UNIVERSIDADE FEDERAL DO CEARÁ

UFC CAMPUS RUSSAS

CURSO DE GRADUAÇÃO EM ENGENHARIA DE SOFTWARE

THALLES PAIVA SOUZA

A TRANSFERÊNCIA DE CONHECIMENTO SOBRE SEGURANÇA DE DADOS, LGPD E *PRIVACY BY DESIGN* NOS CURSOS DE TI DA UFC CAMPUS DE RUSSAS: UMA PERSPECTIVA DISCENTE E DOCENTE

RUSSAS

2026

THALLES PAIVA SOUZA

A TRANSFERÊNCIA DE CONHECIMENTO SOBRE SEGURANÇA DE DADOS, LGPD E *PRIVACY BY DESIGN* NOS CURSOS DE TI DA UFC CAMPUS DE RUSSAS: UMA PERSPECTIVA DISCENTE E DOCENTE

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Software da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de Bacharel em Engenharia de Software.

Orientador: Prof. Ms. Caio César de Freitas Dantas

RUSSAS

2026

THALLES PAIVA SOUZA

A TRANSFERÊNCIA DE CONHECIMENTO SOBRE SEGURANÇA DE DADOS, LGPD E *PRIVACY BY DESIGN* NOS CURSOS DE TI DA UFC CAMPUS DE RUSSAS: UMA PERSPECTIVA DISCENTE E DOCENTE

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Software da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de Bacharel em Engenharia de Software.

Aprovada em: 07/07/2026

BANCA EXAMINADORA

Prof. Ms. Caio César de Freitas Dantas (Orientador)
Universidade Federal do Ceará (UFC)
Campus-Russas

Prof. Dr. Mayrton Dias de Queiroz
Universidade Federal do Ceará (UFC)
Campus-Russas

Prof. Ms. Hugo Nathan Barbosa Regis
Universidade Federal do Ceará (UFC)
Campus-Russas

AGRADECIMENTOS

Primeiramente gostaria de agradecer a Deus por me conceder força de vontade e persistência de enfrentar as dificuldades, agradeço também a minha Mãe e ao meu Pai que sempre me apoiaram e me incentivaram a lutar pelos meus sonhos, agradeço aos professores que sempre estiveram de prontidão para ajudar aos alunos com as disciplinas, em especial a meu professor orientador pois foi com sua dedicação e orientação que eu ganhei confiança para trilhar o meu próprio caminho, agradeço a banca avaliadora pela oportunidade e pelo tempo dedicado em me avaliar, agradeço a coordenação do meu curso, em especial ao coordenador, que sempre fazia de tudo para apoiar e auxiliar os alunos a não desistirem, e por fim agradeço aos meus amigos da universidade, que sempre estiveram lá nos bons e maus momentos, em especial a você Lin sou muito grato por todo apoio e confiança que você dedicou a mim.

RESUMO

Com o aumento de profissionais graduados nas áreas de TI, e do alto índice de procura por uma formação nas áreas de tecnologia, ainda pode-se observar uma significativa lacuna no preparo dos profissionais que estão entrando no mercado de trabalho, em questões relacionadas aos princípios de segurança da informação, compreensão da Lei Geral de Proteção de Dados (LGPD) e de privacy by design (PbD), no processo de desenvolvimento do software. Diante desse cenário, o estudo relata até que ponto a formação acadêmica está alinhada com as demandas de conformidade e segurança exigidas pelo mercado de trabalho atual. Focando em uma análise quali-quantitativa e exploratória, voltando-se ao contexto da UFC Campus Russas, analisando os docentes e discentes que fazem parte das disciplinas do curso de Engenharia de Software (ES) e Ciência da computação (CC), a respeito dos temas abordados e como esse conhecimento está sendo passado pelos docentes aos discentes, que estão em formação, identificando boas práticas e possíveis melhorias.

Palavras-chave: segurança da informação; segurança de dados; lgpd; privacy by design; formação acadêmica.

ABSTRACT

With the increase of graduate professionals in IT areas, and the high demand for education in technology fields, a notable gap remains in the preparedness of professionals entering the job market regarding information security principles, the General Data Protection Law (LGPD), and "privacy by design"(PbD) within the software development process. Against this backdrop, this study examines the extent to which academic training aligns with the compliance and security demands of the current job market. Employing an exploratory, mixed-methods (qualitative and quantitative) approach, the study focuses on the UFC Russas campus-specifically analyzing faculty and students in the Software Engineering (SE) and Computer Science (CS) programs. It investigates the topics covered and how this knowledge is imparted to students, ultimately identifying best practices and areas for improvement.

Keywords: information security; data security; lgpd; privacy by design; academic background.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
CC	Ciência da Computação
ES	Engenharia de Software
LGPD	Lei Geral de Proteção de Dados
PbD	*Privacy By Design*
SI	Segurança da Informação
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

Atualmente com o intenso tráfego de dados no meio digital, têm gerado debates com foco na segurança da informação, e como lidar com o grande volume de dados, de maneira a respeitar os direitos dos usuários e preservar a confiança nas empresas. Em resposta a essa situação, o Brasil constituiu a Lei Geral de Proteção de Dados (LGPD) , que padroniza e estabelece diretrizes legais a serem seguidas (BRASIL, 2018). Contudo, a legislação, isoladamente, não se mostrou suficiente para conter os recorrentes casos de vazamentos de dados no país, como ilustra o exemplo recente, onde foram vazados mais de 7 bilhões de *cookies* que são dados que podem armazenar (Identificadores, *tokens*, dados de autenticação e preferência dos usuários), segundo a pesquisa da NordVPN (AUGUSTO, 2024). Portanto os incidentes de falha de segurança podem acabar gerando um prejuízo monetário que dependendo do tipo de vazamento pode escalar para um grande prejuízo a empresa (SANTOS, 2022). Destacando-se assim a necessidade de boas práticas efetivas no desenvolvimento de softwares.

A fim de alinhar o desenvolvimento técnico com as exigências legislativas e evitar possíveis incidentes de segurança. Os profissionais e as organizações passaram a utilizar a metodologia chamada de *Privacy By Design* (PbD) ou privacidade desde a concepção, para garantir que a proteção de dados seja inserida em todas as etapas do desenvolvimento do software, de forma ativa, desde a coleta de requisitos até a manutenção dos sistemas. Nesse contexto, observa-se uma crescente procura por profissionais que dominem o conhecimento de como aplicar a LGPD juntamente com o PbD no processo de desenvolvimento do software (DUARTE *et al.*, 2025).

Apesar desse aumento de profissionais graduados nas áreas de Tecnologia da Informação (TI), e no alto índice de procura por uma formação nas áreas de tecnologia (MARQUES *et al.*, 2024). Ainda pode-se constatar uma significativa lacuna no preparo dos profissionais que estão entrando no mercado de trabalho conforme destaca (DUARTE *et al.*, 2025). Há carência em questões relacionadas aos princípios de segurança da informação, compreensão da LGPD e de PbD no ciclo da vida do software. E diante desse cenário cabe o questionamento feito por Peixoto (2023), até que ponto a formação acadêmica está alinhada com as demandas de conformidade e segurança exigidas pelo mercado de trabalho atual.

A fim de continuar este questionamento o presente trabalho realiza uma análise voltada ao contexto da UFC Campus Russas, com os objetivos a seguir

1.1 Objetivo

1.1.1 Geral

Analisar o nível em que a UFC prepara os alunos alunos dos cursos de Engenharia de Software (ES) e Ciência da Computação (CC) do Campus Russas, sobre os temas de segurança de dados, LGPD e PbD.

1.1.2 Específicos

(I) Avaliar o conhecimento dos alunos sobre os temas (Segurança de Dados, LGPD e PbD).

(II) Verificar como esses conteúdos estão sendo apresentados aos alunos pelos docentes.

(III) Investigar possíveis métodos de aprendizagem e dificuldades encontradas pelos docentes ao apresentar esses conteúdos.

(IV) Sugerir possíveis melhorias e soluções.

1.2 Organização deste trabalho

Visando concluir esses objetivos, este presente trabalho foi organizado da seguinte forma: Capítulo 2: Fundamentação Teórica onde foi discutido o conhecimento a respeito da Segurança da Informação (SI), LGPD e PbD. Capítulo 3: Trabalhos Relacionados apresenta os trabalhos que foram ultilizados com base para este trabalho, agrupados para facilitar a comparação. Capítulo 4: Metodologia apresenta as principais informações referentes a como o trabalho foi conduzido. Capítulo 5: Resultados apresenta quais foram os resultados dos questionamentos deste trabalho e a discussão desses resultados. Capítulo 6: Conclusão apresenta como foi finalizada a pesquisa, apresenta também os trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta os principais conceitos relacionados a este estudo, com foco em Segurança da Informação, Lei Geral de Proteção de Dados e *Privacy by Design*.

2.1 Segurança da informação

A Segurança da informação é um conjunto de práticas, políticas e ferramentas, destinadas a assegurar os dados de um sistema, contra acessos não autorizados, alterações, exclusões ou interrupções. E tem como objetivo central garantir os 3 pilares fundamentais (Confidencialidade, Integridade e Disponibilidade) conhecidos como a tríade CID, conforme definido pela ABNT NBR ISO/IEC 27002 (2022).

Confidencialidade: é a propriedade que garante que a informação não seja divulgada a indivíduos ou processos que não possuem autorização, garantindo o acesso somente a pessoas e sistemas autorizados (ABNT, 2022).

Integridade: procura assegurar que os dados permaneçam corretos e que não foram alterados por meio de modificações ou exclusões mesmo que de forma acidental (ABNT, 2022).

Disponibilidade: garante que o sistema e as informações estejam disponíveis e funcionando sempre que uma pessoa ou sistema autorizado precisar (ABNT, 2022).

Além da tríade CID, quatro outros conceitos aparecem com frequência na literatura de segurança da informação e estão diretamente interligados aos pilares: ameaça, vulnerabilidade, risco e incidente conforme definido pela ABNT NBR ISO/IEC 27005 (2023).

