Conformidade da LGPD em Instituições Públicas de Ensino Superior no Brasil: as perspectivas de profissionais de TIC

Keyla Oliveira da Silva[1], **Laura Costa Sarkis**[1]

[1]Universidade Federal do Acre (UFAC)
Rio Branco – AC – Brasil

keyla.oliveira@sou.ufac.br, laura.sarkis@ufac.br

Abstract. *The General Data Protection Law (LGPD) defines what is or is not legal in relation to personal data and has ensured individual rights since August 2018. Since then, several studies have sought to understand the scenario of its adequacy. This research is part of this research, whose objective seeks to investigate the compliance of the implementation of the LGPD in public higher education institutions in Brazil. The research used a survey that presents the view of ICT professionals from 19 public higher education institutions from all regions of Brazil. The majority of participants have more than 10 years of experience and the majority in a Governance or IT management role. Data analysis concluded that more than 88% of participants are aware of the LGPD; An alarming fact is that 79.4% of participants do not perform or do not know if the organization performs privacy requirements elicitation; 67% consider that the LGPD had an impact on software development. It is necessary to address culture change and have the support of senior management to carry out action to adequacy the LGPD.*

Resumo. *A Lei Geral de Proteção de Dados (LGPD), define o que é ou não legal, com relação aos dados pessoais e assegura os direitos individuais desde agosto de 2018. Vários estudos buscam entender o cenário de sua adequação. Neste cenário, insere-se esta pesquisa, cujo objetivo busca investigar a conformidade da implantação da LGPD nas instituições públicas de ensino superior no Brasil. A pesquisa utilizou um survey que apresenta a visão de profissionais de TIC de 19 instituições públicas de ensino superior de todas as regiões do Brasil. A maioria dos participantes possuem mais de 10 de experiência e em sua maioria no cargo de Governança ou gestão de TI. Os resultados mostram que mais de 88% dos participantes tem conhecimento sobre a LGPD; um dado inquietante é que 79,4% dos participantes não realizam ou não sabem se a organização realiza elicitação de requisitos de privacidade; 67% consideram que a LGPD gerou impactos no desenvolvimento de software. É necessário tratar mudança de cultura e ter o apoio da alta gestão para a execução de ação de adequação da LGPD.*

Cadernos do IME - Série Informática
e-ISSN: 2317-2193 (online)
DOI: 10.12957/cadinf.2024.80214

1. Introdução

Com o avanço da Internet, a sociedade obteve grandes conquistas, como a democratização da informação, a comercialização e as interações interpessoais, ocasionando novos desafios, principalmente, relacionados a área jurídica. Para garantir que o espaço virtual seja seguro e que as relações entre consumidores e fornecedores sejam equilibradas e justas, se faz necessário o estabelecimento de direitos e deveres também neste ambiente. Segundo Fontes [Fontes, Edison 2007] a segurança da informação tem como objetivo proteger o recurso da informação, para tal utiliza orientações, normas, políticas, procedimentos e ações necessárias para que o negócio da organização seja realizado, assim como, a missão da mesma seja alcançada.

Na área da engenharia de software, a engenharia de requisitos que integra o primeiro estágio do processo de engenharia de software, compreende um conjunto de atividades relacionadas que levam a produção de um sistema de software. A engenharia de requisitos é uma área que requer grande atenção para evoluir junto à normas regulatórias, tendo em vista, ser um processo que compreende e define quais serviços são necessários para o sistema e identifica suas restrições [Sommerville 2011]. Este processo percebe os requisitos de software, que se classificam em requisitos funcionais e requisitos não funcionais.

Os requisitos não funcionais surgem por meio das necessidades dos usuários ou a partir de fatores externos, como regulamentos de segurança ou legislações de privacidade. Por serem mais complexos e difíceis de elicitar, acabam não recebendo a prioridade necessária ou até mesmo não sendo executados, muitas vezes por completo [Sommerville 2019]. Durante o desenvolvimento do software, as técnicas de segurança precisam ser difundidas, principalmente devido ao seu impacto positivo na mitigação de riscos para as empresas, pois fornecem softwares melhores e mais seguros e contribuem para a urgente necessidade da segurança digital [Ribeiro 2002].

Nesta visão, o desenvolvimento de softwares deve sempre atender a legislação que garante a segurança dos dados. Mundialmente, esta legislação, desde o ano de 2018 tem apresentado leis regulamentadoras para proteção de dados, tais como: a *General Data Protection Regulation* (GDPR) [UNIÃO EUROPEIA 2018] que em 25 de maio de 2018 entrou em vigor na União Europeia, intencionando proteger a privacidade dos dados pessoais dos cidadãos europeus e combater os crimes cibernéticos que estavam em crescimento na Europa, servindo assim como inspiração para vários países, como o Brasil, que em agosto de 2018, sancionou a Lei Geral de Proteção de Dados (LGPD), em vigor desde setembro de 2020 [BRASIL].

Com a sanção da LGPD, todas as organizações públicas e privadas no Brasil que possuem informações pessoais armazenadas em seus sistemas devem buscar se adequar e seguir as diretrizes e princípios estabelecidos pela nova Lei, para buscar manter seus dados em segurança. Porém, eventos recentes de vazamentos de dados noticiados na imprensa nacional [CNN BRASIL 2022], inclusive noticiaram que o Brasil ficou em 12º lugar entre os países que mais contabilizaram episódios de vazamento de dados [NIC.BR 2023], o que enfatiza mais ainda, a necessidade de garantir a proteção dos dados pessoais.

Muitas empresas, buscando se adequar à LGPD, criaram ferramentas que facilitassem essa implementação no dia a dia, como exemplo, a plataforma LGPD Educacional, criada pelo Serviço de Processamento de Dados - (SERPRO), que oferece

treinamento e certificação profissional para os setores público e privado [SERPRO 2023]. Cabe destacar ainda que, até o final de 2020, apenas 15% das empresas se mostraram prontas ou na reta final de preparação para a entrada em vigor das sanções da LGPD e 19% não fizeram nenhuma adequação [INFOMONEY 2022].

A LGPD no art. 46, §1º e 2º, cita que as medidas de segurança, técnicas e administrativas para proteção de dados pessoais deverão ser observadas desde a fase de concepção do produto ou do serviço e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo, seguindo até a sua execução, incorporando os conceitos de Privacy *by Design* e *Privacy by Default* [BRASIL].

Diante deste contexto, este artigo busca investigar a conformidade da implantação da LGPD nas instituições públicas de ensino superior no Brasil sob a perspectiva dos profissionais de TIC. Definiu-se então por elaborar um *survey* na qual o público-alvo foram profissionais de TIC com experiência em desenvolvimento de software, segurança da informação e gestores de TIC. O *survey* foi composto de 21 questões, disponibilizado durante quinze dias, com participação de 19 instituições públicas de ensino superior de todas as regiões do Brasil.

