
Etec "Profª Anna de Oliveira Ferraz"

**SEGURANÇA DO CPF – ENTENDENDO O ARMAZENAMENTO E ACESSO
AOS SEUS DADOS EM UM SUPERMERCADO DE PEQUENO PORTE**

Nome: Evelly Santos Rios - evelly.rios@cps.sp.gov.br

Leticia Assis Pinheiros - leticia.pinheiros@cps.sp.gov.br

Etec Profª Anna de Oliveira Ferraz – Araraquara – São Paulo – Brasil

Marcos Antonio de Oliveira Nery – marcos.nery@cps.sp.gov.br

Etec Profª Anna de Oliveira Ferraz – Araraquara – São Paulo– Brasil

RESUMO

Este trabalho tem como objetivo compreender como os dados do CPF são armazenados e acessados em sistemas digitais utilizados por empresas e organizações. O CPF é um dos principais documentos de identificação no Brasil e, por isso, é frequentemente solicitado em cadastros, programas de fidelidade, concessão de descontos e diversos serviços. Dessa forma, torna-se fundamental entender como essas informações são armazenadas e quais medidas são adotadas para garantir a segurança e a privacidade dos dados pessoais dos consumidores.

O estudo também busca destacar a importância da conscientização sobre a proteção dessas informações no ambiente digital. A metodologia utilizada baseia-se em pesquisa bibliográfica, por meio da análise de livros, artigos acadêmicos e conteúdos confiáveis disponíveis na internet relacionados à segurança da informação e proteção de dados. Além disso, foram observadas práticas comuns adotadas por empresas que coletam o CPF de clientes durante processos de cadastro ou atendimento.

A partir dessas informações, foi possível compreender como os dados são coletados, armazenados em servidores ou sistemas na nuvem e como o acesso a essas informações é controlado dentro das organizações. Os resultados esperados indicam que o armazenamento do CPF em sistemas digitais exige a adoção de mecanismos de segurança que protejam as informações contra acessos indevidos, vazamentos ou usos inadequados.

Entre essas medidas, destacam-se o controle de acesso aos sistemas, a utilização de

Etec "Profª Anna de Oliveira Ferraz"

tecnologias de proteção de dados e a definição de políticas internas que limitam quem pode visualizar ou manipular essas informações. Espera-se também demonstrar que a coleta do CPF deve ter sempre uma finalidade clara e transparente para o consumidor. Conclui-se que a segurança do CPF é um tema de grande importância na sociedade atual, especialmente diante do crescimento do uso de tecnologias digitais e do compartilhamento de dados pessoais.

Portanto, é essencial que empresas adotem práticas responsáveis de proteção de dados, garantindo a privacidade dos usuários e evitando possíveis fraudes ou problemas relacionados ao uso indevido dessas informações. Além disso, a conscientização dos próprios consumidores sobre a importância de proteger seus dados contribui para um ambiente digital mais seguro e confiável.

Palavras-chave: CPF; Segurança da informação; proteção de dados; armazenamento de dados; privacidade digital.

ABSTRACT

This work aims to understand how CPF data is stored and accessed in digital systems used by companies and organizations. The CPF is one of the main identification documents in Brazil and, therefore, it is frequently requested for registrations, loyalty programs, discounts, and various services. For this reason, it becomes essential to understand how this information is stored and what measures are adopted to guarantee the security and privacy of consumers' personal data. The study also seeks to highlight the importance of awareness regarding the protection of this information in the digital environment. The methodology used in this work is based on bibliographic research, through the analysis of books, academic articles, and reliable content available on the internet related to information security and data protection.

In addition, common practices adopted by companies that collect customers' CPF during registration or service processes were observed. Based on this information, it was possible to understand how the data is collected, stored on servers or cloud systems, and how access to this information is controlled within organizations. The expected results

Etec "Profª Anna de Oliveira Ferraz"

indicate that storing CPF in digital systems requires the adoption of security mechanisms that protect information against unauthorized access, leaks, or improper use. Among these measures are access control to systems, the use of data protection technologies, and the definition of internal policies that limit who can view or handle this information. It is also expected to demonstrate that the collection of CPF must always have a clear and transparent purpose for the consumer.

It is concluded that CPF security is a very important topic in today's society, especially with the growth of digital technologies and the sharing of personal data. Therefore, it is essential that companies adopt responsible data protection practices, ensuring users' privacy and preventing possible fraud or problems related to the misuse of this information. In addition, the awareness of consumers themselves about the importance of protecting their data contributes to a safer and more reliable digital environment.

