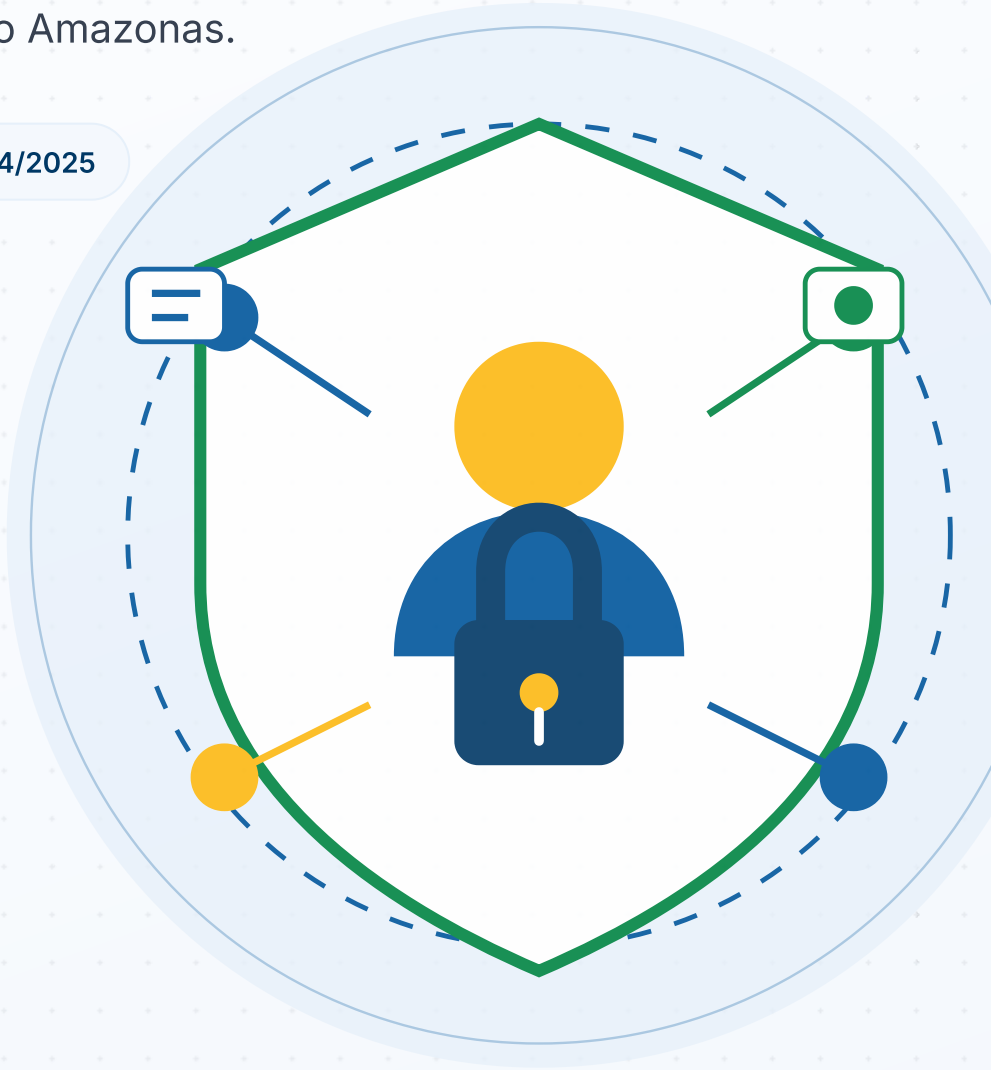
UFAM

17 de Julho
Dia Nacional da Proteção de Dados

Privacidade, confiança e cidadania digital na Universidade Federal do Amazonas.

Instituído pela Lei nº 15.254/2025



Por que a proteção de dados importa para você?

Privacidade | **Segurança** | **Transparência** | **Confiança**

Por que esta data é importante?
A Lei nº 13.709/2018 (LGPD) estabeleceu normas gerais para o tratamento de dados pessoais nos setores público e privado, promovendo maior transparência, segurança jurídica e respeito aos direitos fundamentais. A data celebra essa conquista.

2018

A Lei Geral de Proteção de Dados (LGPD)

Aprovação da legislação que transformou a forma como as instituições brasileiras lidam com a privacidade e o ciclo de vida da informação.

2022

Direito Fundamental Constitucional

A Emenda Constitucional nº 115/2022 incluiu a proteção de dados pessoais no rol de direitos e garantias fundamentais da Constituição Federal (Art. 5º, LXXIX).

2025

Lei nº 15.254 e o Legado de Danilo Doneda

A data de 17 de julho homenageia o jurista Danilo Doneda, um dos principais arquitetos da LGPD, oficializando o dia nacional para fomentar a cultura de privacidade.