Ameaça: é um evento, ação ou circunstância com potencial de causar dano a um ativo de informação, comprometendo a confidencialidade, a integridade ou a disponibilidade. Exemplos: incluem ataques de *hackers*, erros de funcionários, falhas de software e desastres naturais (ABNT, 2023).

Vulnerabilidade: é uma fragilidade ou falha presente em um ativo, processo ou controle que pode ser explorada por uma ameaça. Uma vulnerabilidade, por si só, não causa dano; o problema se materializa quando uma ameaça a explora como um sistema sem criptografia (vulnerabilidade) acessado por um invasor (ameaça) (ABNT, 2023). Exemplo: um software sem atualização (falha de segurança conhecida), ausência de criptografia na transmissão de dados, falta de treinamento dos colaboradores, política de senhas fracas.

Risco: é a probabilidade de uma ameaça explorar uma vulnerabilidade e causar

impacto em um ativo de informação. Em outras palavras, é a medida do potencial de dano, considerando a chance de ocorrência e a gravidade da consequência (ABNT, 2023). Exemplo: se um hospital mantém prontuários médicos sem controle de acesso (vulnerabilidade) e há histórico de ataques a sistemas de saúde (ameaça), o risco de violação de confidencialidade é alto. A organização decide então se vai aceitar, mitigar, transferir ou evitar esse risco.

Incidente: um incidente é a materialização do risco, um evento real que compromete a confidencialidade, a integridade ou a disponibilidade de um ativo, ou que viola uma política de segurança estabelecida (ABNT, 2023). Exemplo: um *ransomware* que criptografa todos os dados de uma universidade (indisponibilidade e possível perda de integridade); um e-mail de *phishing* que leva ao vazamento de credenciais (confidencialidade); alteração maliciosa de notas no sistema acadêmico (integridade)

Apesar desses pilares fundamentais serem essenciais, eles precisam receber uma manutenção constante, pois enfrentam inúmeras ameaças, como vulnerabilidades do sistema e ameaças externas (CASOTTI, 2024).

A preservação da segurança da informação é uma preocupação que precede e muito a comunicação digital dos tempos modernos. Conforme destaca Medeiros (2025) em sua análise sobre a proteção de dados e como ela evoluiu, o desenvolvimento de métodos para preservar a informação e garantir sua segurança, acompanha a própria evolução da comunicação e suas estratégias.

Diante dessas ameaças constantes, o processo de desenvolvimento de software assume um papel estratégico, pois ao implementar a segurança da informação durante o processo de desenvolvimento o sistema torna-se preventivo e não mais reativo (CAVOUKIAN, 2011), (HOEPMAN, 2022). O software passa a ser desenvolvido visando as possíveis ameaças e vulnerabilidades que podem ocasionar falhas futuras, ao invés de manutenção corretiva, posterior ao encerramento do projeto (CAVOUKIAN, 2011), (HOEPMAN, 2022). Tratando as ameaças de forma preventiva, o sistema reduz vulnerabilidades ao evitar problemas de segurança da informação e o cumprimento da Lei Geral de Proteção de Dados (LGPD).

2.2 Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) foi o marco regulatório com respeito do tratamento de dados pessoais, inclusive no meio digital, abrangendo todas as operações que lidam com os dados pessoais, como a coleta, armazenamento, compartilhamento

e exclusão dos dados pessoais (BRASIL, 2018). Além disso, como observado por Oliveira et al. (2021) possui como principal objetivo proteger os direitos fundamentais como a proteção à liberdade, o livre desenvolvimento de personalidade e a privacidade.

A LGPD foi criada com uma forte influência da *General Data Protection Regulation* (GDPR) ou Regulamento Geral de Proteção de Dados da União Europeia que entrou em vigor em 2018 (BELARMINO *et al.*, 2024).

A GDPR estabeleceu um padrão global de conformidade, visando proteger a privacidade dos dados dos cidadãos da União Europeia contra possíveis abusos e vazamentos de dados, fazendo com que instituições públicas e privadas adotassem uma postura transparente e responsável sobre o manuseio dos dados pessoais dos seus usuários (BELARMINO *et al.*, 2024).

O impacto da GDPR serviu de grande influência para a criação da LGPD (CANAAN, 2023). Legislação essa que posuia uma regulamentação rígida, se estendendo até as tecnologias mais recentes, impondo o desafio de manter a transparência e responsabilidade no tratamento dos dados (FERETZAKIS *et al.*, 2024).

Durante o processo de criação dessa regulamentação foi estabelecido em seus artigos conceitos fundamentais, sendo estes: Dados pessoais, Dados sensíveis, Titular, Controlador e Operador (Lei nº 13.709/2018).

Titular: O verdadeiro dono da informação, pessoa a qual os dados se referem.

Controlador: A pessoa ou empresa que, por direito público ou privado, possui as competências para realizar o tratamento dos dados pessoais.

Operador: A pessoa ou empresa que, por direito público ou privado, foi contratado pelo controlador, para realizar o tratamento dos dados.

Dados pessoais: Qualquer informação relacionada a pessoa natural identificada ou identificável, incluindo dados básicos como nome, CPF e endereço, além de dados indiretos como histórico de consumo e endereço de IP.

Dados sensíveis: Qualquer dado que ao ser vazado ou disponibilizado para fontes sem as devidas permissões, vão ocasionar em perdas e danos ao seu titular.

Esses conceitos são utilizados para compor os dez princípios fundamentais que devem ser observados e seguidos nas práticas de atividades que lidam com dados pessoais. Entre esses princípios, os que mais se destacam são:

Finalidade e Adequação - que juntos, exigem que as informações coletadas sejam utilizadas para fins legítimos, específicos e que foram informados ao titular desses dados, não

permitindo mudar essa finalidade após informar aos titulares.

Necessidade - que limita no mínimo possível de dados que podem ser coletados, para somente o indispensável na execução das finalidades pretendidas.

Transparência e segurança - que garantem ao titular dos dados o direito a receber informações claras e precisas sobre o manejo dos seus dados, ao mesmo tempo que obrigam os agentes de tratamento de dados a adotarem medidas técnicas e administrativas, para proteger essas informações de acesso não autorizados e incidentes.

Entretanto, apenas a leitura desses princípios por si só não é tão efetiva, assim, vale ressaltar a importância de sua correta interpretação para a aplicação efetiva da lei e garantia da segurança e confiança no meio digital(Lei nº 13.709/2018).

2.3 *Privacy By Design* (PbD)

O *Privacy by Design* (PbD), ou Privacidade desde a concepção, constitui uma metodologia que propõe a incorporação da privacidade e da proteção de dados como um requisito fundamental de um projeto, desde a fase inicial, e não como um elemento extra a ser acrescentado futuramente. Conforme foi citado por sua criadora Cavoukian (2021) em seu primeiro princípio, trata-se de uma abordagem proativa, preventiva e não reativa, que busca antecipar possíveis violações à privacidade antes que elas aconteçam. Nessa mesma linha de pensamento, Hoepman (2022) argumenta que a privacidade e a segurança de dados devem ser tratadas como um requisito de "primeira classe" sendo implementada desde o início, ao invés de uma ideia ser fixada de forma tardia.

Visto que essa metodologia foi criada nos anos 90 por Ann Cavoukian, ex-comissária de informação e privacidade de Ontário no Canadá, esse conceito tornou-se a base das principais leis de proteção de dados do mundo, incluindo o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e a LGPD no Brasil. Para tornar esse conceito operacional, Cavoukian (2021) estruturou um conjunto de 7 princípios fundamentais servindo de guia para os engenheiros e arquitetos de software, esses princípios podem ser compreendidos da seguinte forma: 1-Proativo, não reativo e preventivo, não corretivo; 2-Privacidade como padrão (*Privacy by default*); 3-Privacidade incorporada ao *design*; 4-Funcionalidade total, soma positiva, e não soma zero; 5-Segurança de ponta a ponta; 6-Visibilidade e transparência; 7-Respeito pela privacidade do usuário;

Os princípios 1 e 3 são voltados ao processo de desenvolvimento, e buscam garantir

que o sistema já seja desenvolvido levando em consideração os riscos e as possíveis vulnerabilidades que podem aparecer no futuro. Já os princípios 2, 4 e 5 visam garantir que a segurança dos dados, incorporada como padrão, permeia todo o ciclo de vida da informação (coleta, armazenamento, processamento, transferência e exclusão) sem abrir mão das funcionalidades do sistema. Por fim, os princípios 6 e 7 representam a confiança que a empresa deve dispor para com seus usuários, revelando como seus dados serão tratados e garantindo sua privacidade e respeito (CAVOUKIAN, 2011).

Referente a isto, atualmente saber aplicar esses princípios e o conceito de PbD como um todo, é um conhecimento requisitado no mercado de trabalho, pois representa a junção ideal dos conhecimentos de desenvolvimento do software com a LGPD, essa importância se dá pela dificuldade em encontrar profissionais talentosos, tanto na área prática de desenvolvimento quando na teoria da legislação, portanto o profissional que detenha o conhecimento de traduzir a lei para o processo de desenvolvimento, é visto como um importante recurso para as empresas de TI (MARQUES *et al.*, 2024), (SARAIVA CLEIDSON DE SOUZA, 2024).