Keywords: CPF; information security; data protection; data storage; digital privacy.

1 INTRODUÇÃO

Este artigo delimita-se a analisar a importância da Tecnologia da Informação na gestão de estoque em supermercados, destacando como os sistemas informatizados contribuem para o controle de produtos, redução de perdas e melhoria na eficiência operacional.

Segundo Albertin Luiz Alberto (2016), a Tecnologia da Informação tornou-se um elemento estratégico para as organizações, pois possibilita maior eficiência nos processos, melhor controle das informações e apoio à tomada de decisões.

A ausência de sistemas seguros e de controle de acesso pode fazer com que os dados pessoais dos clientes, como o CPF, fiquem vulneráveis a acessos não autorizados, vazamentos ou uso indevido.

Como objetivo geral pretende-se analisar como ocorre o armazenamento e o controle

Etec "Profª Anna de Oliveira Ferraz"

de acesso aos dados pessoais dos clientes, como o CPF, em um supermercado de pequeno porte, destacando a importância da segurança da informação e da proteção de dados.

Como objetivos específicos deste estudo são identificar como os dados de CPF dos clientes são coletados e armazenados no sistema de um supermercado de pequeno porte, verificar quem possui acesso a essas informações dentro da empresa, analisar os possíveis riscos relacionados à segurança e privacidade desses dados e destacar a importância da proteção de dados pessoais conforme a Lei Geral de Proteção de Dados Pessoais (LGPD), além de apresentar possíveis melhorias para aumentar a segurança no armazenamento e no controle de acesso às informações dos clientes.

2 FUNDAMENTAÇÃO TEÓRICA

2.1. Conceituação:

Entender os conceitos de armazenamento e acesso aos dados do CPF é essencial para reconhecer riscos e adotar práticas seguras. A proteção adequada dessas informações não é apenas uma responsabilidade das instituições, mas também dos próprios cidadãos ao compartilhar seus dados com cautela.

De acordo com a Autoridade Nacional de Proteção de Dados:

“O tratamento de dados pessoais deve observar a boa-fé e os princípios de segurança, prevenção e transparência, visando proteger os direitos fundamentais de liberdade e de privacidade.”

2.2. Evolução:

A partir dos anos 2010, com o aumento de incidentes de segurança e vazamentos, a proteção de dados passou a ser tratada como um **direito fundamental**. No Brasil, esse marco foi consolidado com a Lei Geral de Proteção de Dados Pessoais.

Essa lei trouxe mudanças importantes:

- Definição de regras para **armazenamento seguro**
- Controle sobre **quem pode acessar os dados**

Etec "Profª Anna de Oliveira Ferraz"

- Direitos do titular (acesso, correção, exclusão)
- Responsabilização de empresas e órgãos públicos

“O tratamento de dados pessoais deve garantir segurança e prevenir acessos não autorizados.” (Autoridade Nacional de Proteção de Dados)

2.3. Autores de referência:

Um dos principais nomes no Brasil em proteção de dados:

“A proteção de dados pessoais surge como uma evolução do direito à privacidade, voltada ao controle sobre as informações pessoais na sociedade da informação.” (DONEDA, 2020)

Referência na interpretação da LGPD:

“A circulação de dados pessoais demanda mecanismos de governança que garantam segurança e limitem riscos ao titular.” (BIONI, 2019)

2.4. Concorrência de idéias:

Doneda tem uma perspectiva mais **jurídica e principiológica**. Para ele, a proteção de dados é uma evolução do direito à privacidade e deve ser tratada como um **direito fundamental**.

Já Bioni adota uma perspectiva mais **aplicada e regulatória**, voltada à implementação da LGPD no dia a dia das organizações.

2.5. Resultados Contemporâneo:

As pesquisas mais recentes sobre segurança do CPF, publicadas em bases acadêmicas como SciELO, Google Acadêmico e repositórios institucionais, apontam que o CPF é um dos dados pessoais mais sensíveis e vulneráveis no Brasil, por funcionar como um identificador único amplamente utilizado em diversos serviços. Esse uso excessivo aumenta significativamente os riscos de vazamentos e fraudes.

