CAMPUS PORTO VELHO ZONA NORTE
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS PARA INTERNET

ARTHUR PEDRO OLIVEIRA DE PAULA
GETÚLIO WERLE DE OLIVEIRA

LGPD POR DESIGN:
PRIVACIDADE E PROTEÇÃO DE DADOS EM PROJETOS DE SOFTWARE

PORTO VELHO/RO
2024

ARTHUR PEDRO OLIVEIRA DE PAULA
GETÚLIO WERLE DE OLIVEIRA

LGPD POR DESIGN:
PRIVACIDADE E PROTEÇÃO DE DADOS EM PROJETOS DE SOFTWARE

Artigo apresentado ao Curso Superior de Tecnologia em Sistemas para Internet do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia – IFRO Campus Porto Velho Zona Norte como requisito avaliativo para obtenção do título de Tecnólogo em Sistemas para Internet.
Orientador: Saulo Souza de Macedo
Coorientador: Albert França Josuá Costa
Coorientador: Douglas Moro Piffer

PORTO VELHO/RO
2024

Ficha catalográfica elaborada pelo Sistema Gerador de Ficha Catalográfica do IFRO,
com dados informados pelo(a) próprio(a) autor(a).

Oliveira de Paula, Arthur Pedro.
LGPD por design: privacidade e proteção de dados em projetos de software / Arthur Pedro Oliveira de Paula, Getúlio Werle de Oliveira, Porto Velho-RO, 2024.
24 f.

Orientador(a): Mestre em Educação Escolar Saulo Souza de Macedo.
Coorientador(a): Mestre em Informática Albert França Josuá Costa.

Trabalho de Conclusão de Curso (Superior de Tecnologia em Sistemas para Internet) – Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO, Porto Velho-RO, 2024.

1. Lei Geral de Proteção de Dados. 2. Desenvolvimento de Software. 3. Controle. 4. Privacidade desde a Concepção. I. Werle de Oliveira, Getúlio. II. de Macedo, Saulo Souza (orient.). III. Josuá Costa, Albert França (coorient.). IV. Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO. V. Título.

Bibliotecário(a) Responsável: Gizele de Melo Viana, CRB-CRB11/914 (Campus Porto Velho Zona Norte)

ISSN: 1696-8352

LGPD por design: privacidade e proteção de dados em projetos de software

LGPD by design: privacy and data protection in software projects

LGPD por diseño: privacidad y protección de datos en proyectos de software

DOI: 10.55905/oelv22n6-258

Receipt of originals: 05/24/2024
Acceptance for publication: 06/14/2024

Arthur Pedro Oliveira de Paula
Tecnólogo em Sistemas para Internet
Instituição: Instituto Federal de Rondônia (IFRO) - campus Zona Norte
Endereço: Porto Velho, Rondônia, Brasil
E-mail: apop14520@gmail.com

Getúlio Werle de Oliveira
Tecnólogo em Sistemas para Internet
Instituição: Instituto Federal de Rondônia (IFRO) - campus Zona Norte
Endereço: Porto Velho, Rondônia, Brasil
E-mail: getuliowerle10@gmail.com

Saulo Souza de Macedo
Mestre em Educação Escolar
Instituição: Universidade Federal de Rondônia (UNIR)
Endereço: Porto Velho, Rondônia, Brasil
E-mail: saulo.macedo@ifro.edu.br

Albert França Josuá Costa
Mestre em Informática
Instituição: Instituto Federal do Amazonas (IFAM) - campus Zona Leste
Endereço: Manaus, Amazonas, Brasil
E-mail: albert.costa@ifam.edu.br

Douglas Moro Piffer
Mestre em Administração
Instituição: Universidade Federal de Rondônia (UNIR)
Endereço: Porto Velho, Rondônia, Brasil
E-mail: douglas.piffer@ifro.edu.br

RESUMO
Devido à evolução tecnológica e à crescente conscientização sobre a segurança de dados, a Lei Geral de Proteção de Dados (LGPD) surge como um marco legal essencial para a privacidade e proteção de dados pessoais, regulando seu tratamento e coleta em um cenário onde vazamentos de dados aumentam significativamente, principalmente no Brasil. Esta pesquisa tem como objetivo principal apresentar um conjunto de boas práticas para o desenvolvimento de software com foco na Privacidade desde a Concepção (PdC), especialmente nas etapas de requerimento e projeto. Este estudo é classificado como qualitativo, transversal, descritivo e ensaio teórico, pois busca compreender e apresentar controles para a implementação da privacidade e proteção de dados no desenvolvimento de software, analisando normas, guias e frameworks internacionais e nacionais. Como resultado, são sugeridos 36 controles divididos em cinco categorias específicas: Governança, Conscientização e Treinamento, Segurança de Dados, Privacidade por Design, e Revisão e Avaliação. Embora este pesquisa atinja minimamente os seus objetivos ao apresentar os controles, por serem baseados em um ensaio teórico, necessitam de validação através de pesquisas empíricas e estudos de caso futuros.

Palavras-chave: Lei Geral de Proteção de Dados, Desenvolvimento de Software, Controle, Privacidade desde a Concepção.

ABSTRACT
Due to technological evolution and growing awareness of data security, the General Data Protection Law (LGPD) emerges as an essential legal framework for privacy and personal data protection, regulating its treatment and collection in a scenario where data breaches significantly increase, especially in Brazil. The main objective of this research is to present a set of best practices for software development with a focus on Privacy by Design (PbD), especially in the requirements and design stages. This study is classified as qualitative, cross-sectional, descriptive, and theoretical essay, as it seeks to understand and present controls for implementing privacy and data protection in software development, analyzing international and national standards, guides, and frameworks. As a result, 36 controls are suggested, divided into five specific categories: Governance, Awareness and Training, Data Security, Privacy by Design, and Review and Evaluation. Although this research minimally achieves its objectives by presenting the controls, being based on a theoretical essay, they require validation through future empirical research and case studies.

Keywords: General Data Protection Law, Software Development, Control, Privacy by Design.