Esta pesquisa está organizada da seguinte forma: a Seção 2, apresenta alguns conceitos fundamentais, na seção 3 descreve-se a metodologia da pesquisa. Na seção 4 relata os resultados das questões de pesquisa e discute os resultados, já a seção 5 apresenta as ameaças a validade e, finalmente na Seção 6 temos a conclusão desta pesquisa.

2. Conceitos fundamentais

Um processo de software é um conjunto de atividades relacionadas que levam a produção de um sistema de software. Enquanto que, os requisitos de um sistema são as descrições dos serviços que o sistema deve fornecer e as restrições do seu funcionamento [Sommerville 2019]. A segurança da informação é alcançada através da implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. No contexto da segurança da informação, um sistema de informação é toda a combinação de meios, procedimentos, regras e pessoas que asseguram o fornecimento de informações para um processo operacional [Hintzbergen et al. 2018]. A privacidade de dados é estabelecida por leis regulatórias que institui normas que são recomendadas para manter os dados em segurança.

2.1. Privacidade de dados

As tecnologias atuais, por um lado, possibilitam e facilitam as interações sociais. Mas, por outro, quando são mal projetadas, invadem a privacidade dos usuários [Thomas et al. 2014]. Pode-se definir privacidade de várias formas, pois não existe uma definição única, alguns autores definem como "o direito de ser deixado em paz” [Samuel, D. Warren and Louis, D. Brandeis 1890], outros como [Solove 2008] observa que privacidade é mais um termo guarda-chuva que se refere a vários conceitos que têm semelhanças e diferenças, já [Petronio 2002] diz que privacidade é "um processo dialético de gerenciamento de limites".

Atualmente, a NBR/ISO 27701 [ISO/IEC 27701] tem o objetivo de estabelecer, instituir, manter e melhorar continuamente o Sistema de Gestão da Privacidade da

Informação. A LGPD, seguindo o modelo da GDPR, trata do controle pessoal dos dados como autodeterminação informativa, ou seja, a capacidade do titular de ter um grau de autodomínio sobre seus dados, sendo este um dos fundamentos da proteção de dados pessoais (art. 2º, II) [BRASIL]. Outro aspecto importante a se considerar é a conscientização de todos os colaboradores da organização quanto ao tratamento de dados pessoais.

2.2. Requisitos de privacidade

Webster *et al.* [Webster et al. 2005] em seu estudo diz que os requisitos de privacidade são aqueles que capturam os objetivos de privacidade e suas medidas associadas para um sistema em desenvolvimento. No entanto, existem muitos desafios na sua identificação. Por essa natureza, os requisitos de privacidade são geralmente categorizados como requisitos não funcionais, pois descrevem o comportamento de um sistema [Behutiye et al. 2017]. Segundo Sommerville [Sommerville 2019] os requisitos não funcionais surgem por meio das necessidades dos usuários ou a partir de fatores externos, como regulamentos de segurança ou legislações de privacidade.

Os requisitos não funcionais por serem mais complexos e difíceis de elicitar, acabam não recebendo a prioridade necessária ou até mesmo não sendo executados, muitas vezes por completo e acabam compartilhando dos mesmos desafios em seu processo de elicitação por não possuírem experiências em compreender as normas [Behutiye et al. 2017], [Ayala-Rivera *and* Pasquale 2018], [Canedo et al. 2020]. Ansari et al. [Ansari et al. 2021] destacam que a identificação e modelagem dos requisitos de privacidade durante as fases preliminares do desenvolvimento de software são essenciais para fornecer proteção de privacidade para as partes interessadas, incluindo os usuários. Mas que continua sendo um desafio para os profissionais de software à medida que os sistemas de informação se tornam mais complexos, dispersos e com exigência leis.

2.3. Leis de Proteção de Dados Pessoais

A segurança da informação através do conjunto de orientações, normas, procedimentos, políticas e ações busca proteger o recurso da informação, possibilitando à organização, alcançar sua missão [Fontes, Edison 2007]. A proteção de dados pessoais, não é uma preocupação atual das empresas. Antes mesmo da criação de leis e regulamentos de privacidade e proteção de dados, como a GDPR e a LGPD, as normas internacionais e nacionais já tratavam de implementação da privacidade dos dados e gestão e riscos de segurança da informação. Essas medidas podem ser encontradas na família das Normas Técnicas ABNT NBR ISO 27000 [ISO/IEC 27002][ISO/IEC 27701], 29100 [ISO/IEC 29100] e a ISO 31000 [ISO/IEC 31000] que trata sobre Gestão de Riscos.

2.3.1. *General Data Protection Regulation* (GDPR)

A GDPR, entrou em vigor na União Europeia em 25 de maio de 2018. Esta Lei é considerada uma atualização de outra lei de privacidade da Europa, *Data Protection Directive*, em vigência desde 1995. Um dos principais fatores que impulsionaram a aprovação da GDPR foi o escândalo da espionagem em massa envolvendo o governo dos Estados Unidos, cuja acusação envolvia o compartilhamento de informações da população americana e de diversos países da Europa e da América Latina - entre eles o Brasil - utilizando servidores de empresas como Google, Apple e Facebook, como noticiado em toda a imprensa nacional e internacional no ano de 2013.

No Artigo 4º da GDPR, os dados pessoais são definidos como “qualquer informação relacionada a uma pessoa física identificada ou identificável (titular dos dados), e por qualquer informação, entende-se a que pode ser usada para identificar um sujeito direta ou indiretamente, podendo os dados serem físicos ou virtuais". A GDPR não garante ao titular dos dados, a propriedade sobre seus dados, apenas o controle sobre o que pode ser feito com eles, garantindo o direito de exigir que empresas deletem seus dados pessoais (desde que não sejam necessários para fins científicos, históricos, de saúde pública e estatísticos); direito de acessar e transferir os dados pessoais de um serviço para o outro sem deixar rastros; e direito à transparência total sobre qualquer operação realizada com os dados [UNIÃO EUROPEIA 2018].

Pode-se ressaltar que a GDPR impõe regras para países que desejarem manter relações comerciais com a União Europeia, nesse sentido, para dar continuidade a negócios é necessário que o país em questão possua uma regulamentação completa e abrangente sobre proteção de dados e uma autoridade reguladora para garantir a eficácia da regulação. Essa ação influenciou vários países a elaborar ou alterar suas regulamentações, como o Brasil.

