

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Controle de versão:

Data de Criação: 15/04/2026

Última atualização: 15/04/2026

DPO: Wellington Luiz Barbosa Junior

1. Objetivo

A presente Política de Segurança da Informação tem como objetivo estabelecer diretrizes para a proteção das informações do Instituto Dédalus de Psicanálise e Terapias, garantindo sua confidencialidade, integridade e disponibilidade, em conformidade com a legislação vigente e boas práticas de governança.

2. Escopo

Esta Política aplica-se a:

- a) Colaboradores, professores e prestadores de serviço;
- b) Alunos e profissionais vinculados ao Instituto;
- c) Usuários de sistemas e plataformas digitais;
- d) Terceiros que tenham acesso a informações institucionais.

Abrange todas as informações geradas, processadas, armazenadas ou transmitidas no âmbito do Instituto, incluindo dados acadêmicos, administrativos e clínicos.

3. Princípios de Segurança da Informação

O Instituto Dédalus adota os seguintes princípios:

- a) Confidencialidade: acesso restrito às informações apenas a pessoas autorizadas;
- b) Integridade: garantia de exatidão e completude das informações;
- c) Disponibilidade: acesso às informações quando necessário;
- d) Responsabilização: identificação clara de responsabilidades no uso e tratamento das informações.

4. Classificação da Informação

O Instituto Dédalus adota um modelo de classificação da informação com o objetivo de assegurar níveis adequados de proteção, conforme a sensibilidade dos dados.

As informações são classificadas nas seguintes categorias:

- a) Pública: informações que podem ser divulgadas sem restrição;
- b) Interna: informações de uso restrito ao ambiente institucional;
- c) Confidencial: informações sensíveis, cujo acesso deve ser limitado;
- d) Restrita: informações críticas, incluindo dados pessoais sensíveis e dados clínicos.

A classificação deve ser aplicada no momento da criação ou recebimento da informação, sendo responsabilidade de quem a gera ou a manipula.

5. Controle de Acesso e Perfis de Usuários

O acesso às informações e sistemas do Instituto Dédalus é controlado com base no princípio do menor privilégio.

O Instituto estabelece perfis de usuários, definidos conforme função e necessidade de acesso, incluindo:

- 1. Perfis administrativos;
- 2. Perfis acadêmicos;
- 3. Perfis clínicos; 4. Perfis técnicos.

Cada usuário terá acesso apenas às informações estritamente necessárias ao desempenho de suas atividades.

O acesso será concedido mediante autenticação individual, sendo proibido o compartilhamento de credenciais.

6. Uso de Sistemas e Recursos Tecnológicos

Os sistemas e recursos tecnológicos do Instituto devem ser utilizados exclusivamente para fins institucionais.

É vedado:

- a) Compartilhar acessos ou senhas;
- b) Utilizar sistemas para fins ilícitos ou não autorizados;
- c) Armazenar ou transmitir informações institucionais em ambientes não seguros.

O Instituto poderá monitorar o uso de seus sistemas, respeitando a legislação aplicável.

7. Proteção de Dados e Informações Sensíveis

Considerando a natureza de suas atividades, o Instituto Dédalus trata informações sensíveis, especialmente no contexto clínico.

Essas informações devem ser tratadas com nível máximo de proteção, observando:

- a) Sigilo profissional;
- b) Acesso restrito;
- c) Armazenamento seguro;
- d) Conformidade com a LGPD.

8. Armazenamento e Retenção da Informação

As informações devem ser armazenadas em ambientes seguros, físicos ou digitais, com controle de acesso adequado.

O período de retenção observará:

- a) Finalidade do uso;
- b) Obrigações legais;
- c) Necessidade institucional.

Após o prazo, as informações deverão ser eliminadas ou anonimizadas de forma segura.

9. Incidentes de Segurança

Qualquer incidente que comprometa a segurança da informação deve ser imediatamente reportado ao responsável designado.

O Instituto adotará medidas para:

- a) Identificação e contenção do incidente;
- b) Avaliação de impacto;
- c) Mitigação de danos;
- d) Adoção de medidas preventivas.

10. Responsabilidades

Todos os usuários são responsáveis pela proteção das informações às quais têm acesso.

O Instituto, por sua vez, é responsável por:

- a) Definir diretrizes de segurança;
- b) Promover boas práticas;
- c) Garantir mecanismos de controle e proteção.

11. Atualizações da Política

Esta Política poderá ser atualizada a qualquer momento para adequação a mudanças legais, tecnológicas ou institucionais.

12. Disposições Finais

Esta Política entra em vigor na data de sua publicação e permanecerá válida até que nova versão seja oficialmente divulgada.

Assinaturas:



DPO Wellington Luiz Barbosa Junior



Responsável Legal Ana Caracas



Responsável Legal Heráclito Aragão Pinheiro

