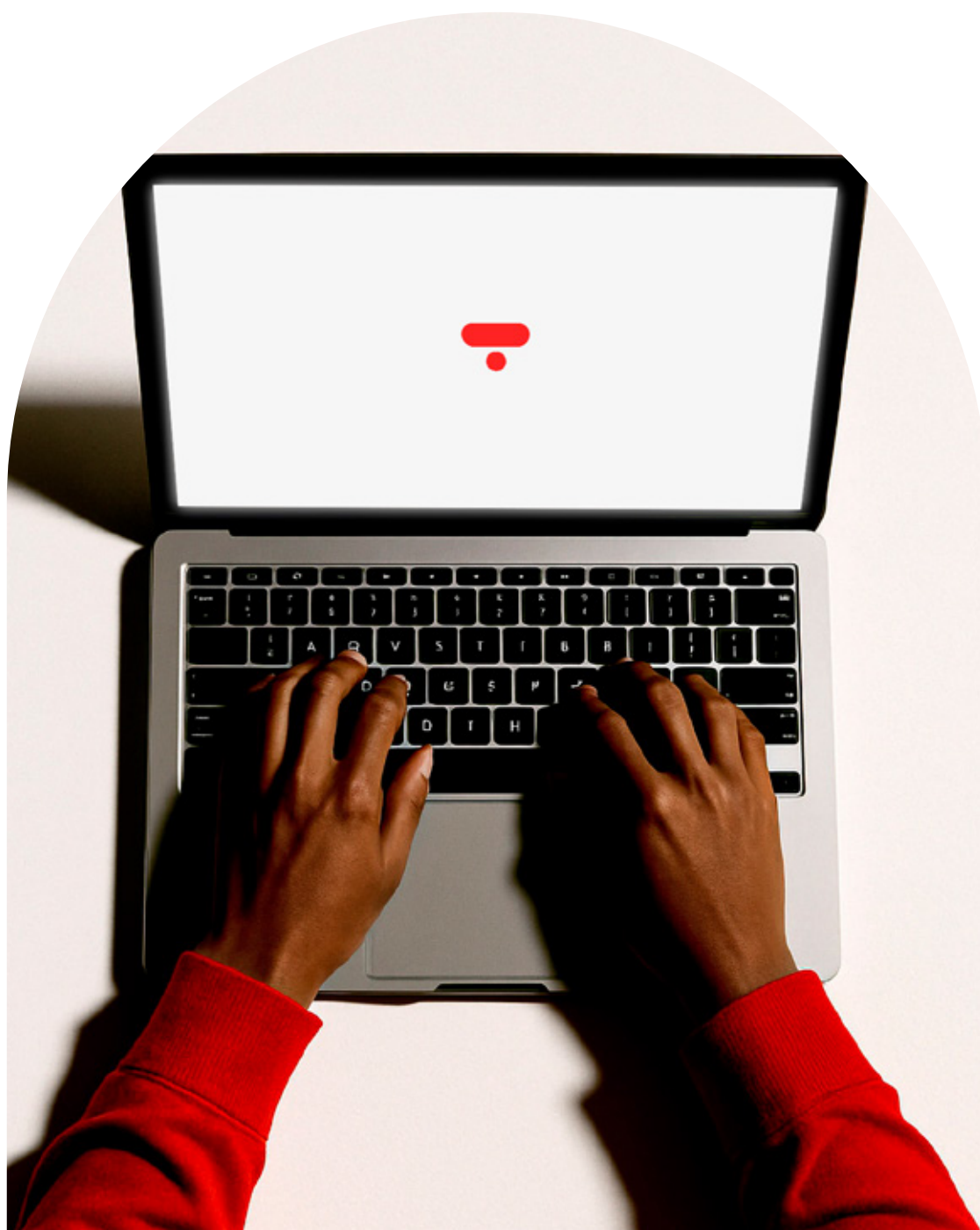




Cartilha da Lei Geral de Proteção de Dados (LGPD)





Sumário

Sumário	2
1. Objetivos da cartilha da lei geral de proteção de dados pessoais	3
Público alvo	3
2. Conceitos básicos da LGPD.....	4
O que é a LGPD?.....	4
Dados pessoais e sensíveis	4
Titulares dos dados	4
Tratamento de dados pessoais	5
3. Princípios da LGPD.....	7
Principais atores	7
4. Pilares da segurança da informação	9
I - Confidencialidade	9
II -Integridade.....	9
III - Disponibilidade	9
5. Práticas simples e econômicas que ajudam a garantir a proteção e privacidade das informações	10
Exemplos práticos	11
6. Conclusão	12
7. Referências	12



1 Objetivos da cartilha da lei geral de proteção de dados pessoais

Informar sobre a LGPD

Explicar a importância da Lei Geral de Proteção de Dados Pessoais e como ela impacta os negócios.

