FACULDADE PARA O DESENVOLVIMENTO SUSTENTÁVEL DA AMAZÔNIA
CURSO TECNÓLOGO EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

JEFFERSON CORREIA DO NASCIMENTO

ANÁLISES DA LGPD ALIADA À SEGURANÇA DA INFORMAÇÃO NO CONTEXTO DO DESENVOLVIMENTO DE SOFTWARES NO BRASIL

PARAUAPEBAS
2024

JEFFERSON CORREIA DO NASCIMENTO

ANÁLISES DA LGPD ALIADA À SEGURANÇA DA INFORMAÇÃO NO CONTEXTO DO DESENVOLVIMENTO DE SOFTWARES NO BRASIL

Trabalho de Conclusão de Curso (TCC) apresentado à Faculdade para o Desenvolvimento Sustentável da Amazônia (FADESA), como parte das exigências do Programa do curso Tecnólogo em Análise e Desenvolvimento de Sistemas para a obtenção do Título de Tecnólogo.

Orientador: Prof.ª Sara Debora Carvalho Cerqueira.

PARAUAPEBAS
2024

NASCIMENTO, Jefferson Correia

ANÁLISES DA LGPD ALIADA À SEGURANÇA DA INFORMAÇÃO NO CONTEXTO DO DESENVOLVIMENTO DE SOFTWARES NO BRASIL; Sara Debora Carvalho Cerqueira - 2024.

48 f.

Trabalho de Conclusão de Curso (Graduação) – Faculdade para o Desenvolvimento Sustentável da Amazônia - FADESA, Parauapebas – PA, 2024.

Palavras – Chave: LGPD. Banco de dados. *Softwares*. Criptografia. ANPD.

Nota: A versão original deste trabalho de conclusão de curso encontra-se disponível no Serviço de Biblioteca e Documentação da Faculdade para o Desenvolvimento Sustentável da Amazônia – FADESA em Parauapebas – PA.

JEFFERSON CORREIA DO NASCIMENTO

ANÁLISES DA LGPD ALIADA À SEGURANÇA DA INFORMAÇÃO NO CONTEXTO DO DESENVOLVIMENTO DE SOFTWARES NO BRASIL.

Trabalho de Conclusão de Curso (TCC) apresentado à Faculdade para o Desenvolvimento Sustentável da Amazônia (FADESA), como parte das exigências do Programa do Curso de Análise e Desenvolvimento de Sistemas para a obtenção do Título de Tecnólogo.

Aprovado em: 11 / 06 /2025 .

Banca Examinadora

Prof. Esp. Antônio Soares da Silva
Faculdade para o Desenvolvimento Sustentável da Amazônia
(Avaliador)

Prof.ª Sara Debora Carvalho Cerqueira
Faculdade para o Desenvolvimento Sustentável da Amazônia
(Orientadora)

Prof. Esp. Adriano Louzada Bollas
Faculdade para o Desenvolvimento Sustentável da Amazônia
(Avaliador)

Data de depósito do trabalho de conclusão ____/_____/_____.

JEFFERSON CORREIA DO NASCIMENTO

ANÁLISES DA LGPD ALIADA À SEGURANÇA DA INFORMAÇÃO NO CONTEXTO DO DESENVOLVIMENTO DE SOFTWARES NO BRASIL.

Trabalho de Conclusão de Curso (TCC) apresentado à Faculdade para o Desenvolvimento Sustentável da Amazônia (FADESA), como parte das exigências do Programa do Curso tecnólogo em Análise e Desenvolvimento de Sistemas, para a obtenção do Título de tecnólogo.

Aprovado em: _____/_____/_____.

gov.br
Documento assinado digitalmente
JEFFERSON CORREIA DO NASCIMENTO
Data: 07/08/2025 18:46:57-0300
Verifique em https://validar.iti.gov.br

_____
Jefferson Correia Do Nascimento
(Discente)

_____
Prof. Esp. Antônio Soares da Silva
(Coordenador do Curso de Análise e Desenvolvimento de Sistemas)

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me acompanhado em todos os momentos da minha vida, à Ele seja dada toda a honra, glória e louvor, sou grato por ter a oportunidade de conquistar mais uma vitória, à minha família, principalmente minha esposa, e amigos pelo apoio incondicional dando-me força em todos os momentos, aos colegas de turma e de trabalho, que me motivaram diáriamente a seguir trabalhando em busca dos meus sonhos, de grande importância foi para mim conhecê-los.

Aos coordenadores, professores, com ênfase à minha orientadora, professora Sara Debora Carvalho Cerqueira, e todo o efetivo da universidade, que não mediram esforços e se doaram por inteiro em todo esse processo acadêmico, que necessita de muito conhecimento e empenho para uma melhor disseminação do aprendizado, e todos que participaram e contribuíram diretamente ou indiretamente para a conclusão deste curso.

“História nossas histórias, dias de lutas dias de glória.” Charlie Brown Jr.

RESUMO

A LGPD surgiu como um marco regulatório fundamental para a proteção de dados no Brasil. O presente trabalho busca fazer uma análise a respeito das aplicações da LGPD no contexto da segurança da informação com ênfase no desenvolvimento de software no Brasil. A pesquisa foi dividida em 2 partes. Na primeira buscou-se através de revisão bibliográfica analisar a história da LGPD, as aplicações da mesma na segurança da informação, história e conceitos sobre banco de dados, criptografia, ambiente de desenvolvimento seguro, crimes cibernéticos e penalidades para o descumprimento da lei. Na segunda parte foi realizada uma análise documental com o levantamento de alguns dados quantitativos, retirados do site oficial da ANPD que apresentam números oficiais relacionados ao tratamento de dados no Brasil. Através desse trabalho espera-se que o leitor tenha a percepção da importância da adequação junto à LGPD, para tornar um mundo digital mais seguro.

Palavras-chave: LGPD. Banco de dados. *Softwares*. Criptografia. ANPD.

ABSTRACT

The LGPD emerged as a fundamental regulatory framework for data protection in Brazil. This work seeks to analyze the applications of the LGPD in the context of information security with an emphasis on software development in Brazil. The research was divided into 2 parts. In the first, we sought through a bibliographic review to analyze the history of the LGPD, its applications in information security, history and concepts about databases, cryptography, secure development environment, cybercrimes and penalties for non-compliance with the law. In the second part, a documentary analysis was carried out with the collection of some quantitative data, taken from the official ANPD website, which presents official figures related to data processing in Brazil. Through this work, it is hoped that the reader will understand the importance of adapting to the LGPD, to make a safer digital world.

Keywords: LGPD. Database. Software. Cryptography. ANPD

LISTA DE ILUSTRAÇÕES

FIGURA

QUADRO

LISTAS DE ABREVIATURAS E SIGLAS

TIC - Tecnologias de Informação e Comunicação
LGPD - Lei Geral de Proteção de Dados
GDPR - *General Data Protection Regulation*
ANPD - Agência Nacional de Proteção de Dados
CGF - Coordenação-Geral de Fiscalização
SSH - *Secure Shell*
TLS - *Transport Layer Security*
SQL - *Structured Query Language*
JSON - *JavaScript Object Notation*
BSON - *Binary JSON*
DPO - *Data Protection Officer*
CIS - Comunicados de Incidentes de Segurança
RIPD - Relatório de Impacto à Proteção de Dados
CI/CD - *Continuous Integration/Continuous Deployment*
IA - Inteligência Artificial
ML - *Machine Learning*

SUMÁRIO

1. INTRODUÇÃO

A nova era digital tem transformado de forma surreal a maneira como o ser humano interage entre si nos dias atuais, nesse contexto o uso de ferramentas digitais como softwares tem se popularizado cada vez mais, tornando-os indispensáveis no dia-a-dia das pessoas. São as chamadas Tecnologias de Informação e Comunicação (TIC's), que tem desempenhado o papel de conectar a sociedade ao novo mundo digital.

As tecnologias de informação e comunicação (TICs) modernas, como os computadores, o acesso à internet e os telefones celulares estão revolucionando a forma como as pessoas se comunicam, se socializam, buscam, trocam informações e adquirem conhecimento (Abreu, 2013).

No Brasil esta enorme crescente digital tem sido bastante perceptível, e traz consigo o surgimento de inúmeros softwares e ferramentas web que visam suprir necessidades identificadas por seus desenvolvedores. Aliado a todo esse crescimento há também inúmeras vantagens, mas também tem se levantado sérias preocupações relacionadas à privacidade e à segurança das informações dos usuários, já que essas ferramentas necessitam fazer o uso de dados pessoais em alguns de seus processos.

Com o grande aumento no desenvolvimento de softwares de diversas modalidades e com funcionalidades capazes de chamar a atenção dos usuários, tornou-se mais fácil a propagação de softwares maliciosos, que visam apropriar-se ilegalmente de informações sensíveis dos usuários. Sendo assim é valido afirmar que a problemática em torno do tema está atrelada ao seguinte questionamento: Em que sentido o surgimento da LGPD afeta a relação entre desenvolvedores de software e os usuários no que se refere à segurança da informação e privacidade dos dados pessoais no cenário brasileiro?

A Lei Geral de Proteção de Dados (LGPD), implementada no Brasil em setembro de 2020, surgiu como um marco regulatório fundamental para garantir a proteção dos direitos individuais em um mundo cada vez mais conectado. É válido frisar que a LGPD foi inspirada em regulamentos europeus como o GDPR (General Data Protection Regulation), e como a norma acima citada a LGPD estabelece um novo paradigma para o tratamento de dados pessoais por organizações públicas e privadas.

De acordo com Soler (2022, p.10) à respeito da LGPD,

> A LGPD é uma norma robusta que traz previsões acerca da forma pela qual são tratados dados pessoais, tanto no meio físico quanto digital, por pessoas físicas ou jurídica, de direito público ou privado, sendo aplicável, inclusive, a todos os entes federativos em razão de sua relevância nacional.

Portanto a presente pesquisa tem como objetivo geral, contribuir com o conhecimento por meio de uma análise aprofundada da Lei Geral de Proteção de Dados (LGPD), no contexto do desenvolvimento de software e dos usuários. Para que o objetivo geral desse trabalho seja alcançado, foram definidos os seguintes objetivos específicos: explorar a LGPD; investigar o impacto da LGPD nas práticas de coleta e tratamento de dados no contexto da segurança da informação e do desenvolvimento de software no Brasil; frisar a importância da conformidade com a LGPD e as penalidades do não cumprimento da mesma pelas organizações.

Com a transformação digital citada nos parágrafos anteriores e o surgimento da LGPD para regulamentar o tratamento de dados pessoais, a presente pesquisa justifica-se pela necessidade de analisar o considerável aumento dos casos de vazamentos de dados no Brasil, já que, segundo Otávio (2023) “Pesquisa da Tenable, empresa americana especializada em gerenciamento de exposição cibernética, aponta que 984,7 milhões de dados foram vazados no Brasil no ano passado”.

A aplicação da LGPD no contexto da segurança da informação e do desenvolvimento de software no Brasil, representa um desafio significativo, porém de suma importância, pois no que se refere à dados pessoais é indispensável a adoção de algumas práticas seguras de tratamento destes, para que mantenham-se íntegros e estejam seguros de possíveis vazamentos. Medidas como a criptografia, controle de acesso, monitoramento de sistemas e treinamento contínuo dos funcionários são práticas recomendadas que ajudam a garantir a confidencialidade, integridade e disponibilidade dos dados pessoais.