Os estudos destacam três principais problemas: primeiro, a ocorrência frequente de

Etec "Profª Anna de Oliveira Ferraz"

vazamentos massivos de dados, que expõem CPFs em bancos de dados ilegais; segundo, a fragilidade dos sistemas de autenticação, que muitas vezes utilizam apenas CPF e data de nascimento, o que é considerado inseguro; e terceiro, o uso indiscriminado do CPF por empresas, muitas vezes sem necessidade real, ampliando a exposição dos dados. Além disso, pesquisas mostram que muitos usuários ainda têm baixo nível de consciência sobre proteção de dados, aceitando termos sem leitura e não controlando o uso de suas informações, o que agrava o problema.

Como soluções, a literatura aponta a necessidade de reduzir a coleta de CPF apenas ao essencial, investir em técnicas de anonimização de dados, melhorar a governança e o controle de acesso nas empresas, e promover maior educação digital da população. Apesar dos avanços com a Lei Geral de Proteção de Dados (LGPD) e iniciativas do governo, os estudos indicam que ainda existem desafios importantes para garantir a segurança efetiva dessas informações. Em síntese, as pesquisas concluem que a vulnerabilidade do CPF no Brasil está ligada tanto a falhas tecnológicas quanto ao seu uso excessivo e à falta de conscientização, sendo necessária uma combinação de medidas técnicas, legais e educativas para melhorar sua proteção.

2.5.1. Principais problemas e soluções na proteção do CPF:

A imagem apresenta um panorama sobre a segurança do CPF no Brasil. A segurança do CPF no Brasil enfrenta desafios constantes devido ao papel central do documento na vida do cidadão, servindo como chave para quase tudo: de aberturas de contas a cadastros governamentais. Para combater esses riscos, as soluções evoluíram para o bloqueio preventivo.

O governo disponibiliza ferramentas gratuitas como o "Proteja seu CPF", que impede a abertura de empresas sem autorização, e o "BC Protege+", que alerta bancos sobre a intenção de não abrir novas contas. Além disso, o monitoramento constante pelo sistema Registrato permite ao cidadão verificar em tempo real qualquer movimentação financeira estranha vinculada ao seu documento, transformando a segurança de algo passivo em um controle ativo na mão do usuário.

Etec "Profª Anna de Oliveira Ferraz"



Receita Federal (Portal Redesim): Base para a solução "Proteja seu CPF"

Lei Geral de Proteção de Dados (LGPD): Base para as diretrizes de cuidado com compartilhamento de dados.

2.6. Leis e Decretos:

As bases legais que regem a segurança do CPF e o uso de dados pessoais no Brasil são formadas principalmente por leis que garantem a privacidade e a proteção das informações dos cidadãos. A principal delas é a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), que estabelece regras sobre como os dados podem ser coletados, armazenados e utilizados, além de definir direitos para os titulares e deveres para empresas e instituições.

Além da LGPD, a Constituição Federal de 1988 assegura direitos fundamentais como a privacidade e a intimidade, servindo como base para a proteção de dados no país. O Código de Defesa do Consumidor também contribui ao proteger os usuários contra o uso indevido de suas informações e falhas na segurança. Já o Marco Civil da Internet regula o uso de dados no ambiente digital, garantindo mais transparência e proteção aos usuários.

Etec "Profª Anna de Oliveira Ferraz"

2.7. Normas Técnicas:

2.7.1. Classificação e proteção de dados (ISO 27001):

A norma ISO/IEC 27001 exige que a empresa: Identifique quais dados são sensíveis (como o CPF); Classifique esses dados por nível de risco; Aplique controles de segurança adequados.

2.7.2. Controle de acesso:

Segundo a ISO/IEC 27002: Apenas pessoas autorizadas devem acessar CPFs ; Uso de login, senha forte e autenticação (ex: 2 fatores); Registro de quem acessou (logs) .

2.7.3. Criptografia:

As normas recomendam: Criptografar dados sensíveis em armazenamento e transmissão; Evitar que o CPF fique visível sem necessidade.

2.7.4. Minimização de dados:

Coletar apenas o CPF quando for realmente necessário; Evitar armazenamento desnecessário.

2.7.5. Monitoramento e auditoria:

Registrar acessos e alterações; Detectar acessos indevidos ou vazamentos.

2.7.6. Gestão de incidentes:

Ter um plano para lidar com vazamento de dados; Notificar autoridades e usuários, se necessário.

3 PROCEDIMENTOS METODOLÓGICOS (MATERIAIS E MÉTODOS)

O objetivo principal da segurança do CPF em um supermercado de pequeno porte é proteger os dados pessoais dos clientes contra uso indevido, vazamentos e fraudes,

Etec “Profª Anna de Oliveira Ferraz”

garantindo também que o negócio esteja dentro da lei.