2.3.2. *Lei Geral de Proteção de Dados Pessoais (LGPD)*

A Lei Federal 13.709/2018, que trata da LGPD foi sancionada em 14 de agosto de 2018 e entrou em vigor no dia 18 de setembro de 2020 [BRASIL]. Porém, as penalidades associadas à lei passaram a ser efetivadas a partir de 1º de agosto de 2021. A Figura 1, retrata os principais acontecimentos que levaram ao surgimento da LGPD.

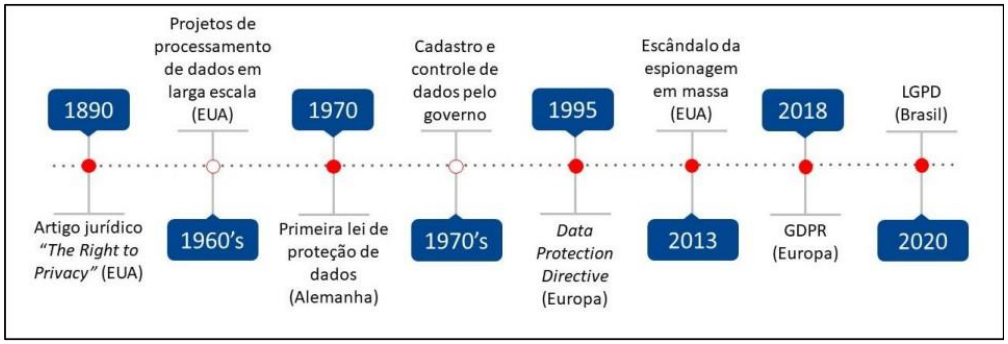


Figura 1. Acontecimentos para surgimento da LGPD

Fonte: [Santos 2020]

A LGPD corresponde a um regulamento geral para proteção de dados pessoais, apesar destes passarem por fluxos da Internet ou não, ou seja, tanto dados físicos ou eletrônicos. Assim, quaisquer organizações que coletem dados pessoais estão submetidas às disposições legais. Segundo o artigo 5º, Inciso I, da LGPD, dado pessoal é "informação relacionada a pessoa natural identificada ou identificável" e no Inciso X, define o tratamento de dados pessoais como: “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” [BRASIL].

De acordo com a LGPD, a Autoridade Nacional de Proteção de Dados (ANPD) compete principalmente zelar pela proteção dos dados pessoais; elaborar diretrizes para a

Política Nacional de Proteção de Dados Pessoais e da Privacidade; fiscalizar e aplicar sanções; apreciar petições de titular contra controlador; promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais; dispor sobre as formas de publicidade das operações de tratamento de dados pessoais; elaborar relatórios de gestão anuais acerca de suas atividades; realizar auditorias; editar normas, orientações e procedimentos; garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento; implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei [BRASIL].

3. Método

Para responder as questões de pesquisa utilizou-se um *survey* contendo 21 questões para investigar as percepções dos profissionais de TIC que exercem ou exerceram atividades como desenvolvedores de software, em segurança e os gestores de TIC, sobre conceitos, levantamento de requisitos de privacidade e métodos, ferramentas ou técnicas utilizadas para garantir privacidade de software. Com o objetivo de investigar, como está a conformidade da implantação da LGPD nas instituições públicas de ensino superior no Brasil.

O procedimento que se seguiu na pesquisa teve como base os princípios de Pfleeger e Kitchenham [Pfleeger and Kitchenham 2001] que afirmam que um *survey* faz parte de um processo de pesquisa mais amplo com atividades claramente definidas e que foram executadas neste trabalho: estabelecer objetivos específicos e mensuráveis; planejar e programar a pesquisa; preparar o instrumento de coleta de dados; validar o instrumento; selecionar os participantes; analisar os dados e relatar os resultados.

Com foco no objetivo da pesquisa foram elencadas as seguintes questões de pesquisa:

- RQ1. Qual o perfil e experiência dos participantes sobre o uso de elicitação de requisitos de privacidade?
- RQ2. Qual o nível de conhecimento sobre o conceito de privacidade em relação a LGPD?
- RQ3. As organizações realizam atividades e treinamentos sobre segurança e privacidade de dados?
- RQ4. Qual a percepção dos profissionais de TIC sobre os desafios e dificuldades para garantir a conformidade entre a LGPD e os sistemas da sua organização?
- RQ5. Qual o conhecimento que os profissionais de TIC possuem sobre ferramentas, métodos ou modelos que podem apoiar a especificação de requisitos de privacidade?

A realização da pesquisa iniciou com a elaboração de um survey com profissionais de TIC, cujos questionamentos encontram-se na Tabela 1.

Tabela 1: Questões do *survey*

Pergunta	Tipo
Q1- Qual o nome da empresa ou instituição?	Objetiva
Q2- Qual a natureza de atuação da sua organização?	Objetiva
Q3- Qual a área de atuação da sua instituição?	Objetiva
Q4- Qual o seu papel atual na organização?	Objetiva
Q5- Quantos anos de experiência você possui na função indicada?	Objetiva
Q6- Você tem conhecimento sobre a Lei Geral de Proteção de Dados (LGPD)?	Objetiva
Q7- Sua organização já iniciou, de maneira formal, ações de adequação a LGPD?	Objetiva
Q8- Na sua opinião, o ambiente organizacional interfere nas práticas de privacidade?	Objetiva
Q9- Na LGPD, o conceito de "tratamento de dados" é toda operação realizada com dados pessoais, como as que se referem à coleta, classificação, utilização, acesso, reprodução, processamento, armazenamento, eliminação, controle da informação, entre outros. Você considera que a sua organização realiza tratamento de dados?	Objetiva
Q10- Para LGPD, o conceito de "dados pessoais" é o de qualquer informação relacionada à pessoa natural identificada ou identificável (nome, endereço, e-mail, telefone, números de documentos). A sua organização trata dados pessoais?	Objetiva
Q11- Considerando que, para a LGPD, o conceito de "dados pessoais sensíveis" é aquele que trata da origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico. A sua organização trata de dados pessoais sensíveis?	Objetiva
Q12- Sua organização específica de forma clara os requisitos de privacidade e proteção de dados ao desenvolver softwares?	Objetiva
Q13- Se sua resposta, anterior foi sim, em qual fase esses dados são especificados?	Objetiva
Q14- Os requisitos de privacidade quando coletados, podem ser acessados a qualquer momento pelos *stakeholders* (partes interessadas), possibilitando serem atualizados ou corrigidos?	Objetiva
Q15- Sua empresa tem o hábito de aplicar nos dados coletados, técnicas de segurança da informação como: anonimização, criptografia?	Objetiva
Q16- Desde a aplicação da LGPD (2020), a mesma vem impactando o desenvolvimento de novos sistemas ou afetando na conformidade de sistemas existentes?	Objetiva
Q17- Na sua opinião, sua organização tem desenvolvido atividades/plano para se adequar aos requisitos de tratamento de dados pessoais presentes na LGPD?	Objetiva
Q18- Na sua organização ocorre treinamentos dos funcionários para atitudes seguras associadas a Engenharia Social (técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com *malware* ou abrir links para sites infectados?	Objetiva
Q19- Na sua opinião, quais são os principais desafios e as dificuldades para garantir a conformidade entre a LGPD e os sistemas da sua organização?	Subjetiva
Q20- Na sua opinião, quais ferramentas, métodos ou modelos podem apoiar a especificação de requisitos de privacidade durante o desenvolvimento de um produto ou serviço?	Subjetiva
Q21- Alguma pergunta que você gostaria de acrescentar que não foi colocada aqui?	Subjetiva