RESUMEN
Debido a la evolución tecnológica y la creciente concienciación sobre la seguridad de los datos, la Ley General de Protección de Datos (LGPD) surge como un marco legal esencial para la privacidad y protección de datos personales, regulando su tratamiento y recolección en un escenario donde las filtraciones de datos aumentan significativamente, especialmente en Brasil. El objetivo principal de esta investigación es presentar un

conjunto de buenas prácticas para el desarrollo de software con um enfoque en la Privacidad desde el Diseño (PdD), especialmente en las etapas de requerimientos y diseño. Este estudio se clasifica como cualitativo, transversal, descriptivo y ensayo teórico, ya que busca comprender y presentar controles para la implementación de la privacidad y protección de datos en el desarrollo de software, analizando normas, guías y marcos internacionales y nacionales. Como resultado, se sugieren 36 controles divididos en cinco categorías específicas: Gobernanza, Concienciación y Capacitación, Seguridad de Datos, Privacidad por Diseño, y Revisión y Evaluación. Aunque esta investigación logra mínimamente sus objetivos al presentar los controles, al estar basados en un ensayo teórico, necesitan validación a través de investigaciones empíricas y estudios de caso futuros.

Palabras clave: Ley General de Protección de Datos, Desarrollo de Software, Control, Privacidad desde el Diseño.

1 INTRODUÇÃO

Com o avanço constante da tecnologia e a revolução digital transformandonossas vidas, surgem crescentes preocupações com a segurança e privacidade dos dadospessoais. Neste cenário, a Lei Geral de Proteção de Dados (LGPD), cuja competência para normatização é da Autoridade Nacional de Proteção de Dados (ANPD), emerge como um marco legal crucial, abrangendo pessoas jurídicas e físicas para regular o tratamento e a coleta de dados, visando oferecer maior segurança digital às pessoas que fornecem suas informações (Bertan et al., 2022).

Atualmente, o processamento de dados é realizado predominantemente por softwares, que são projetados para lidar com grandes volumes de informações, utilizando algoritmos complexos e recursos de computação avançados, necessitando de sistemas seguros para proteger os dados dos usuários. Uma pesquisa do Massachusetts Institute of Technology (MIT) revelou que mais de 205 milhões de dados de brasileiros foram expostos em 2019, com um aumento de 493% nos vazamentos de dados no Brasil(Pereira; Silva, 2021). Desde o início da pandemia de COVID-19, houve um aumento significativo nos vazamentos de dados e tentativas de roubo de informaçõesem todo o mundo, com o Brasil sendo particularmente afetado (Vasconcelos, 2022). Portanto, é crucial adotar

uma abordagem robusta que integre os princípios de privacidade desde as etapas iniciais do desenvolvimento de software.

Esta pesquisa visa especificar um guia de boas práticas para o desenvolvimento de software com foco na Privacidade desde a Concepção (PdC), especialmente nas etapas de requerimento e projeto, com objetivos específicos de identificar diretrizes nacionais e internacionais de privacidade e proteção de dados, facilitar o desenvolvimento de sistemas que respeitem a privacidade do usuário, compartilhar descobertas com a comunidade científica e a indústria de software, e conscientizar sobre a inclusão da privacidade no desenvolvimento de software. Conhecer essas práticas é crucial para profissionais de tecnologia garantirem a segurança dos dados e o cumprimento da LGPD. A questão central é: "Quais controles devem ser seguidos para garantir a privacidade e a proteção de dados no desenvolvimento de software?".

2 REFERENCIAL TEÓRICO

Este capítulo apresenta os conceitos essenciais e o referencial teórico que fundamentam a pesquisa, começando com os guias de privacidade e proteção de dados na Seção 2.1, seguidos de uma comparação entre suas principais características na Seção 2.2. A Seção 2.3 oferece uma visão abrangente sobre a importância da privacidade digital no desenvolvimento de software, enquanto a Seção 2.4 descreve os desafios da implementação da proteção e privacidade de dados.

2.1 GUIAS DE BOAS PRÁTICAS

Os guias e normas de boas práticas em privacidade e segurança de dados são documentos que fornecem orientações e recomendações para garantir a proteção adequada dos dados. Eles são projetados para ajudar as organizações a melhorarem a sua estrutura de privacidade e proteção de dados. Neste sentido, essas padronizações de

boas práticas servem de referência para profissionais e organizações, ajudando a promover as melhores práticas e a garantia de resultados.

2.1.1 ABNT NBR ISO/IEC 27001:2022

A norma ABNT NBR ISO/IEC 27001:2022 é uma referência global que define os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI), oferecendo orientações e práticas recomendadas para proteger ativos digitais. Parte de uma série de padrões de segurança da informação, esta norma é crucial para estabelecer,implementar, manter e melhorar continuamente um SGSI, garantindo a confidencialidade, integridade e disponibilidade dos dados, e ajudando a mitigar riscos relacionados à segurança da informação (ABNT, 2022).

2.1.2 ABNT NBR ISO/IEC 27002:2022

A ABNT NBR ISSO/IEC 27002:2022, parte da família ISSO/IEC 27000, foca na segurança da informação (SI), abordando temas como governança de SI, controles de acessos, gestão de incidentes, segurança de redes e criptografia. Este documento serve como referência para definir e aplicar controles para tratamento de riscos de SI em um SGSI baseado na ABNT NBR ISSO/IEC 27001, ou como guia para organizações que estão definindo e implementando controles de SI geralmente aceitos (ABNT, 2022).

2.1.3 ABNT NBR ISO/IEC 27701:2019

A ABNT NBR ISSO/IEC 27701, diferente das normas abordadas anteriormente, éuma extensão da 27001 e 27002 que inclui a gestão da privacidade da informação, estabelecendo requisitos e diretrizes. Este documento especifica os requisitos para um Sistema de Gestão de Privacidade da Informação (SGPI) e oferece orientações para controladores e operadores de dados pessoais, abordando aspectos como consentimento,

direitos dos titulares, minimização de dados, segurança, responsabilidades e prestação de contas no tratamento de dados pessoais (ABNT, 2019).

2.1.4 ABNT NBR ISO/IEC 29100:2020

A ABNT NBR ISO/IEC 29100:2020 aborda os princípios fundamentais de privacidade e proteção de dados, definindo termos-chave, descrevendo atores e suas funções, estabelecendo requisitos para salvaguardar a privacidade e discutindo princípios reconhecidos internacionalmente. Esses princípios incluem consentimento, legitimidade do objetivo, limitação de coleta, minimização de dados, uso limitado, precisão, transparência, acesso, responsabilização, segurança da informação e conformidade com a privacidade (ABNT, 2020ª).

