo, 10 de fevereiro de 2026.

Michelle Aparecida Pereira Nistico

Presidente do Conselho de Administração do Instituto de Ciências Médicas Canaã

Documento aprovado em Assembleia Geral do Instituto de Ciências Médicas Canaã, realizada em 10/02/2026 — Assembleia Geral Ordinária nº 01/2026.