Orientar sobre a aplicação da LGPD

Fornecer diretrizes práticas para que microempreendedores e pessoas jurídicas (PJ) possam implementar as exigências da LGPD em suas operações diárias.

Promover a segurança da informação

Ensinar práticas simples e econômicas para proteger os dados pessoais e sensíveis.

Público alvo

- **Microempresas:** Empresas de pequeno porte que lidam com dados pessoais e sensíveis.
- **Profissionais autônomos:** Profissionais que atuam de forma independente e precisa proteger os dados de seus clientes



2 Conceitos básicos da lgpd

O que é a LGPD?

- **Definição:** A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) é uma legislação brasileira que regula o tratamento de dados pessoais.
- **Objetivo:** Proteger a privacidade e os direitos dos titulares dos dados.
- **Aplicação:** A lei se aplica a qualquer operação de tratamento de dados realizada por pessoa natural ou jurídica, pública ou privada, desde que a operação ocorra no território nacional ou os dados sejam de indivíduos localizados no Brasil.

Esta cartilha apresenta um resumo dos pontos principais da lei, de modo que o público alvo conheça melhor o tema, se engaje na adequação à LGPD e, ao mesmo tempo, saiba quais são seus direitos e deveres.



Dados pessoais e sensíveis

- **Dados pessoais:** São informações que identificam ou podem identificar uma pessoa (ex.: nome, CPF, e-mail, endereço, entre outros). Esses dados são essenciais para diversas atividades cotidianas, como cadastros em serviços, compras online e interações em redes sociais.
- **Dados sensíveis:** São informações que revelam informações mais delicadas sobre uma pessoa. Isso inclui origem racial ou étnica, convicção religiosa, opinião política, dados genéticos, entre outros. Devido à natureza sensível dessas informações, a LGPD impõe regras mais rigorosas para seu tratamento, garantindo maior proteção e privacidade.

Titulares dos dados

- **Definição:** Pessoas físicas a quem os dados pessoais se referem.
- **Direitos:** Acesso, correção, exclusão, portabilidade e revogação do consentimento.



Integração entre dados pessoais, sensíveis e os titulares

A relação entre dados pessoais, dados sensíveis e titulares dos dados é fundamental para a aplicação da LGPD. Veja como esses conceitos se interligam:

- **Identificação e Proteção:** Os dados pessoais permitem identificar os titulares dos dados. Quando esses dados são sensíveis, a proteção deve ser ainda mais rigorosa para evitar discriminação e violações de privacidade.
- **Direitos dos Titulares:** Os titulares dos dados têm o direito de acessar, corrigir, excluir, portar e revogar o consentimento sobre o uso de seus dados pessoais e sensíveis. Isso garante que eles tenham controle sobre suas informações e possam tomar decisões informadas sobre seu uso.
- **Responsabilidade dos Fornecedores:** Empresas e fornecedores que lidam com dados pessoais e sensíveis devem implementar medidas de segurança e privacidade para proteger essas informações. Isso inclui obter consentimento explícito dos titulares e garantir que os dados sejam utilizados de forma ética e transparente.