Apesar disso, uma das principais dificuldades encontradas para a aplicação do *Privacy by Design*, contudo, não é técnica, mas algo cultural. A engenharia de software tradicionalmente se consolidou sob uma lógica de "funcionalidade primeiro", onde o objetivo primário é entregar um produto que funcione, com prazos e orçamentos muitas vezes apertados (CAVOUKIAN, 2011), (MARQUES *et al.*, 2024). Exigir que a privacidade seja um requisito de "primeira classe", como argumenta Hoepman (2022), significa romper com essa ideia que muitas vezes já está intrínseca nos profissionais de TI. Não se trata apenas de usar uma nova ferramenta de criptografia, mas de reeducar times inteiros para que a pergunta "isso é seguro e respeita a privacidade do usuário?", seja tão instintiva quanto, "isso funciona?"(PEIXOTO, 2023). Essa mudança de mentalidade, lenta e por vezes enfrentada com resistência, representa o maior desafio e, ao mesmo tempo, a razão da alta demanda por profissionais capazes de atuar como um "tradutor", entre as equipes de desenvolvimento do produto e as exigências legais da LGPD (CAVOUKIAN, 2011).

2.3.1 Privacy by Design no ciclo de desenvolvimento do software

A incorporação efetiva do *Privacy by Desig*n ao processo de desenvolvimento de software exige que a privacidade deixe de ser uma preocupação tardia e se torne um requisito de primeira classe, estando presente em todas as etapas do ciclo de vida do sistema (HOEPMAN,

2022). Cavoukian (2011) apresenta em seu livro intitulado "*Privacy by Design: The 7 Foundational Principles*", os princípios detalhados de PbD e utilizando esse conhecimento como base, Hoepman (2022) em seu artigo intitulado "*Privacy Design Strategies*" criou estratégias para aplicar esses princípios no processo de desenvolvimento. Adiante é exibido alguns dos exemplos estratégicos criados por Hoepman (2022) divididos em etapas que fazem parte do processo de desenvolvimento do software.

Levantamento de requisitos - Neste início, o PbD é aplicado na identificação de quais dados pessoais serão coletados, com qual finalidade e sob qual base legal, em conformidade com o princípio da minimização que diz que deve-se ser coletado apenas o que for estritamente necessário.

Projeto(*design*) - Durante a arquitetura do sistema, a privacidade deve ser incorporada como padrão como é pontuado em um dos princípios de PbD que é o *Privacy by Default*. Isso significa projetar configurações que, por padrão, ofereçam o maior nível de proteção, sem exigir ação do usuário.

Implementação - Na codificação, o PbD exige práticas de desenvolvimento seguro: validação de entradas, controle rigoroso de acesso, proteção contra vazamento de dados em *logs* e uso de bibliotecas confiáveis e atualizadas.

Testes - A etapa de testes deve incluir, além dos tradicionais testes funcionais e de segurança, verificações específicas de privacidade. Isso envolve testar se as configurações de privacidade funcionam conforme especificado, se a exclusão de uma conta remove efetivamente os dados pessoais, e se há vazamento de informações em respostas de erro ou em logs.

Implantação - Ao colocar o sistema em produção, é fundamental garantir que o ambiente esteja configurado com os controles de segurança adequados: criptografia em trânsito e em repouso, políticas de retenção de dados ativadas, restrição de acessos administrativos e anonimização de dados em ambientes de homologação que são testes realizados para verificar se o sistema atende as normas de uma autoridade competente, por exemplo, a LGPD.

Manutenção - O *Privacy by Design* não termina com a entrega do software. Durante a manutenção, é necessário reavaliar periodicamente a necessidade dos dados coletados, novas funcionalidades e possíveis mudanças na legislação. Atualizações de segurança, correções de vulnerabilidades e respostas a incidentes devem seguir os mesmos princípios de proatividade.

3 TRABALHOS RELACIONADOS

Neste capítulo serão abordados os trabalhos que investigam aspectos relacionados à segurança da informação, LGPD, PbD e ensino, e qual a importância do ensino desse tema em toda a graduação em disciplinas sobre o Desenvolvimento de Software, incluídos conceitos básicos e metodologias como o PbD. Esses trabalhos foram agrupados levando em consideração seus pontos discutidos pelos autores.

3.1 Estudos sobre LGPD

Em Medeiros (2025) o autor relata a importância da segurança de dados e a trajetória de como aconteceu o surgimento da LGPD, através de uma revisão bibliográfica, e traçando uma linha do tempo desde as primeiras leis de segurança de dados internacionais na década de 70 até a consolidada LGDP de 2020. O estudo conta a trajetória jurídica brasileira de proteção à individualidade, privacidade e segurança da informação, a partir da constituição de 1988 até a criação da atual Autoridade Nacional de Proteção de Dados (ANPD) em 2019 (MEDEIROS, 2025).

Já Quintiliano (2021) o autor aborda a evolução da LGPD e da segurança de dados de uma maneira jurídica-histórica, onde é apresentado a evolução do tema, através de momentos históricos inclusive internacionais como o marco da Declaração Universal de Direitos Humanos, de 1948 e o pacto São José da Costa Rica, ressaltando a Lei Proteção dos Direitos do Homem e das Liberdades Fundamentais, de 1950 na europa, até a atual Lei Geral de proteção de Dados do Brasil. Destacando principalmente a importância do direito à privacidade, escolha e dignidade humana (QUINTILIANO, 2021).

Por fim Oliveira (2021) busca examinar e apresentar de forma detalhada cada um dos princípios da LGPD que estrutura a legislação brasileira, como a finalidade, a adequação, a necessidade, a transparência e a segurança, entre outros. A obra, de natureza didático-jurídica, realiza uma interpretação do texto legal (BRASIL, 2018) para orientar profissionais e organizações na correta aplicação da lei, demonstrando como cada princípio deve ser observado nas atividades de tratamento de dados pessoais (OLIVEIRA *et al.*, 2021).

Enquanto os estudos anteriores concentram-se na evolução histórica e jurídica da LGPD, o presente trabalho desloca essa discussão para o contexto da formação acadêmica, pois debate de forma mais atual a importância da LGPD e investiga como seus princípios são

apresentados e ensinados aos alunos de ES e CC da UFC no Campus de Russas debatendo assim a importância da LGPD no contexto educacional.

3.2 Estudo sobre o ensino de segurança e o conhecimento dos profissionais

No seu trabalho Cristani et al. (2020), analisa o ensino de Segurança da Informação (SI) nos cursos de Bacharelado em Sistemas de Iformação em cada região do Brasil, utilizando-se de uma revisão de grades curriculares das universidades e um questionário avaliativo dos conhecimentos dos alunos a respeito do assunto. Assim, correlaciona a quantidade de horas e disciplina acerca de SI com o conhecimento dos alunos, não obtendo um resultado conclusivo.

Ademais, Queiroz e Cavalcanti (2024) avalia através de uma pesquisa quali-quantitativa e exploratória, o nível de formação e preparação que os estudantes de desenvolvimento de software recebem sobre SI. Questionando se há algum impacto direto na empregabilidade dos alunos. Focando em formados e atuantes na área de tecnologia, obtendo que esses profissionais tiveram um preparo insuficiente, com ênfase na ausência de prática, com recursos desatualizados, impactando na empregabilidade destes.

Voltando para o meio empresarial Duarte et al. (2025) investiga, por meio de um estudo de caso e uma análise quali-quantitativa, o nível de compreensão de profissionais de TI sobre a LGPD e quais as principais dificuldades na adequação em empresas. Demonstrando como a lei impacta nos meios públicos e privados, concluindo a partir de seus resultados que há um baixo ou médio conhecimento por parte dos profissionais acerca do tema, demonstrando uma lacuna no aprendizado sobre esses assuntos.

Ainda em questões empresariais Marques et al. (2024) procura por meio de técnicas de Mineração de Dados, num estudo descritivo, identificar o perfil profissional dos egressos dos cursos superiores da Universidade Federal do Ceará (UFC) Campus de Quixadá. Focando nas dificuldades para integrar no mercado de trabalho e na atuação deste. Concluindo-se que os ingressantes de SI possuem uma facilidade maior a ingressar no mercado de trabalho e crescer profissionalmente mais rápido, apresentando em boa parte, um salário maior. Buscando inserir conteúdos de SI em outras graduações nos cursos de TI.

Diferentemente dos trabalhos anteriores, ao passo que Duarte et al. (2025) e Marques et al. (2024) focam no meio corporativo e seu público são os profissionais que já atuam no mercado de trabalho, este trabalho foca em como esse conhecimento sobre a LGPD está sendo transmitido em sala de aula e o quanto os discentes conhecem e sentem que estão preparados

para aplicar e interpretar esses conceitos. Se divergindo também de Cristani et al. (2020) e Queiroz e Cavalcanti (2024) por além de não avaliar apenas o conhecimento dos alunos, analisa também o preparo e a percepção dos docentes a respeito desses temas e como é transmitido em suas aulas.

3.3 Comparação dos Trabalhos Relacionados com Este Trabalho

Após analisar os trabalhos relacionados, foi possível identificar algumas lacunas em comparação com este trabalho, sendo estas, pouca investigação da LGPD no decorrer do ensino, nenhum avalia simultaneamente docentes e discentes, poucos discutem sobre *Privacy by Design* e inexistem estudos na UFC Russas e portanto em comparação com este trabalho foi elaborado o Quadro 1 que apresenta o que este trabalho propõe-se a realizar e o Quadro 2, que apresenta o que foi investigado e as limitações dos trabalhos relacionados, em comparação com este trabalho.

Quadro 1 – Comparação dos trabalhos relacionados com Este trabalho

	Análise dos conhecimento dos Discentes sobre (Segurança de dados, LGPD e PbD)	Análise dos conhecimento de profissionais de TI (Docentes)	Analisar os métodos pedagógicos, e fazer recomendações	Avalia a opinião dos Docentes
(CRISTANI *et al.*, 2020)	X			
(QUEIROZ; CAVALCANTI, 2024)	X		X	
(DUARTE *et al.*, 2025)		X		
(MARQUES *et al.*, 2024)		X		
Este Trabalho	X	X	X	X

Fonte: Elaborado pelo autor (2026)

Quadro 2 – Informações sobre as investigações e limitações dos trabalhos relacionados

TRABALHOS	**INVESTIGOU**	**LIMITAÇÔES**
(CRISTANI *et al.*, 2020)	Ensino de SI na formação acadêmica	Não avaliou os docentes
(QUEIROZ; CAVALCANTI, 2024)	Ensino de segurança de dados na formação acadêmica (foco em boas práticas e ferramentas)	Não avaliou sobre a LGPD
(DUARTE *et al.*, 2025)	Profissionais de TI	Não avaliou a formação acadêmica
(MARQUES *et al.*, 2024)	Profissionais de TI	Não avaliou sobre a LGPD
Este Trabalho	Discentes e Docentes sobre (Segurança de dados, LGPD e PbD)	Somente na UFC Campus Russas

Fonte: Elaborado pelo autor (2026)

4 METODOLOGIA

Este capítulo descreve como a pesquisa foi conduzida. Isto é, desde a caracterização metodológica do estudo, passando pela definição da amostra; coleta, extração e análise dos dados.