2.1.5 ABNT NBR ISO/IEC 29151:2020

A normativa ABNT NBR ISSO/IEC 29151, estende os controles presentes na 27002 trazendo diretrizes adicionais de proteção de dados, visando auxiliar os controladores de DP. Além disso, ela apresenta em um anexo normativo um conjunto ampliado de controles específicos para a proteção de DP, organizados em duas categorias que se alinham à política de privacidade e aos 11 princípios de privacidade estabelecidos pela ABNT NBR ISSO/IEC 29100 (ABNT, 2020b).

2.1.6 Controles CIS Versão 8

Os Controles CIS são um conjunto de recomendações para práticas de segurança da informação desenvolvidos pelo Center for Internet Security (CIS), uma organização sem fins lucrativos (CIS, 2021). Estas diretrizes são formuladas por especialistas em tecnologia da informação e segurança cibernética com base em dados de ataques reais e defesas eficazes (VALDIVIA, 2021). Atualmente na versão 8, lançada em 2021, os Controles CIS consistem em 18 controles principais que abrangem diversos aspectos de

segurança da informação, cada um detalhado em subcontroles para atender às necessidades específicas das organizações. A versão mais recente introduziu os Grupos de Implementação de Controles CIS (IGs), oferecendo orientações graduadas para a implementação dos controles de acordo com as necessidades e capacidades das organizações em termos de segurança cibernética (CIS, 2021).

Os IGs estão expostos no Quadro 1:

Quadro 1: Grupos de Implementação dos Controles

Identificador	Termos
IG.1	Composto por empresas de pequeno a médio porte que possuem experiência limitada em TI e segurança cibernética, focando na proteção de ativos e em uma equipe de TI reduzida.
IG.2	Composto por empresas que normalmente armazenam e processam dados sensíveis de clientes ou empresas e conseguem tolerar interrupções de serviço de curta duração.
IG.3	Composto por empresas em que os ativos e dados incluem informações ou funções sensíveis que estão sujeitos à supervisão regulatória e exigências de conformidade.

Fonte: Elaborado pelos autores, 2024.

2.1.7 NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management, Version 1.0

O NIST Privacy Framework é um instrumento desenvolvido pelo National Institute of Standards and Technology (NIST) para melhorar a privacidade através do gerenciamento de riscos organizacionais (NIST, 2020). Ele enfatiza medidas de engenharia de privacidade e suporta a proteção de dados por meio de princípios de design, auxiliando as organizações na preservação da privacidade dos indivíduos (NIST,2020). Composto por três componentes principais – o Núcleo, Perfis e Níveis de Implementação – o framework facilita a comunicação sobre atividades essenciais de proteção à privacidade em todos os níveis organizacionais. Os Perfis ajudam na definição das prioridades de proteção à privacidade com base nos valores da organização e seus objetivos comerciais específicos, enquanto os Níveis de Implementação orientam a avaliação da capacidade da organização para lidar comriscos de privacidade. Além de

ser compatível com regulamentos como o GDPR da União Europeia, o framework também suporta a implementação de Princípios de Privacidade por Design (PdC).

2.1.8 Software development with Data Protection by Design and by Default, guia da Datatilsynet (Autoridade Norueguesa de Proteção de Dados)

O guia "Software Development with Data Protection by Design and by Default" publicado pela Datatilsynet é uma ferramenta essencial para desenvolvedores de software e organizações que buscam integrar práticas de privacidade desde o início do ciclo de vida do desenvolvimento de software, conforme estabelecido pelo GDPR.Dividido em nove capítulos abrangendo áreas como Treinamento, Requisitos, Projeto, Codificação, Teste, Implantação e Manutenção, o framework oferece diretrizes detalhadas e medidas específicas para incorporar a proteção de dados e privacidade em cada fase do desenvolvimento (Datatilsynet, 2017).

2.2 COMPARAÇÃO DOS GUIAS DE BOAS PRÁTICAS

O Quadro 2 apresenta uma comparação dos guias de boas práticas considerados neste trabalho. São consideradas as características escopo e objetivo.

Quadro 2: Comparação entre os guias

Guia	Escopo	Objetivo
ABNT NBR ISO/IEC 27001	Segurança deDados	Define os requisitos para um SGSI.
ABNT NBR ISO/IEC 27002	Segurança deDados	Apresenta controles destinados ao tratamento de riscos deSI em um SGSI.
ABNT NBR ISO/IEC 27701	Privacidade de Dados	Fornece um SGPI que apoia organizações a 8ecnolo requisitos de privacidade e proteger DP.
ABNT NBR ISO/IEC 29100	Segurança e Privacidade deDados	Define termos importantes para a privacidade da informação, identifica os atores e suas funções, 8ecnologí requisitos para proteger a privacidade e aborda 8ecnología reconhecidos de privacidade.
ABNT NBR ISO/IEC 29151	Privacidade deDados	Define metas para controle, controles e orientações para implementar esses controles, visando atender aos requisitos identificados em uma avaliação de risco e impacto referente à proteção de DP.

CIS Controls v8	Segurança deDados	Fornece um conjunto claro e prático de diretrizes e práticas recomendadas para ajudar as organizações a fortalecer sua segurança cibernética.
NIST PrivacyFrame-work	Segurança e Privaci-dade deDados	Aumentar o 9ecno de privacidade por meio do gerenciamento de riscos da organização, apresentando uma9ecnología orien-tativa e flexível para abordar questões de privacidade em um contexto de 9ecnolog e 9ecnología.
Software development with Data Protection by Design and by Default	Segurança e Privaci-dade deDados	Oferece orientações para auxiliar as organizações na com-preensão e no cumprimento do requisito de proteçãode da-dos desde a concepção e por padrão, conforme estabelecido no artigo 25 da GDPR.

Fonte: Elaborado pelos autores, 2024.

2.3 LEI GERAL DE PROTEÇÃO DE DADOS E PRIVACIDADE DESDE A CONCEPÇÃO

Recentemente, cresceu a percepção da importância da privacidade digital, equiparando-a à privacidade física em termos de valorização da intimidade pessoal e proteção da identidade. Assim como cuidamos da nossa privacidade em ambientes físicos e conversas privadas, agora também nos preocupamos em preservar nossa privacidade no contexto da sociedade digital contemporânea (Garcia et al., 2020). A privacidade digital envolve não apenas a segurança contra roubo ou intrusão física, mas principalmente a proteção contra divulgações não autorizadas de informações pessoais. Esse conceito reflete um direito fundamental de controlar nossos próprios dados e tem se tornado essencial nas regulamentações de proteção de dados (Garrido, 2023).