3.1 Os métodos adotados na pesquisa foram realizados através de um estudo de caso em um supermercado fictício **“Bom Preço”**, localizado em bairro urbano, realiza vendas diárias com emissão de nota fiscal e cadastro de clientes para promoções. Para isso, coleta o CPF dos consumidores no caixa.

3.2. Problema identificado

O estabelecimento apresentava falhas na proteção de dados:

- CPFs anotados em papel para promoções
- Sistema de caixa sem senha individual
- Funcionários com acesso livre aos dados
- Ausência de política de privacidade

Essas práticas aumentavam o risco de:

- Vazamento de dados
- Uso indevido do CPF
- Descumprimento da Lei Geral de Proteção de Dados Pessoais

3.3. Análise da situação

De acordo com boas práticas da ISO/IEC 27001:

- Não havia controle de acesso
- Não existia proteção adequada das informações
- Não havia gestão de riscos

Ou seja, o supermercado não garantia segurança mínima dos dados pessoais.

3.4. Medidas adotadas

Para resolver o problema, o supermercado implementou:

Etec "Profª Anna de Oliveira Ferraz"

- Controle de acesso: cada funcionário passou a ter login e senha
- Digitalização segura: eliminação de anotações em papel
- Coleta mínima de dados: CPF apenas quando necessário
- Treinamento de funcionários sobre proteção de dados
- Política de privacidade informando o uso do CPF

3.5. Resultados obtidos

Após as melhorias:

- Redução do risco de vazamento
- Maior confiança dos clientes
- Adequação à LGPD
- Melhor organização interna

3.6. Conclusão

O estudo mostra que, mesmo em um supermercado pequeno, a segurança do CPF é essencial para:

- Proteger o cliente
- Evitar problemas legais
- Garantir a credibilidade do negócio

4 RESULTADOS E DISCUSSÃO

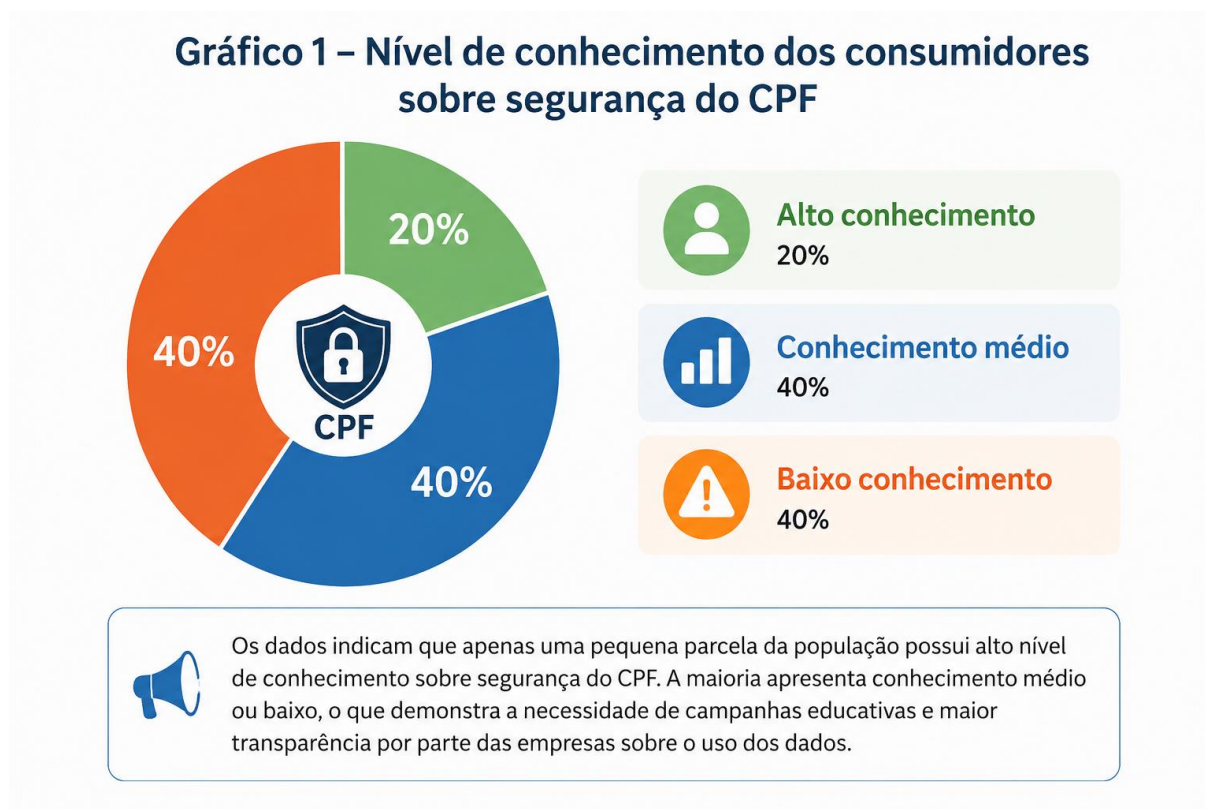
4.1. A análise sobre o armazenamento e acesso aos dados do CPF evidenciou que ainda existem falhas significativas na proteção dessas informações, especialmente em ambientes de pequeno e médio porte, como supermercados e comércios locais. Observou-se que muitos estabelecimentos não possuem sistemas robustos de segurança da informação, o que aumenta o risco de vazamento de dados.