Princípios da LGPD

A Universidade Federal do Amazonas trata dados pessoais observando rigorosamente os 10 princípios estabelecidos na Lei:

- ✓ Finalidade
- ✓ Adequação
- ✓ Necessidade
- ✓ Livre acesso
- ✓ Qualidade dos dados
- ✓ Transparência
- ✓ Segurança
- ✓ Prevenção
- ✓ Não discriminação
- ✓ Responsabilização

Você sabia?

Muitas pessoas acreditam que a LGPD existe para impedir o uso de dados pessoais. Na realidade, seu objetivo é garantir que os dados sejam tratados de forma lícita, transparente, segura e apenas quando necessário.

Por isso, o consentimento é apenas uma das bases legais previstas na Lei. Na Administração Pública, diversos tratamentos são realizados legitimamente com fundamento em outras bases, como:

- Obrigação legal ou regulatória
- Execução de políticas públicas
- Execução de contratos
- Proteção da vida/incolumidade
- Tutela da saúde
- Exercício regular de direitos
- Interesse legítimo

Onde os dados estão na UFAM?

Praticamente todas as atividades de Ensino, Pesquisa, Extensão e Administração envolvem o tratamento de dados pessoais. O ciclo de vida do dado está presente em:

- **Matrícula e SIGAA**
  Histórico, notas e cadastros.
- **Biblioteca Central**
  Empréstimos e multas.
- **Saúde (HUGV)**
  Prontuários de pacientes.
- **Cursos de Extensão**
  Comunidade externa.
- **Concursos e RH**
  Folha de ponto e pagamentos.
- **E-mail Institucional**
  Comunicações oficiais.
- **Assistência Estudantil**
  Bolsas e auxílios.
- **Ouvidoria**
  Denúncias e manifestações.
- **Licitações / Contratos**
  Dados de fornecedores.
- **Diplomação / Pós**
  Certificados e titulação.

Pesquisas também seguem a LGPD

Projetos de pesquisa científica que utilizam dados pessoais devem observar a LGPD, as normas éticas aplicáveis e, quando pertinente, as diretrizes do Sistema CEP/CONEP. O pesquisador deve adotar medidas de minimização de dados, garantir a segurança e priorizar a anonimização.

Direitos e Responsabilidades

Direitos do Titular

Como titular (estudante, servidor ou cidadão), o Art. 18 da LGPD assegura:

- ✓ Confirmação da existência de tratamento.
- ✓ Acesso facilitado aos dados.
- ✓ Correção de dados incompletos ou inexatos.
- ✓ Anonimização de dados desnecessários.
- ✓ Bloqueio ou eliminação.
- ✓ Portabilidade dos dados (mediante ANPD).
- ✓ Informação sobre o compartilhamento com entidades.
- ✓ Informação sobre a possibilidade de não fornecer consentimento e consequências.
- ✓ Revogação do consentimento.
- ✓ Revisão de decisões automatizadas.

Responsabilidades

A proteção é dever de todos. No exercício da sua função (servidor/bolsista), você deve:

- ✓ Tratar apenas dados estritamente necessários para sua atribuição.
- ✓ Manter absoluto sigilo sobre dados sensíveis (saúde, raça, biometria).
- ✓ Respeitar a finalidade pela qual o dado foi coletado (não desviar o uso).
- ✓ Seguir rigorosamente as normas internas do CTIC e EPDP.

O Encarregado pelo Tratamento de Dados Pessoais (DPO) atua como canal oficial entre a UFAM, os titulares e a ANPD, mas a proteção ocorre na ponta, na ação diária de cada servidor.

Boas Práticas de Segurança da Informação

Alinhamento Normativo: PPSI 2.0 e Padrões Internacionais

Nossas diretrizes baseiam-se na **ISO/IEC 27001:2022, ISO/IEC 27002, CIS Controls v8, NIST** e no **PPSI 2.0** (Portaria SGD/MGI nº 9.511/2025). O programa protege a instituição estruturando-se em 5 pilares: Governança, Maturidade, Metodologia, Tecnologia e Pessoas, guiado pelo Controle 14 (Conscientização).

Senhas e Acessos

Use senhas fortes com frases-senha longas e fáceis de lembrar, contendo pelo menos 14 caracteres (letras maiúsculas e minúsculas, números e caracteres especiais). Nunca reutilize senhas entre sistemas e jamais compartilhe suas credenciais de e-mails e redes sociais, mesmo com colegas, estagiários, terceirizados ou chefias.

Autenticação Multifator (MFA)

Ative a verificação em múltiplo fator de autenticação (MFA) em duas ou mais etapas a todos os serviços que ofereçam esse recurso, especialmente no e-mail institucional, sistemas administrativos, redes sociais e serviços em nuvem, criando uma camada extra de segurança.