4.1 Caracterização da Pesquisa

A presente pesquisa caracteriza-se como um estudo de natureza mista, combinando abordagens quantitativa e qualitativa, com finalidade exploratória e descritiva. Isto é, o caráter exploratório justifica-se pela necessidade de compreender como os conhecimentos relacionados à LGPD e aos princípios de *Privacy by Design* vêm sendo discutidos no contexto acadêmico, enquanto a dimensão descritiva permite mapear o nível de conhecimento de discentes e docentes dos cursos de Engenharia de Software (ES) e Ciência da Computação (CC) da Universidade Federal do Ceará, Campus Russas. A adoção de métodos mistos possibilita uma análise mais abrangente do fenômeno investigado, integrando dados objetivos sobre o conhecimento técnico dos participantes com percepções qualitativas relacionadas às práticas pedagógicas adotadas.

4.2 Contexto da Pesquisa

Sendo uma pesquisa direcionada ao Campus Russas, um polo de tecnologia que foi criado em 2011 no interior do Ceará, e teve suas atividades iniciadas em 2014. Voltado para os cursos de TI que segundo descreve a UFC Russas, tem como objetivo formar profissionais aptos a participarem ativamente do mercado local e global, oferecendo a base teórica suficiente para que os seus egressos possam se manter constantemente atualizados. Além disso, é objetivo deste curso preparar profissionais para desenvolver, usando as técnicas da Engenharia de Software e Ciência da Computação, sistemas de software corretos e eficientes. O que por fim é indicado que o público alvo dessa pesquisa, são os alunos dos dois cursos citados, e os docentes que ensinam para estes alunos. Em 2024 em seu site oficial a UFC Russas informou os seguintes dados “Atualmente conta com 5 cursos, que são Ciencia da Computação Engenharia de Software, Engenharia de produção, Engenharia Civil, e Engenharia Mecânica, e possui 50 Docentes, entre efetivos e substitutos, 54 Técnicos Administrativos em Educação (TAEs), 33 colaboradores terceirizados, e 1313 alunos.

4.3 Seleção dos Participantes

A seleção dos participantes foi realizada de forma intencional e por conveniência, considerando indivíduos diretamente relacionados ao objetivo de estudo. No grupo dos discentes, estão incluídos alunos regularmente matriculados nos cursos de ES e CC da UFC Campus Russas, independentemente do período, desde que já tenham cursado ou estejam cursando disciplinas relacionadas ao desenvolvimento de software. Já o grupo dos docentes, contou com a participação de professores que atuam em disciplinas do curso voltadas diretamente ao desenvolvimento de um software, com potencial relação com os temas de SI, LGPD e PbD.

Prosseguindo, o estudo contou com 74 respostas dos discentes, os quais foram agrupados em dois subgrupos, sendo estes, (i) Grupo A: alunos que não realizaram a disciplina de segurança de dados, como opcional nos 2 semestres que foi ministrada, e (ii) Grupo B: alunos que realizaram a disciplina. Onde o grupo A contou com 68 respostas e o grupo B com 6 respostas. A baixa quantidades de participantes do Grupo B decorre de 2 fatores, um deles e do fato da disciplina ter sido ofertada apenas em duas ocasiões, e o segundo fator é que a maioria dos alunos que participaram da disciplina, eram alunos que já se encontravam no estágio final do curso, logo, ao finalizar a disciplina, eles se formaram e saíram da UFC.

Além disso, a pesquisa também contou com 4 professores, que juntos eram responsáveis por 13 disciplinas voltadas ao processo de desenvolvimento de software.

Essa estratégia de seleção permitiu contemplar diferentes níveis de experiência acadêmica e distintas perspectivas sobre o ensino e a aprendizagem dos conteúdos investigados, contribuindo para uma análise mais rica e contextualizada dos resultados.

4.4 Instrumento de coleta

4.4.1 Questionário

A extração dos dados quantitativos foi realizada a partir das respostas obtidas por meio de um questionário criado utilizando a ferramenta Google Formulário, com um total de 6 perguntas voltadas ao perfil dos usuários, e 16 perguntas direcionadas aos conteúdos debatidos. As questões foram elaboradas de forma objetiva, abordando conceitos fundamentais da LGPD, princípios de segurança da informação e noções de PbD, cada tema recebeu um determinado número de questões, que foram 9 sobre segurança de dados, 4 sobre LGPD e 3 voltado ao método

de PbD, assim possibilitando a mensuração do nível de conhecimento dos respondentes. As perguntas foram criadas utilizando o material disponível por cursos de segurança, oferecidos por empresas bancárias, para capacitar melhor seus funcionários a respeito da segurança de dados e a LGPD.

4.4.2 Entrevista

No que se refere à etapa qualitativa, os dados foram extraídos a partir das entrevistas semiestruturadas que por sua vez oferecem um equilíbrio entre o rigor metodológico e a naturalidade do diálogo, tendo como principal vantagem a sua riqueza de dados e o aprofundamento nas respostas dadas pelos entrevistados. As entrevistas foram realizadas utilizando como base um mesmo roteiro, direcionando os temas debatidos com os docentes participantes. O roteiro contou com um total de 9 perguntas abertas, possibilitando o aprofundamento de temas considerados relevantes durante a condução da conversa, e as entrevistas possuíram um tempo médio de duração de 15 minutos. As respostas dos docentes foram registradas através de gravação de áudio e transcritas manualmente para serem utilizadas na análise, garantindo fidelidade às percepções expressas pelos entrevistados.

Abaixo seguem as perguntas presentes no roteiro da entrevista e alternativas para as respostas dadas pelos entrevistados.

1-Quais matérias você está lecionando neste semestre?

2-Nessas respectivas matérias você inclui questões relacionadas a segurança de software?

Sim : E quais os conteúdos são abordados? É teórico ou prático ou ambos ?

Não : Existe algum motivo para não abordar ? Você considera importante incluir ?

3-E ensinado algum conteúdo relacionado a LGPD (Lei Geral de Proteção de Dados)?

Sim: Como esse conteúdo é trabalhado? Fala sobre os Princípios ?

Não: Considera o conteúdo importante para a graduação ? deveria ter uma matéria dedicada a esse tipo de conteúdo ?

4-E ensinado algum conteúdo relacionado a PbD (*Privacy by Design*)?

Sim: Esse conceito é aplicado ou ensinado ? Em atividades ou práticas?

Não: E de seu conhecimento essas práticas?

5-“Se ensina alguma dessas matérias” Quais as dificuldades encontradas ao passar esse tipo de conteúdo aos alunos? Os alunos tiram dúvidas sobre os temas ?

6-Você acredita que o curso de ES ou CC prepara adequadamente os alunos a respeito da segurança da informação e LGPD ?

7-Sabia que foi ofertada a cadeira de segurança de software como optativa aqui na UFC ?

8-Você tem conhecimento acerca desses conteúdos?

9-Considera esses conteúdos importantes para você e para os alunos ?

4.5 Procedimentos de coleta

Em relação aos dados quantitativos, o formulário ficou disponível para respostas a partir de 28 de abril até o dia 15 de junho, quando foi encerrado totalizando 50 dias. Sendo divulgado através da secretaria dos cursos por email para os alunos de ES e CC, além de contar com a ajuda de alguns professores que disponibilizaram em suas disciplinas pelo SIGAA.

Já as entrevistas, foram enviados e-mails para os professores solicitando as entrevistas e solicitando que o docente informasse a sua preferência entre entrevista presencial ou remota, e qual dia e horário eles possuíam disponibilidade. Esses e-mails começaram a ser enviados a partir do dia 6 de maio até o dia 12 de maio, logo após esse período foram obtidas as respostas dos professores com os horários escolhidos, e nas 3 semanas seguintes ocorreram as entrevistas.

A integração entre os resultados quantitativos e qualitativos possibilitou uma interpretação consistente dos achados, permitindo relacionar o nível de conhecimento identificado com as práticas pedagógicas descritas e subsidiar a formulação de reflexões e recomendações alinhadas aos objetivos do estudo.