Tratamento de dados pessoais

- **Definição:** Qualquer operação realizada com dados pessoais por meios digitais ou físicos, como: coleta, armazenamento, uso, compartilhamento e eliminação.
- **Requisitos:** O tratamento de dados pessoais só pode ser realizado com o consentimento do titular ou nas outras hipóteses previstas na lei, como:
 - **Cumprimento de obrigação legal ou regulamentar**
 - Exemplo: Uma empresa precisa enviar informações fiscais dos funcionários para a Receita Federal. Esse tratamento de dados é necessário para cumprir obrigações legais.
 - **Execução de políticas públicas**
 - Exemplo: O governo coleta dados de saúde da população para implementar campanhas de vacinação. Esses dados são usados para planejar e executar políticas públicas de saúde.
 - **Estudos por órgão de pesquisa**
 - Exemplo: Uma universidade realiza uma pesquisa sobre hábitos de consumo e coleta dados anonimizados dos participantes para análise. Esses dados são usados exclusivamente para fins acadêmicos.
 - **Execução de contrato**
 - Exemplo: Você contrata um serviço de internet e fornece seus dados pessoais para que a empresa possa instalar e fornecer o serviço contratado.
 - **Exercício regular de direitos**
 - Exemplo: Em um processo judicial, seus dados pessoais podem ser usados como prova para defender seus direitos.
 - **Proteção da vida ou da incolumidade física**
 - Exemplo: Em uma emergência médica, seus dados de saúde são compartilhados com os paramédicos para garantir que você receba o tratamento adequado.



- **Tutela da saúde**
 - Exemplo: Um hospital coleta e armazena seus dados médicos para fornecer um atendimento contínuo e adequado durante suas consultas e tratamentos.
- **Interesses legítimos**
 - Exemplo: Uma empresa de segurança usa câmeras de vigilância para proteger suas instalações. Os dados coletados são usados para garantir a segurança de funcionários e visitantes.
- **Proteção ao crédito**
 - Exemplo: Uma instituição financeira consulta seu histórico de crédito antes de aprovar um empréstimo.
- **Dados Sensíveis:** O tratamento desses dados requer consentimento específico e destacado do titular.
- **Dados de Crianças e Adolescentes:** O tratamento deve ser realizado com o consentimento específico de pelo menos um dos pais ou responsável legal.

As etapas do ciclo de vida dos dados pessoais ilustram, de maneira geral, como ocorre o tratamento de dados dentro de uma organização.

Etapas do Ciclo de Vida: antes de iniciar a identificação e implementação de medidas de segurança, é essencial analisar os processos, projetos, serviços e ativos envolvidos no ciclo de vida do tratamento dos dados pessoais.

- 1 Coleta:** Obtenção, recepção ou produção de dados pessoais, independentemente do meio utilizado (documento físico, eletrônico, sistema de informação, etc.).
- 2 Retenção:** Arquivamento ou armazenamento de dados pessoais, independentemente do meio utilizado (documento físico, eletrônico, banco de dados, arquivo de aço, etc.).
- 3 Processamento:** Qualquer operação que envolva a classificação, utilização, reprodução, processamento, avaliação ou controle da informação, bem como a extração e modificação de dados pessoais.
- 4 Compartilhamento:** Qualquer operação que envolva a reprodução, transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais.
- 5 Eliminação:** Qualquer operação que vise apagar ou eliminar dados pessoais, incluindo o descarte dos ativos organizacionais quando necessário para o negócio da instituição.

3 Alguns princípios da LGPD



Principais atores

Além do titular dos dados pessoais, a LGPD também define outros atores que estão envolvidos no processo de tratamento dos dados, assim como na fiscalização. São eles:

- **Agentes de tratamento**
 - **Controlador:** Pessoa física ou jurídica, pública ou privada, responsável pelas decisões referentes ao tratamento de dados pessoais. Neste relacionamento, cabe as empresas do grupo Tecban tal papel.
 - **Operador:** Pessoa física ou jurídica, pública ou privada, que realiza o tratamento de dados pessoais em nome do controlador. Em outras palavras, o operador executa as atividades de tratamento de dados conforme as instruções do controlador, mas não toma decisões sobre como esses dados serão utilizados. Neste relacionamento está você, microempresa ou PJ, que presta serviços as empresas do grupo Tecban. Vamos ver alguns exemplos para esclarecer essa função:
 - **Execução de Tarefas Específicas:** Uma empresa de marketing digital (operador) é contratada por uma loja online (controlador) para gerenciar campanhas de e-mail marketing. A empresa de marketing usa os dados dos clientes da loja para enviar promoções, mas segue as instruções da loja sobre quais dados usar e como.
 - **Garantia de Segurança dos Dados:** Um provedor de serviços de armazenamento em nuvem (operador) armazena dados de uma empresa de saúde (controlador). O provedor deve garantir que os dados sejam protegidos contra acessos não autorizados e vazamentos, seguindo as políticas de segurança definidas pela empresa de saúde.