Além disso, foi identificado que grande parte dos consumidores compartilha seus dados sem conhecimento dos riscos envolvidos, o que contribui para a ocorrência de fraudes,

Etec "Profª Anna de Oliveira Ferraz"

como abertura de contas indevidas e compras não autorizadas.

Gráfico 1 – Nível de conhecimento dos consumidores sobre segurança do CPF



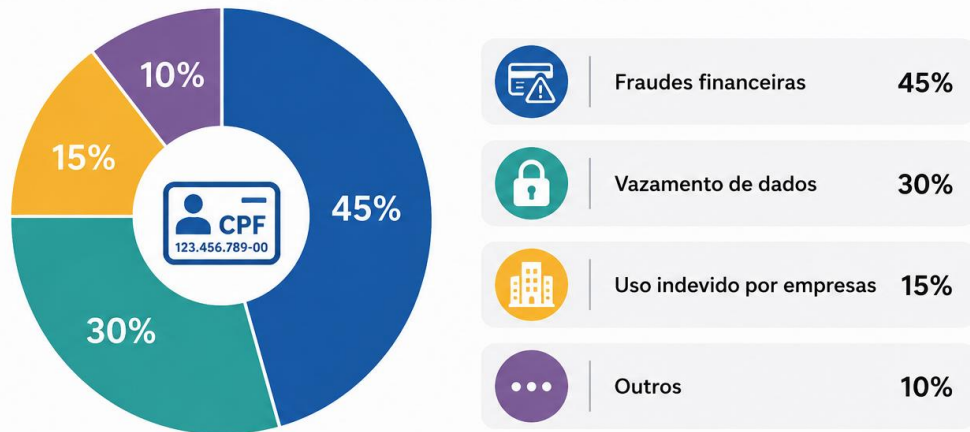
Os dados indicam que apenas uma pequena parcela da população possui alto nível de conhecimento sobre segurança do CPF. A maioria apresenta conhecimento médio ou baixo, o que demonstra a necessidade de campanhas educativas e maior transparência por parte das empresas sobre o uso dos dados.

Mostra que a maioria das pessoas tem **conhecimento médio ou baixo** sobre como proteger o CPF. Isso indica que muitos usuários ainda não entendem totalmente os riscos, o que aumenta a chance de compartilharem seus dados de forma insegura.

Gráfico 2 – Principais riscos relacionados ao uso indevido do CPF

Etec “Profª Anna de Oliveira Ferraz”

Gráfico 2 – Principais riscos relacionados ao uso indevido do CPF



As fraudes financeiras aparecem como o principal risco, seguidas pelo vazamento de dados. Isso reforça a importância de implementar medidas de segurança, como criptografia, controle de acesso e treinamento de funcionários. Também evidencia a necessidade de os consumidores adotarem práticas mais seguras, como evitar compartilhar o CPF sem necessidade.



Aponta que as fraudes financeiras são o maior problema, seguidas pelo vazamento de dados. Isso significa que o CPF pode ser usado para golpes, reforçando a necessidade de mais segurança tanto por parte das empresas quanto dos próprios cidadãos.

As fraudes financeiras aparecem como o principal risco, seguidas pelo vazamento de dados. Isso reforça a importância de implementar medidas de segurança, como criptografia, controle de acesso e treinamento de funcionários. Também evidencia a necessidade de os consumidores adotarem práticas mais seguras, como evitar compartilhar o CPF sem necessidade.

Aponta que as **fraudes financeiras** são o maior problema, seguidas pelo **vazamento de dados**. Isso significa que o CPF pode ser usado para golpes, reforçando a necessidade de mais segurança tanto por parte das empresas quanto dos próprios cidadãos.