4.6 Procedimentos de análise

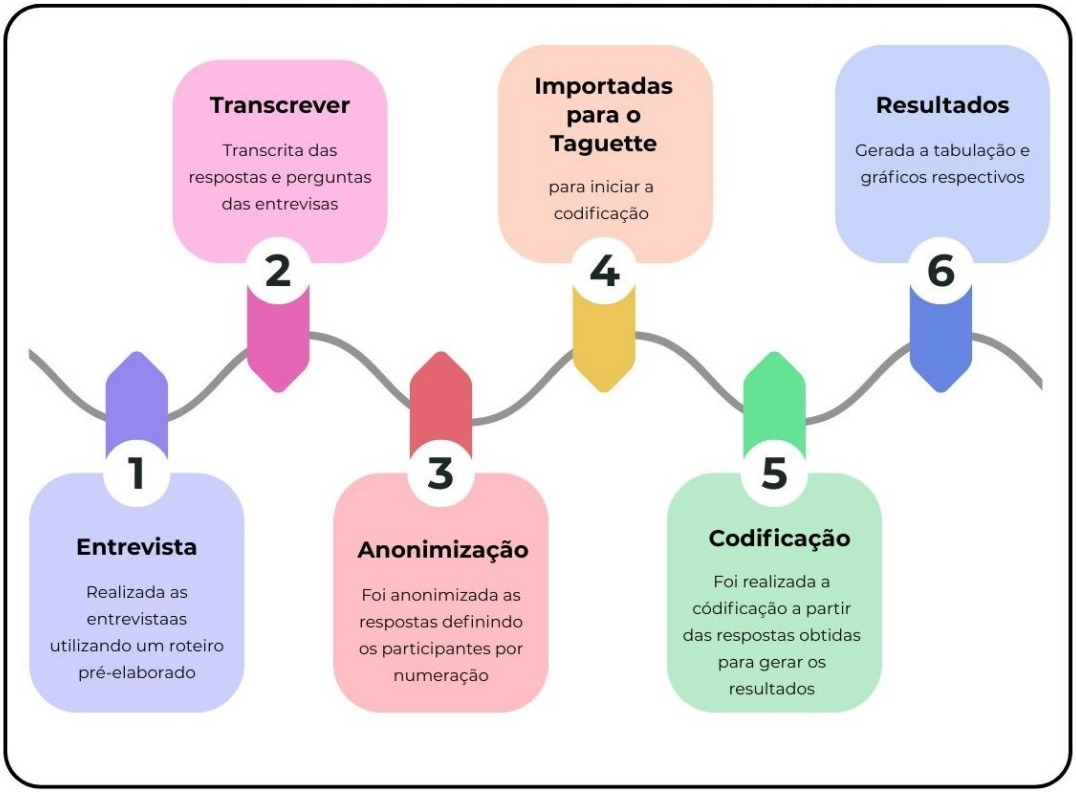
4.6.1 Análise qualitativa

A análise qualitativa se utilizou do método de codificação aberta, como será melhor detalhada nos resultados e sua extração de dados, como mostra a Figura 1.

(i) Foi realizada e gravadas as entrevistas seguindo um roteiro de perguntas para que este possa ser a base para a codificação.(ii) Logo após foram transcritas as gravações conforme o que foi dito. (iii) Com a transcrição, pode-se iniciar o processo de anonimização das respostas, convertendo-as e importando-as. (iv) Após importar para a ferramenta auxiliar Taguette, que pode começar a codificação. (v) A codificação foi gerada a partir dos padrões de respostas a cada

questão. (vi) Para só assim serem obtidos os resultados para gerar a tabulação e os gráficos.

Figura 1 – Sequência de passos para realizar a análise qualitativa



Fonte: Elaborada pelo Autor (2026)

4.6.2 Análise quantitativa

Os dados quantitativos foram analisados por meio de estatística descritiva, utilizando medidas simples, como frequências, moda e médias, com o objetivo de sintetizar as respostas e identificar padrões relacionados ao nível de conhecimento dos participantes. Essa análise permite identificar possíveis lacunas na formação acadêmica no que diz respeito à LGPD e ao *Privacy by Design*.

Assim, na análise quantitativa, os dados foram extraídos do formulário criando uma planilha com as respostas que os discentes preencheram. Logo após, para conseguir analisar e realizar os gráficos, foram atribuídos valores para as questões, onde a resposta correta era transformada no valor 1, e a resposta incorreta era transformada no valor 0. Após a codificação das respostas, foi realizada a soma de acertos de cada estudante. Ademais, com todos os valores já definidos, as respostas foram divididas entre o grupo A e o grupo B.

Após obter essa divisão, a planilha foi exportada para a ferramenta auxiliar, JASP,

que calculou a média, e com estes dados, foi realizada uma comparação visual com as notas e dados descritivos dos dois grupos com o intuito de discutir a diferença entre eles. Assim, com a análise, foram gerados gráficos que melhor retratam o que foi observado, com o auxílio da ferramenta Flourish. Ademais, na etapa seguinte, foi avaliada a importância desses assuntos na perspectiva dos alunos e dos professores.

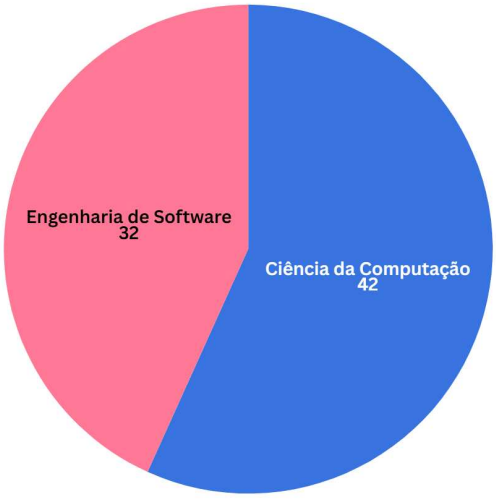
5 RESULTADOS

5.1 Análise Quantitativa

A análise quantitativa inicia-se com a caracterização da amostra (Figuras de 2 a 5) e em seguida, apresenta a avaliação do nível de conhecimento dos alunos (Figuras de 6 a 8) considerando o desempenho geral, por semestre e entre aqueles que cursaram ou não a disciplina de segurança de dados.

5.1.1 Caracterização

Figura 2 – Divisão dos alunos por os cursos

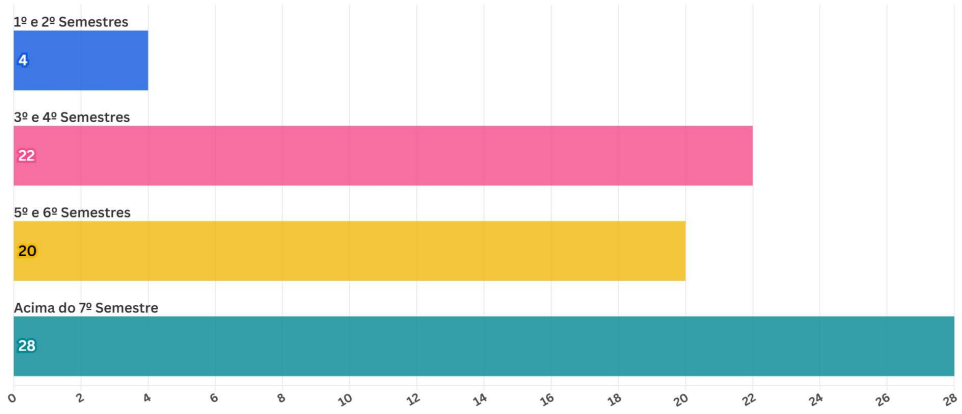


Fonte: Elaborada pelo Autor (2026)

No gráfico da Figura 2, pode-se observar a divisão dos 74 respondentes na pesquisa, entre os cursos de ES e CC com predominância em Ciência da computação, porém com valores muito próximos, assim podendo manter um equilíbrio entre os cursos.

Na Figura 3, tem-se a distribuição dos alunos por semestres, onde 64% dos que responderam à pesquisa encontra-se acima do quinto semestre, isso pode acontecer já que os alunos dos semestres iniciais, não sentem que possuem conhecimentos para ajudar na pesquisa, assim optando por não responder o questionário.

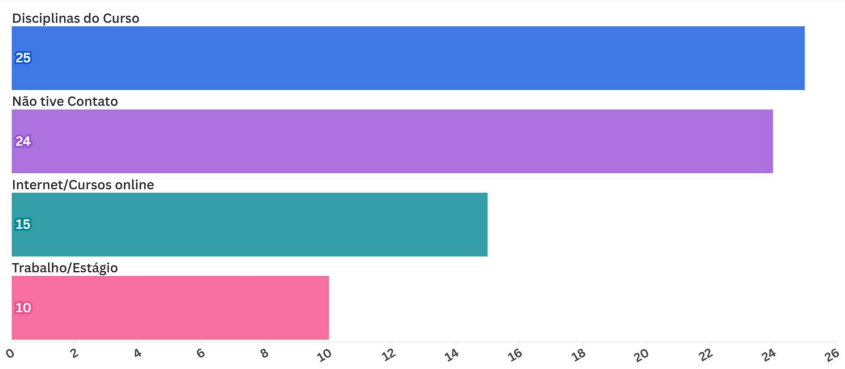
Figura 3 – Divisão dos alunos por semestre



Fonte: Elaborada pelo Autor (2026)

Na Figura 4, foi questionado aos alunos como tiveram contato com os conteúdos discutidos, observa-se que as disciplinas dos cursos de CC e ES foram responsáveis por esse conhecimento para 25 discentes. Outros 15 obtiveram o aprendizado por meio de cursos online, e 10, por meio de trabalho ou estágio. Em contrapartida, uma parcela, composta por 24 alunos, informaram que não tiveram contato com os temas abordados, isso é preocupante, pois, levando em conta a Figura 5, onde a maioria dos alunos que responderam o questionário são de semestres avançados no cursos, um número alto de alunos que não tiveram contato com os temas, pode representar, que os formandos, podem acabar entrando no mercado de trabalho sem terem contato com a área de segurança de dados, o que se assemelha no trabalho de Queiroz e Cavalcanti (2024), onde 66.1% dos participantes, afirmam que suas formações acadêmicas, não contribuiu para o mercado de trabalho na área de segurança da informação.