Phishing e Links Suspeitos

Desconfie de mensagens que criem senso de urgência ou solicitem senhas, códigos de autenticação ou dados pessoais. Antes de clicar em links ou abrir anexos, confirme a autenticidade do remetente pelos canais oficiais. O CTIC/UFAM não solicita redefinição de senha por e-mail, SMS, redes sociais ou outros aplicativos de mensagens.

Mesa Limpa e Tela Bloqueada

Sempre que se ausentar do posto de trabalho, bloqueie imediatamente o computador pressionando **(Win + L)** e mantenha documentos físicos sensíveis contendo informações institucionais ou dados pessoais guardados em local seguro.

Compartilhamento Mínimo

Compartilhe apenas as informações estritamente necessárias para a finalidade pretendida, seguindo o princípio do menor privilégio e da necessidade de conhecimento (*Need to Know*), que é um princípio que limita o acesso a dados confidenciais. Ele garante que um colaborador só veja as informações estritamente necessárias para realizar o seu trabalho.

Descarte Seguro

Documentos físicos contendo informações institucionais ou dados pessoais devem ser fragmentados antes do descarte. Arquivos digitais devem ser eliminados conforme os procedimentos institucionais, evitando seu armazenamento desnecessário.

Trabalho Remoto e Dispositivos

Durante o teletrabalho, utilize redes Wi-Fi confiáveis e protegidas por senha, evitando redes públicas. Sempre que disponível, utilize VPN. Mantenha o sistema, navegadores e aplicativos sempre atualizados, utilize antivírus ativo, proteja o dispositivo com senha/biometria e não permita que terceiros utilizem o equipamento. As atualizações corrigem vulnerabilidades. Evite imprimir documentos contendo dados pessoais em ambientes domésticos e assegure o descarte adequado.

Reporte Incidentes

Caso identifique e-mails suspeitos, perda de equipamentos, acesso indevido, vazamento de informações ou qualquer comportamento anormal dos sistemas, comunique imediatamente a equipe responsável pela Segurança da Informação do CTIC, através do canal institucional: **denunciaseginfo@ufam.edu.br**. O reporte rápido e com informações completas reduz impactos e facilita a resposta ao incidente.

Uso Responsável da Inteligência Artificial

Atenção aos dados inseridos em ferramentas de IA

O uso de Inteligência Artificial generativa (como ChatGPT, Gemini, Copilot) traz eficiência, mas apresenta alto risco de vazamento de dados se não for utilizado com cautela. O que você digita lá, pode ser usado para treinar o modelo globalmente.

Antes de submeter textos, ofícios ou planilhas a uma ferramenta de IA aberta, você deve garantir que:

- ✗ Remova CPFs e RGs
- ✗ Remova nomes completos
- ✗ Remova prontuários e laudos médicos
- ✗ Remova números de Matrícula
- ✗ Remova dados bancários/financeiros
- ✗ Remova detalhes de processos sigilosos

- ✓ Utilize versões institucionais, corporativas ou fechadas (quando disponibilizadas).
- ✓ Siga a Política de Segurança da Informação vigente na UFAM.
- ✓ Anonimize os textos. Ex: Troque "João da Silva, aluno de Medicina" por "Aluno A".

A inovação tecnológica deve caminhar lado a lado com a proteção aos direitos fundamentais. Ao integrar IA aos processos da UFAM, a preservação da privacidade da comunidade acadêmica deve ser inegociável.

Fluxo de Incidentes de Segurança

Um incidente ocorre quando há acesso não autorizado, destruição, perda, alteração ou vazamento de dados. **Não tente ocultar falhas.** A transparência e a rapidez na comunicação minimizam os danos. Siga o fluxo institucional:

Privacy by Design

Privacidade desde a concepção. Todo projeto novo (sistemas, pesquisas, licitações, normas) deve considerar a privacidade *antes* de iniciar, e não como um conserto corretivo final.

Segurança Proativa	**Privacidade como Padrão**	**Minimização**
Transparência	**Integração do Ciclo**	**Foco no Usuário**

Proteger dados pessoais
é proteger pessoas.

Uma cultura de privacidade promove confiança e constrói uma **administração pública mais ética, transparente e responsável.**

Portal LGPD da UFAM

Portal da Ouvidoria da UFAM

dadospessoais@ufam.edu.br

Política de Privacidade

Formulário de Exercício de Direitos

Aviso Institucional: Esta cartilha possui caráter educativo e informativo. Seu conteúdo não substitui a Lei nº 13.709/2018 (LGPD), a Lei nº 15.254/2025, normativas internas da Universidade Federal do Amazonas (UFAM) ou orientações formais da Autoridade Nacional de Proteção de Dados (ANPD).

Gabriel Becil Amoêdo da Silva - Encarregado Pelo Tratamento de Dados Pessoais

Escritório de Proteção de Dados Pessoais (EPDP)

Coordenação de Segurança da Informação (CSGINFO)

LGPD • CF/88 • Lei nº 15.254/2025