Os participantes tiveram que indicar sua concordância ou discordância com as afirmações derivadas das questões de análise, que representavam afirmações com as quais nem todos os participantes da nossa pesquisa concordaram. A maioria das opções de

resposta variaram de discordo totalmente a concordo totalmente, utilizando a escala Likert de cinco pontos com opção neutra [Albaum 1997].

O survey é composto por 21 perguntas, das quais 19 são de múltipla escolha e 02 subjetivas, conforme Tabela 1 e foram elaboradas em três eixos: questões demográficas, conhecimentos sobre privacidade de dados e a LGPD e sobre as percepções da conformidade ou não com a lei. Para isto, a pesquisa foi disponibilizada por meio da ferramenta do Google Forms e o tempo estimado para respostas foi entre oito e dez minutos. O público-alvo da pesquisa eram profissionais de TIC, preferencialmente, que atuam na área de desenvolvimento, segurança da informação e gestores de TIC das instituições públicas de ensino superior.

A pesquisa foi realizada em organizações e lugares distintos, apesar de fazerem parte do mesmo eixo, a educação. O survey foi divulgado em grupos de e-mails com 976 participantes (entre técnicos de TIC e desenvolvedores), grupo de WhatsApp dos gestores de TIC dos institutos federais que podiam compartilhar com suas equipes e universidades, além do LinkedIn, no período de 07 a 22/06/2022. Antes de disponibilizar o survey realizou-se teste piloto para analisar a compreensão das questões pela autora e com três pessoas externas, para posterior ajuste.

4. Resultado e Discussões

Finalizado o período de coleta de dados, obteve-se as respostas das questões de pesquisa que foram obtidas das respostas de 34 profissionais de TIC das 19 instituições que responderam à pesquisa online, que estão apresentadas nesta seção.

Esta pesquisa buscou compreender o ponto de vista de profissionais de TIC, em várias organizações públicas educacionais instaladas no país, em relação à implantação da LGPD em suas organizações. Vários trabalhos têm sido realizados buscando a auxiliar no processo de implantação da segurança de dados pessoais, alguns a exemplo desta pesquisa, utilizam a visão investigativa que antecedem futuras implementações.

Carina e Moisés [Alves and Neves 2021] investigaram em um estudo de caso, a perspectiva de cinco analistas de requisitos, em uma organização do poder judiciário, em relação à privacidade e proteção de dados. Com base nos resultados eles puderam ter a percepção das necessidades administrativas e que no contexto das equipes de trabalho há dificuldade de interpretar a LGPD. Em relação a este trabalho, nossa pesquisa difere em buscar analisar a compreensão dos profissionais de TIC sobre os conceitos e uso da LGPD em Organizações, que embora tenham o mesmo perfil educacional, localizam-se em diferentes regiões do país. O que pode proporcionar novos insigths para uma visão técnica ampla da LGPD.

4.1. Demografia dos participantes

Para estabelecer o perfil dos 34 profissionais de TIC que responderam à pesquisa, a identificação da localização demográfica denota que houve participação de instituições das cinco regiões do Brasil. A maioria (44%) eram da região Nordeste, 29% do Centro-Oeste, 12% Norte, 9% do Sudeste, 12% do Sul, conforme demonstrado na Figura 2.

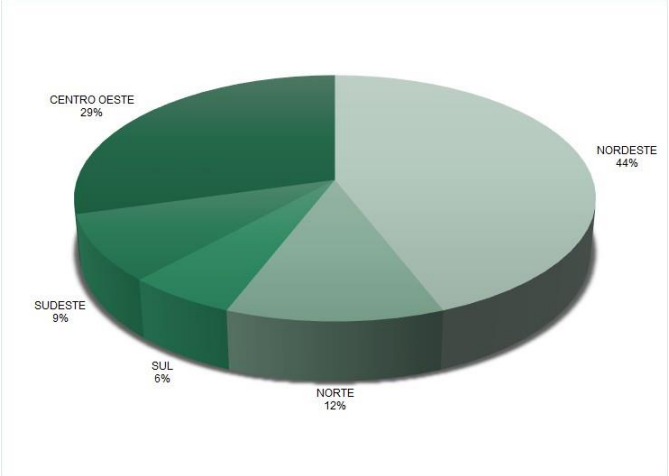


Figura 2. Localidade dos participantes

A Figura 3 apresenta os resultados sobre função/cargo dos participantes, com base nas respostas obtidas da Q4 da Tabela 1, a maioria atua como Técnico/Analista de governança ou Gestão de TIC (38,2%), 23,5% são da área de Infraestrutura e redes, sendo que apenas 20,6% escolheram a opção de desenvolvedor de software e Analista de TI que tem a mesma correspondência de função em uma instituição pública de ensino superior.

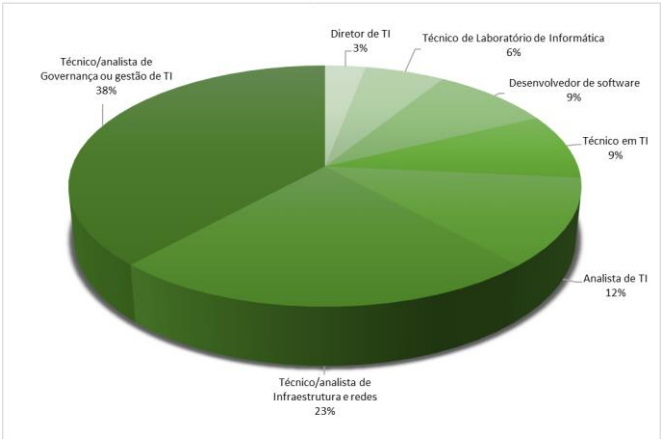


Figura 3. Função/cargo dos profissionais de TIC

Na Figura 4, no quesito experiência dos profissionais de TIC, com base nas respostas obtidas da Q5 da Tabela 1, identificou-se que 58,8% possuem mais de 10 anos de experiência na suas funções, 20,6% entre 7 e 9 anos de experiência, 11,8% entre 4 e 6 anos e 8,8% entre 1 e 3 anos de experiência.