Para garantir que a privacidade de dados seja uma prioridade nos novos sistemas, é essencial integrá-la ao longo de todo o ciclo de desenvolvimento de software(Drozd, 2016). Com a promulgação da LGPD, cujo foco é a proteção e gestãoadequada de dados pessoais, estabelecendo diretrizes rigorosas para assegurar a segurança e privacidade das informações dos cidadãos brasileiros, incluindo o desenvolvimento de sistemas (BRASIL, 2018), a abordagem de Privacidade desde a Concepção (PdC) emerge como uma estratégia crucial para incorporar esses princípios desde o início (Bertan et al., 2022). Os desenvolvedores de software devem estar familiarizados com essas leis para implementar medidas adequadas de proteção de dados, conforme ensinado em

metodologias como a PdC. Assim, ao considerar a privacidade no desenvolvimento de software, estamos enfatizando a importância de adotar medidas que garantam a proteção dos dados pessoais dos usuários em todas as fases do processo, com a PdC estabelecida como uma prática fundamental desde sua adoção como padrão internacional em 2010 (Santos, 2022).

A LGPD surgiu como um marco importante na imposição da privacidade e proteção de dados no Brasil, inspirada na GDPR. A lei regulamenta o tratamento de dados por pessoas naturais ou jurídicas, públicas ou privadas, nos meios digitais ou físicos. No art. 46, é descrito a obrigatoriedade dos agentes de tratamento de adotarem medidas para proteger os DP de "[...] situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" eno § 2° do mesmo artigo é exposto que as ações mencionadas no início do artigo devem ser levadas em consideração desde o momento da criação do produto ou serviço até a sua implementação (BRASIL, 2018).

A Privacidade desde a Concepção (PdC) é integralmente alinhada ao art. 46 da LGPD, pois visa sensibilizar as organizações sobre o amplo uso de dados, especialmente dados pessoais (Guido, 2023). A PdC se baseia em sete princípios fundamentais que devem guiar o desenvolvimento de sistemas: proatividade, privacidade por padrão, incorporação da privacidade desde o design, funcionalidade completa, segurança abrangente, transparência e visibilidade, e respeito pela privacidade do usuário (Cavoukian, 2009). Esses princípios são aplicáveis como controles e diretrizes para assegurar uma proteção efetiva dos dados e para garantir a conformidade com os requisitos legais de privacidade.

A conscientização sobre a importância da privacidade digital enfatiza a urgência de ajustes no desenvolvimento de software, impulsionada por princípios históricos e normas como a LGPD, agora uma obrigação legal e não apenas ética. A abordagem de Privacidade desde a Concepção (PdC) destaca-se como eficaz, alinhada aos princípios legais e à crescente demanda por sistemas seguros desde o início. Implementar práticas como controle de acesso, anonimização, minimização de dados e criptografia é crucial, respaldado por organizações internacionais. Conscientemente adotando essas diretrizes,

reforçamos a segurança das organizações e promovemos um ambiente digital mais confiável e respeitoso à privacidade, como observado por Melo e colaboradores (2023, p. 131), que destacam a necessidade de equilíbrio entre respeitar os limites relacionados à liberdade e dignidade pessoal, e promover a iniciativa econômica privada.

2.4 IMPLICAÇÕES DA GARANTIA DA PROTEÇÃO E PRIVACIDADE DOS DADOS

A LGPD tem um impacto direto sobre os profissionais de TI, dada sua função crucial na criação de ferramentas para coleta e processamento de dados. No entanto, a conformidade com a legislação muitas vezes é delegada exclusivamente ao departamento jurídico, resultando na falta de participação efetiva dos profissionais de tecnologia no processo regulatório. Segundo Canedo e colaboradores (2020, p. 20), profissionais de TIC frequentemente indicam falta de conhecimento necessário para implementar os princípios de privacidade e diretrizes da LGPD. Essa falta de envolvimento e desconhecimento pode resultar em violações das diretrizes estabelecidaspela legislação.

Considerando que a LGPD impõe sanções severas para a não conformidade, como multas diárias, suspensão de banco de dados e interrupção das atividades de tratamento de dados (BRASIL, 2018), o cumprimento rigoroso do regulamento pelos profissionais de tecnologia torna-se crucial. Apesar do art. 46 da LGPD enfatizar a necessidade de medidas de segurança para proteger dados pessoais, surgem interpretações variadas sobre os padrões técnicos mínimos definidos pela ANPD, levantando dúvidas sobre a uniformidade na aplicação dessas diretrizes. Cerqueira, Mello e Travassos (2023) observam que, embora a LGPD estabeleça princípios, não especifica detalhadamentesua implementação prática em contextos como o desenvolvimento de sistemas de software.

A abordagem de Privacidade desde a Concepção (PdC) preconiza uma estratégia proativa para prevenir problemas de privacidade antes mesmo de surgirem, visando proteger os dados dos usuários desde o início e reduzir o risco de violações (Get Privacy, 2022). No entanto, sua implementação pode ser desafiadora, exigindo o compromisso com padrões de privacidade mais rigorosos do que os exigidos pelas leis de proteção de

dados vigentes. Seguir o modelo da PdC não resolve todos os desafios deproteção de dados e conformidade com a LGPD, mas seus princípios são valiosos como diretrizes para o desenvolvimento de novas soluções de software (Bernardo; Pinzegher, 2021). Ao demonstrar um compromisso inicial com a privacidade, as organizações podem fortalecer a confiança com seus clientes e usuários, o que contribui para melhorar sua reputação no mercado.

A necessidade de integrar medidas de privacidade e segurança desde a concepção até a execução de produtos ou serviços apresenta desafios significativos, especialmente em um ambiente tecnológico dinâmico. É crucial considerar a privacidade e segurança dos dados dos usuários desde as etapas iniciais do ciclo de vida do software, particularmente durante a identificação dos requisitos e o design do sistema, para evitar problemas futuros de segurança e privacidade (Omoronyia, 2019). A fase de design é especialmente propícia para incorporar essas preocupações, pois problemas identificados tardiamente no ciclo de vida do software tendem a sermais complexos e dispendiosos para remediar.