Figura 4 – Relatos dos locais onde os alunos tiveram contato com os conteúdos



Fonte: Elaborada pelo Autor (2026)

Na Figura 5, apresenta-se a autoavaliação dos respondentes sobre seu nível de conhecimento em cada conteúdo. Os níveis foram definidos como:

Nível 1 - Não possuo nenhum conhecimento sobre o conteúdo

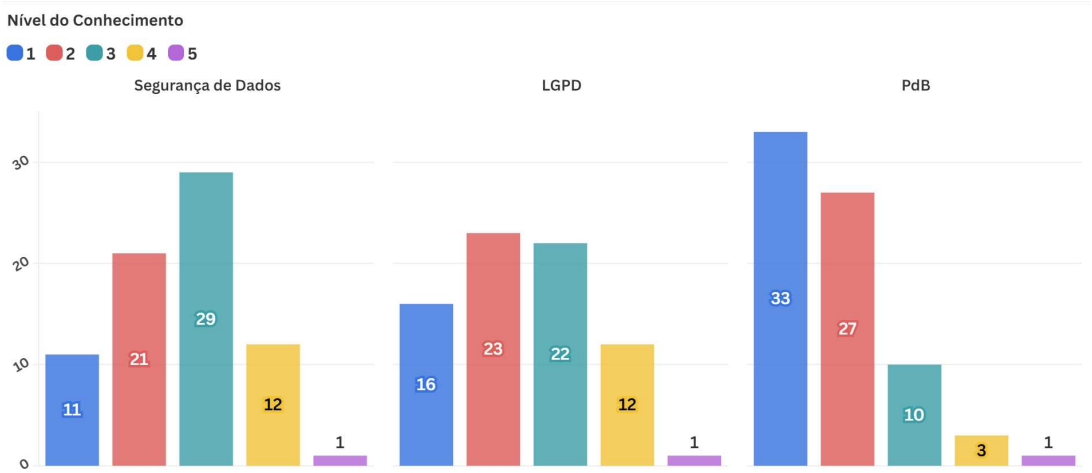
Nível 2 - Não possuo conhecimento porém sei da existência desse conteúdo

Nível 3 - Eu Possuo um conhecimento mediano sobre o conteúdo

Nível 4 - Eu Possuo um ótimo conhecimento sobre o conteúdo

Nível 5 - Eu domino o conhecimento sobre o conteúdo

Figura 5 – Auto avaliação dos alunos sobre o conhecimento dos conteúdos



Fonte: Elaborada pelo Autor (2026)

Nota-se na Figura 5, que a maioria dos alunos afirma possuir um conhecimento de nível 3 ou inferior, nos três temas: 61 de 74 alunos em segurança de dados, 61 de 74 alunos sobre LGPD e dado mais expressivo é que 70 de 74 alunos situam-se nesses níveis quando o assunto é PbD, isso pode ocorrer por alguns fatores, entre eles, a falta de disciplinas que apresentam conteúdos relacionados aos de segurança, professores que não apresentam esses conteúdos devido a ementa, e a falta de interesse dos alunos em aprender esses conteúdos fora das disciplinas.

É possível reparar também que apenas um aluno de todos os respondentes, sente que realmente domina os conteúdos apresentados.

5.1.2 Avaliação do questionário

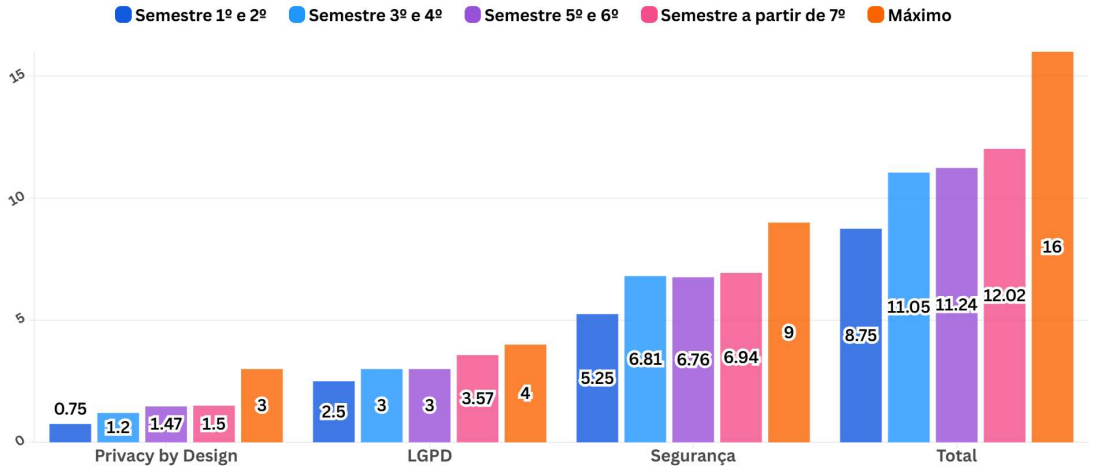
Iniciando a análise das questões avaliativas, a Figura 6 compara a média geral dos participantes com a pontuação máxima possível. Assim, as médias situam-se entre 70% e 77% da nota máxima, com exceção da nota de PbD, que foi de 46% da pontuação máxima.

Figura 6 – Média geral dos alunos em relação com a nota máxima

Fonte: Elaborada pelo Autor (2026)

Ademais detalhando o conhecimento por semestre, na Figura 7, os participantes foram analisados de acordo com o semestre que estão, através de uma análise visual do gráfico observa-se um aumento na média de acertos conforme o avanço do semestre, sendo a diferença entre o semestre inicial e o último bastante expressiva.

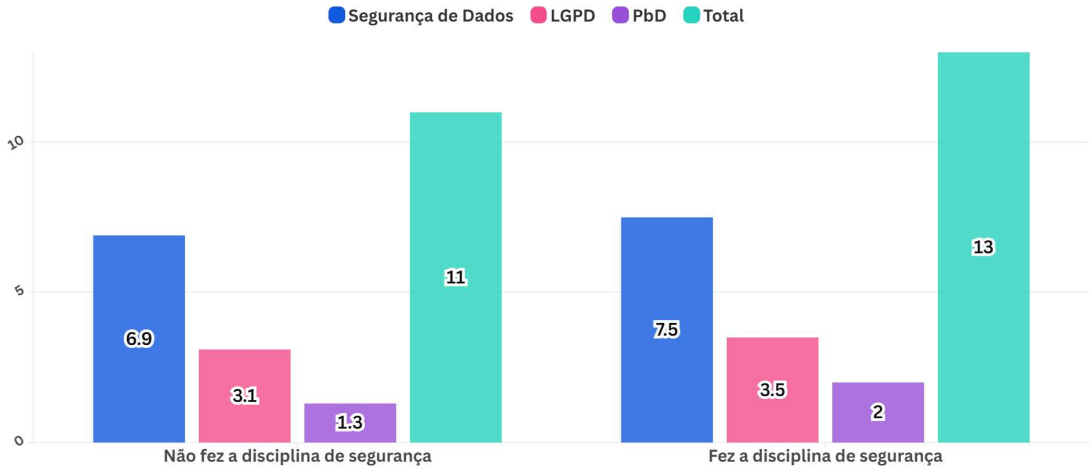
Figura 7 – Comparativo das médias entre os semestres dos alunos



Fonte: Elaborada pela Autor (2026)

Porém, além deste, na Figura 8 revela uma diferença ainda mais acentuada ao comparar os alunos que cursaram a disciplina de segurança de dados com aqueles que não a cursaram. Em todos os temas analisados, o grupo B que realizou a disciplina obteve pontuação superior aos alunos do grupo A que não fizeram a disciplina, o total de alunos é de cada grupo é : Grupo A (68 alunos) e Grupo B (6 alunos).

Figura 8 – Comparativo entre Grupo A e Grupo B



Fonte: Elaborada pelo Autor (2026)

A seguir, a análise qualitativa trará a perspectiva docente, complementando os achados quantitativos e evidenciando o que é ensinado, bem como as principais lacunas e desafios.

5.2 Análise Qualitativa

A partir da análise qualitativa utilizando o método de codificação aberta de Grounded Theory (GLASER B. G., 1967), o presente trabalho apresenta informações sobre a didática e a percepção que os docentes têm sobre os temas debatidos, em relação aos alunos dos cursos de ES e CC no Campus Russas.

Abaixo são apresentados os resultados das questões que foram feitas durante a entrevista dos professores. As tabelas a seguir estão organizadas da seguinte forma:

(I) Código - Afirmativa criada, que pode responder a questão de forma positiva ou negativa.

(II) Quantidade - Número de professores que deram uma resposta que se assemelha ao Código.

(III) Exemplo - Uma ou mais frases ditas pelos entrevistados respondendo a questão.

A primeira questão buscou identificar as disciplinas que os entrevistados estavam lecionando. Foram mencionadas as seguintes: Desenvolvimento de Software para Web, Engenharia de Software (CC), Experimentação em Engenharia de Software, Empreendedorismo, Estru-

tura de Dados Avançados, IPRS – Introdução a Processos e Requisitos de Software, Interação Humano-Computador, Manutenção de Software, Projeto Detalhado de Software, Processos de Software, Processos de Análise de Algoritmo, Requisitos de Software e Verificação e Validação.

Observa-se nas questões presentes nas Tabelas 1 e 2, que a maioria dos professores entrevistados não ensina ou apresenta nenhum dos conteúdos citados (Segurança de software e PbD) e isso se deve à falta desses tópicos nas ementas das disciplinas analisadas, como afirma um dos entrevistados, *"Não, não tem nada na minha grade"*. Esses dados dialogam diretamente com os dados da Figura 5, que mostram que os alunos não se sentem preparados e atribuem a si mesmos níveis baixos de domínio dos temas.

Tabela 1 – Resposta da questão 2: Nessas respectivas matérias você inclui questões relacionadas a segurança de software?

Código	**Quantidade**	**Exemplo**
Não tem na ementa e não apresento	4	"Não, não tem nada na minha grade" "Não, segurança não tem na minha ementa"
Tem na minha ementa e apresento	0	

Fonte: Elaborada pelo autor (2026).

Tabela 2 – Resposta da questão 4: E ensinado algum conteúdo relacionado a PbD (Privacy by Design)?

Código	**Quantidade**	**Exemplo**
Comento um pouco, pois tem na ementa	1	"É eu cito por alto, mas nada muito apontando para lei não só somente quando eu tô falando ali sobre privacidade"
Não comento pois não tem na ementa	3	"Não, especificamente sobre isso, não falo não" "Voltado para esse termo em específico não tem"

Fonte: Elaborada pelo autor (2026).