O estudo das análises da LGPD aliada à segurança da informação no contexto do desenvolvimento de softwares no Brasil é justificado pela necessidade de entender o cumprimento da legislação, proteger a privacidade dos usuários, prevenir violações de dados, aumentar a competitividade empresarial, desenvolver softwares mais seguros, estimular a inovação responsável e proteger a soberania nacional. Por essas razões destaca-se a importância crítica desse campo de estudo

para a segurança, privacidade e desenvolvimento tecnológico do país, incluindo a necessidade de medidas técnicas e administrativas para garantir a segurança da informação.

2. HISTÓRIA E EVOLUÇÃO DA LGPD

A LGPD (Lei Geral de Proteção de Dados) ou Lei n. 13.709, é uma legislação brasileira que foi sancionada em 14 de agosto de 2018 mas só entrou em vigor no ano de 2020, mais precisamente em setembro. Desde então esta lei passou a representar um marco histórico no que se refere à proteção de dados pessoais no Brasil, alinhando o país às melhores práticas internacionais nesse sentido.

Para explorar um pouco da história da LGPD é necessário que se volte à meados do início do século XXI, onde com a explosão da era digital e o avanço da tecnologia em grandes proporções, passaram a surgir inúmeras preocupações à respeito da privacidade e da segurança dos dados pessoais dos cidadãos brasileiros. Ao redor do mundo, governos e organizações começaram a dar mais atenção para a necessidade de regulamentar o tratamento dessas informações sensíveis, o que garante direitos fundamentais de privacidade aos indivíduos.

No Brasil não foi diferente, e esse processo resultou na criação da Lei n. 13.709, a chamada LGPD (Lei Geral de Proteção de Dados), que foi sancionada em 2018, porém só entrou em vigor em meados de setembro de 2020. No entanto desde o ano de 2010 a LGPD já vinha sendo desenvolvida, e desde então o Brasil passou a fazer parte dos países que possuem legislações sobre proteção de dados (LUGATI, 2020).

A necessidade de proteção á privacidade dos cidadãos ganhou destaque em escala mundial através da aprovação do Regulamento Geral de Proteção de Dados (GDPR) pela União Europeia, no ano de 2018. O GDPR estabeleceu um padrão rigoroso para a proteção de dados pessoais, e através dessa lei passou a surgir legislações semelhantes em todo o mundo, incluindo o Brasil. Segundo Lugati (2020, p.2):

> A União Europeia, que já tinha históricos de legislações como a Convenção 108 e a Diretiva 95/46, implementou uma legislação de proteção de dados extensiva e que regulamentou o tratamento de dados pelos seus signatários, qual seja, a General Data Protection Regulation (GDPR). A criação dessa legislação serviu como catalisador para outros países e dessa forma, o Brasil cria, em 2018, a Lei Geral de Proteção de Dados (LGPD).

Portanto é válido afirmar que a LGPD foi inspirada em princípios semelhantes aos do GDPR, tendo como o objetivo principal dar maior controle aos cidadãos brasileiros sobre suas informações pessoais. Esta lei garante direitos fundamentais aos cidadãos como: o direito à informação, o direito de acesso aos dados, o direito à correção e exclusão de informações incorretas, e o direito de ser informado sobre o tratamento dos seus dados.

Além disso a legislação também impõe obrigações às organizações que coletam e tratam dados pessoais, exigindo que elas adotem medidas rigorosas de segurança e transparência. Empresas e órgãos governamentais passaram a ser responsáveis por garantir que os dados pessoais sejam usados de maneira ética e segura, sob pena de multas significativas em caso de violações.

Outro passo importantíssimo no processo de implementação da LGPD foi a criação da Autoridade Nacional de Proteção de Dados ANPD, que de acordo com Luz, Maia, Magalhães (2023, p. 64) “é o órgão responsável pela regulamentação e fiscalização da LGPD no Brasil”. Sendo assim pode-se dizer que o papel da ANPD é fiscalizar o cumprimento da Lei Geral de Proteção de Dados, além de orientar as organizações sobre as melhores práticas em proteção de dados, e por fim atuar como um mediador em casos de disputa.

Em resumo, a história da LGPD está associada à adaptação do Brasil à nova realidade digital que se encontra em constante crescente, reconhecendo a importância da privacidade e da proteção dos dados pessoais no mundo moderno. A implementação eficaz dessa legislação é crucial para garantir que os direitos fundamentais dos cidadãos sejam preservados, evitando vazamentos de dados pessoais e acessos não autorizados estabelecendo as diretrizes e obrigações legais para o tratamento de dados em um ambiente cada vez mais digitalizado e interconectado.

2.1 Conceitos importantes sobre a LGPD

Como foi visto nos parágrafos anteriores a Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que tem como objetivo principal regulamentar o tratamento de dados pessoais no país, visando proteger a privacidade e os direitos fundamentais dos cidadãos em relação às suas informações pessoais. Essa lei

aliada à segurança da informação, se torna um componente essencial para a gestão e proteção dos dados pessoais. Sendo assim, a seguir serão listados alguns conceitos fundamentais que regem a LGPD:

Quadro 1 - Conceitos fundamentais que regem A LGPD

Conceito	Definição
Dados Pessoais	A LGPD define dados pessoais como informações relacionadas à uma pessoa natural identificada ou identificável. Isso inclui nome, CPF, RG, endereço, e-mail, entre outros.
Tratamento de Dados	Refere-se à todas as operações realizadas através do uso de dados pessoais, tais como: coleta, armazenamento, uso, compartilhamento e exclusão.
Controlador	É a pessoa ou entidade responsável por tomar decisões sobre o tratamento dos dados pessoais. Isso pode ser uma empresa, organização ou mesmo uma pessoa física.
Operador	É a pessoa ou entidade que realiza o tratamento de dados em nome do controlador. Por exemplo, um provedor de serviços de nuvem que armazena dados de uma determinada empresa é considerado um operador.
Consentimento	Segundo o que a LGPD estabelece, o tratamento de dados pessoais deve ser realizado com o consentimento do titular dos dados. Sendo assim esse consentimento deve ser livre, informado e inequívoco, tendo o titular o direito de retirá-lo a qualquer momento.
Princípios da LGPD	A lei estabelece princípios fundamentais, como a finalidade específica, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização, que devem ser seguidos no tratamento de dados pessoais.
DPO (Data Protection Officer)	Em muitas organizações há a obrigação de designar um DPO, que nada mais é do que um profissional responsável por garantir o cumprimento da LGPD dentro da organização, e atuar como ponte de contato entre os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
Direitos dos Titulares	A LGPD estabelece aos titulares dos dados diversos direitos, como o direito ao acesso dos seus dados, correção, solicitação de exclusão, revogação do consentimento, entre outros.
Notificação de Incidentes	A lei exige que as organizações notifiquem imediatamente a ANPD e os titulares dos dados em caso de incidentes de segurança que possam comprometer a privacidade dos dados pessoais.
Sanções e Penalidades	A LGPD prevê sanções para o não cumprimento da lei, que podem ir de multas significativas, advertências, bloqueio dos dados e até mesmo a proibição total ou parcial das atividades de tratamento de dados.

Fonte: Desenvolvimento do autor (2024).

É fundamental que as empresas estejam em conformidade com a lei para evitar sanções e, ao mesmo tempo, conquistar a confiança dos consumidores em relação à proteção de seus dados. Para isso a Lei Geral de Proteção de Dados estabelece diretrizes claras sobre como os dados pessoais devem ser coletados, armazenados, processados e compartilhados, impondo obrigações às empresas e concedendo direitos aos titulares dos dados.

Portanto conclui-se que a LGPD representa um marco importante no processo de proteção da privacidade e dos direitos individuais no Brasil, incentivando as empresas e organizações a adotarem práticas responsáveis no tratamento de dados pessoais.

2.2 A proteção de dados no Brasil

Antes que seja abordado à respeito da proteção de dados é necessário analisar brevemente o conceito referente à bancos de dados. Primeiramente à respeito de banco de dados, de acordo com Wikipédia (2024) “são conjuntos de arquivos relacionados entre si, podendo conter registros sobre pessoas, lugares ou informações em geral”. Ou seja, pode-se afirmar que bancos de dados são sistemas complexos e inter-relacionados que têm como principal objetivo armazenar, organizar e fornecer acesso eficiente à diversos dados, fornecendo assim inúmeras aplicações no âmbito digital.

Sendo assim, pode-se dizer que os bancos de dados são repositórios estruturados que armazenam informações de forma organizada. Os bancos de dados são dinâmicos, e não estáticos, permitindo assim a rápida recuperação, atualização e manipulação dos dados contidos. Portanto no que se diz respeito à banco de dados Doneda (2011, p. 92) conceitua:

> Bancos de dados são, em sua acepção fundamental, um conjunto de informações estruturado de acordo com uma determinada lógica – e esta lógica é sempre uma lógica utilitarista, uma lógica que procura proporcionar a extração do máximo de proveito possível a partir de um conjunto de informações.

Então é correto afirmar que os banco de dados são projetados para lidar com grandes volumes de informações, e oferecer eficiência no acesso a esses dados, proporcionando uma base sólida para diversas aplicações. Além disso é válido frisar que um banco de dados possui sua estrutura moldada por seu modelo, sendo que cada modelo possui uma estrutura lógica que contém relações e restrições de forma à determinar como serão armazenados e acessados os dados. Modelos estes que serão representados nos próximos parágrafos.

Modelo hierárquico Organiza dados em uma estrutura em forma de árvore. Nesse modelo, os dados são armazenados em registros que são conectados

através de relacionamentos de "pai e filho". Cada registro pode ter múltiplos filhos, mas cada filho só pode ter um único pai, refletindo uma hierarquia.

Modelo relacional organiza os dados em tabelas, também chamadas de relações. Cada tabela é composta por linhas e colunas, onde cada linha representa um registro único e cada coluna representa um atributo desse registro. Os bancos de dados relacionais utilizam a linguagem SQL (Structured Query Language) para definição, manipulação e consulta dos dados.

Modelo de rede permite que os dados sejam organizados em uma estrutura de gráfico, onde os registros podem ter múltiplos relacionamentos complexos entre si. Isso é diferente do modelo hierárquico tradicional que permite apenas relações de um-para-muitos. No modelo de rede, as entidades são organizadas em um gráfico, onde os nós representam registros e os arcos representam as relações.

Modelo orientado para objetos integra conceitos da programação orientada a objetos com os sistemas de banco de dados. Nesse modelo, os dados são armazenados na forma de objetos, similarmente ao modo como são manipulados em linguagens de programação orientadas a objetos como Java, C++, ou Python.

Modelo entidade-relacionamento é uma metodologia de modelagem de dados que ajuda a descrever a estrutura lógica dos dados de um sistema de informação. Esse modelo é amplamente utilizado na fase de design de sistemas de bancos de dados relacionais, ajudando a identificar e organizar os dados de maneira lógica e clara.

Modelo documental é um tipo de sistema de gerenciamento de banco de dados NoSQL que armazena dados na forma de documentos. Esses documentos são tipicamente representados em formatos como JSON (JavaScript Object Notation), BSON (Binary JSON), XML (eXtensible Markup Language), ou YAML (Ain't Markup Language). Cada documento é uma unidade autônoma de dados que pode conter uma variedade de tipos de informações, incluindo listas, arrays e objetos aninhados.