Portanto, a LGPD impacta significativamente os profissionais de TI, mas ainda há pouco conhecimento adequado, o que pode resultar em violações da legislação e prejudicar a reputação das empresas. A LGPD não fornece orientações práticas sobre as ações e meios necessários para a adequação dos sistemas, sendo essencialmente formada por conceitos e terminologias (Costa; Alves; Guimarães, 2022). Nessecontexto, a PdC se mostra uma abordagem proativa para integrar a privacidade nas etapas iniciais do desenvolvimento de software.

3 METODOLOGIA

Considerando a classificação metodológica de Creswell e Clark (2015), o presente estudo é classificado como: qualitativo, quanto à natureza da abordagem metodológica, pois busca obter dados que contribuam para a compreensão de controlese medidas para a implementação da privacidade e proteção de dados nas fases de requerimento e projeto do processo de desenvolvimento de software; transversal, quantoà temporalidade, pois

são observados dados relativos ao tema nas publicações científicas nos últimos 5 anos, a serem coletados entre fevereiro e julho de 2024; descritivo, quanto aos objetivos de pesquisa, posto que propõe a descrição de medidas a partir da análise de normas, guias e frameworks de privacidade e segurança de dados; e quanto ao método, como ensaio teórico, pois os dados serão coletados após a análise de documentos e frameworks de privacidade e proteção dados, com o propósito de criarum embasamento teórico-científico sobre a temática que facultem ao desenvolvedor de softwares subsídios ao processo de tomada de decisões quanto aos métodos de segurança de dados a serem implementados em sua prática.

A análise documental foi realizada sob os controles de privacidade dos guias expostos na Seção 2.2. O escopo deste trabalho se estende além dos padrões brasileiros para incluir o guia Controles CIS Versão 8, o NIST Privacy Framework e as diretrizesda Agência Norueguesa de Proteção de Dados para "Desenvolvimento de software para proteção de dados por design e por padrão". Os métodos e tecnologias utilizados por estes mecanismos seguem padrões reconhecidos internacionalmente e são concebidos para garantir a proteção e segurança dos dados. Todavia, embora representem umavanço importante na proteção da privacidade, é importante ressaltar que as medidas propostas por organizações internacionais estão baseadas na GDPR e são divergentes dos requisitos estabelecidos pela LGPD, ainda que pouco. Nesse sentido, Soler (2022, p.43) afirma que "[...] a GDPR não é igual à LGPD e, por essa razão, não necessariamente teremos entendimentos idênticos, mas, tão somente, indícios e inspirações, fontes alternativas para a solução de certos desafios do dia a dia".

Portanto, há ainda espaço para melhorias e para a incorporação de medidas adicionais que efetivamente cumpram os princípios de proteção de dados estabelecidos na legislação. Esta pesquisa também visa aumentar a conscientização sobre a integração da privacidade de dados no desenvolvimento de software, especialmente nas fases de requerimento e projeto. A implementação de controles de privacidade nessas etapas representa um avanço significativo em termos de foco na privacidade, abordando aspectos críticos para empresas e profissionais envolvidos no desenvolvimento de software.

4 RESULTADOS E DISCUSSÕES

Os controles foram agrupados em cinco categorias para abordar aspectos específicos da proteção e privacidade de dados no desenvolvimento de software. Estas categorias incluem Governança, Conscientização e Treinamento, Segurança de Dados, Privacidade por Design e Revisão e Avaliação, conforme ilustrado na Figura 1. Ao todo, são 36 controles distribuídos nas categorias: 5 controles em Governança, 1 controle em Conscientização e Treinamento, 8 controles em Segurança de Dados, 17 controles em Privacidade por Design, e 5 controles em Revisão e Avaliação.

Figura 1: Categorias de Controles

Fonte: Elaborado pelos autores, 2024.

A categoria Governança abrange controles que envolvem liderança, políticas, procedimentos e responsabilidades dentro da organização, assegurando que a privacidade e a proteção de dados sejam integradas às políticas e processos organizacionais. Além disso, a LGPD menciona em seu art. 50 que os responsáveis pelotratamento de dados podem estabelecer diretrizes de boas práticas e governança, que definem condições de organização, operação, procedimentos, normas de segurança,padrões técnicos e outras obrigações específicas para os envolvidos no tratamento de dados pessoais (BRASIL, 2018).

Nesse cenário, controles propostos desta categoria estão expostos no Quadro 3.

Quadro 3: Controles de Governança

Identificador	Controle	Descrição
G.1	Integração da segurança da informação no gerenciamento de projetos	A SI deve ser integrada ao gerenciamento de todos os projetos para que os riscos sejam tratados desdeo início.
G.2	Conformidade com requisitos de privacidade e proteção de dados	A organização deve cumprir os requisitos de privacidade e proteção de dados dispostos em leis, regulamentos e contratos.
G.3	Documentação de procedimentos operacionais	Os procedimentos de operação de tratamento devem ser documentados.
G.4	Definição de políticas para uso e processamento de dados	Organizações devem ter uma política para uso e proteção de DP que seja adequada, transparente, e forneça uma estrutura para objetivos de proteção de DP.
G.5	Atribuição de responsabilidade	Nomeação de um responsável pela proteção de dados (Encarregado) para garantir a conformidade com as políticas e a responsabilidade.

Fonte: Elaborado pelos autores, 2024.

A categoria Conscientização e Treinamento enfatiza a necessidade de treinar funcionários e estabelecer uma cultura de privacidade dentro da organização. A conscientização é crucial para garantir a conformidade com a LGPD e mitigar os riscos associados ao tratamento de dados. É fundamental que toda a organização esteja bem informada sobre a legislação e implemente práticas adequadas (SOLER, 2022). Além disso, conforme destacado por Garcia et al. (2020, p. 83), o artigo 50 da LGPD sublinha a importância da educação em segurança, uma responsabilidade dos Controladores e Operadores na definição de boas práticas, o que se reflete no controle específico "Conscientização e treinamento em segurança da informação", consolidado a partir da integração de outros controles (Quadro 4).

Quadro 4: Controle de Conscientização e Treinamento

Identificador	Controle	Descrição
CT.1	Conscientização e treinamento em segurançada informação	O pessoal da organização e partes interessadas devem receber treinamento regular em SI e atualizações das políticas de segurança, incluindo treinamento anual em código seguro e princípios de segurança de aplicativos.

Fonte: Elaborado pelos autores, 2024.

