

Política de Segurança da Informação (PSI)

Diretrizes técnicas e organizacionais para proteger dados pessoais contra acessos não autorizados e incidentes.

Obrigatório · Novo - revisar · Atualizado: Julho de 2026

Base legal: Art. 46 e Art. 48, LGPD

1. Objetivo e escopo

Controlador: INFO8 DESENVOLVIMENTO DE SISTEMAS E SITE LTDA (INFO8)

CNPJ: 20.251.527/0001-04

Endereço: Rua Jornalista Djalma Andrade, nº 1505, Sala 01, Belvedere, Belo Horizonte/MG, CEP 30.320-595

Plataforma: Doctor8 (app.doctor8.org / doctor8.com.br)

Esta Política de Segurança da Informação (PSI) estabelece diretrizes para proteção dos dados pessoais e dados sensíveis de saúde tratados pela plataforma Doctor8, em conformidade com a LGPD, normas do CFM/CFP aplicáveis à telemedicina e boas práticas de mercado.

Aplica-se a colaboradores, prestadores, operadores contratados e profissionais que utilizam a plataforma.

2. Controles técnicos implementados

- Criptografia: dados de saúde (PHI) criptografados em repouso com AES-256-GCM.
- Controle de acesso: autenticação por login/senha, papéis (RBAC) e segregação por perfil (paciente, profissional, empregador, admin).
- Sessão: timeout automático de 15 minutos de inatividade.
- Proteção de conta: bloqueio após 5 tentativas inválidas de login.
- Auditoria: registro de visualização, criação, alteração, exclusão, compartilhamento e exportação de dados sensíveis.
- Comunicação: HTTPS obrigatório, headers de segurança (CSP, HSTS).
- Arquivos: uploads sem endpoint genérico de leitura por ID (prevenção de IDOR).
- Residência de dados: armazenamento por região da conta (BR, US, EU) quando aplicável.

3. Gestão de credenciais e acessos

Acessos administrativos são restritos ao mínimo necessário. Senhas devem ser pessoais e intransferíveis. Chaves de API, tokens e segredos de produção são armazenados em variáveis de ambiente seguras, nunca em código-fonte.

Profissionais de saúde só acessam prontuários de pacientes vinculados ou com compartilhamento autorizado. Compartilhamentos de prontuário são registrados e podem ser revogados.

4. Backup, continuidade e subprocessadores

Backups e infraestrutura são mantidos em provedores de nuvem com contratos de confidencialidade.

Subprocessadores relevantes: AWS (hospedagem/armazenamento), Daily.co e Google (videoconferência), Stripe (pagamentos), Certillion (assinatura ICP-Brasil).

A INFO8 avalia periodicamente a segurança dos fornecedores críticos e exige cláusulas de proteção de dados

nos contratos.

5. Incidentes e revisão

Incidentes de segurança seguem o Plano de Resposta a Incidentes. Esta PSI é revisada anualmente ou quando houver mudança relevante na arquitetura ou regulamentação.