- 
- **Processamento de Dados:** Uma empresa de contabilidade (operador) processa folhas de pagamento para várias empresas (controladores). A empresa de contabilidade usa os dados fornecidos pelas empresas para calcular salários e impostos, mas não decide como esses dados serão utilizados além dessa finalidade.

Embora o operador não tome decisões sobre o tratamento dos dados, ele tem responsabilidades importantes:

- **Seguir Instruções do Controlador:** O operador deve sempre seguir as instruções do controlador e não pode usar os dados para outros fins.
 - **Implementar Medidas de Segurança:** O operador deve adotar medidas técnicas e organizacionais para proteger os dados pessoais contra acessos não autorizados, perdas ou vazamentos.
 - **Colaborar com o Controlador:** O operador deve colaborar com o controlador para garantir o cumprimento da LGPD, incluindo a resposta a solicitações dos titulares dos dados.
- **Encarregado dos dados (DPO):** Pessoa indicada para atuar como canal de comunicação entre o controlador, operador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.
 - **Autoridade Nacional de Proteção de Dados (ANPD):** Órgão da administração pública federal responsável por zelar pela proteção de dados pessoais e por implementar e fiscalizar o cumprimento da LGPD no Brasil.

4 Pilares da segurança da informação



I - Confidencialidade

- **Definição:** Garantir que apenas pessoas autorizadas tenham acesso aos dados.
- **Exemplo:** Restrição de acesso a documentos confidenciais.

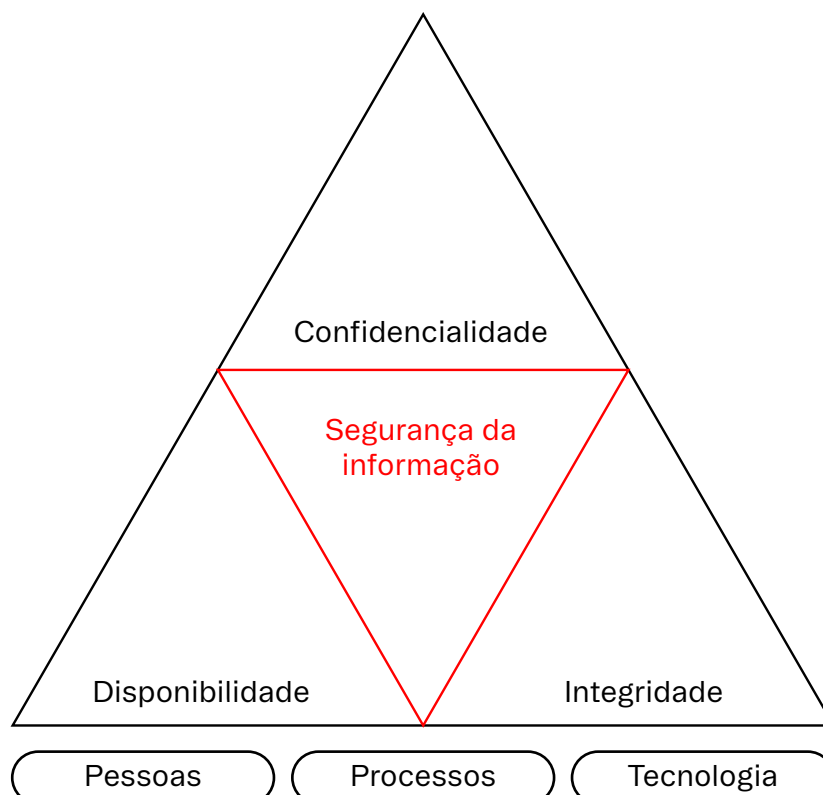
II - Integridade

- **Definição:** Assegurar que os dados não sejam alterados ou destruídos de forma indevida.
- **Exemplo:** Fazer backup regular dos dados importantes.

III - Disponibilidade

- **Definição:** Garantir que os dados estejam acessíveis quando necessário.
- **Exemplo:** Manter sistemas de armazenamento de dados funcionando corretamente.

Para que os pilares da SI sejam efetivamente suportados e executados, é essencial contar com a integração de pessoas, tecnologias e processos.



