

PROGRAMA DE COMPLIANCE – LGPD
Lei nº 13.709/2018



1. OBJETIVO

Estabelecer as diretrizes para garantir que a INAB trate dados pessoais de colaboradores, clientes, parceiros e terceiros em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), protegendo a privacidade e minimizando riscos de vazamento ou uso indevido, sem burocratizar excessivamente a operação diária.

2. ABRANGÊNCIA

Esta política aplica-se a todos os colaboradores (CLT, estagiários, aprendizes), sócios, prestadores de serviço e fornecedores da INAB que tenham acesso a qualquer tipo de dado pessoal (físico ou digital) em nome da empresa.

3. PRINCÍPIOS FUNDAMENTAIS (A REGRA DE OURO)

Todo colaborador, ao lidar com dados pessoais (nome, CPF, telefone, dados bancários, saúde, etc.), deve seguir três regras básicas:

- 1º Finalidade e Necessidade:** Só colete e guarde o que for estritamente necessário para realizar o trabalho. Se não precisa do dado, não peça e não guarde.
- 2º Segurança:** Dados pessoais não podem ficar expostos. Documentos físicos devem estar em gavetas/armários e arquivos digitais protegidos por senha.
- 3º Transparência:** O titular do dado (seja funcionário ou cliente) tem o direito de saber por que seus dados estão sendo solicitados.

4. DIRETRIZES DE SEGURANÇA E CONDUTA

4.1. No Ambiente Físico ("Mesa Limpa")

- É proibido deixar documentos contendo dados pessoais (holerites, contratos, atestados médicos, listas de clientes) sobre as mesas sem supervisão. Ao sair da sala, guarde-os.
- Impressões sensíveis não devem ser esquecidas na impressora.
- O descarte de papel com dados pessoais deve ser feito preferencialmente em fragmentadora ou picotado, nunca no lixo comum inteiro.

4.2. No Ambiente Digital

- Senhas: As senhas de acesso aos sistemas da INAB são pessoais e intransferíveis. É proibido compartilhar senhas com colegas.
- Compartilhamento: É vedado enviar bases de dados de clientes ou planilhas de RH para e-mails pessoais (Gmail, Hotmail, etc.) ou via WhatsApp pessoal. Todo tráfego de dados deve ocorrer nos canais oficiais da INAB.
- Armazenamento: Arquivos com dados sensíveis devem ser salvos na rede corporativa (servidor/nuvem da empresa) e não na área de trabalho (desktop) da máquina local.

4.3. RH e Departamento Pessoal

O setor de RH é responsável pelo tratamento de dados pessoais e dados sensíveis, tais como informações de saúde, histórico médico, biometria, filiação sindical, informações de dependentes, folha salarial e declarações trabalhistas

- O acesso a dados sensíveis deve ser restrito ao RH e ao Diretor Presidente, sendo proibido compartilhamento com terceiros ou demais setores sem fundamento legal ou autorização formal.
- Informações como atestados, laudos médicos, resultado de exames, CID, afastamentos e dados relacionados à saúde do colaborador devem ser armazenados de forma criptografada e com controles de acesso.
- Documentos físicos com dados sensíveis devem permanecer trancados e sob custódia exclusiva do RH, observando o princípio de necessidade e minimização.
- Currículos, contratos de trabalho e fichas funcionais devem ser mantidos em ambiente seguro pelo tempo necessário ao cumprimento legal e, após, descartados mediante fragmentação/eliminação segura.
- É vedado o envio de dados pessoais por e-mail pessoal, WhatsApp particular ou sistemas externos sem autorização interna expressa.

4.4. Comercial e Marketing

É proibido comprar ou vender listas de contatos (leads) de origem desconhecida.

O envio de e-mail marketing ou mensagens promocionais deve respeitar a opção de descadastramento (opt-out) do cliente.

4.5. Tecnologia da Informação (TI) e Infraestrutura Digital

O setor de TI é responsável por garantir que sistemas, servidores, e contas corporativas sigam padrões de segurança, rastreabilidade e governança digital compatíveis com a LGPD.