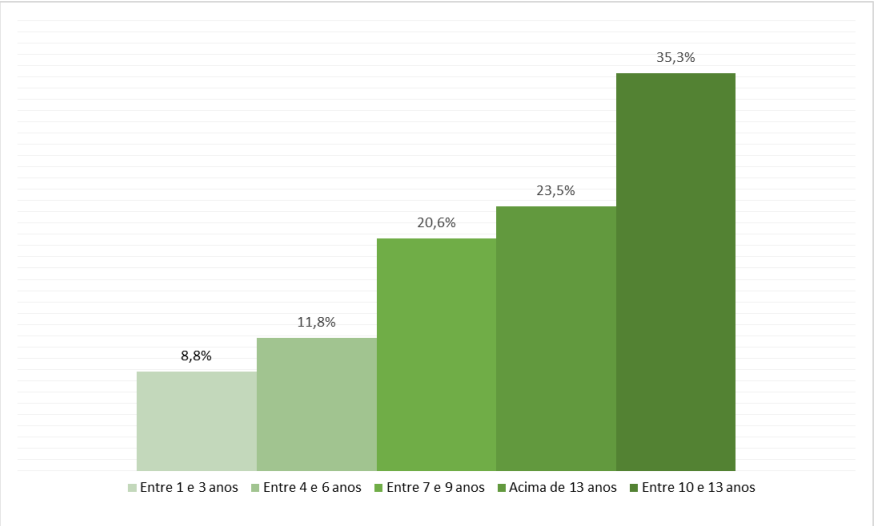
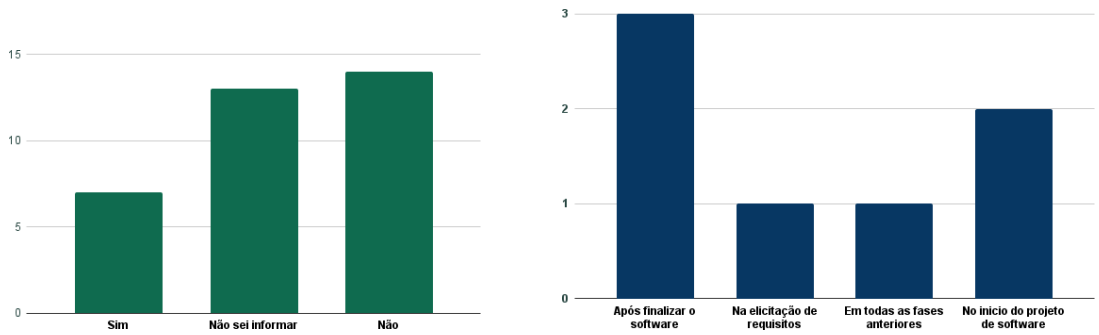


Figura 4. Experiência dos profissionais de TIC

Os resultados encontrados permitem inferir que o perfil dos profissionais de TIC que responderam o survey são em sua maioria Analista de Governança ou Gestão de TI, o que se configura positivamente, pois numa instituição pública de ensino, deve-se buscar habilidades que culminem em ter ou obter conhecimento sobre as legislações que podem impactar na manutenção e desenvolvimento de sistemas. Além disso, mais de 79\% dos entrevistados têm mais de 07 anos de experiência nas suas áreas de atuação e pertencem as cinco regiões do Brasil com predominância na região nordeste.

4.2. Perfil e Experiência: RQ1. Qual o perfil e experiência dos participantes sobre o uso de elicitação de requisitos de privacidade?

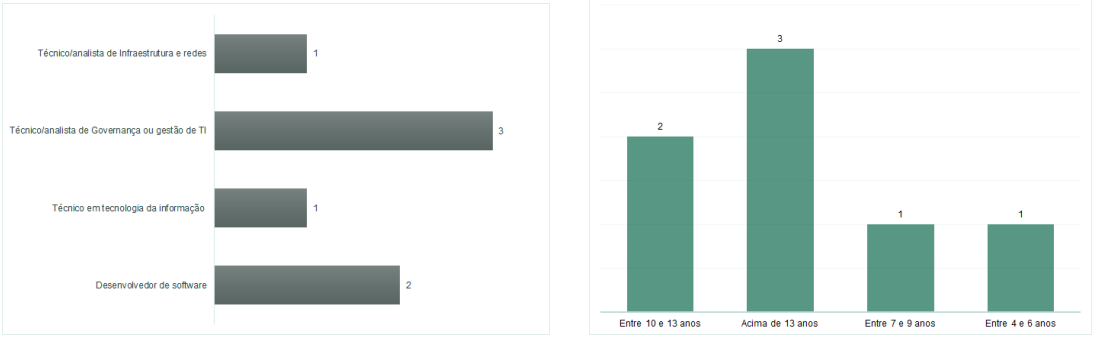
Nesta questão de pesquisa buscou-se verificar o perfil e experiência apenas dos profissionais de TIC que afirmam realizar elicitação de requisitos de privacidades. De acordo com a Q12 do survey dos 34 respondentes, apenas sete afirmaram realizar a especificação (20,6\%). Já na questão 13, os mesmos sete que responderam sim, deveriam informar em que fase do ciclo de desenvolvimento isso ocorria, as respostas obtidas foram: no início, na elicitação de requisitos, no final ou em todas as fases, conforme a Figura 5.



(a) Questão 12 (b) Questão 13

Figura 5. A Figura (a) apresenta se especificam ou não requisitos de privacidade, enquanto na Figura (b) quem respondeu SIM, informa em que fase ocorre.

Ao observar o perfil e a experiência apenas dos sete profissionais que afirmam realizar elicitação de requisitos de privacidade, infere-se que isso ocorre também devido ao cargo que exercem na instituição, na qual em sua maioria informa atuar como Técnico de Governança ou Gestão de TI e possuem no mínimo quatro anos de experiência, detalhado na Figura 6.



(a) Cargo (b) Experiência

Figura 6. A Figura (a) apresenta o cargo, enquanto na Figura (b) está descrito a experiência.

> **Resumo do RQ1:** Os resultados obtidos apontam que 79,4% dos respondentes não realizam ou tem conhecimento sobre a elicitação de requisitos de privacidade, ou seja, apenas 20,6% dos participantes fazem levantamento de requisitos de privacidade. Portanto, o maior desafio a ser superado pelos profissionais de TIC está no uso de uma abordagem de privacidade de dados para elicitar os requisitos.

4.3. Privacidade x LGPD: RQ2. Qual o nível de conhecimento sobre o conceito de privacidade em relação a LGPD?

Para buscar entender o nível de compreensão sobre o conceito de privacidade e LPGD foram elaboradas seis questões, que estão apresentadas na Figura 7.