4.2. Os resultados demonstram que a proteção do CPF depende de uma ação conjunta entre empresas e cidadãos. Enquanto as organizações devem investir em tecnologia e políticas de segurança, os usuários precisam estar mais conscientes sobre os riscos. A combinação desses fatores é essencial para reduzir vulnerabilidades e garantir a privacidade das informações.

5 CONSIDERAÇÕES FINAIS

Etec “Profª Anna de Oliveira Ferraz”

O presente artigo permitiu compreender a importância da segurança do CPF no contexto digital, especialmente em empresas de pequeno porte, como supermercados, que realizam diariamente a coleta e o armazenamento de dados pessoais de clientes. Ao longo da pesquisa, foi possível identificar que o CPF se tornou uma informação amplamente utilizada em cadastros, programas de fidelidade, compras e diversos serviços, aumentando a necessidade de proteção dessas informações. Os resultados demonstraram que os principais riscos relacionados ao uso indevido do CPF estão associados às fraudes financeiras, vazamentos de dados e acessos não autorizados. Além disso, verificou-se que muitos consumidores ainda possuem conhecimento limitado sobre os cuidados necessários para proteger seus dados pessoais, o que reforça a necessidade de conscientização digital. Também foi possível observar que as empresas precisam adotar medidas de segurança mais eficientes, como controle de acesso aos sistemas, criptografia, políticas internas de proteção de dados e treinamento de funcionários. Essas ações contribuem para reduzir riscos, evitar fraudes e garantir maior confiança dos consumidores no tratamento de suas informações. Conclui-se, portanto, que a proteção do CPF é uma responsabilidade compartilhada entre empresas e usuários. Enquanto as organizações devem garantir transparência e segurança no armazenamento das informações, os consumidores também precisam adotar práticas seguras ao compartilhar seus dados. Dessa forma, a combinação entre tecnologia, conscientização e responsabilidade pode proporcionar um ambiente digital mais seguro, confiável e alinhado às necessidades atuais de proteção de dados pessoais.

REFERÊNCIAS

Albertin Luiz Alberto.

ALBERTIN, Luiz Alberto. Administração de informática: funções e fatores críticos de sucesso. 6. ed. São Paulo: Atlas, 2016.

BRASIL. Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais). Dispõe sobre o tratamento de dados pessoais.

Autoridade Nacional de Proteção de Dados

ANPD. Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento, 2021. Documento que detalha medidas de segurança, prevenção de vazamentos e controle de acesso a dados pessoais.

Etec "Profª Anna de Oliveira Ferraz"

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. São Paulo: Forense, 2019.

COELHO, F. C.; CARVALHO, A. M. A.
A Ciência da Informação e a Lei Geral de Proteção de Dados (LGPD): uma revisão sistemática de literatura.
Revista Informação & Informação, 2025.

Receita Federal (Portal Redesim): Base para a solução "Proteja seu CPF" (bloqueio de abertura de empresas).
Banco Central do Brasil (BC): Base para as ferramentas "BC Protege+" e "Registrato".

Lei Geral de Proteção de Dados (LGPD): Base para as diretrizes de cuidado com compartilhamento de dados.

BRASIL.
Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).
Brasília, DF, 2018.

BRASIL.
Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Brasília, DF, 2014.

BRASIL.
Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Brasília, DF, 1990.

Associação Brasileira de Normas Técnicas.
ABNT NBR ISO/IEC 27001:2022 – Sistemas de Gestão de Segurança da Informação.

Brasil. Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD).

VARELLA, João Pedro.
ISO/IEC 27002 x LGPD: abrangência da ISO em relação à LGPD.
Faculdade de Tecnologia de São Paulo, 2021.

DONEDA, Danilo.
Da Privacidade à Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2019.

► Obra clássica sobre proteção de dados no Brasil.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais.
ABNT. NBR ISO/IEC 27001:2022.

Etec “Profª Anna de Oliveira Ferraz”

ABNT. NBR ISO/IEC 27002:2022.

ABNT. NBR ISO/IEC 27701:2020.

ANPD. Guia de Segurança da Informação para Pequenos Negócios.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Dispõe sobre a proteção de dados pessoais. Disponível em:

<https://www.planalto.gov.br>. Acesso em: 24 abr. 2026.

SILVA, J. R.; SOUZA, M. A. Segurança da informação e proteção de dados pessoais no Brasil. Disponível em: Google Acadêmico. Acesso em: 24 abr. 2026.