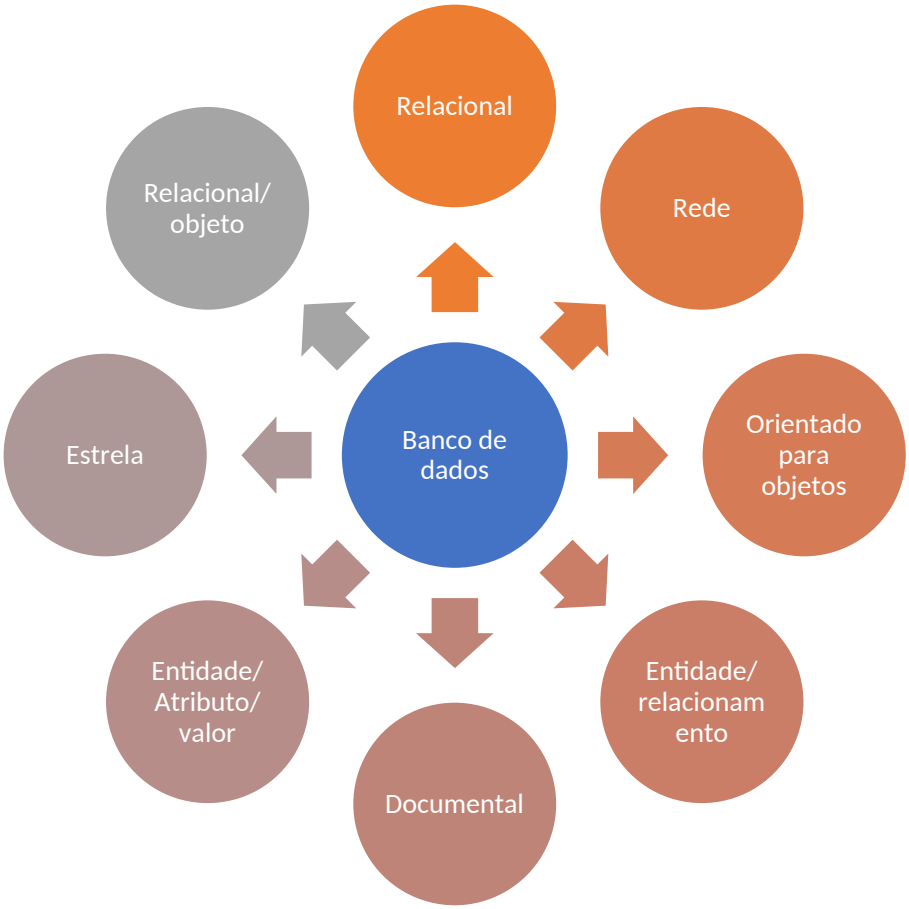
Modelo entidade-atributo-valor é uma abordagem para armazenar dados em que os valores são armazenados em uma estrutura de tabela altamente flexível. Este modelo é particularmente útil quando os atributos de dados variam amplamente entre diferentes registros e quando a estrutura de dados não é fixa ou bem definida.

Esquema em estrela é uma arquitetura de modelagem de dados comumente utilizada em sistemas de data warehouse e em ambientes de Business Intelligence

(BI). Este esquema facilita a análise de grandes volumes de dados, oferecendo uma estrutura simples e eficiente para consultas complexas.

Modelo relacional-objeto combina conceitos de banco de dados relacionais com características de orientação a objetos. Este modelo visa integrar a robustez e a simplicidade dos bancos de dados relacionais com a flexibilidade e a capacidade de modelagem dos sistemas orientados a objetos. A Figura 1 abaixo representa os modelos de banco de dados citados a cima.

Figura 1 – Modelos de Banco de Dados



Fonte: Desenvolvimento do autor (2024).

Em resumo, os bancos de dados são mais do que meros depósitos de dados; pelo contrário, são eles que dão forma à paisagem informacional da sociedade moderna. A contínua evolução dos bancos de dados refletem não apenas os avanços tecnológicos, mas também a crescente necessidade de gerenciar de forma inteligennte e precisa a imensidão de dados que impulsionam o mundo digital.

Agora que foi abordado um pouco à respeito do conceito de banco de dados, é possível analisar que na era da informação, onde os dados fluem de maneira vital nos sistemas digitais, a responsabilidade associada à coleta, armazenamento e utilização dessas informações tornou-se uma questão de atenção contínua, pois essa enorme quantidade de dados requer maiores cuidados na forma como protegê-los.

Na sociedade brasileira contemporânea houve uma explosão crescente na geração de dados, potencializada por novas tecnologias que se fazem presentes na vida das pessoas. Nesse sentido a responsabilidade na proteção de dados não é apenas uma obrigação técnica, mas uma responsabilidade ética. À medida que as organizações e indivíduos acumulam uma grande quantidade de informações, a confiança no tratamento dos dados pessoais torna-se um elemento crucial. A criação da LGPD fez com que o público, clientes e parceiros se tranquilizassem pela garantia de que seus dados serão tratados com respeito, integridade e segurança.

Proteger a privacidade surge como a premissa para a proteção de dados. Sendo assim a lei que antecedeu à LGPD, o Marco Civil da Internet (mci, Lei nº 12.965/2014) nos seus artigos. 3º, 7º e 8º define no que se refere ao direito de acesso à rede que, a garantia da privacidade e de proteção de dados pessoais é indispensável (BRASIL,2014).

Portanto à medida que a tecnologia avança, a coleta de dados pessoais torna-se inevitável durante o processamento dos serviços digitais. No entanto, a transparência no processo e a implementação de medidas robustas de segurança são imperativas para assegurar que os dados sensíveis estejam sendo manipulados de forma devida.

Além disso, a responsabilidade de dados estende-se ao ciclo de tratamento de dados completo, desde a coleta até a exclusão. A devida atenção na exclusão segura de dados é tão crucial quanto sua proteção durante o armazenamento. Isso não apenas respeita o direito à privacidade, mas também reduz os riscos associados ao vazamento de informações, adotando medidas técnicas e administrativas para proteger esses dados garantindo assim os pilares da responsabilidade na proteção de dados, tais como: Conformidade Legal, Segurança da Informação, Transparência, Responsabilidade Interna e Resposta a Incidentes.

Em última análise, a responsabilidade na proteção de dados é uma jornada constante que demanda o equilíbrio entre a inovação tecnológica e o respeito pelos

direitos individuais. À medida que avançamos em um mundo cada vez mais digital, cultivar uma cultura de responsabilidade de proteção de dados é essencial para sustentar a confiança, preservar a privacidade e construir um futuro digital ético e sustentável. A responsabilidade na proteção de dados é um compromisso contínuo que requer a colaboração de todos os níveis da organização, afim de manter-se em conformidade com as diretrizes da LGPD.

3. LGPD E A SEGURANÇA DA INFORMAÇÃO

Como já abordado no presente trabalho, a Lei Geral de Proteção de Dados (LGPD), instituída no Brasil, surgiu como um marco regulatório no intuito de salvaguardar a privacidade e a segurança das informações pessoais dos cidadãos. Essa importante legislação está diretamente ligada ao âmbito da Segurança da Informação, sendo que ambas formam uma sinergia vital no ambiente digital brasileiro contemporâneo.

A LGPD, lei que entrou em vigor em setembro de 2020, confere aos indivíduos o controle sobre seus dados pessoais, exigindo transparência, segurança e consentimento no tratamento dessas informações sensíveis. Essa abordagem não apenas reforça a confiança entre as organizações e seus clientes, mas também redireciona o foco para a necessidade imperativa de proteção contra incidentes de segurança cibernética.

A interseção entre a LGPD e a Segurança da Informação é evidente na própria essência da lei. Proteger dados pessoais vai além da conformidade legal; é uma questão de preservar a integridade, confidencialidade e disponibilidade da informação. As organizações são instigadas não apenas a aderir às normativas da LGPD, mas a internalizar práticas robustas de segurança da informação.

A implementação eficaz da LGPD implica a adoção de medidas proativas para prevenir, detectar e responder a violações de dados. Isso inclui a criação de políticas de segurança da informação abrangentes, a implementação de sistemas de criptografia, a condução de avaliações de riscos regulares e a capacitação contínua dos colaboradores em práticas seguras.

Porém quando se fala em conformidade entre as instituições e a LGPD no que se refere à dados pessoais, é importante citar o papel dos agentes de tratamento de dados que segundo a ANPD (2022, p.6) ”Os agentes de tratamento são os responsáveis pelo tratamento dos dados pessoais, sujeitos às regras da

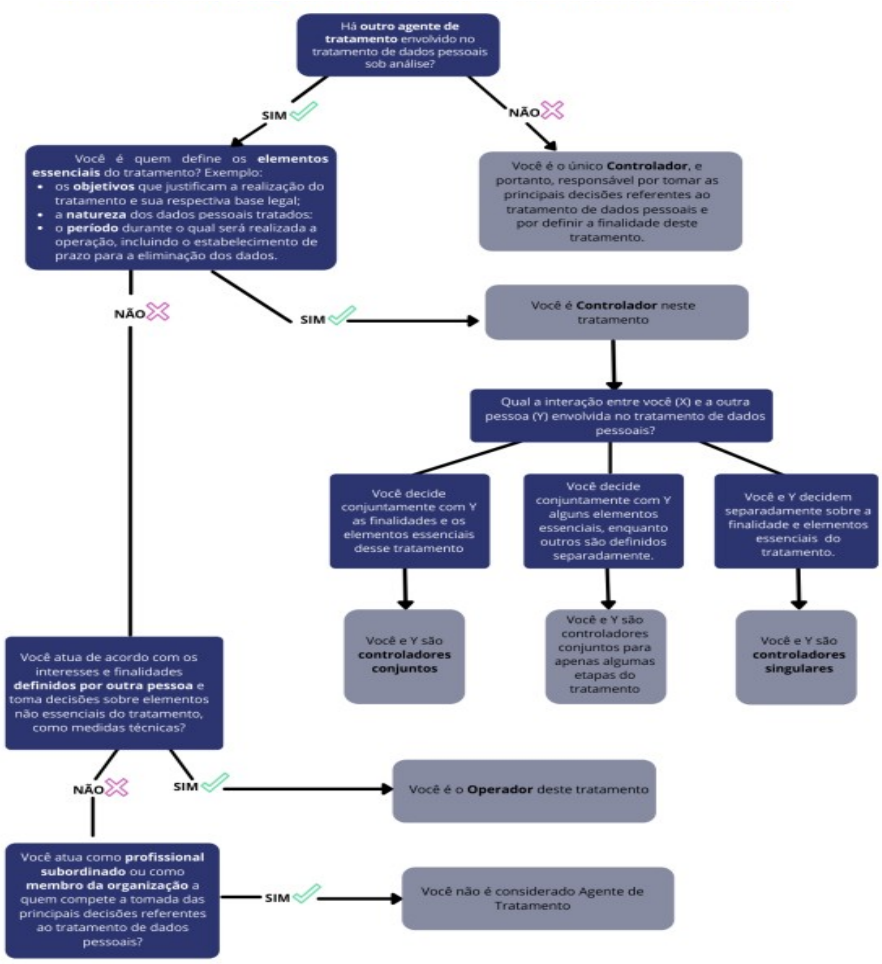
LGPD e à fiscalização da ANPD". De forma simples os agentes de tratamento de dados são indivíduos ou entidades responsáveis pela manipulação de informações pessoais, abrangendo atividades de coleta, armazenamento, processamento e compartilhamento de dados.

Esses agentes podem ser classificados em duas categorias principais: controlador e operador. Referente à controlador de acordo com a LGPD (LEI Nº 13.709 art. 5º, VI/2018) "controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;". Ou seja, o controlador é aquele que detém a responsabilidade de decidir sobre o tratamento dos dados, definindo as finalidades e os meios utilizados.