A categoria Segurança de Dados abrange um conjunto de medidas destinadas a proteger os dados pessoais contra acessos não autorizados, uso indevido, roubo ou perda,

visando assegurar a confidencialidade, integridade e disponibilidade das informações (FONTES, 2012). Conforme estipulado pelo art. 47 da LGPD, tanto os agentes de tratamento quanto qualquer pessoa envolvida no processo são responsáveis por garantir a segurança da informação após o tratamento dos dados, conforme determinado pela legislação (BRASIL, 2018). Essa exigência sublinha a importância contínua da proteção dos dados pessoais para evitar possíveis vulnerabilidades de segurança e salvaguardar a privacidade dos indivíduos mesmo após o término do processo de tratamento.

Controles classificados nessa categoria estão expostos no Quadro 5.

Quadro 5: Controles de Segurança de Dados

Identificação	Controle	Descrição
SD.1	Uso de criptografia no *software* e no seu desenvolvimento	É necessário definir e implementar regras para o uso efetivo da criptografia na organização e no *software* a ser desenvolvido.
SD.2	Adoção de medidas de desenvolvimento seguro	Devem ser adotadas medidas de desenvolvimentoseguro.
SD.3	Gerenciamento de requisitos de segurança do *software*	Os requisitos de SI devem ser identificados, especificados e aprovados ao desenvolver aplicações.
SD.4	Adoção de princípios de arquitetura e engenharia desistemas seguros	Princípios de engenharia para sistemas de segurança devem ser estabelecidos, documentados, mantidos e aplicados a todas as atividades de desenvolvimento de sistemas.
SD.5	Proteção dos dados com a segurança da informação	Os ambientes de desenvolvimento, teste e produção devem ser separados e protegidos,
SD.6	Segurança do *software* a ser desenvolvido	O *software* deve restaurar rapidamente a disponibilidade, proteger a integridade e a confidencialidade.
D.7	Uso de controle de acesso	Devem ser criadas regras para controle de acesso físico e lógico.
SD.8	Controle de acesso do *software* a ser desenvolvido	O *software* deve ter controle de acesso, permitindo que usuários acessem apenas as informações necessárias, suportando e exigindo autenticação forte, e monitorando tentativas de acesso não autorizado.

Fonte: Elaborado pelos autores, 2024.

A categoria Privacidade por Design engloba controles que incorporam os princípios da Privacidade por Design no desenvolvimento de software, integrando ações para proteger a privacidade de dados desde as etapas iniciais do desenvolvimento de sistemas e aplicativos. Isso inclui a implementação de medidas como minimização e anonimização de dados sempre que possível, além de garantir que as configurações de

privacidade sejam definidas por padrão. Conforme estabelecido pelo art. 46 § 2° da LGPD, tais medidas de proteção de dados devem ser aplicadas desde a concepção do produto ou serviço até sua execução (BRASIL, 2018).

Quadro 6: Controles de Privacidade por Design

Identificador	Controle	Descrição
PD.1	Transparência para os titulares dos dados	O *software* deve fornecer informações claras sobre o controlador de dados e o tratamento dos DP. Devepermitir que os titulares solicitem informações.
D.2	Controle do titular de dados	O *software* deve ser projetado para facilitar os titulares de DP modificar ou cancelar seus consentimentos.
PD.3	Limite de coleta	Limitar a coleta de DP ao mínimo necessário para propósitos legítimos e especificados.
PD.4	Precisão e qualidade	A organização deve garantir que os DP sejam precisos, completos e atualizados de acordo com o propósito do tratamento.
PD.5	Descarte e anonimização	Deve-se descartar os DP ou entregá-los de modo que não seja possível a identificação do titular, como a
		anonimização, quando se atingir a finalidade do tratamento de dados.
PD.6	Minimização de dados	A organização deve minimizar a quantidade de DPsendo tratado somente o necessário e legítimo.
PD.7	Descarte de arquivostemporários	A organização deve garantir que os arquivos temporários gerados durante o tratamento sejam eliminados conforme procedimentos documentados e dentro de prazos estabelecidos.
PD.8	Retenção de dados pessoais	A organização deve reter os DP apenas pelo tempo necessário para os propósitos identificados.
PD.9	Identificação de requisitos para proteção da privacidade	Questões de privacidade devem ser resolvidas antes da implementação para garantir conformidade desde o início.
PD.10	Acesso e participação do titular	O *software* deve permitir que os titulares de dados questionem e corrijam seus DP.
PD.11	Demonstração	O *software* deve ser projetado e desenvolvido para que o controlador possa documentar e demonstrar conformidade com a legislação de proteção de dados.
PD.12	Ocultação e agregação	Os DP devem ser processados de forma a limitar a observabilidade e identificação dos titulares, evitando comunicação, processamento ou armazenamentovisíveis.
PD.13	Definição do tratamento	A organização deve definir o tratamento e ter uma visão geral dos DP necessários.
PD.14	Seleção de subcontratados com garantias de proteção de dados	Os subcontratados devem garantir conformidade comnormas de privacidade e proteção de dados.
PD.15	Definição de nível aceitável de risco	A organização deve estabelecer níveis de tolerância para proteção de dados e SI.
PD.16	Separação dos dados pessoais	Os DP devem ser armazenados separadamente, emdiferentes bancos de dados ou áreas.

PD.17	Adoção de privacidade por padrão	O *software* deve ter configuração padrão favorável à privacidade

Fonte: Elaborado pelos autores, 2024.

A categoria Revisão e Avaliação engloba controles que monitoram a conformidade com a legislação e revisam continuamente as práticas de privacidade de uma organização. Esses controles são fundamentais para revisar políticas e procedimentos, avaliar riscos e garantir a conformidade com a legislação, promovendo a evolução constante dos processos de privacidade e segurança. Conforme estipulado pelo subitem h) do § 2º do art. 50° da LGPD, um programa de governança em privacidade requer atualizações frequentes baseadas em monitoramento contínuo e avaliações regulares (BRASIL, 2018).

Controles classificados em Revisão e Avaliação são apresentados no Quadro 7.

