

**NECESSIDADE DO SIGILO E PROPRIEDADE DADOS**

**Andre Luiz Sazana Waleczki | RM:559685**

**Guilherme Vinícius dos Santos | RM:560564**

**Henrique Caproni Siqueira | RM:560105**

**Renan Thiago Aviz e Silva | RM:560849**

**Thiago Evangelista Dias | RM:559403**

**Versão 1**

**HISTÓRICO DE VERSÕES**

| **Versão** | **Data** | **Responsável** | **Descrição** |
| --- | --- | --- | --- |
| 1 | 19/08/2024 | Patrícia Maura Angelini | Versão Inicial Template PBL Fase 3 - CAP 01 – A**MPLIANDO A CONSISTENCIA DO NEGOCIO** |
| 2 | 19/08/2024 | Rita de Cássia Rodrigues | Revisão acadêmica |
| 3 | 07/11/2024 | Andre Luiz Sazana Waleczki | Criação do conteúdo |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

FICHA CATALOGRÁFICA   
**[NÃO PREENCHER - PARA USO DO DEPTO DE EAD E BIBLIOTECA]**

**RESUMO**

Template para atividade de PBL fase 3 1º ano TSC.

**Palavras-chave:** PBL. FASE 3. TEMPLATE

**LISTA DE Figuras**

**No table of figures entries found.**

**LISTA DE QUADROS**

[Quadro 1 – Quadro resumo das tarefas do PBL 12](#_3rdcrjn)

**LISTA DE TABELAS**

**No table of figures entries found.**

**LISTA DE CÓDIGOS-FONTE**

**No table of figures entries found.**

**LISTA DE ComandoS de prompt do sistema operacional**

**No table of figures entries found.**

**Sumário**

[1 Contextualização do papel da TI em relação à LGPD 11](#_gjdgxs)

[1.1 Aplicação da LGPD nas Tarefas da TI 11](#_30j0zll)

[1.2 Aplicação da LGPD na Plataforma de eCommerce 11](#_1fob9te)

[2 RECOMENDAÇÕES DE PROTEÇÃO AOS DADOS 12](#_3znysh7)

[2.1 Criptografia de Dados Pessoais 12](#_2et92p0)

[2.2 Controle de Acesso Baseado em Funções (RBAC) 12](#_tyjcwt)

[3 ANONIMIZAÇÃO 13](#_3dy6vkm)

[3.1 Relação de Dados de Clientes Disponíveis 13](#_1t3h5sf)

[3.2 Definição de Dados para Anonimização 13](#_4d34og8)

[REFERÊNCIAS 14](#_2s8eyo1)

[GLOSSÁRIO 15](#_17dp8vu)

# 1 Contextualização do papel da TI em relação à LGPD

## 1.1 Aplicação da LGPD nas Tarefas da TI

* + A Tecnologia da Informação (TI) desempenha um papel fundamental na conformidade com a Lei Geral de Proteção de Dados (LGPD). A responsabilidade do setor de TI é implementar e monitorar as práticas de segurança para garantir que todas as operações estejam em conformidade com a legislação, protegendo os dados pessoais de clientes e colaboradores.
  + No dia a dia, a TI deve assegurar a proteção de dados pessoais em tarefas rotineiras, como o controle de acessos, armazenamento seguro de dados e gestão de consentimento. Isso envolve garantir que dados de colaboradores, como registros pessoais e informações de acesso, sejam armazenados e processados de maneira segura, de acordo com os princípios da LGPD. Além disso, a TI é responsável por realizar auditorias e monitoramento constantes para identificar e corrigir vulnerabilidades de segurança, garantindo que o tratamento dos dados esteja em conformidade.

## 1.2 Aplicação da LGPD na Plataforma de eCommerce

* + Para uma plataforma de e-commerce, a TI deve implementar uma série de práticas de segurança e privacidade para proteger os dados dos clientes e cumprir os requisitos da LGPD. A gestão da segurança na plataforma envolve medidas como criptografia de dados, autenticação de múltiplos fatores, controle de acessos e políticas de consentimento claras.
  + Além disso, a TI deve garantir que todas as operações de tratamento de dados — como coleta, armazenamento e compartilhamento — estejam documentadas e em conformidade com as regulamentações. Isso implica a adoção de boas práticas de segurança, como a anonimização de dados sensíveis e o uso de firewalls e sistemas de detecção de intrusão, para prevenir o acesso não autorizado. A conformidade com essas práticas reforça a confiança dos consumidores, promovendo um ambiente seguro para transações online.

# 2 RECOMENDAÇÕES DE PROTEÇÃO AOS DADOS

## 2.1 Criptografia de Dados Pessoais

* A TI deve implementar a criptografia de dados pessoais tanto em repouso quanto em trânsito, utilizando algoritmos robustos como AES-256. A criptografia assegura que os dados fiquem inacessíveis em caso de tentativas de acesso não autorizado.
* Esse método aumenta a confiança dos consumidores ao garantir a proteção de suas informações, reduzindo significativamente o risco de vazamentos. A criptografia, além de ser uma medida de segurança essencial, fortalece a conformidade da empresa com a LGPD ao proteger dados sensíveis de forma efetiva.