Também de acordo com a LGPD (LEI Nº 13.709/2018) no artigo 5º VII o operador é uma pessoa natural ou jurídica, de direito público ou privado que segue as instruções do controlador e realiza o tratamento de dados pessoais em nome do mesmo (BRASIL,2018). Ambos os papéis são essenciais para garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD) no Brasil, assegurando assim que as informações sejam tratadas de maneira segura, ética e transparente.

A Figura1 ilustra o fluxo que define os papéis do controlador e operador:

Figura 2: Aplicação dos conceitos de Controlador e Operador



Fonte: ANPD (2022).

Sendo assim, para garantir tal conformidade com a lei, a gestão de incidentes torna-se uma peça fundamental. Com isso, seguindo a LGPD, as organizações são obrigadas a notificar incidentes de segurança que possam comprometer a privacidade dos dados. Uma resposta rápida e eficaz não apenas ameniza os danos, mas também demonstra o comprometimento da organização com a proteção dos dados de seus clientes, incorporando medidas de segurança desde o início do desenvolvimento de produtos e serviços, garantindo que a proteção de dados seja uma consideração central em todas as etapas.

A LGPD e a Segurança da Informação devem caminhar juntas com o propósito de resguardar a confiança digital. As organizações que se adequam à lei não apenas cumprem os requisitos legais, mas estabelecem uma base sólida na construção de relacionamentos duradouros com seus clientes, baseados na confiança mútua e na certeza de que os dados pessoais estarão seguros.

3.1 A criptografia

Quando se fala à respeito da história da criptografia nota-se uma incrível jornada ao longo dos séculos, cheia de surpresas e, principalmente, uma busca incessante por proteger informações sensíveis. Desde os primórdios da civilização até a era atual, também chamada de era digital, a humanidade tem desenvolvido e moldado técnicas de criptografia afim de proteger mensagens importantes e garantir a confidencialidade das informações compartilhadas através do processo de comunicação. O presente tópico tem como objetivo retratar a história do processo de criptografia, através de uma abordagem cronológica dos fatos.

Históricamente falando, os primeiros vestígios da criptografia remontam às civilizações antigas, sendo que um dos modelos mais famosos de criptografia são as chamadas Cifras de César, método utilizado por Júlio César na Roma Antiga para criptografar suas mensagens. O conceito adotado na Cifra de César consistia na substituição de cada letra do alfabeto por outra letra correspondente seguindo um determinado padrão, definidos por uma tabela (Takata, 2017).

Já durante o Renascimento, Leon Battista Alberti, um polímata italiano, introduziu a cifra polialfabética, um avanço significativo que consistia em utilizar diferentes alfabetos para cifrar uma mensagem. Esse método aumentou a complexidade das cifras, tornando-as mais difíceis de quebrar. A respeito do método de criptografia de Leon Battista Alberti segundo Paixão (2020, p.123) “Propôs o uso de dois ou mais alfabetos cifrados, usados de maneira alternada, de modo a confundir criptoanalistas em potencial”. Ou seja, as cifras de Alberti tiveram um papel muito importante no processo de evolução da criptografia.

Porfim, já em um contexto mais contemporâneo, em meados de 1918, foi desenvolvida e patenteada na Alemanha por Arthur Scherbius, a máquina de criptografia Enigma, máquina que posteriormente seria utilizada pela Alemanha durante a Segunda Guerra Mundial. A Enigma foi um dispositivo eletromecânico utilizado para proteger comunicações militares através de complexos sistemas de cifragem. A Enigma teve seu uso pelo governo alemão iniciado no ano de 1926. Desde então as mensagens que os militares alemães trocavam foram impossibilitadas de serem lidas pelo resto do mundo (Silva, 2011).

Com seu design inovador, a Enigma consistia em uma série de rotores intercambiáveis que substituíam letras de mensagens com múltiplas camadas de encriptação, criando um vasto número de possíveis configurações. Essa complexidade tornou a criptografia Enigma extremamente difícil de ser quebrada, desempenhando um papel crucial na estratégia militar alemã. No entanto, os esforços combinados de matemáticos, criptógrafos e engenheiros aliados, incluindo o trabalho notável de Alan Turing e sua equipe em Bletchley Park, levaram à decifração do código Enigma. Portanto Silva (2011, p.44) destaca que:

> Graças a Turing tornou-se possível quebrar a cifra da Enigma mesmo sob as circunstâncias mais difíceis". Esse cientista, que fora professor da Universidade de Cambridge anos antes, já era bastante respeitado aos seus 26 anos, após o lançamento do seu trabalho mais influente, o "Sobre os números computáveis".

Os feitos significativos de Turing não apenas alteraram o curso da guerra, proporcionando vantagens táticas aos Aliados, mas também impulsionaram avanços importantes na computação e na teoria da informação que hoje são tão importante na vida das pessoas.

Com a ascensão da computação, a criptografia evoluiu rapidamente. A criação do RSA (Rivest, Shamir e Adleman) em 1977 marcou o advento da criptografia de chave pública, revolucionando a segurança digital. A capacidade de cifrar e decifrar mensagens utilizando chaves distintas representou um avanço notável.

Na era da internet, a criptografia é essencial para proteger transações online e garantir a segurança das comunicações. Protocolos como o SSH e SSL são usados para criar conexões seguras, enquanto algoritmos avançados, como AES, protegem dados sensíveis. A ascensão das criptomoedas, como o Bitcoin, trouxe consigo a tecnologia blockchain. Baseada em princípios criptográficos, a blockchain utiliza algoritmos para garantir a integridade e a segurança das transações, tornando-as praticamente imutáveis.

Apesar dos avanços, a criptografia enfrenta desafios constantes, especialmente diante de ameaças como computação quântica. Pesquisadores buscam algoritmos resistentes a essas tecnologias emergentes para manter a segurança no futuro digital. A história da criptografia é um testemunho da incessante busca por segurança e privacidade nas comunicações. Desde os primeiros hieróglifos até as complexas operações criptográficas contemporâneas, a evolução

dessas técnicas reflete a eterna batalha entre quem quer proteger informações e aqueles que buscam desvendá-las.

3.1.1 Secure Shell (SSH) e Transport Layer Security (TLS).

Como já foi abordado na presente pesquisa a segurança da informação é uma preocupação fundamental na atual era digital. A troca de dados sensíveis e a comunicação entre sistemas devem ser protegidas contra ameaças cibernéticas. Nesse contexto, dois protocolos desempenham papéis cruciais: o SSH (Secure Shell) e o TLS (Transport Layer Security). Ambos foram projetados para garantir a confidencialidade e integridade das informações durante a transmissão.

O SSH é um protocolo de rede que permite a comunicação segura entre dois sistemas, geralmente um cliente e um servidor. Ele utiliza criptografia para proteger a autenticação, a confidencialidade e a integridade dos dados transmitidos, por isso é amplamente utilizado para realizar operações seguras em redes inseguras. Desenvolvido nos anos 1990, ele substitui protocolos antigos, como Telnet e rlogin, que transmitem dados sem criptografia, expondo informações sensíveis ao risco de interceptação. Sobre o protocolo SSH Gomes (2020, p.12) afirma que:

> O SSH é um protocolo para acesso remoto, uma tecnologia que permite a interação entre duas máquinas que estejam conectadas à rede. O protocolo oferece a troca segura de dados, para isso, utiliza-se um canal seguro entre dois dispositivos de redes, que por padrão utilizam a porta 22. Os serviços que implementam esse protocolo são bastante utilizados em sistemas baseados no Unix para permitir acesso ao Shell dos servidores.

Para melhor entendimento o SSH permite a administração remota segura de sistemas e a transferência de arquivos entre computadores e é amplamente utilizado em ambientes de administração de sistemas, permitindo acesso remoto a servidores de forma segura. O quadro 2 mostra três conceitos relacionados ao protocolo SSH.

Quadro 2 – SSH

Atividade	Definição
Criptografia Assimétrica	O SSH utiliza pares de chaves pública e privada para autenticação e estabelecimento de uma conexão segura.
Túneis Criptografados	As comunicações entre cliente e servidor são criptografadas, garantindo a confidencialidade dos dados durante a transmissão.
Autenticação Multi-Fator	Além da chave privada, o SSH suporta a autenticação por senha, proporcionando uma camada adicional de segurança.

Fonte: Desenvolvimento do autor (2024).

Em resumo, o protocolo SSH é uma ferramenta essencial para garantir a segurança das comunicações e operações remotas em ambientes de rede, oferecendo uma ampla gama de funcionalidades que protegem contra interceptações e ataques maliciosos, proporcionando maior segurança, flexibilidade e eficiência.

Já o TLS (Transport Layer Security) é um protocolo criptográfico projetado para fornecer comunicação segura sobre uma rede de computadores. TLS é a evolução do protocolo SSL (Secure Sockets Layer) e é amplamente utilizado para garantir a privacidade e a integridade dos dados transmitidos entre aplicações na Internet. Ele é fundamental para a segurança de transações online, como navegação na web, e-mails, e transferências bancárias. No quadro 3 há três benefícios proporcionados pelo protocolo TLS.

Quadro 3 – TLS

Atividade	Definição
Criptografia de Dados	TLS utiliza algoritmos de criptografia fortes para proteger os dados transmitidos entre cliente e servidor, garantindo que eles não possam ser lidos por terceiros interceptadores.
Certificados Digitais	Utiliza certificados digitais para autenticar a identidade do servidor, evitando ataques de intermediários mal-intencionados.
Integridade dos Dados	Utiliza funções de hash criptográficas para verificar a integridade dos dados, assegurando que a informação não foi alterada durante a transmissão.

Fonte: Desenvolvimento do autor (2024).

Portanto o protocolo TLS é indispensável para a segurança na internet moderna. Ele proporciona uma camada robusta de proteção para a transmissão de dados, garantindo que informações sensíveis permaneçam privadas e íntegras. De acordo com Gomes (2020, p.16) “O objetivo principal do TLS é garantir uma comunicação segura entre dois pares, transportando os dados em um canal seguro”.

Com a constante crescente das ameaças cibernéticas, a importância de protocolos como o TLS, que se adaptam e melhoram continuamente, não pode ser subestimada. A adoção e correta implementação do TLS são fundamentais para proteger a comunicação online e assegurar a confiança dos usuários nas tecnologias da informação.

Concluindo pode-se afirmar que tanto o SSH quanto o TLS desempenham papéis cruciais na criação de ambientes seguros na internet. O SSH sendo essencial

para a administração segura de sistemas remotos, enquanto que o TLS garante a segurança das transmissões de dados em aplicações web. Ambos os protocolos desempenham um papel indispensável na proteção contra ameaças cibernéticas, permitindo uma comunicação digital confiável em um mundo cada vez mais interconectado.

3.1.2 Privacidade de dados no desenvolvimento de software no Brasil

No cenário contemporâneo, a Lei Geral de Proteção de Dados (LGPD) emerge como um guia no processo do desenvolvimento de software, impondo diretrizes essenciais para garantir a proteção dos dados pessoais dos usuários. A convergência entre inovação tecnológica e respeito à privacidade é vital para promover um ambiente digital ético e seguro. Nesse tópico será explorado como a LGPD influencia e molda o desenvolvimento de software.

A LGPD estabelece princípios que devem ser observados no tratamento de dados pessoais. Princípios estes como a finalidade, necessidade, consentimento, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. É de responsabilidade dos desenvolvedores de software incorporar esses princípios desde a fase inicial do ciclo de vida do desenvolvimento, ou seja, precisam realizar um mapeamento detalhado dos dados que estão sendo tratados pelo software. Classificá-los de acordo com sua sensibilidade é crucial para a adoção de medidas adequadas de segurança e garantir o cumprimento da LGPD.