Quadro 7: Controles de Revisão e Avaliação

Identificador	Controle	Descrição
RA.1	Revisão da conformidade	A organização deve revisar regularmente sua conformidade com a política de SI e outras regras relacionadas.
RA.2	Avaliação de riscos de segurança da informação eprivacidade	A organização deve realizar avaliações de riscos de SI e de privacidade para identificar riscos dentro do escopo do Sistema de Gestão de Privacidade da Informação (SGPI).
RA.3	Realização de avaliação de impacto de privacidade (AIP)	A organização deve realizar Avaliações de Impacto de Privacidade (AIP) ao planejar novos tratamentos de DP ou fazer alterações significativas em tratamentos existentes.
RA.4	Realização de modelagem de ameaças	A organização deve realizar modelagem de ameaças para identificar e corrigir falhas de segurança no projeto da aplicação antes da codificação.
RA.5	Realização de análise desuperfície de ataque	Antes de iniciar o projeto, a organização deve analisar a superfície de ataque para reduzir oportunidades deexploração de fraquezas.

Fonte: Elaborado pelos autores, 2024.

Ao seguir esta proposta, espera-se que a empresa alcance um ambiente de desenvolvimento de software robusto e seguro e que priorize a privacidade dos usuários. Isso resultará na conformidade com, no mínimo, parte das exigências da LGPD, minimizando riscos legais e financeiros associados a violações de dados. Além disso, a

empresa fortalecerá a confiança dos clientes e usuários ao demonstrar um compromisso com a proteção de suas informações pessoais.

Por questão de limitação do texto, os controles propostos estão disponíveis integralmente no material suplementar hospedado em: https://tinyurl.com/c8bur7ht.

5 CONSIDERAÇÕES FINAIS

O estudo atingiu seus objetivos ao especificar boas práticas para o desenvolvimento de software com foco na privacidade, principalmente nas etapas de requerimento e projeto. Analisou diretrizes nacionais e internacionais de privacidade e proteção de dados, permitindo a construção de um framework robusto para facilitar o desenvolvimento de sistemas que respeitem a privacidade do usuário desde o início.Este framework enfatiza a inclusão da privacidade e proteção de dados no desenvolvimento de novos sistemas.

Os achados principais foram organizados em cinco áreas de controle: Governança, Conscientização e Treinamento, Segurança de Dados, Privacidade por Design, e Revisão e Avaliação. Cada área aborda aspectos específicos para garantir a integração da privacidade e segurança de dados em todo o processo de desenvolvimento de software. Na Governança, os controles asseguram que a liderança e políticas organizacionais integrem a proteção de dados, alinhando-se com a LGPD e outras regulamentações de privacidade.

A categoria de Conscientização e Treinamento sublinha a importância de educar e treinar funcionários sobre segurança da informação (SI) e privacidade de dados, incluindo a realização de treinamentos regulares e atualizações sobre políticas de segurança. Isso é essencial para a conformidade contínua com a LGPD e para aumentar a conscientização sobre a proteção de dados, reduzindo riscos associados ao tratamento inadequado de informações pessoais.

Segurança de Dados inclui controles para proteger dados pessoais contra acessos não autorizados, utilizando criptografia, princípios de desenvolvimento seguro e gestão de requisitos de segurança, garantindo confidencialidade, integridade e disponibilidade

dos dados. A Privacidade por Design envolve práticas como minimização de dados e anonimização. Revisão e Avaliação focam na revisão contínua das políticas de privacidade e avaliação dos sistemas em desenvolvimento, garantindo a eficácia e atualização das práticas de proteção de dados.

Embora o estudo tenha especificado boas práticas para o desenvolvimento de software com foco na privacidade, reconhece-se que é um ensaio teórico e necessita de validação empírica. Recomenda-se a realização de novos estudos para validar e expandir as propostas apresentadas, tornando as práticas de proteção de dados mais confiáveis e eficientes. Futuras pesquisas podem explorar a eficácia desses controles emdiferentes projetos e setores, avaliar a percepção dos desenvolvedores sobre sua implementação e investigar o impacto na conformidade regulatória, qualidade do software e experiência do usuário.

REFERÊNCIAS

ABNT - Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27001**: Segurança da Informação, Segurança Cibernética e Proteção à Privacidade - Sistemas de Gestão da Segurança da Informação - Requisitos. Rio de Janeiro: ABNT, 2022.

ABNT - Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002**: Segurança da Informação, Segurança Cibernética e Proteção à Privacidade - Controles de Segurança da Informação. Rio de Janeiro: ABNT, 2022.

ABNT - Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27701**: Técnicas de Segurança - Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para Gestão da Privacidade da Informação - Requisitos e Diretrizes. Rio de Janeiro: ABNT, 2019.

ABNT - Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 29100**: Tecnologia da Informação - Técnicas de Segurança - Estrutura de Privacidade. Rio de Janeiro: ABNT, 2020a.

ABNT - Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 29151**: Tecnologia da Informação - Técnicas de Segurança - Código de Prática para Proteção de Dados Pessoais. Rio de Janeiro: ABNT, 2020b.

BERNARDO, Taynara Rodrigues; PINZEGHER, Igor Pacheco. **LGPD Aplicada ao Desenvolvimento de Software**. [*S. l.*]: Lawquest, 2021. Disponível em: https://lawquest.com.br/lgpd-aplicada-ao-desenvolvimento-de-software/. Acesso em: 08 abr. 2024.

BERTAN, Beatriz Cesário *et al.* **Abordagem da LGPD no Desenvolvimento de Software**. 2022. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) - Faculdade de Computação e Informática, Instituto Presbiteriano Mackenzie, São Paulo, 2022. Disponível em: https://dspace.mackenzie.br/items/7f1cab18-e780-4655-9696-da240f31f57e. Acesso em: 11 abr. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei nº 13.853, de 2019. Brasília, DF: Senado Federal, 2018. Disponível em:https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 fev. 2024.

CANEDO, Edna Dias *et al.* Perceptions of ICT Practitioners Regarding Software Privacy. **Entropy**, Basel, v. 22, 4th ed., p. 429, 2020. Disponível em: https://www.mdpi.com/1099-4300/22/4/429#metrics. Acesso em: 28 abr. 2024.

CAVOUKIAN, Ann. Privacy by Design: The 7 Foundational Principles. **Information and Privacy Commissioner of Ontario**, Canada, v. 5, p. 12, 2009.

CERQUEIRA, Diego André; MELLO, Rafael Maiani de; TRAVASSOS, Guilherme Horta. Um Checklist para Inspeção de Privacidade e Proteção de Dados Pessoais em Artefatos de Software. *In*: CONGRESSO IBERO-AMERICANO EM ENGENHARIA

DE SOFTWARE (CIBSE), 26., 2023, Montevideo. **Anais** [...]. Porto Alegre: Sociedade Brasileira de Computação, 2023. p. 206-213. Disponível em: https://sol.sbc.org.br/index.php/cibse/article/view/24704. Acesso em: 07 mar. 2024.