- Todo colaborador deve possuir login pessoal e intransferível, com nível de acesso limitado às funções inerentes ao seu cargo — sendo proibido o uso de credenciais compartilhadas.
- O acesso a sistemas, e-mails, plataformas internas, bancos de dados e recursos financeiros será concedido com base no critério menor privilégio (least privilege), assegurando acesso apenas ao que é necessário para execução da atividade.
- O setor de TI realizará revisões periódicas de acessos, bloqueando senhas quando houver demissão, mudança de setor ou suspeita de violação, registrando logs para auditoria.
- Dados sensíveis armazenados digitalmente devem ser protegidos por criptografia, firewall, antivírus corporativo e autenticação multifator.
- É proibido instalar softwares sem licença, utilizar dispositivos pessoais para armazenar informações corporativas ou transferir base de dados fora dos servidores autorizados.
- Incidentes digitais (vazamento, phishing, acesso indevido, perda de dispositivo, adulteração de credenciais) devem ser reportados imediatamente ao TI, DPO e à Diretoria, conforme item 7 deste Programa.

5. COMPARTILHAMENTO COM TERCEIROS

A INAB só compartilha dados pessoais com terceiros (Ex: escritório de contabilidade, empresas de benefícios, órgãos públicos) quando:

1. Houver obrigação legal (Ex: e-Social, Receita Federal);
2. For necessário para a execução de contrato (Ex: entrega de mercadoria);
3. O terceiro garantir, contratualmente, que também respeita a LGPD.

6. DIREITOS DOS TITULARES E O ENCARREGADO (DPO)

A INAB disponibiliza um canal de comunicação para que os titulares dos dados exerçam seus direitos (como corrigir dados, saber o que a empresa possui, ou pedir exclusão quando cabível).

- Canal de Contato: As solicitações devem ser encaminhadas para o e-mail específico (dataprivacy@inab.com.br) ou direcionadas ao Setor Jurídico/Compliance.
- Prazo: A empresa tem prazos legais para responder. Nenhum colaborador deve responder solicitações de LGPD informalmente; encaminhe sempre ao Encarregado/Jurídico.

7. INCIDENTES E VIOLAÇÕES

Qualquer suspeita de vazamento de dados (ex: perda de notebook, e-mail enviado errado com planilha de clientes, ataque de hacker) deve ser comunicada imediatamente ao Setor de TI e à Diretoria.

- A omissão na comunicação de incidentes é considerada falta grave.
- O descumprimento desta política sujeita o colaborador às sanções disciplinares previstas no Programa de Compliance (advertência, suspensão ou justa causa), sem prejuízo das responsabilidades civis e criminais.

8. INTEGRAÇÃO COM A POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

O presente Programa de Compliance LGPD possui caráter complementar e integrativo à Política de Privacidade e Proteção de Dados Pessoais da INAB, que permanece como documento-base para interpretação, aplicação e cumprimento das regras relativas ao tratamento de dados pessoais, inclusive dados sensíveis, nos termos da Lei nº 13.709/2018.

Todas as diretrizes, restrições e obrigações previstas nesta política devem ser aplicadas em conjunto com a Política de Privacidade, prevalecendo sempre o entendimento harmônico entre os documentos para garantir segurança jurídica, proteção da informação e conformidade legal.

Sendo assim, qualquer operação de coleta, armazenamento, compartilhamento, eliminação, consulta, uso ou transferência de dados pessoais somente será considerada regular quando estiver simultaneamente alinhada a este Programa de Compliance e à Política de Privacidade e Proteção de Dados Pessoais.

O descumprimento de uma ou ambas as normas constitui infração institucional, sujeitando o colaborador responsável às penalidades previstas, sem prejuízo das responsabilidades administrativas, civis e criminais cabíveis.

Este Código entra em vigor a partir de 21 de novembro de 2025 e substitui os códigos de conduta anteriores.

Alterações poderão ser realizadas ocasionalmente, conforme oportunamente comunicado.

TABELA 2: HISTÓRICO DE CONTROLE DE ALTERAÇÕES

Versão	Data	Seção Alterada	Descrição da Alteração / Motivo	Responsável
1.0	21/11/2025	Documento Original	Criação da política para adequação à Lei 13.709/2018, definindo regras de "mesa limpa", segurança digital e fluxo de direitos dos titulares.	Setor Jurídico

TABELA 3: APROVAÇÕES E VALIDAÇÃO

Função	Nome/Cargo	Data	Assimatura
Elaborado por:	Setor Jurídico / TI (Adequação Legal e Técnica)	21/11/2025	
Revisado por:	Gerência Administrativa / RH (Validação de Processos)	21/11/2025	
Aprovado por:	Diretor Presidente (Responsável Controlador)	21/11/2025	



Saul Brandalise Neto