O desenvolvimento de software deve incluir mecanismos para obter consentimento claro e transparente dos usuários para o tratamento de seus dados pessoais. Isso envolve explicar de maneira compreensível como os dados serão utilizados, garantindo que os usuários estejam plenamente informados. Como analisado no princípio da finalidade da LGPD (Lei Nº 13.709/2018) no artigo 6º inciso I só é possível realizar tratamento de dados se houver a ciência do titular à respeito das finalidades específicas desses dados, não havendo possibilidade de tratamento para outros fins (BRASIL, 2018).

A Lei Geral de Proteção de Dados (LGPD) ainda enfatiza a necessidade de implementar medidas de segurança adequadas para proteger os dados pessoais contra acessos não autorizados. Algumas práticas robustas de segurança da informação devem ser adotadas pelos desenvolvedores, tais como: criptografia,

controle de acesso e monitoramento contínuo. Além disso destaca-se a importância da anonimização e pseudonimização dos dados pessoais para mitigar riscos. Os desenvolvedores devem incorporar técnicas que protejam a identidade dos titulares dos dados, mantendo a utilidade das informações.

A capacidade de rastrear e documentar o tratamento de dados é essencial para cumprir os requisitos da LGPD. Devendo ser implementadas funcionalidades que permitam a manutenção de registros e a realização de auditorias para demonstrar conformidade. A LGPD não é apenas uma responsabilidade jurídica, mas também cultural. As equipes de TI assim como os desenvolvedores devem receber treinamento contínuo sobre a devida observância da LGPD e a importância de integrar práticas de privacidade no desenvolvimento de software.

A LGPD e o desenvolvimento de software estão intrinsecamente ligados na era da transformação digital. Ao alinhar a inovação com os princípios da privacidade, os desenvolvedores não apenas atendem aos requisitos legais, mas também constroem confiança entre os usuários. Em última análise, a harmonização entre a LGPD e o desenvolvimento de software cria um ecossistema digital sustentável, onde a inovação prospera em paralelo com o respeito à privacidade e à segurança dos dados.

3.1.3 Evolução dos softwares

Desde os primórdios da computação até a atualidade, a evolução dos softwares tem sido marcada por avanços extraordinários, moldando a forma como interagimos com a tecnologia e transformando fundamentalmente a sociedade. Esta jornada fascinante é pontuada por diversas fases que refletem não apenas o progresso tecnológico, mas também as mudanças culturais e econômicas. A seguir está apresentado de forma breve a evolução dos softwares do início até os dias atuais.

A fase Inicial dos sotwares foi entre os anos de 1940-1950 com a Programação de Baixo Nível, nesse período os primeiros softwares eram escritos em linguagem de máquina, exigindo conhecimento detalhado da arquitetura do hardware. Os programadores criavam códigos de baixo nível, inserindo instruções diretamente nas máquinas.

Logo após entre os anos de 1950-1960, surgiram as Linguagens de Montagem e COBOL. A introdução de linguagens de montagem facilitou a programação, proporcionando uma abstração mais amigável para os programadores. COBOL, criada na década de 1950, surgiu como uma linguagem mais orientada a negócios.

Então entre os anos de 1960-1970 houve a revolução das linguagens de alto nível. A ascensão de linguagens como Fortran, Lisp e C proporcionou uma programação mais acessível e eficiente. A ideia de programação estruturada e modular começou a ganhar destaque, simplificando o desenvolvimento de software.

Na próxima década ente os anos de 1970-1980 surgiram os sistemas operacionais e interfaces gráficas. O surgimento de sistemas operacionais, como UNIX e MS-DOS, simplificou a interação com hardware. A década de 1980 testemunhou a popularização das interfaces gráficas de usuário (GUI), introduzindo sistemas como o Macintosh da Apple e o Windows da Microsoft.

Mais à frente no período de 1990-2000 surgiu era da internet e desenvolvimento ágil. A expansão da internet abriu novas possibilidades, softwares começaram a migrar para modelos distribuídos e sistemas cliente-servidor. O desenvolvimento ágil ganhou destaque, promovendo uma abordagem mais flexível e iterativa.

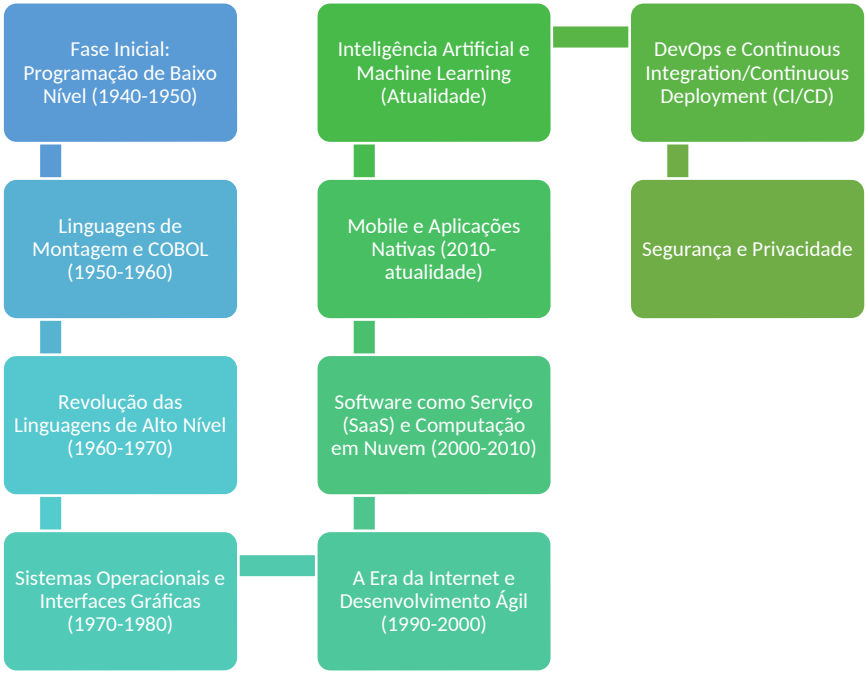
Já entre 2000-2010 surgiram o Software como Serviço (SaaS), e a Computação em Nuvem. O modelo SaaS transformou a entrega de softwares, permitindo o acesso através da web. A computação em nuvem revolucionou a infraestrutura, proporcionando escalabilidade e flexibilidade.

No período entre 2010 e atualidade houve a ascensão do mobile e aplicações nativas. O advento dos smartphones impulsionou o desenvolvimento em massa de aplicativos móveis. Plataformas como iOS e Android tornaram-se vitais, levando a uma proliferação de aplicativos para diversas finalidades e com ferramentas cada vez mais avançadas.

Continuando na atualidade houve então o surgimento de diversas tecnologias baseadas em inteligência artificial e *machine learning*. A aplicação de inteligência artificial (IA) e machine learning (ML) passou a transformar softwares em sistemas mais autônomos e adaptativos. Chatbots, assistentes virtuais e análise preditiva são apenas alguns exemplos dessa revolução.

Ainda no contexto atual surgiram o DevOps e *Continuous Integration/Continuous Deployment* (CI/CD). A metodologia DevOps e práticas CI/CD trouxeram automação e eficiência ao ciclo de vida do desenvolvimento de software, permitindo entregas rápidas e frequentes. E porfim o foco passou a ser principalmente em Segurança e Privacidade, pois com o aumento das ameaças cibernéticas, a segurança de software tornou-se uma prioridade. Questões de privacidade, como as regulamentações GDPR e LGPD, influenciam a forma como os softwares são desenvolvidos e mantidos.

Figura 3: Linha do tempo do desenvolvimento de software



Fonte: Desenvolvimento do autor (2024).

A evolução dos softwares é uma narrativa de inovação, superação de desafios e adaptação às necessidades crescentes da sociedade. Desde linhas de código de baixo nível até ecossistemas complexos de IA, os softwares continuam a moldar nosso mundo de maneiras inimagináveis, desempenhando papéis cruciais na próxima fase desta jornada tecnológica fascinante.

3.2 Ambiente de desenvolvimento seguro

No cenário brasileiro atual onde a cibersegurança é uma preocupação constante, garantir que haja um ambiente de desenvolvimento seguro é essencial na

proteção dos dados sensíveis, resguardar a integridade do software e controlar riscos de ameaças cibernéticas. No quadro 4 a seguir serão elencados alguns elementos fundamentais para que se possa criar e manter um ambiente de desenvolvimento seguro.

Quadro 4: Práticas de desenvolvimento seguro

Elemento	Definição
Segurança desde o Início	A abordagem mais eficaz é incorporar a segurança desde o início do ciclo de vida do desenvolvimento de software. Isso envolve educar a equipe sobre práticas seguras, estabelecer políticas de segurança claras e integrar avaliações de segurança nas fases iniciais do desenvolvimento.
Controle de acesso e autenticação forte	A implementação de controles de acesso rigorosos é vital. A autenticação forte, como a utilização de autenticação de dois fatores (2FA), adiciona uma camada extra de segurança, garantindo que apenas usuários autorizados tenham acesso ao ambiente de desenvolvimento.
Criptografia	O uso de criptografia para proteger dados em repouso e em trânsito é crucial. Isso impede que informações sensíveis sejam acessadas ou interceptadas por terceiros não autorizados.
Gestão de vulnerabilidades	Realizar varreduras regulares em busca de vulnerabilidades no código e nas dependências do software é uma prática importante. Corrigir rapidamente as falhas identificadas ajuda a manter o ambiente seguro.
Segregação de ambientes	Manter ambientes de desenvolvimento, teste e produção separados é essencial. Isso evita que testes ou desenvolvimentos incorretos afetem a integridade do sistema em produção.
Monitoramento contínuo	Implementar ferramentas de monitoramento contínuo permite a detecção rápida de atividades suspeitas. Logs e alertas devem ser analisados regularmente para identificar possíveis ameaças.
Atualizações e p*atching*	Manter todos os sistemas e software atualizados com as últimas correções de segurança é crucial. Isso inclui o sistema operacional, servidores web, bibliotecas e *frameworks* utilizados no desenvolvimento.
Educação e conscientização	Promover a educação e conscientização sobre segurança entre os membros da equipe é fundamental. A compreensão dos riscos e das melhores práticas de segurança contribui significativamente para a criação de um ambiente mais seguro.
Práticas de desenvolvimento seguro	Incorporar práticas de desenvolvimento seguro, como revisões de código, testes de segurança automatizados e revisões de arquitetura, ajuda a identificar e corrigir problemas de segurança durante o processo de desenvolvimento.
Backup e recuperação	Implementar políticas de backup regulares e testar procedimentos de recuperação é essencial para garantir a disponibilidade dos dados em caso de falhas ou ataques.

Fonte: Desenvolvimento do autor (2024).

A LGPD promove a integração de princípios de privacidade desde o início do processo de desenvolvimento, conhecido como *Privacy by Design*, que é um conceito fundamental na área de proteção de dados, que preconiza a integração da privacidade e proteção de dados pessoais desde as fases iniciais de desenvolvimento de produtos, serviços e sistemas. Sobre *Privacy by Design* Ribeiro (2022, p. 34) diz que.

> Representa uma mudança no modo de garantir a privacidade e a proteção de direitos e liberdades dos indivíduos, já que é pensado e incorporado às práticas de negócio antecipadamente, ou seja, desde o momento inicial quando são concebidos os processos produtivos, procedimentos e mecanismos internos do processamento de dados pessoais por Controladores, Operadores e terceiros.