Por outro lado, nas respostas reunidas na Tabela 3, observa-se que a maioria dos professores ensina ou apresenta conteúdos sobre LGPD, ainda que, segundo eles, o tema não integre formalmente a ementa. Um dos entrevistados diz, *"lgpd eu falo um pouco, mas eu não me aprofundo, porque não é da minha ementa"*. Percebe-se, portanto, que a importância atribuída à legislação é tamanha que alguns docentes optam por inseri-la em sala de aula, mesmo sem a obrigação, com o intuito de ao menos apresentar sua existência aos alunos. Esse esforço adicional parece refletir-se diretamente no desempenho dos discentes: a Figura 6 mostra que a maior média geral foi obtida justamente nos conteúdos de LGPD, o que sugere que, mesmo quando abordada de forma introdutória e por iniciativa que parte dos docentes, a presença do

tema em sala de aula contribui para um nível de conhecimento mais elevado em comparação aos demais assuntos investigados. Contudo, essa dedicação encontra obstáculos na transferência do conhecimento, conforme indicado nas Tabelas 4 e 5, por sua natureza teórica e legislativa, a LGPD tende a gerar desinteresse entre os discentes, como expressa outro entrevistado: *"Quando tende a ser mais teórico eles tendem a não gostar"*. Emerge, assim, uma contradição: o tema é considerado relevante a ponto de ser ensinado mesmo sem exigência formal, mas o formato predominantemente expositivo reduz o engajamento dos alunos.

Tabela 3 – Resposta da questão 3: E ensinado algum conteúdo relacionado a LGPD (Lei Geral de Proteção de Dados)?

Código	**Quantidade**	**Exemplo**
Apresento um pouco, mais não tem na ementa	2	"Quando eu mostro o termo de consentimento que às vezes a gente utiliza nas pesquisas, aí eu apresento a parte da LGPD" "LGPD eu falo um pouco, mas eu não me aprofundo, porque não é da minha ementa"
Apresento um pouco, pois tem na ementa	1	"É mencionado em algum momento da disciplina, mas ali no começo da disciplina e falado sobre a Lei Geral de Proteção de Dados né a LGPD por questões relacionadas ao empreendedorismo"
Não apresento	1	"Não, também não"

Fonte: Elaborada pelo autor (2026).

Tabela 4 – Resposta da questão 5: Possuem alguma dificuldade ao transmitir esse conteúdo?

Código	**Quantidade**	**Exemplo**
Sim, possuo dificuldades	4	"Quando tende a ser mais teórico eles tendem a não gostar." "Nas minhas disciplinas eu não consigo encaixar tanto porque não faz parte ne da ementa"
Não possuo dificuldades	0	

Fonte: Elaborada pelo autor (2026).

Tabela 5 – Resposta da questão 5: Eles tiram dúvidas sobre esses conteúdos ?

Código	**Quantidade**	**Exemplo**
Sim, tiram dúvidas	0	
Não tiram dúvidas	4	"Não tiram, infelizmente não tiram muitas dúvidas não" "Eles às vezes só não se interessam por ser mais teórico"

Fonte: Elaborada pelo autor (2026).

Outro ponto que merece atenção diz respeito ao nível de conhecimento dos próprios docentes entrevistados. De acordo com a Tabela 6, apenas um deles demonstrou conhecimento aprofundado sobre os temas, como evidencia sua resposta: *"Conheço, conheço, trabalho num projeto do governo"* Os demais afirmaram possuir apenas conhecimento básico e reconheceram

a necessidade de estudo adicional para aprofundar-se. Uma das falas ilustra essa realidade: “Eu tenho que estudar um pouco mais, pra ser sincera eu não tenho esse conhecimento todo, tanto da lei (LGPD) quanto de alguns tipos de técnicas, talvez relacionadas à segurança ou voltadas ao desenvolvimento mesmo”

Esse cenário reforça a importância de se contar com um docente especializado na área. Nota-se que a disciplina de segurança de dados, mesmo ofertada por apenas dois semestres, já acrescentou de forma significativa ao conhecimento dos alunos como mostra a Figura 8. Contudo, sem o preparo adequado dos professores, a transferência desse conhecimento permanece limitada.

Tabela 6 – Resposta da questão 8: Você tem conhecimento acerca desses conteúdos?

Código	**Quantidade**	**Exemplo**
Detenho esse Conhecimento	1	“Conheço, conheço, trabalho num projeto do governo”
Detenho o básico desse conhecimento	3	“Eu tenho que estudar um pouco mais, pra ser sincera eu não tenho esse conhecimento todo sobre, tanto a lei (LGPD) quando quanto sobre alguns tipos de técnicas talvez relacionadas a segurança ou voltadas ao desenvolvimento mesmo”

Fonte: Elaborada pelo autor (2026).

Retomando-se ao questionamento sobre a preparação que a UFC Russas dá a seus alunos dos cursos de ES e CC sobre os temas do presente trabalho, foi questionado aos professores se possuíam o conhecimento de ter sido ofertado uma disciplina chamada Segurança de Dados, como optativa nos semestres de 2025.1 e 2025.2, os resultados apresentados na Tabela 7 mostra que em sua maioria, os professores responderam negativamente, não possuindo o conhecimento sobre a existência dessa disciplina, como pode ser indicado pela afirmação a seguir, *“Não sabia que a UFC ofertou cadeira de segurança de dados”*. E quando perguntado sobre a opinião deles a respeito da preparação que a UFC Russas oferece aos alunos como mostra a Tabela 8, uma parte respondeu de forma negativa, *“Respondendo de forma mais sucinta, ao meu ver as grades dos cursos de ES e CC não preparam os alunos para trabalhar com a questão da LGPD”* E a outra parte afirma que os alunos têm sim a oportunidade de aprender porém, fora do quesito institucional estudando por conta própria ou em outras matérias que não se sabem ao certo sobre, e adquirir esses conhecimentos, como é possível notar na afirmação a seguir, *“Eles têm oportunidade sim, eles veem a importância, eles não vão ver realmente a norma aberta, um item da ementa, não, mas como eles tem que saber, tem que adotar nos projetos de software deles, então eles tem como ir atrás e desenvolver essa expertise”*.

Tabela 7 – Resposta da questão 7: Sabia que foi ofertada a cadeira de segurança de software como optativa aqui na UFC ?

Código	Quantidade	Exemplo
Não sabia	3	"Não sabia que a ufc ofertou cadeira de segurança de dados"
Sim, sabia	1	"Verdade eu não lembrava, foi até com o professor . . . "

Fonte: Elaborada pelo autor (2026).

Tabela 8 – Resposta da questão 6: Você acredita que o curso de ES ou CC prepara adequadamente os alunos a respeito da segurança da informação e LGPD ?

Código	Quantidade	Exemplo
Acredito que não	2	"Nunca vi na UFC nada sobre segurança nas disciplinas." "Respondendo de forma mais sucinta, ao meu ver as grades dos cursos de ES e CC não prepara os alunos para trabalhar com a questão da LGPD."
Acredito que sim	2	"Acho que sim" "Eles têm oportunidade sim, eles vem a importância, eles não vão ver realmente a norma aberta, um item da ementa, não, mas como eles tem que saber, tem que adotar nos projetos de software deles, então eles tem como ir atrás e desenvolver essa expertise"

Fonte: Elaborada pelo autor (2026).

Por fim, quando se questiona sobre a importância destes ensinamentos para os discentes como mostra a Tabela 9, todos concordaram que a importância é alta, principalmente na atualidade, diz um dos entrevistados, *"Sim, sem dúvida, ainda mais hoje em dia que as pessoas produzem tanta informações, e a gente tem acesso a tantas informações aí pela internet"*. Logo podemos observar que os professores reconhecem a importancia desses temas debatidos, porem são limitados a ensinar somente o que tem na ementa, o que ocasiona em conteudos importantes que são deixados de fora.

Tabela 9 – Resposta da questão 9: Considera esse conteúdo importante para você e os alunos?

Código	Quantidade	Exemplo
Sim, considero importante	4	"Sim, sem dúvida, ainda mais hoje em dia que as pessoas produzem tanta informações, e a gente tem acesso a tantas informações aí pela internet" "Sim sem dúvidas"
Não considero importante	0	

Fonte: Elaborada pelo autor (2026).

5.3 Discussão

Os resultados apresentados nas seções 5.1 e 5.2 evidenciam um cenário de conhecimento parcial e, por vezes, superficial sobre a LGPD e o *Privacy by Design* entre os discentes, além de revelarem desafios estruturais na abordagem desses conteúdos pelos docentes. Nesta seção, busca-se interpretar esses achados de forma integrada.

Um primeiro ponto a ser destacado, é a própria percepção dos discentes sobre os seus conhecimentos. Conforme mostra a Figura 5, a maioria dos alunos se auto avaliou nos nível 3 ou inferiores, apenas um aluno se classificou como nível 5. essa percepção corrobora com desempenho da avaliação (Figura 6), especialmente sobre o tema de PbD que a média dos alunos ficou abaixo de 50% enquanto as outras chegaram nos 70% a 80%, esse cenário também é encontrado no estudo de Duarte et al. (2025), que identificou que a maior parte dos seus entrevistados, 89%, afirma saber muito pouco, ou possuírem conhecimento mediano sobre a LGPD, sugerindo que a insegurança quanto ao conhecimento do tema não é algo particular desta pesquisa, mas sim um traço recorrente dos estudantes e dos profissionais em formação acadêmica.

A ausência de vivência prática emergiu como um fator relevante tanto nas falas dos docentes quanto na análise dos perfis dos alunos. A Figura 4 mostrou que 24 dos estudantes não tiveram contato com os temas, e outros 10 relataram ter vivenciado no estágio ou trabalho. A literatura, como apontam os artigos de Queiroz e Cavalcanti (2024), reforça que a fixação de conceitos como a LGPD e o *Privacy by Design* é potencializada quando os alunos têm oportunidade de aplicá-los em projetos reais ou simulados. A sensação de despreparo manifestada na autoavaliação, portanto, parece estar não só relacionada à ausência de menção teórica aos assuntos, quanto também, a carência de espaços estruturados de prática, lacuna essa que os docentes reconheceram nas entrevistas ao relatar dificuldades de inserir conteúdos e atividades práticas sobre os temas em suas disciplinas, devido a ementa.