De acordo com as respostas obtidas da questão 6 (Q6) da Tabela 1 é possível observar que 88,2% dos participantes concordaram que tem conhecimento sobre a LGPD. Decorre-se ainda que 76,4% das organizações iniciaram de alguma forma a adequação da LGPD internamente (Q7), o que nos permite inferir que existe uma conscientização por parte da alta gestão da organização e que as instituições estão buscando atender a LGPD. Na questão 8 (Q8), ao perguntar sobre a concordância ou não, se a organização pode interferir na aplicação de práticas de privacidade, 88,2% concordaram com a afirmativa.

Pode-se observar ainda na Figura 7, dados referentes ao questionamento sobre o conceito de tratamento de dados, cujos resultados apontam que 70,6% concordam que a organização realiza o tratamento dos dados (Q9), já sobre o conceito de dados pessoais apenas 70,% afirmam que a organização trata os dados pessoais (Q10), na questão 11 (Q11) ao perguntar se concordam com a afirmativa de que a organização trata os dados pessoais sensíveis 70,6% concordam, 14,7% discordam e 14,7% são neutros. Pode-se assim concluir que já existe por parte das instituições o conhecimento e ações em andamento acerca dos princípios básicos da LGPD.

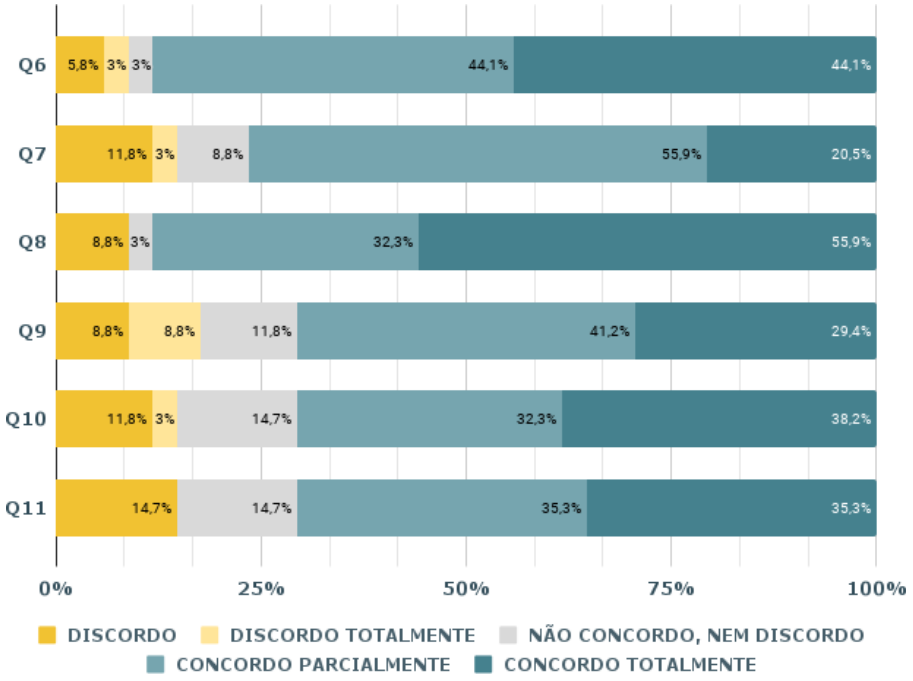


Figura 7. Conhecimento da LGPD pelos profissionais de TIC e de ações implementadas pelas organizações (Q6 a Q11 da Tabela 1)

Resumo do RQ2: Os resultados encontrados permitem denotar que tanto a organização quanto os profissionais de TIC tem algum conhecimento sobre a LGPD e que realizam tratamento de dados pessoais. O maior desafio a ser superado pelos profissionais de TIC está no conhecimento e consequentemente no uso de uma abordagem

4.4. Atividades e Treinamento: RQ3. As organizações realizam atividades e treinamentos sobre segurança e privacidade de dados?

Para buscar responder essa questão foram estabelecidas três questões objetivas. Na Figura 8, a questão 16 (Q16) fala do impacto no desenvolvimento de software após a aplicação da LGPD, a maioria (67,6%) consideram que houve sim impactos, 17,6% são neutros e 14,7% discordam. A questão 17 (Q17) quer saber se a organização vem se preparando para atender a LGPD, fato este que 70,6% dos respondentes concordam que as organizações tem desenvolvido ações para se adequar aos requisitos de tratamento de dados pessoais presentes na LGPD, 11,8% são neutros e 17,6% discordam.

Na Figura 8, a questão 18 (Q18), levanta o questionamento sobre os treinamentos dos funcionários referente a segurança e privacidade de dados, observa-se que 50\% discorda dessa afirmação, ou seja, há um grande número de instituições que necessitam realizar treinamentos dos seus colaboradores, para que possam se proteger contra atitudes maliciosas, minimizando assim os riscos de incidentes, bem como garantir maior segurança e proteção dos dados pessoais.

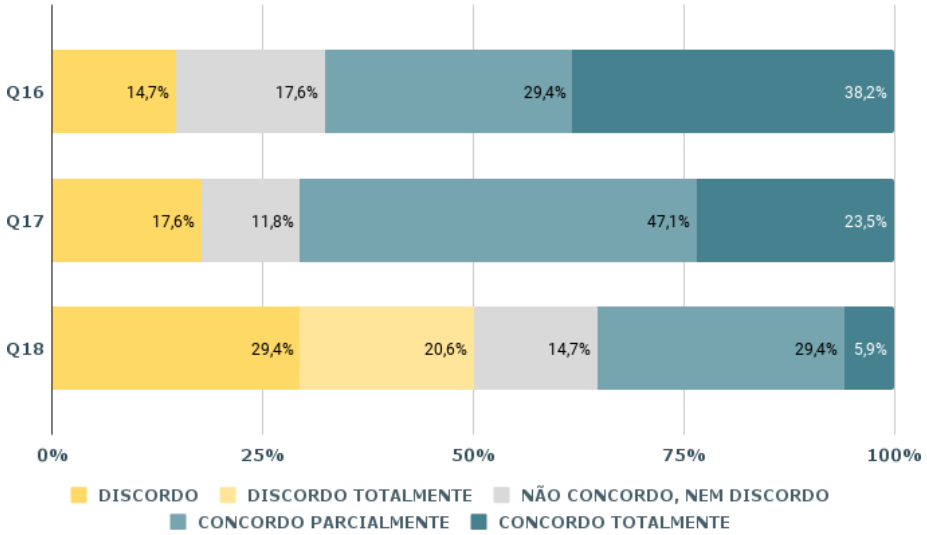


Figura 8. {Percepção dos respondentes sobre os impactos da LGPD e das ações realizadas pela organização (Q16 a Q18 da Tabela 1).