A aplicação do *Privacy by Design* é especialmente relevante para desenvolvedores de software no contexto da conformidade com a Lei Geral de Proteção de Dados (LGPD) no Brasil, este princípio enfatiza que a privacidade não deve ser tratada como uma adição ou um complemento, mas sim como um componente essencial e inerente ao design e à arquitetura de qualquer projeto. Isso implica a adoção de práticas que garantam a minimização da coleta de dados, a implementação de medidas de segurança robustas, a transparência no uso das informações e o controle contínuo sobre o acesso aos dados.

Além disso outro conceito muito importante para um ambiente de desenvolvimento seguro é o *Privacy by Default* que incentiva a configuração padrão mais restritiva em relação ao acesso aos dados pessoais. Sobre *Privacy by Default* Ribeiro (2022, p. 34) destaca que ”consiste na parametrização de que assim que um produto ou serviço for lançado ao público, as configurações mais seguras de privacidade deverão ser aplicadas por padrão, sem nenhuma entrada manual do usuário final”.

Ou seja, o *Privacy by Default* é um princípio complementar ao *Privacy by Design*, focado em garantir que as configurações padrão de qualquer sistema ou serviço respeitem a privacidade dos usuários de forma automática. Esse princípio assegura que, por padrão, apenas os dados pessoais estritamente necessários para o propósito específico sejam coletados, processados e retidos.

Porfim garantir que haja um ambiente de desenvolvimento seguro é a base para a inovação digital sustentável. Com o avanço da tecnologia, as ameaças cibernéticas também evoluem, deixando em evidência a importância da adoção de

práticas de segurança atualizadas e eficazes. Ivestir desde o início em segurança, promover a conscientização e educação digital além de adotar medidas proativas de cuidados são passos fundamentais para garantir a confiança dos usuários e proteger ativos digitais contra ameaças emergentes.

3.2.1 Crimes Cibernéticos

Os crimes cibernéticos, também chamados de cibercrimes, são delitos cometidos através dos meios digitais, e são cometidos através do uso indevido de computadores, redes de internet e ferramentas tecnológicas como *softwares* e *smatphones*. De acordo com Almeida et al. (2015) “Tais comportamentos são conhecidos de diversas formas, tais como crimes virtuais, crimes cibernéticos, digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, crimes de internet, fraude informática, crimes transnacionais, entre outras”.

Sendo assim com os perceptíveis avanços tecnológicos vivenciados nas últimas décadas alguns problemas passaram a surgir, sendo o principal deles a dependência da sociedade em relação à internet, com isso os crimes cibernéticos passaram a ser tratados com maior preocupação no Brasil, portanto no contexto dos crimes cibernéticos estão inseridos um amplo número de atividades criminosas, como mostra o quadro a seguir:

Quadro 5 – Atividades criminosas

Atividade	Definição
Phishing	Trata-se da criação de mensagens falsas ou sites em nome de entidades legítimas, com o intuito de enganar as vítimas, e através dos artifícios da engenharia social obter informações confidenciais, como senhas e informações financeiras.
Roubo de Identidade	Os criminosos conseguem obter posse das informações pessoais de uma pessoa, como nome, CPF e data de nascimento, e através destas informações cometem fraudes ou crimes financeiros em nome da vítima.
Ransomware	Envolve a infecção de um dispositivo através de um software malicioso, a partir de então esse software passa a criptografar informações, arquivos ou até bloquear o dispositivo da vítima, e enfim os criminosos passam a exigir valores de resgate em troca de uma chave de descriptografia.
Ataques DdoS	Ataques de negação de serviço distribuído (DDoS) sobrecarregam servidores ou redes com tráfego falso,

	tornando os serviços inacessíveis para os usuários legítimos.
Cyberbullying	É a prática considerada criminosa de intimidar, ameaçar ou difamar pessoas online, podendo causar danos psicológicos e emocionais às vítimas.

Fonte: Desenvolvimento do autor (2024).

Existem várias motivações para um criminoso cibernético praticar tais atos, que podem ser, para se beneficiar financeiramente, praticar espionagem, vandalizar, defender causas políticas e até mesmo apenas na intenção de provocar caos. Estes crimes podem gerar vários impactos, e as consequências podem ser graves, tanto para cidadãos quanto para organizações. Podendo incluir vazamentoo de dados confidenciais, danos à reputação, prejuízos financeiros, interrupção de serviços essenciais e até mesmo ameaças à segurança nacional.

O combate aos crimes cibernéticos é feito através da cooperação entre governos, forças de segurança, empresas e indivíduos. Os orgãos de manutenção da lei trabalham afim de identificar e prender os criminosos. Já o papel das empresas e cidadãos é adotar medidas de segurança cibernética, como *firewalls*, antivírus e autenticação de dois fatores, mantendo assim maior proteção dos seus dados.

Outras medidas que valem à pena é a educação e conscientização que são fundamentais na prevenção de crimes cibernéticos pois mostram as melhores práticas para proteger suas informações pessoais. Em um mundo cada vez mais digital, os crimes cibernéticos representam uma ameaça persistente que exige vigilância constante e esforços coordenados para proteger indivíduos, empresas e governos. A prevenção, a detecção e a punição dos criminosos cibernéticos são desafios contínuos que requerem a adaptação constante das leis e das medidas de segurança cibernética.

3.3 Penalidades para o descumprimento da LGPD

O descumprimento da Lei Geral de Proteção de Dados (LGPD) no Brasil pode acarretar diversas penalidades para as organizações que não seguem as normas estabelecidas para a proteção de dados pessoais. Portanto o presente tópico visa destacar algumas dessas penalidades previstas na LGPD para os casos de descumprimento da mesma. Tais penalidades são aplicadas pela Autoridade

Nacional de Proteção de Dados (ANPD) e podem variar conforme a gravidade da infração.

Como já citado as penalidades da lei tem como objetivo garantir que as organizações tratem os dados pessoais de maneira segura e responsável, protegendo os direitos dos titulares dos dados e promovendo a conformidade com as normas de proteção de dados. As penalidades variam em severidade de acordo com a natureza e a gravidade da infração, bem como o impacto sobre os titulares dos dados. De acordo com o artigo 52 da LGPD (Lei Nº 13.709/2018) as sanções administrativas aplicáveis em caso de infrações contra as normas previstas na lei por parte dos agentes de tratamento de dados são de cargo da ANPD (BRASIL, 2018).

Para evitar essas penalidades, é necessário que as instituições implementem uma série de medidas de conformidade com a LGPD. Isso inclui a designação de um encarregado pelo tratamento de dados (DPO), a criação de políticas de privacidade, a realização de treinamentos internos, e a adoção de práticas de segurança da informação. Tudo isso para evitar o descumprimento da lei, como ocorreu com a empresa Telekall em 2023.

> Dentre os processos administrativos sancionadores instaurados, um deles, face à empresa Telekall Infoservices, foi concluído em primeira instância. A fiscalização foi iniciada a partir de denúncia que alegava que a empresa estaria ofertando uma listagem de contatos de WhatsApp de eleitores para fins de disseminação de material de campanha eleitoral. Os fatos denunciados foram relativos à eleição municipal de 2020, em Ubatuba/SP. Diante dos indícios de infração à LGPD e do não atendimento de determinações exaradas ao longo do processo de fiscalização, a CGF lavrou Auto de Infração, iniciando o Processo Administrativo Sancionador. Da análise do processo, resultou a aplicação de sanções de multa simples e de advertência. A CGF constatou que a empresa infringiu os arts. 7º e 41, da LGPD, além do art. 5º do Regulamento de Fiscalização da ANPD (ANPD, 2023, p.29).

Ao analisar o trecho é possível observar que em caso de descumprimento da lei, as sanções cabíveis serão aplicadas sempre de acordo com a severidade da infração. Em resumo, as penalidades pelo descumprimento da LGPD podem ter consequências significativas para as empresas, tanto financeiras quanto reputacionais. Portanto, é essencial que as organizações invistam na implementação de práticas robustas de proteção de dados para assegurar a conformidade com a lei e proteger os direitos dos titulares.

4. METODOLOGIA

A metodologia foi cuidadosamente planejada para garantir a obtenção de dados relevantes e a análise precisa dos mesmos, abordando tanto os aspectos teóricos quanto práticos da conformidade com a LGPD (Lei Geral de Proteção de Dados) e sua aplicação na segurança da informação durante o desenvolvimento de softwares.

A abordagem de revisão bibliográfica permite detalhar através de artigos científicos, livros, leis, dentre outros, as aplicações da LGPD no contexto da segurança da informação e do desenvolvimento de softwares, enquanto a análise documental busca entender por meio de dados quantitativos em sites do governo, a dimensão dos desafios enfrentados por usuários e instituições no processo de adequação à LGPD no Brasil no que se refere à tratamento de dados.

Para Marconi e Lakatos (2003, p.158),

> A pesquisa bibliográfica é um apanhado geral sobre os principais trabalhos já realizados, revestidos de importância, por serem capazes de fornecer dados atuais e relevantes relacionados com o tema. O estudo da literatura pertinente pode ajudar a planificação do trabalho, evitar publicações e certos erros, e representa uma fonte indispensável de informações, podendo até orientar as indagações

A revisão bibliográfica foi realizada com foco em artigos científicos, livros, teses e dissertações, além de documentos legais e diretrizes da LGPD. Fontes de referência incluirão bases de dados acadêmicas como Scielo, Google Acadêmico e Biblioteca Virtual da FADESA. Enquanto que durante a análise documental foram examinados documentos oficiais da Autoridade Nacional de Proteção de Dados (ANPD), tal como artigos da LGPD e Marco Civil da Internet, e apresentados em forma de elementos visuais como: gráficos, tabelas e imagens, afim de visualizar os números oficiais relacionados à tratamento de dados no Brasil.

Para concluir, a metodologia descrita buscou assegurar uma abordagem abrangente e rigorosa, para investigar e proporcionar ao leitor um melhor entendimento sobre como a LGPD impacta a segurança da informação e o desenvolvimento de softwares no Brasil. Ao combinar diferentes métodos de coleta e análise de dados, espera-se obter uma compreensão profunda e prática dos desafios e soluções aplicáveis nesse contexto.

5. RESULTADOS E DISCUSSÃO

Desde a implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil em setembro de 2020, o cenário de vazamentos de dados tem estado nos holofortes. A LGPD surgiu com uma estrutura robusta que visa a proteção de dados pessoais, impondo obrigações rigorosas às empresas e organizações quanto ao tratamento e segurança das informações, no entanto, os números de vazamentos de dados ainda continuam alarmantes. E o presente tópico visa apresentar dados estatísticos à respeito de tratamento de dados pessoais no Brasil e descumprimentos à LGPD, embasado por fontes confiáveis, afim de agregar conhecimento ao leitor.

Como antes abordado a LGPD estabelece a obrigatoriedade de notificação de incidentes de segurança junto à ANPD, que por sua vez exerce um papel crucial na fiscalização e na orientação das empresas para a implementação de medidas adequadas de segurança. De acordo com a ANPD em seu Relatório do Ciclo de Monitoramendo (2023, p.9): “no primeiro semestre de 2023 foram recebidos, pela CGF, 496 requerimentos, sendo 167 petições de titular e 329 denúncias”.

Uma petição de titular é um mecanismo através do qual os titulares de dados pessoais exercem seus direitos garantidos pela Lei Geral de Proteção de Dados (LGPD). Segundo a ANPD (2023, p.9) “A Petição de Titular é o instrumento para exercício de direito pelo titular de dados em relação ao tratamento de seus dados pessoais”. Esses direitos incluem, entre outros, o acesso aos dados, a correção de informações incompletas, inexatas ou desatualizadas, a anonimização, o bloqueio ou a eliminação de dados desnecessários ou excessivos, e a portabilidade dos dados a outro fornecedor de serviço ou produto.