O confronto entre as falas dos docentes e o desempenho dos discentes revela divergências importantes. Os professores entrevistados indicaram que os temas de segurança e privacidade são abordados de modo transversal em disciplinas como Empreendedorismo, Experimentação em Engenharia de Software e IPRS, mas não há no Campus de Russas um docente cuja área de atuação seja especificamente segurança da informação ou proteção de dados. Essa ausência reflete-se no caráter introdutório com que os assuntos são tratados e, em última instância, no conhecimento dos alunos. A diferença de pontuação entre quem cursou a disciplina

de segurança de dados e quem não cursou, evidenciada na Figura 8, reforça que a existência de um componente curricular dedicado impacta positivamente a aprendizagem, porém com a ausência de um docente na área de segurança de dados impossibilita que a cadeira continue sendo ofertada, limitando assim o preparo e o conhecimento que os alunos poderiam adquirir.

6 CONCLUSÃO

O presente trabalho teve como objetivo analisar o nível de conhecimento sobre segurança de dados, LGPD e os princípios de *Privacy by Design* entre discentes e docentes dos cursos de ES e CC da UFC Campus Russas, bem como investigar as práticas pedagógicas adotadas. Os resultados da análise quantitativa revelaram um conhecimento mediano dos alunos, com destaque para o baixo desempenho no tema PbD, enquanto a análise qualitativa evidenciou que os docentes abordam os assuntos de forma superficial, mas enfrentam desafios como a falta de tempo e a ausência desses conteúdos nas ementas, por fim a falta de um especialista na área e a escassez de componentes curriculares específicos, levam a percepção de preparo insuficiente apresentado pelos discentes.

Os achados sugerem que há, nos cursos investigados, uma oportunidade de fortalecimento da formação em proteção de dados e privacidade desde a concepção de software. Não se trata de apontar negligência, mas de reconhecer que a velocidade com que as exigências legais e de mercado avançam sobretudo com a LGPD demanda uma atenção institucional contínua à atualização de matrizes curriculares, à oferta regular de disciplinas específicas e à inserção transversal da prática de PbD e da LGPD em outras disciplinas acadêmicas, juntamente com uma melhor capacitação dos docentes a respeito dos presentes temas, formam caminhos promissores já sinalizados pelos próprios professores entrevistados, como possíveis contribuições para uma melhor formação profissional.

Em síntese a Engenharia de Software nem a ciência da computação podem restringir-se aos aspectos técnicos do desenvolvimento. Em um cenário marcado pelo crescimento das exigências legais e pela intensificação do tratamento de dados pessoais, torna-se essencial que temas como Segurança da Informação, LGPD e *Privacy by Design* sejam incorporados de forma contínua ao processo formativo dos futuros profissionais. Dessa forma, espera-se que os resultados desta pesquisa possam contribuir para reflexões institucionais e servir como subsídio para futuras iniciativas de atualização curricular e fortalecimento da formação em privacidade e proteção de dados.

6.1 Trabalhos futuros

Cabe reconhecer algumas limitações deste estudo. A amostra, embora tenha contemplado 74 discentes, contou com apenas 6 respondentes que cursaram a disciplina de segurança

de dados, o que restringe a força comparativa entre os grupos. O recorte geográfico e institucional limitado ao Campus de Russas impede generalizações para outros contextos. Ademais, a participação de 4 docentes, ainda que as disciplinas lecionadas, que são 13, representam uma grande parte do núcleo de desenvolvimento de software, não esgota a diversidade de perspectivas pedagógicas existentes. Esses fatores devem ser considerados ao interpretar os resultados.

Para trabalhos futuros, recomenda-se a realização de pesquisas que ampliem a amostra, incluindo mais alunos que cursaram a cadeira de segurança de dados e também outros Campus da universidade que por exemplo já possuem na sua grade curricular uma disciplina obrigatória de segurança e privacidade. Estudos que acompanham egressos no mercado de trabalho também poderão aferir como a formação recebida em diferentes Campus da UFC se traduzem em prática profissional, preenchendo as lacunas que este trabalho não pôde responder. Investigar também o impacto da disciplina de segurança, em lugares que ela é considerada obrigatória, e em lugares que possuem aplicação prática do *Privacy by Design*. Por fim buscar exemplos sobre a criação de material didático que auxilie os discentes. E acompanhar a evolução longitudinal dos alunos.

REFERÊNCIAS

ABNT, A. B. N. T. **ABNT NBR ISO/IEC 27002: Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação.** [S.l.]: Rio de Janeiro:ABNT, 2022.

ABNT, A. B. N. T. **ABNT NBR ISO/IEC 27005: Segurança da informação, segurança cibernética e proteção à privacidade - Diretrizes para gestão de riscos de segurança da informação.** [S.l.]: Rio de Janeiro:ABNT, 2023.

AUGUSTO, J. **Caindo na armadilha: pesquisa revela os riscos dos cookies da web**. 2024. Disponível em: <https://nordvpn.com/pt-br/blog/pesquisa-cookies/?srsltid=AfmBOop8k5d5CJ6PpwwpDIaDVDX2r4Q-uyhp3P3XuumVfWmgQbBi6d_w>. Acesso em: 25 Out. 2025.

BELARMINO, G. da S.; RICARRTE, D. R. D.; MOTA, G. H. M. B. A lei geral de proteção de dados do brasil à luz do regimento europeu: Um exame comparativo e prospectivo através de uma revisão sistemática. **WORKSHOP SOBRE AS IMPLICAÇÕES DA COMPUTAÇÃO NA SOCIEDADE (WICS).**, Sociedade Brasileira de Computação, n. 5, 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).** [S.l.]: Diário Oficial da União: seção 1, Brasília, DF, 15 ago., 2018.

CANAAN, R. G. The effects on local innovation arising from replicating the gdpr into the brazilian general data protection law. **INTERNET POLICY REVIEW**, v. 12, n. 1, 2023.

CASOTTI, I. J. Garantindo a segurança da informação na era digital: riscos e soluções. **Revista Delos**, p. 01–18, 2024.

CAVOUKIAN, A. **Privacy by Design: The 7 Foundational Principles**. [S.l.]: Information and Privacy Commissioner of Ontario, Canada, 2011.

CRISTANI, M. de J.; ALVES, W. C.; PEREIRA, G. F. K.; LAZARIN., N. M. Um breve panorama sobre a disciplina de segurança nos cursos de sistemas de informação no brasil. **Workshop de Iniciação Cientifica em Sistemas de Informação - Simpósio Brasileiro de Sistemas de Informação (SBSI)**, Porto Alegre: Sociedade Brasileira de Computação, v. 16, 2020.

DUARTE, N.; EDUARDO, A.; SANTOS, E. A compreensão dos profissionais de ti quanto às implicações da lgpd na segurança da informação. **Revista do Programa de Pós-graduação em Ciências Contábeis e Administração da Unochapecó**, Universidade Comunitaria da Região Chapeco (UNO), v. 18, n. 2, 2025.

FERETZAKIS, G.; VAGENA, E.; KALODANIS, K.; PERISTERA, P.; KALLES, D.; ANASTASIOU, A. Gdpr and large language models: technical and legal obstacles. **FUTURE INTERNET**, v. 17, n. 4, 2024.

GLASER B. G., . S. A. L. **The discovery of grounded theory: Strategies for qualitative research**. [S.l.]: ALDINE PUBLISHING COMPANY, 1967. 271 p.

HOEPMAN, J.-H. **Privacy Design Strategies**. [S.l.]: Nijmegen: Radboud University, 2022. v. 2.

MARQUES, L. T.; MARQUES, B. T.; SILVA, C. A. M. Análise do perfil profissional de egressos de cursos de tecnologia da informação: um estudo de caso na (oculto). **RENOTE**, v. 22, n. 1, 2024.

MEDEIROS, N. G. L. de. A evolução da proteção de dados no brasil: Uma análise histórica e legislativa até o advento da lgpd. **Revista de Ciências Jurídicas e Empresariais**, v. 25, n. 2, p. 86–91, 2025.

OLIVEIRA, A. C. R.; FERREIRA, H. d. C.; PIRES, F. I. **Princípios da Lei Geral de Proteção de Dados (LGPD)**. Salvador, 2021.

PEIXOTO, M. The perspective of brazilian software developers on data privacy. **Journal of Systems and Software**, Science Direct, v. 195, n. 111523, 2023.

QUEIROZ, P. S.; CAVALCANTI, G. J. d. C. **O impacto do suporte metodológico e ferramental orientado à segurança da informação no ensino prático de cursos de desenvolvimento de software.** 2024. Dissertação (Graduação em Engenharia de Software) — Instituto Federal de Pernambuco, Campus Belo Jardim, Belo Jardim., 2024.

QUINTILIANO, L. Contexto histórico e finalidade da lei geral de proteção de dados (lgpd). **JUSBRASIL**, 2021.

SANTOS, G. C. **Recomendações de boas práticas para implementação da LGPD em processos de desenvolvimento de software.** 2022. p.15. Dissertação (Graduação em Engenharia de Computação) — Escola Politécnica, Pontifícia Universidade Católica de Goiás, Goiânia., 2022.

SARAIVA CLEIDSON DE SOUZA, S. S. J. Desafios de compliance da lgpd: Implantação na indústria de software brasileira. In: SOCIEDADE BRASILEIRA DE COMPUTAçãO. **WORKSHOP SOBRE ASPECTOS SOCIAIS, HUMANOS E ECONÔMICOS DE SOFTWARE (WASHES)**. Porto Alegre, 2024. p. 193–198.