Resumo do RQ3: Os resultados encontrados inferem que, embora a maioria dos profissionais de TIC acreditem que após a LGPD tenha havido impactos no desenvolvimento de software e que as organizações iniciaram ações para adequação a LGPD, cerca de 50% dos respondentes afirmam que não há treinamentos para os profissionais de TIC em segurança e privacidade de dados.

4.5. Desafios e Dificuldades na conformidade da LGPD e os sistemas: RQ4. Qual a percepção dos profissionais de TIC sobre os desafios e dificuldades para garantir a conformidade entre a LGPD e os sistemas da sua organização?

Neste survey foram disponibilizadas três questões subjetivas (abertas) e não obrigatórias. A primeira autora utilizou a técnica Card Sorting [Spencer 2009], para categorizar respostas com termos similares, enquanto a outra pesquisadora procedeu, individualmente, com a revisão.

Na questão 19, ao serem indagados sobre os principais desafios e as principais dificuldades para garantir a conformidade da LGPD e os sistemas da sua organização, na quais as principais respostas fortalecem os resultados das análises das questões objetivas, como a falta de treinamento de pessoal, a importância de envolvimento da organização e a necessidade de realizar a especificação de requisitos no início do processo. Afim de manter a anonimização dos participantes, eles foram identificados como P1 a P34, ou seja, 34 respondentes. Após a devida análise, por fim, discutiu-se os resultados e definiu-se sete categorias, conforme a Tabela 2.

Tabela 2. Análise da Questão subjetiva nº 19

Categorias	**Algumas Respostas**
Treinamento	“Falta de treinamento e mudança cultural" (P14)
Qualificação	"Capacitação da equipe responsável pela implementação da LGPD" (P18)
Mudança de cultura	"Mudança de cultura de todos os funcionários e da alta administração" (P03)
Envolvimento da gestão	"Apoio da alta gestão" (P15, P17)
Comunicação	"A falta de conhecimento da legislação" (P04)
Especificação de Requisitos	"A especificação de requisitos e o desenvolvimento" (P28)
Armazenamento	"Adequar dados já armazenados há algum tempo" (P07)

Nota-se que as categorias identificadas e apresentada na Tabela 2, reforça o entendimento de que já havia sido apontado nas questões objetivas como a falta de treinamento, a necessidade de mudança de cultura e o apoio da alta gestão são imprescindíveis para atendimento à LGPD.

Resumo do RQ4: Com os resultados obtidos, pode-se inferir que é necessário que as organizações realizem mudanças, dado que as dificuldades estão tanto no processo de desenvolvimento de software quanto na questão de envolvimento da alta gestão, na mudança de cultura, realizar treinamentos e qualificação dos profissionais de TIC. Não perdendo à atenção ao desafio de conciliar e adequar os dados de sistemas legados, que permanecem armazenados na organização, à LGPD.

4.6. Mecanismos para especificar requisitos de privacidade: RQ5. Os profissionais de TIC envolvidos, possuem conhecimento sobre ferramentas, métodos ou modelos que podem apoiar a especificação de requisitos de privacidade?

Para responder esta questão de pesquisa, toma-se como base as respostas obtidas na questão 20 da Tabela 1, na qual os participantes demonstram o nível de conhecimento em métodos, ferramentas, legislação que podem auxiliá-los na especificação de privacidade. Destacam-se algumas respostas:

”CMMI for Development, CMMI for Services, ISO 20000, ITIL Service Design, MPS.BR Guia SV e de Serviços.”

”frameworks, ISOS e metodologias já consolidadas no mercado como: Owasp, CIS, NIST, etc.”

”Boas práticas Nacionais e Internacionais...”

”Seguir padrões, frameworks e controles de segurança da informação, como: ePing; ABNT NBR ISO/IEC 27001:2013; ABNT NBR ISO/IEC 27002:2013; ABNT NBR ISO/IEC 27005:2019; ABNT NBR ISO/IEC 31000:2018; ABNT NBR ISO/IEC 27701:2019; ...”

Resumo do RQ5: Nota-se pela análise das respostas que alguns profissionais possuem conhecimento em modelos, como o CMMI e MPS-BR, *frameworks*, metodologias, normas técnicas nacionais e internacionais que apoiam a especificação de requisitos de privacidade. Denotando que os profissionais das organizações possuem conhecimento das ações necessárias, que devem ser avaliadas pela organização para serem utilizadas quando necessário, de forma a atender a adequação à LGPD.

5. Ameaças a Validade

Durante a elaboração do survey adotou-se algumas respostas pré-definidas em algumas questões fechadas, além disso, também foi deixado um espaço aberto permitindo que fosse adicionado fatores não listados na pergunta. Também foi aplicado um teste piloto do survey com três profissionais de TIC, afim de avaliar a compreensão e relevância das perguntas.

A quantidade de respondentes para este survey pode ser considerado uma limitação. Porém não há como medir precisamente a quantidade de profissionais de TIC que exercem atividades em desenvolvimento de software. Este estudo usou uma amostra não probabilística, termo apresentado por Kitchenham et. Al [Kitchenham and Pfleeger 2002] pois amostras não probabilísticas são criadas quando os entrevistados são escolhidos, porque são facilmente acessíveis ou os pesquisadores têm alguma justificativa para acreditar que são representativos da população.

Os participantes que responderam à pesquisa foram convidados por e-mail, listas de contatos, grupos de WhatsApp e no LinkedIn e encorajados para que compartilhassem com demais colegas que fizessem parte do público-alvo. Visando garantir que apenas pessoas com experiência respondessem ao questionário, foi reforçado essa informação seja no convite ou na própria pergunta. Buscou-se ainda ter diversidade demográfica com participantes de todas as regiões do Brasil.

Uma outra limitação é o nível de conhecimento dos respondentes sobre as ações de sua organização e é possível que eles não conheçam todas as iniciativas. Além disso, as perguntas abordam muitos conceitos profundos relacionados à privacidade e a falta de conhecimento sobre esses conceitos pode resultar em respostas imprecisas.

6. Conclusão

Neste artigo, realizou-se uma pesquisa para investigar a conformidade durante a implantação da LGPD nas instituições públicas de ensino superior no Brasil, identificando o uso de requisitos de privacidade, o nível de conhecimento e o cumprimento da legislação sob a perspectiva dos profissionais de TIC. A maior parte dos profissionais (58,8%) possuem mais de 10 anos de experiência em suas funções e possuem conhecimento sobre os princípios básicos da LGPD.