Ao fazer uma petição, o titular solicita formalmente à organização que possui seus dados que tome uma ação específica em relação a essas informações. A empresa ou entidade deve responder à petição dentro de um prazo razoável, geralmente fornecendo informações claras sobre como os dados estão sendo utilizados e que medidas serão tomadas em resposta à solicitação. A petição de titular é um componente crucial da LGPD, pois assegura a transparência e o controle dos indivíduos sobre seus dados pessoais.

Os números de denúncias junto à ANPD apontam que muitas empresas ainda estão em processo de adequação e ainda enfrentam sérios desafios técnicos e financeiros para cumprir todas as exigências da lei. O quadro 5 demonstra dados da ANPD referentes aos controladores mais citados em denúncias no primeiro semestre de 2023.

Quadro 6 - Controladores mais citados em denúncias no 1º semestre de 2023

Requerido	Quantidade de Menções em Denúncias Recebidas
Transparencia.CC	11
Fundação Petrobras de Seguridade Social - PETROS	6
Tim S.A.	6
Instituto Nacional do Seguro Social – INSS	6
Claro S.A.	4
Banco Pan	4
Empresas Web	4
XP Investimentos Corretora de Câmbio, Títulos e Valores Mobiliários S.A.	3
Conselho Regional de Engenharia e Agronomia (CREA) – SP	3
Banco Itaú	3

Fonte: ANPD (2023).

Como já foi abordado, o controlador de dados pessoais tem diversas responsabilidades cruciais conforme estipulado pela Lei Geral de Proteção de Dados (LGPD). Entre suas principais obrigações, destacam-se a necessidade de assegurar a conformidade com os princípios da LGPD, como a transparência, segurança, e finalidade específica do tratamento de dados. O artigo 38 da LGPD (Lei Nº 13.709/2018) estipula que.

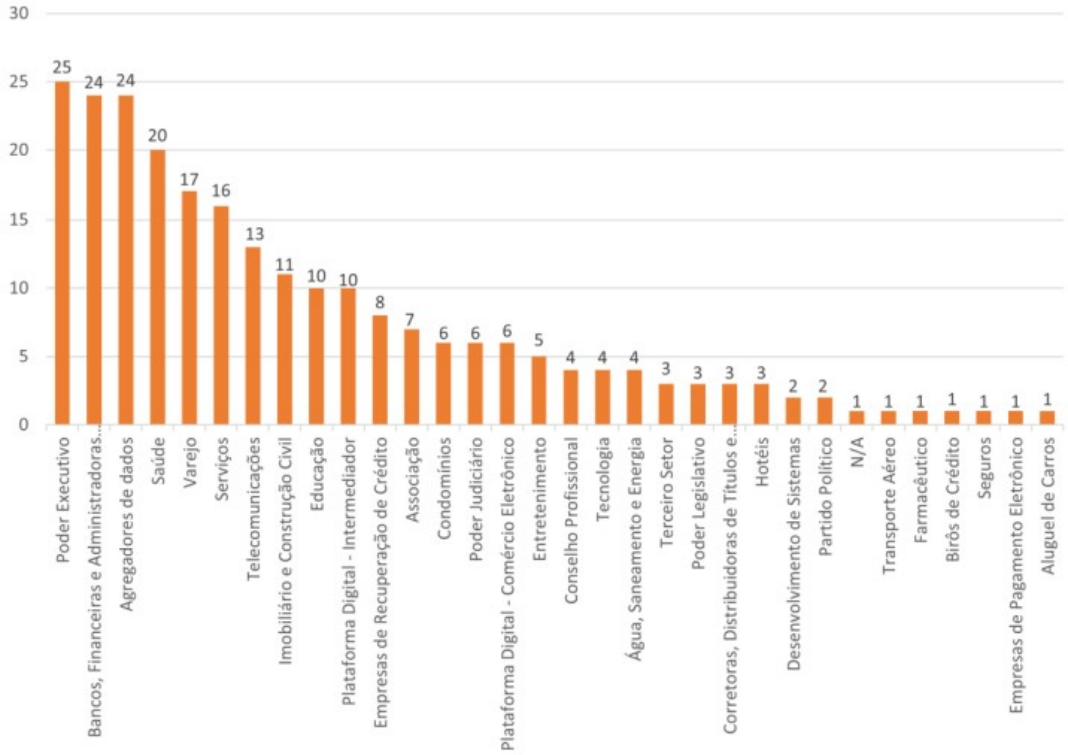
> A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial (BRASIL, 2018).

Ou seja, através da elaboração desses relatórios o controlador, garante que os dados pessoais estão sendo coletados e processados apenas para finalidades

legítimas, explícitas e informadas ao titular, e que as operações com esses dados são tratadas com transparência, mantendo assim o titular informado sobre o vazamento, ou qualquer forma de processamento inadequado.

A quantidade significativa de denúncias em setores variados evidencia a necessidade de maior conscientização e implementação de boas práticas de proteção de dados em todas as áreas que lidam com informações pessoais. A conformidade com a LGPD não apenas protege os direitos dos titulares, mas também fortalece a confiança e a reputação das organizações. O papel da ANPD é crucial na fiscalização e orientação das organizações para garantir que os dados pessoais sejam tratados com a devida seriedade e segurança. A figura 4 apresenta um gráfico demonstrando a quantidade de denúncias recebidas no 1º semestre de 2023 por setor.

Figura 4 - Denúncias recebidas por setor – 1º Semestre de 2023.



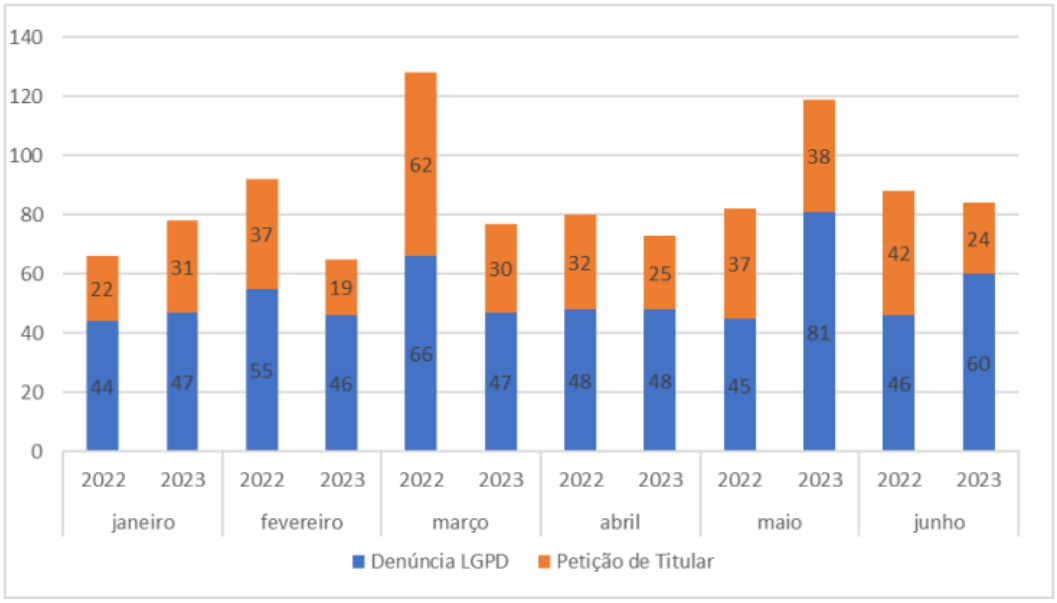
Fonte: ANPD (2023).

A Autoridade Nacional de Proteção de Dados (ANPD) tem recebido denúncias de diversos setores que não estão cumprindo adequadamente as normas estabelecidas pela Lei Geral de Proteção de Dados (LGPD). Os setores mais denunciados refletem áreas onde há um grande volume de dados pessoais sendo

coletados e processados, frequentemente sem o devido cuidado ou transparência, o que leva a um número significativo de reclamações dos titulares de dados.

No primeiro semestre de 2023, a Autoridade Nacional de Proteção de Dados (ANPD) registrou uma queda no número de petições de titulares em comparação ao mesmo período do ano anterior, 2022. Esse fenômeno pode ser atribuído a diversos fatores que refletem mudanças significativas no ambiente de proteção de dados no Brasil. A redução no número de petições pode indicar avanços na conformidade das empresas com a Lei Geral de Proteção de Dados (LGPD) e uma maior eficácia das medidas preventivas implementadas pelas organizações para proteger os dados pessoais. Esses dados podem ser confirmados no gráfico representado na Figura 5.

Figura 5 – Variação de recebimento de requerimentos – 1º semestre 2022 X 1º semestre 2023



Fonte: ANPD (2023).

Por outro lado no primeiro semestre de 2023, a Autoridade Nacional de Proteção de Dados (ANPD) registrou um aumento no número de CIS (Comunicados de Incidentes de Segurança) em comparação ao mesmo período do ano anterior, 2022. Esse crescimento pode ser atribuído a diversos fatores que refletem tanto uma maior conscientização e cumprimento das obrigações legais pelas organizações, quanto ao aumento dos desafios de segurança cibernética enfrentados pelas empresas. O aumento no número de comunicados de incidentes de segurança tem implicações significativas tanto para as empresas quanto para os titulares de dados.

Sendo assim O aumento no número de comunicados de incidentes de segurança feitos à ANPD refletem um cenário de segurança cibernética cada vez

mais desafiador. Para que haja solução aos problemas envolvendo tratamento de dados pessoais é necessário que as instituições estejam cada vez mais atentas e comprometidas com a proteção dos dados pessoais, cumprindo suas obrigações legais e buscando constantemente aprimorar suas defesas contra ameaças cibernéticas.

A ANPD, desempenha um papel crucial ao incentivar essa cultura de conformidade ao fornecer orientações, suporte e fiscalização para a gestão eficaz dos incidentes de segurança, sendo a grande responsável na busca constante por ações que visam minimizar o número de incidentes com dados pessoais. A redução efetiva dos vazamentos de dados exige um esforço contínuo e colaborativo entre governo, setor privado e sociedade civil para fortalecer a cultura de proteção de dados no Brasil. Ações relacionadas à requerimentos, setores, procedimentos e processos, estão em pauta na ANPD para o biênio de 2024 e 2025.

Referente à requerimentos a ANPD prevê como uma de suas ações a regulamentação de obrigatoriedade do controlador na disponibilização de uma ferramentas de contato mais rápido para que a Autoridade possa entrar em contato, como um endereço de correio eletrônico dedicado para essa finalidade por exemplo. Esta medida tem por objetivo eliminar a dificuldade da ANPD em encontrar algum canal de contato com o controlador (ANPD, 2023).

No que se refere à setores a CGF (Cordenação-Geral de Fiscalização) prevê a conclusão dos processos de fiscalização desses setores que estão em andamento. Além do encerramento dos processos, publicizar estas decisões também pode contribuir significativamente para que os agentes de tratamento desses setores se adequem à LGPD, pois a Autoridade tem por responsabilidade proporcionar o entendimento sobre tratamento de dados.

Por último uma das ações que tratam de procedimentos e processos prevê a realização do mapeamento dos fluxos de requerimentos, incluindo também ações de auditoria entre as atividades rotineiras da CGF (Cordenação-Geral de Fiscalização), sendo que, o mecanismo de auditoria é utilizado pela ANPD na verificação dos critérios de tratamento de dados por parte do agente de tratamento, principalmente relacionado à requisitos técnicos de segurança da informação e de governança (ANPD, 2023).