CIS - Center for Internet Security. **Controles CIS Versão 8**. East Greenbush: Center for Internet Security, 2021. Disponível em:https://learn.cisecurity.org/cis-controls-download?_gl=1*1g7leqk*_ga*MTE4Njc2NjA5Mi4xNzEwMTY5NjAx*_ga_N70Z2MKMD7*MTcxMjcwNTA0My4yLjAuMTcxMjcwNTA0My42MC4wLjA.*_ga_3FW1B1JC98*MTcxMjcwNTA0My4yLjAuMTcxMjcwNTA0My4wLjAuMA. Acesso em: 08 abr. 2024.

COSTA, Lucas Matheus Torres; ALVES, Moabe Barbosa; GUIMARÃES, Rafael Figueredo. **LGPD Compliance**: Aplicando Checklist para Avaliação de Sistemas à Luz da Lei Geral de Proteção de Dados. 2022. Trabalho de Conclusão de Curso (Bacharelado em Engenharia da Computação) - Instituto Federal da Paraíba, Campina Grande, 2022. Disponível em: https://repositorio.ifpb.edu.br/handle/177683/2484. Acesso em: 20 maio 2024.

CRESWELL, John W.; CLARK, Vicki L. Plano. **Pesquisa de Métodos Mistos**: Série Métodos de Pesquisa. 2. ed. Porto Alegre: Penso Editora, 2013. *E-book*. Disponível em: https://www.google.com.br/books/edition/Pesquisa_de_M%C3%A9todos_Mistos_2_ed/HPyzCAAAQBAJ?hl=pt-BR&gbpv=0. Acesso em 19 mar. 2024.

DATATILSYNET - Norwegian Data Protection Authority. **Software Development with Data Protection by Design and by Default**. Oslo: Datatilsynet, 2017. Disponível em: https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/data-protection-by-design-and-by-default/. Acesso em 08 abr. 2024.

DROZD, Olha. Privacy Pattern Catalogue: A Tool for Integrating Privacy Principles of ISO/IEC 29100 into the Software Development Process. *In*: PRIVACY AND IDENTITY. **Privacy and Identity Management. Time for a Revolution? 10th**. International Summer School, Edinburgh, UK, August 16-21, 2015, Revised Selected Papers. Cham: Springer International Publishing, 2016. p. 129–140. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-41763-9_9. Acesso em: 08 mar. 2023.

FONTES, Edison Luiz Gonçalves. **Segurança da informação**. 1. ed. São Paulo: Editora Saraiva, 2012. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502122185/. Acesso em: 11 mai. 2024.

GARCIA, Lara Rocha *et al*. **Lei Geral de Proteção de Dados (LGPD)**: Guia de implantação. São Paulo: Editora Blucher, 2020. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555060164/. Acesso em: 07 mar. 2024.

GARRIDO, Patricia Peck. **Proteção de Dados Pessoais**: Comentários à Lei n. 13.709/2018 (LGPD). 4. ed. São Paulo: Editora Saraiva, 2023. *E-book*. Disponível em:

https://integrada.minhabiblioteca.com.br/#/books/9786555599480/. Acesso em: 18 mar. 2024.

GET PRIVACY. **Entenda o Conceito De Privacy by Design e sua Relação com a LGPD**. Curitiba: Portal Get Privacy, 2022. Disponível em: https://getprivacy.com.br/privacy-by-design-lgpd/. Acesso em: 08 abr. 2024.

GUIDO, Bárbara. **Privacy by Design**: Conheça os 7 Princípios e a Importância de Cada um Deles. Barueri: Uplexis, 2023. Disponível em: https://uplexis.com.br/blog/artigos/privacy-by-design-principios/. Acesso em: 03 jun. 2023.

MELO, Jonas Ferrigolo; ROCKEMBACH, Moisés; SILVA, Armando Malheiro da. Ciência da Informação e Privacy by Design: Aspectos Éticos e Possibilidades de Pesquisa. **Logeion**: Filosofia da Informação, Rio de Janeiro, v. 9, n. 2, p. 124–143, 2023. Disponível em: https://revista.ibict.br/fiinf/article/view/6099. Acesso em: 16 abr. 2024.

NIST - National Institute of Standards and Technology. **NIST Privacy Framework**: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. Gaithersburg: National Institute of Standards and Technology, 2020. Disponível em: https://www.nist.gov/privacy-framework/privacy-framework. Acesso em: 08 abr. 2024.

OMORONYIA, Inah. Why is Baking Privacy into Software Design Hard? **ITNOW**, [Oxford],v.61,3thed.,p.44–45,21 ago. 2019. Disponível em:

https://doi.org/10.1093/itnow/bwz077. Acesso em: 03 jun. 2024.

PEREIRA, Fabio Luiz Barbosa; SILVA, Cecília Alberton Coutinho. **Vazamento de Dados Aumentaram 493% no Brasil, Segundo Pesquisa do MIT**. [S.l]: VC S/A, 2021.Disponível em:https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil- segundo-pesquisa-do-mit. Acesso em: 08 maio 2024.

SANTOS, Grasielle Costa. **Recomendações de Boas Práticas para Implementação da LGPD em Processos de Desenvolvimento de Software**. 2022. Trabalho de Conclusão de Curso (Bacharelado em Engenharia de Computação) - Pontifícia Universidade Católica de Goiás, Goiânia, 2022. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/4428. Acesso em: 07 mar. 2023.

SOLER, Fernanda Galera. **Proteção de Dados**: Reflexões Práticas e Rápidas Sobre a LGPD. São Paulo: Editora Expressa, 2022. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553622500/. Acesso em: 24 abr. 2024.

VALDIVIA, Gustavo. **Implementação do CIS Controls V8**. São Paulo: GAT, 2021. Disponível em: https://www.gat.digital/blog/implementacao-de-controles-cis/. Acesso em: 22 abr. 2024.

ISSN: 1696-8352

VASCONCELOS, Márcia Linhares de. **Vazamento de Dados Pessoais**: Um Problema em Crescimento. 2022. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) - Instituto Federal Goiano, Ceres, GO, 2022. Disponível em: https://repositorio.ifgoiano.edu.br/handle/prefix/3234. Acesso em: 08 maio 2024.