Um fato que requer destaque é de que apenas 20,6% dos respondentes afirmaram fazer uso de abordagem de privacidade nas especificações de requisitos, e que mesmo quando isso acontece, normalmente é realizado apenas no final do desenvolvimento do software. Destaca-se que estes respondentes possuem no mínimo quatro anos de experiência em suas funções. Nesse sentido, as instituições devem estar atentas em realizar levantamento de requisitos de privacidade utilizando, dentre outros, mapeamento

dos processos, elaboração de políticas, levando-se em consideração o art. 46, §1º da LGPD, o qual afirma que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo.

A maioria das instituições já iniciaram ações de adequações, porém percebe-se que ainda é necessário que exista um plano de de ação da instituição que contenha no mínimo a capacitação dos servidores e das áreas de TIC através do envolvimento da alta gestão nas ações e nas implicações da LGPD.

Pode-se pensar como trabalho futuro, a avaliação de *frameworks* disponíveis na literatura para uso nas organizações públicas, considerando que empresas privadas lançam soluções condicionadas à recursos que as tornam inviáveis. Um estudo envolvendo mais participantes seria interessante como forma de obter resultados com maior nível de significância. Além disso, levantar e analisar o perfil das organizações que sofreram sanções aplicadas pela ANPD. E por fim, identificar os métodos para elicitação de requisitos de privacidade com foco na LGPD.

Referências

Albaum, G. (1997). The Likert Scale Revisited. *Market Research Society. Journal.* 39(2):1–21.

Alves, C. and Neves, M. (2021). Especificação de requisitos de privacidade em conformidade com a LGPD: Resultados de um estudo de caso. In *Anais do WER21 - Workshop em Engenharia de Requisitos*, Brasília, Brasil. Editora PUC-Rio.

Ansari, M. T., Baz, A., Alhakami, H., Alhakami, W., Kumar, R., and Khan, P. R. (2021). P-STORE: Extension of STORE methodology to elicit privacy requirements. *ARABIAN JOURNAL FOR SCIENCE AND ENGINEERING*, 46:8287–8310.

Ayala-Rivera, V. and Pasquale, L. (2018). The Grace Period Has Ended: An Approach to Operationalize GDPR Requirements. In *2018 IEEE 26th International Requirements Engineering Conference (RE)*, pages 136–146.

Behutiye, W., Karhapää, P., Costal, D., Oivo, M., and Franch, X. (2017). Non-functional Requirements Documentation in Agile Software Development: Challenges and Solution Proposal. In *Product-Focused Software Process Improvement*, Lecture Notes in Computer Science, pages 515–522, Cham. Springer International Publishing.

BRASIL. Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais - LGPD. Disponível em: https://www.planalto.gov.br/ccivil03/ato2015-2018/2018/lei/L13709. Acesso em 20 de abril de 2023.

Canedo, E., Toffano Seidel Calazans, A., Toffano Seidel Masson, E., Teixeira Costa, P. H., and Lima, F. (2020). Perceptions of ICT Practitioners Regarding Software Privacy. *Entropy*, 22(4).

CNN BRASIL (2022). Banco central anuncia vazamento de dados ligados a mais de 130 mil chaves pix. Disponível em: https://www.cnnbrasil.com.br/economia/banco-central-anuncia-vazamento-de-dados-ligados-a-mais-de-130-mil-chaves-pix/. Acesso em 25 de abril de 2023.

Fontes, Edison (2007). Segurança da Informação - o Usuário Faz a Diferença, volume 2. Saraiva, Estante Virtual.

Hintzbergen, J., Hintzbergen, K., Smulders, A., and Baars, H. (2018). Fundamentos de Seguranc ̧a da Informação: com base na ISO 27001 e ISO 27002. Brasport.

INFOMONEY (2022). As empresas estão preparadas para LGPD? Disponível em: https://www.infomoney.com.br/negocios/lgpd-multas-comecam-a-ser-aplicadas. Acesso em 13 de junho 2022.

ISO/IEC 27002. ISO - International Organization for Standardization.information Technology - Security Techniques - code of practice for information security controls. Geneva: ISO, 2013.

ISO/IEC 27701. ISO - International Organization for Standardization. security Techniques - extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - requirements and guidelines. Geneva: ISO, 2019

ISO/IEC 29100. ISO - International Organization for Standardization. 29100:2011 information technology - security techniques - privacy framework. Geneva: ISO, 2011. 26p.

ISO/IEC 31000. ISO - International Organization for Standardization. 31000:2018: Risk management - Guidelines. Geneva: ISO, 2022. 32 p.

Kitchenham, B. and Pfleeger, S. L. (2002). Principles of survey research: Part 5: Populations and samples. SIGSOFT Softw. Eng. Notes, 27(5):17–20.

NIC.BR (2023). Dia da internet segura: Brasil ocupa o 12º lugar entre países com mais vazamento de dados em 2022. Disponível em: https://nic.br/noticia/na-midia/dia-da-internet-segura-brasil-ocupa-o-12-lugar-entre-paises-com-mais-vazamento-de-dados-em-2022/. Acesso em 27 de outubro de 2023.

Petronio, S. (2002). Boundaries of Privacy: Dialectics of Disclosure. State Univ of New York Pr, Albany.

Pfleeger, S. L. and Kitchenham, B. A. (2001). Principles of survey research: part 1: turning lemons into lemonade. ACM SIGSOFT Software Engineering Notes, 26(6).

Ribeiro, Bruno. Albuquerque, R. (2002). Segurança No Desenvolvimento De Software. Elsevier, Rio de Janeiro.

Samuel, D. Warren and Louis, D. Brandeis (1890). The Right to Privacy, volume 4. Harvard Law Review.

Santos, J. G. D. (2020). Lei geral de proteção de dados pessoais sobre a governança e segurança de dados. Harvard University Press, London.

SERPRO (2023). LGPD Educacional. Disponível em 20 de abril de 2023.

Solove, D. J. (2008). Understanding Privacy. Harvard University Press, London.

Sommerville, I. (2011). Engenharia de software, 9a. São Palo, SP, Brasil, page 63.

Sommerville, I. (2019). Engenharia de Software. Pearson Universidades, 10ª edição.

Spencer, D. (2009). Card sorting: Designing usable categories. Rosenfeld Media.

Thomas, K., Bandara, A. K., Price, B. A., and Nuseibeh, B. (2014). Distilling privacy requirements for mobile applications. In Proceedings of the 36th International Conference on Software Engineering, pages 871–882, Hyderabad India. ACM.

UNIÃO EUROPEIA (2018). General Data Protection Regulation (GDPR). Disponível em: https://gdpr-info.eu/. Acesso em 03 de junho 2022.

Webster, I., Ivanova, V., and Cysneiros, L. (2005). Reusable Knowledge for Achieving Privacy: A Canadian Health Information Technologies Perspective. 2005. pages 112–122.