5 Práticas simples e econômicas que ajudam a garantir a proteção e privacidade das informações



Senhas Fortes

Crie senhas complexas que incluam uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais.
Altere suas senhas regularmente e evite usar a mesma senha para diferentes contas.

Backup Regular

Faça backups frequentes dos dados importantes em dispositivos externos ou serviços de armazenamento em nuvem.
Verifique periodicamente se os backups estão funcionando corretamente e se os dados podem ser restaurados.

VPN

Utilize redes privadas virtuais para acessar sistemas da empresa de forma segura quando estiver fora do escritório.
Configure a VPN para criptografar a conexão e proteger os dados transmitidos.

Antivírus e Antimalware

Utilize e mantenha softwares de segurança atualizados para proteger contra vírus e malwares.
Realize varreduras regulares no sistema para identificar e remover possíveis ameaças.

Atualizações de Software

Mantenha todos os softwares e sistemas operacionais atualizados com as últimas versões e patches de segurança.
Ative as atualizações automáticas sempre que possível para garantir que seu sistema esteja protegido contra vulnerabilidades conhecidas.

Educação e Treinamento

Promova a conscientização sobre a importância da proteção de dados entre todos os colaboradores.
Realize treinamentos periódicos sobre boas práticas de segurança da informação e como identificar possíveis ameaças, como phishing.

Controle de Acesso

Restrinja o acesso aos dados pessoais apenas às pessoas que realmente precisam dessas informações para realizar seu trabalho.



Utilize autenticação de dois fatores para adicionar uma camada extra de segurança ao acesso aos sistemas que possuem essa possibilidade de configuração.

Criptografia

Criptografe dados sensíveis tanto em trânsito quanto em repouso para proteger as informações contra acessos não autorizados.

Utilize métodos de criptografia fortes e atualizados para garantir a segurança dos dados.

Política de Privacidade

Desenvolva e implemente uma política de privacidade clara e acessível para informar os clientes como seus dados serão utilizados e protegidos.

Revise e atualize regularmente essa política para garantir que esteja em conformidade com a legislação.

Descarte Seguro de Dados

Adote práticas seguras para o descarte de dados pessoais que não são mais necessários, como a destruição física de documentos ou a exclusão segura de arquivos digitais.

Certifique-se de que os dados sejam completamente irrecuperáveis após o descarte.

Exemplos práticos

I - Cadastro de Clientes

- **Definição:** Garantir que apenas pessoas autorizadas tenham acesso aos dados.
- **Exemplo:** Restrição de acesso a documentos confidenciais.

II - Prestação de Serviços

- **Situação:** Um consultor autônomo coleta dados de contato e informações sobre os projetos dos clientes.
- **Ação:** Utilizar senhas fortes para proteger esses dados, fazer backup regularmente e utilizar uma VPN para acessar os dados de forma segura quando estiver fora do escritório.

III - Atendimento ao Cliente

- **Situação:** Uma pequena empresa de suporte técnico coleta dados de contato e informações sobre os problemas dos clientes.
- **Ação:** Garantir que esses dados sejam acessados apenas por funcionários autorizados, utilizar antivírus para proteger os sistemas e informar aos clientes como seus dados serão utilizados.



6 Conclusão

A conformidade com a LGPD é essencial para proteger os dados pessoais e sensíveis dos clientes e garantir a segurança da informação. Aplicar práticas simples e econômicas pode ajudar microempreendedores e fornecedores PJ a se adequarem à legislação sem grandes investimentos.

7 Referências

NACIONAL, I. LEI No 13.709, DE 14 DE AGOSTO DE 2018 - Imprensa Nacional.

Disponível em:

<https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337>. Acesso em: 13 fev. 2025.

Lei geral de proteção de dados pessoais: Lei n. 13.709/2018. Senado.leg.br, 2018.

Disponível em: <<https://www2.senado.leg.br/bdsf/handle/id/658231>>. Acesso em: 13 fev. 2025.

Tratamento de Dados Pessoais. Disponível em:

<<https://www.gov.br/dnit/pt-br/aceso-a-informacao/tratamento-de-dados-pessoais>>. Acesso em: 13 fev. 2025.

CERT.BR, C. DE E., Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de Segurança para Internet. 2012. ed. São Paulo: Comitê Gestor da Internet no Brasil, [s.d.]. v. 2a. Acesso em: 13 fev. 2025.