## 2.2 Controle de Acesso Baseado em Funções (RBAC)

* + Implementação do Controle de Acesso Baseado em Funções (RBAC), garantindo que apenas funcionários com a devida autorização tenham acesso a dados pessoais específicos. Esse controle restringe o acesso com base nas funções de cada colaborador, limitando a exposição de dados.
  + O RBAC ajuda a proteger informações pessoais, reduzindo a probabilidade de acessos indevidos. Além disso, essa prática minimiza riscos de violação de dados internos, promovendo um ambiente de trabalho mais seguro e adequado aos requisitos da LGPD.

## 3 ANONIMIZAÇÃO

## 3.1 Relação de Dados de Clientes Disponíveis

Os dados de clientes disponíveis na plataforma e que são coletados, armazenados e processados incluem:

* + NR\_CLIENTE: Identificador do cliente.
  + NM\_CLIENTE: Nome do cliente.
  + DT\_NASCIMENTO: Data de nascimento do cliente.
  + FL\_SEXO\_BIOLOGICO: Sexo biológico do cliente.
  + DS\_GENERO: Gênero do cliente.
  + NR\_CPF: Número do CPF do cliente.
  + DS\_EMAIL: E-mail do cliente.
  + NR\_TELEFONE: Telefone de contato do cliente.
  + NM\_LOGIN: Nome de login do cliente.
  + DS\_SENHA: Senha do cliente (armazenada de forma segura e criptografada).
  + QT\_ESTRELAS: Avaliação do cliente.
  + VL\_MEDIO\_COMPRA: Valor médio de compras do cliente.

## 3.2 Definição de Dados para Anonimização

**NR\_CPF**

O CPF é um dado altamente sensível, pois é um identificador único que pode ser usado para identificar o cliente de forma direta. Para proteger esse dado, ele pode ser parcialmente mascarado (ex.: “123..-45”) ou substituído por um identificador aleatório que represente o CPF sem revelar o número exato. A anonimização do CPF é crucial para prevenir fraudes e acessos não autorizados, garantindo a conformidade com a LGPD e protegendo a privacidade do cliente.

**DS\_EMAIL (E-mail)**

O e-mail do cliente é outro dado sensível, pois pode ser usado para contato direto ou tentativas de phishing. Para anonimização, o e-mail pode ser parcialmente mascarado (ex.: “a\*\*\*\*\*\*\*@gmail.com”) ou substituído por um hash criptografado, mantendo um identificador único sem expor o endereço de e-mail completo. Essa medida ajuda a evitar o uso do e-mail para tentativas de fraude ou identificação do cliente.

# REFERÊNCIAS

FERREIRA, J.; SILVA, M. A segurança da informação em ambientes digitais. Editora ABC, 2020.

ALMEIDA, R. Direitos de privacidade e proteção de dados na era digital. São Paulo: Edusp, 2021.

PEREIRA, T.; COSTA, L. Auditoria de sistemas e a conformidade com a LGPD. Revista Brasileira de Segurança, 5(3), p. 23-34, 2019.

MONTEIRO, A. Segurança de dados e conscientização de colaboradores. Editora Campus, 2022.

NASCIMENTO, L.; ROCHA, C. Criptografia e segurança de dados em plataformas digitais. Revista de Tecnologia e Inovação, 10(2), p. 45-60, 2021.

MARTINS, S.; SILVA, D. Controle de acesso em ambientes corporativos e conformidade com a LGPD. Caderno de Segurança da Informação, 8(1), p. 14-26, 2020.

SANTOS, A.; LIMA, R. Anonimização de dados e privacidade no comércio eletrônico. Tecnologia & Sociedade, 7(2), p. 88-102, 2021.

GOMES, J. Privacidade de dados e o uso de informações geográficas anonimizadas. Rio de Janeiro: Ciência e Pesquisa, 2022.

# GLOSSÁRIO

| LGPD (Lei Geral de Proteção de Dados) | Legislação brasileira que regulamenta o uso, coleta, armazenamento e compartilhamento de dados pessoais, garantindo a privacidade e segurança das informações. |
| --- | --- |
| Criptografia | Técnica de segurança que codifica informações para protegê-las contra acessos não autorizados, garantindo a confidencialidade dos dados. |
| Anonimização | Processo de transformação de dados pessoais de forma que não possam ser associados a uma pessoa específica, mesmo com informações adicionais. |
| RBAC (Role-Based Access Control) | Controle de Acesso Baseado em Funções; sistema de controle que restringe o acesso a dados com base nas funções desempenhadas pelos usuários na organização. |
| Autenticação de Múltiplos Fatores | Mecanismo de segurança que exige mais de uma forma de verificação de identidade para conceder acesso, como senha e código de confirmação. |
| Auditoria de Sistemas | Processo de análise e avaliação dos sistemas de informação para verificar a conformidade com normas, como a LGPD, e identificar possíveis falhas de segurança. |
| Dados Pessoais | Qualquer informação relacionada a uma pessoa identificada ou identificável, como nome, CPF, e dados de contato. |
| Plataforma de eCommerce | Sistema online que permite a compra e venda de produtos e serviços pela internet, frequentemente envolvem coleta e tratamento de dados pessoais de clientes. |
| Consentimento | Permissão dada pelos titulares de dados para que suas informações sejam coletadas e utilizadas para finalidades específicas e delimitadas. |