Portanto conclui-se que criação da ANPD representa um avanço significativo na proteção de dados pessoais no Brasil, trazendo mais segurança jurídica e clareza

para empresas e cidadãos sobre as obrigações e direitos relacionados ao tratamento de dados pessoais. Ao garantir a aplicação efetiva da LGPD, a ANPD promove um ambiente de confiança e respeito pela privacidade, essencial para o desenvolvimento da economia digital e para a proteção dos direitos fundamentais dos indivíduos, fortalecendo a confiança dos mesmos no uso de suas informações pessoais.

6. CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo principal analisar a aplicação da Lei Geral de Proteção de Dados (LGPD) aliada à segurança da informação no contexto do desenvolvimento de softwares no Brasil. Ao longo da pesquisa, foi possível identificar os principais desafios e práticas adotadas pelas empresas de tecnologia para garantir a conformidade com a LGPD, bem como avaliar o impacto dessas práticas na segurança dos dados tratados e armazenados por aplicações de software.

Os resultados obtidos mostram que a LGPD tem desempenhado um papel fundamental na conscientização sobre a importância da proteção de dados pessoais no Brasil, incentivando as empresas a adotarem medidas mais rigorosas de segurança da informação.

No entanto, a pesquisa também revelou que muitas organizações ainda enfrentam dificuldades significativas para se adequarem plenamente às exigências da lei. Entre os desafios mais comuns, destacam-se a complexidade técnica das implementações de segurança, a necessidade de treinamento contínuo dos funcionários e a dificuldade em acompanhar as constantes atualizações e interpretações da LGPD.

Através da revisão bibliográfica e análise documental, foi possível observar que as empresas que investem em uma cultura organizacional voltada para a proteção de dados e segurança da informação tendem a ter um processo de conformidade mais eficaz. Estratégias como a integração de políticas de privacidade desde as fases iniciais de desenvolvimento de software (*privacy by design*) e a realização de avaliações de RIPD (Relatório de Impacto à Proteção de Dados) foram identificadas como boas práticas que contribuem para a mitigação de riscos e a proteção dos direitos dos titulares dos dados.

Além disso, o conteúdo levantado evidenciou a importância da colaboração entre as instituições desenvolvedoras, usuários, especialistas em segurança da informação e departamentos jurídicos, aliados à ANPD, no sentido de buscarem sempre o pleno entendimento dos direitos e deveres impostos pela Lei Geral de Proteção de Dados (LGPD).

Em termos de contribuição acadêmica e prática, este trabalho oferece uma visão abrangente das interseções entre a LGPD e a segurança da informação, destacando tanto os avanços quanto as áreas que ainda necessitam de melhorias. A pesquisa proporciona uma base sólida para futuros estudos.

Esse estudo aliado à segurança da informação, oferece uma contribuição robusta e multifacetada para a academia. A interseção de disciplinas não apenas enriquece o corpo teórico existente, mas também promove avanços práticos que beneficiam tanto a pesquisa quanto a formação de profissionais aprimorando capacidades como desenvolvimento teórico e integração disciplinar, habilidade de realizar pesquisa aplicada e inovação, melhoria das práticas de desenvolvimento, contribuição para políticas públicas e regulação, sensibilização e educação sobre privacidade e segurança, apoio ao desenvolvimento sustentável e ético, interdisciplinaridade e novas perspectivas de pesquisa.

O estudo também proporciona uma série de benefícios vitais para a sociedade tratando sobre a proteção dos direitos individuais, fortalecendo a segurança digital, fomentando a confiança dos usuários, prevenindo abusos, promovendo a responsabilidade corporativa, incentivando a inovação sustentável, educando a população, estimulando a competitividade econômica, apoiando a formulação de políticas públicas eficientes e reduzindo riscos e custos. Esses impactos positivos contribuem para a construção de uma sociedade digital mais segura, justa e confiável.

Por fim, em contribição para com os profissionais da área o estudo ajuda na capacitação técnica, desenvolvimento de competências específicas, incentiva a atualização constante sobre regulamentações, traz a importância de ter capacidade para lidar com desafios complexos e do aprimoramento da segurança de sistema, trata sobre redução de riscos e responsabilidade, e incentiva a diferenciação profissional buscando oportunidades de carreira contribuindo para a inovação responsável

A conformidade com a LGPD não deve ser vista apenas como uma obrigação legal, mas como uma oportunidade para as empresas aprimorarem seus processos e fortalecerem a confiança de seus clientes. A evolução contínua das tecnologias e das ameaças cibernéticas exige um compromisso permanente com a segurança da informação e a proteção dos dados pessoais, reforçando a importância de uma abordagem proativa e integrada para enfrentar os desafios do cenário digital atual.

7. REFERENCIAS

ABREU, Cristiano N.; EISENSTEIN, Evelyn; ESTEFENON, Susana G B. **Vivendo esse mundo digital.** Editora Artmed, 2013. E-book. ISBN 9788582710005. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582710005/. Acesso em: 08 out. 2023.

ALMEIDA, Jéssica et al. **Crimes cibernéticos**. Ciências Humanas e Sociais Unit. Aracaju, v. 2, n.3, p. 222-223, Março 2015. Disponível em: https://periodicos.grupotiradentes.com/cadernohumanas/article/view/2013/1217. Acesso em: 20 out. 2023.

ANPD. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado.** v. 2, p. 6, abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em 20 mai. 2024.

ANPD. **Relatório de Ciclo de Monitoramento.** v. 1, p. 29, 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/2023-11-07-relatorio-do-ciclo-de-monitoramento-2023-versao-final.pdf. Acesso em 24 mai. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco civil da internet**. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 17 mai. 2024.

BRASIL. Lei nº LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 20 mai. 2024.

DONEDA, D. **A proteção dos dados pessoais como um Direito fundamental.** Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://br.search.yahoo.com/search?fr=mcafee&type=E211BR714G0&p=%2F%2F%2FC%3A%2FUsers%2Fnasci

%2FDownloads%2FDialnet-AProtecaoDosDadosPessoaisComoUmDireitoFundamental-4555153.pdf. Acesso em: 16 mai. 2024.

GOMES C. F. **Proposta de implementação de uma camada de segurança em um servidor de rede: serviços proftpd, apache http server e openssh.** Palmas – TO. p. 12 , 2020. Disponível em: https://br.search.yahoo.com/search?fr=mcafee&type=E211BR714G0&p=Proposta+de+implementa%C3%A7%C3%A3o+de+uma+camada+de+seguran%C3%A7a+em+um+servidor+de+rede%3A+servi%C3%A7os+proftpd%2C+apache+http+server+e+openssh. Acesso em: 24 mai. 2024.

LUGATI, L. N.; ALMEIDA, J. E. **Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa**. REVISTA DE DIREITO, VIÇOSA, v.12, n.02, p. 2 de 33, 2020. Disponível em: https://periodicos.ufv.br/revistadir/. Acesso em: 23 set. 2023.

LUZ, Gabriel G.; MAIA, Matheus O.; MAGALHÃES, Rodrigo Almeida. **Revista de Direito Contemporâneo UNIDEP.** Pato Branco, ano 2, n. 1, jan./jun. 2023. Disponível em: https://periodicos.unidep.edu.br/rdc-u/article/view/203/116. Acesso em: 06 out. 2023.

MARCONI, Marina A.; LAKATOS, Eva M. **Fundamentos de Metodologia Científica**. EDITORA ATLAS, São Paulo, 5. ed, p. 158, 2003. Disponível em: https://epidemiologiagestao.wordpress.com/wp-content/uploads/2017/05/aula-4-cic3aancia-e-conhecimento-cientc3adfico.pdf. Acesso em: 29 jul. 2024.

OTÁVIO, Chico. **Golpistas vazaram quase 1 bilhão de dados no Brasil em 2022. Quadrilhas montam painéis para vender na internet.** O Globo, 2023. Disponível em: <https://oglobo.globo.com/economia/defesa-do-consumidor/noticia/2023/06/dossies-com-dados-publicos-e-privados-municiam-golpes-eletronicos.ghtml>. Acesso em: 18 set. 2023.

PAIXÃO Jéssica S. **Criptografia: história, atividades e divulgação científica.** São Carlos-SP. p.123 , out. 2020. Disponível em: https://www.teses.usp.br/teses/disponiveis/55/55136/tde-09112020-182912/publico/JessicaShayannedaPaixao_revisada.pdf. Acesso em: 22 mai. 2024.

RIBEIRO F. S. **Construção de uma startup com o conceito de privacy by design Um estudo sobre a connect point.** Belo Horizonte. p.34 , 2022. Disponível em: https://repositorio.ufmg.br/bitstream/1843/46504/1/FredericoSRibeiro.pdf. Acesso em: 24 mai. 2024.

SOLER, Fernanda G. **Proteção de dados: reflexões práticas e rápidas sobre a LGPD.** Editora Saraiva, 2022. E-book. ISBN 9786553622500. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553622500/. Acesso em: 07 out. 2023.

SILVA, A. F.; MARTINS, R. M. **Criptografia: aspectos históricos e matemáticos**. Belém-PA, p. 41 de 94, 2011. Disponível em: https://ccse.uepa.br/downloads/tcc/2011/silva_martins_2011.pdf. Acesso em: 22 mai. 2024.

TAKATA Guilherme O. **O exercício da escrita.** Revista Resgates. São Paulo, n. 7, p. 85, dez. 2017. Disponível em: https://static1.squarespace.com/static/637bb31bc82d6a0e64a33d3d/t/6470f6db2d5c8b1814aba6c2/1685124838690/stockler-2017-revista-resgates.pdf#page=82. Acesso em: 21 mai. 2023.

WIKIPÉDIA. **Banco de dados.** 2024. Disponível em: <https://pt.wikipedia.org/wiki/Banco_de_dados>. Acesso em: 16 mai. 2024.

Página de assinaturas

Sara Carvalho
017.799.872-50
Signatário

Adriano Bollas
669.522.202-91
Signatário

Antonio Silva
032.290.192-88
Signatário

HISTÓRICO

06 ago 2025 22:18:45 — **Jefferson Correia do Nascimento** criou este documento. (Email: nascimentojefferson1995@gmail.com, CPF: 035.907.742-07)

06 ago 2025 22:47:15 — **Adriano Louzada Bollas** *(Email: adriano.louzadabollas@gmail.com, CPF: 669.522.202-91)* visualizou este documento por meio do IP 200.124.94.133 localizado em Parauapebas - Pará - Brazil

06 ago 2025 22:47:18 — **Adriano Louzada Bollas** *(Email: adriano.louzadabollas@gmail.com, CPF: 669.522.202-91)* assinou este documento por meio do IP 200.124.94.133 localizado em Parauapebas - Pará - Brazil

07 ago 2025 12:36:42 — **Antonio Soares da Silva** *(Email: ads@fadesa.edu.br, CPF: 032.290.192-88)* visualizou este documento por meio do IP 200.9.67.64 localizado em Parauapebas - Pará - Brazil

07 ago 2025 12:36:47 — **Antonio Soares da Silva** *(Email: ads@fadesa.edu.br, CPF: 032.290.192-88)* assinou este documento por meio do IP 200.9.67.64 localizado em Parauapebas - Pará - Brazil

06 ago 2025 22:19:50 — **Sara Carvalho** *(Email: csaradeboracontato@gmail.com, CPF: 017.799.872-50)* visualizou este documento por meio do IP 170.239.200.86 localizado em Parauapebas - Pará - Brazil

06 ago 2025 22:20:02 — **Sara Carvalho** *(Email: csaradeboracontato@gmail.com, CPF: 017.799.872-50)* assinou este documento por meio do IP 170.239.200.86 localizado em Parauapebas - Pará - Brazil