ISSN: 1983-6635

RGO Revista Gestão Organizacional

A COMPREENSÃO DOS PROFISSIONAIS DE TI QUANTO ÀS IMPLICAÇÕES DA LGPD NA SEGURANÇA DA INFORMAÇÃO[1]

IT PROFESSIONALS' UNDERSTANDING OF THE IMPLICATIONS OF THE LGPD ON INFORMATION SECURITY

NAIRA MARIA SILVA DUARTE
Universidade Federal da Bahia (UFBA)
Mestre em Administração
https://orcid.org/0009-0001-4489-6174
nairaduarte28@gmail.com

ANTONIO EDUARDO DE ALBUQUERQUE JUNIOR
Universidade Federal da Bahia (UFBA)
Doutor em Administração
https://orcid.org/0000-0002-4128-4666
eduardo.albuquerque@fiocruz.br

ERNANI MARQUES DOS SANTOS
Universidade Federal da Bahia (UFBA)
Doutor em Administração
https://orcid.org/0000-0001-8618-9489
emarques@ufba.br

Editor científico: Juliana Fabris

Submissão: 07/02/2025. Revisão: 10/07/2025. Aceite: 21/07/2025. Publicação: 02/10/2025.

Como citar: Duarte, N. M. S., Albuquerque Junior, A. E., Santos, E. M. (2025). A compreensão dos profissionais de TI quanto às implicações da LGPD na segurança da informação. *RGO - Revista Gestão Organizacional, 18*(2), 94-120. http://dx.doi.org/10.22277/rgo.v18i2.8355.

RESUMO

Objetivo: Investigar a percepção dos profissionais de TI sobre as implicações da Lei Geral de Proteção de Dados Pessoais (LGPD) nos controles de segurança da informação e seu impacto na adequação organizacional à legislação.
Método/abordagem: Estudo de caso descritivo com abordagem quantitativa e qualitativa. Foram coletados dados por meio de um levantamento com 64 profissionais de TI e um grupo focal com gestores. A análise quantitativa foi conduzida no SPSS, enquanto a qualitativa utilizou codificação temática e sumário etnográfico.
Principais resultados: Os participantes relataram pouco conhecimento sobre a LGPD, mas reconheceram a importância de treinamentos e divulgação para a cultura organizacional e aceitação das mudanças exigidas pela legislação. Avaliaram que as diretrizes da política

[1] Este é um artigo publicado em acesso aberto (Open Access) sob a licença Creative Commons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

organizacional de segurança da informação não estão adequadas à LGPD e que são necessárias atualizações tecnológicas e administrativas. Apesar disso, consideram que a organização está tecnologicamente atualizada, embora precise de ajustes em processos, papéis internos e infraestrutura para estar em conformidade.
Contribuições teóricas/práticas/sociais: O estudo amplia o conhecimento sobre a relação entre segurança da informação, legislação de proteção de dados e conformidade regulatória, com foco em profissionais e gestores de TI. Também auxilia as organizações na implementação de estratégias de conformidade, enfatizando a importância de treinamento e ajustes internos, além de contribuir para a proteção de dados pessoais e a conscientização sobre privacidade e segurança da informação.
Originalidade/relevância: A pesquisa explora a percepção de profissionais de TI sobre a LGPD e seus impactos na segurança da informação, abordando desafios e necessidades organizacionais para a conformidade com a legislação.
Palavras-chave: LGPD. Segurança da Informação. Conformidade regulatória.

ABSTRACT

Purpose: Investigate IT professionals' perception of the implications of the Brazilian General Data Protection Law (LGPD) on information security controls and its impact on organizational compliance with the legislation.
Method/approach: A descriptive case study with a quantitative and qualitative approach. Data were collected through a survey with 64 IT professionals and a focus group with managers. Quantitative analysis was conducted using SPSS, while qualitative analysis employed thematic coding and ethnographic summary techniques.
Main findings: Participants reported limited knowledge of the General Law on the Protection of Personal Data (LGPD) but acknowledged the importance of training and awareness initiatives for organizational culture and acceptance of the changes required by the legislation. They assessed that the organization's information security policy guidelines are not adequately aligned with the LGPD and that technological and administrative updates are necessary. Nevertheless, they consider the organization to be technologically up to date, although adjustments in processes, internal roles, and infrastructure are required for full compliance.
Theoretical/practical/social contributions: This study expands knowledge on the relationship between information security, data protection legislation, and regulatory compliance, focusing on IT professionals and managers. It also supports organizations in implementing compliance strategies by emphasizing the importance of training and internal adjustments, while contributing to personal data protection and raising awareness of privacy and information security.
Originality/relevance: This research explores IT professionals' perception of the LGPD and its impact on information security, addressing organizational challenges and requirements for regulatory compliance.
Keywords: LGPD. Information Security. Regulatory Compliance.

1 INTRODUÇÃO

O uso disseminado de tecnologia, o aumento do volume e da diversidade de dados coletados pelas organizações e a possibilidade de tratamento inadequado desses dados levaram governos e organizações internacionais a regulamentar a coleta e o processamento

de dados pessoais, como pode ser visto em Baumer, Earp e Payton (2000), Kitiyadisai (2005), Hallinan, Friedewald e McCarthy (2012), Jasserand (2018) e Poullet (2018).

Leis e regulamentos são resultados de uma crescente preocupação com a proteção dos dados pessoais, exigindo integridade das informações, respeito à sua finalidade de uso e o consentimento para utilização (Mulholland, 2018). No Brasil, a necessidade de proteger os dados pessoais traduziu-se na Lei n. 13.709 (2018), mais conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), que estabeleceu um marco legal para o tratamento desses dados em organizações públicas e privadas. Vigente desde setembro de 2020, a lei implica mudanças na gestão de tecnologia da informação (TI) (Ismail, Malone & Geest, 2019), trazendo responsabilidades sobre o mapeamento, proteção e controle do uso desses dados. A LGPD demanda ainda revisões nos controles tecnológicos e em políticas de segurança da informação, ampliando a importância de compreender seus impactos (Almeida & Soares, 2022).

Embora diversos estudos analisem os impactos da LGPD e seus desafios organizacionais, como os trabalhos de Casotti et al. (2024), Silva e Antunes Neto (2023), Haddara, Salazar e Langseth (2023) e Georgiadis e Poels (2022), não foram identificados na literatura consultada trabalhos que articulem as dimensões técnica, formal e informal da conformidade organizacional com a LGPD. Além disso, a maioria dos trabalhos sobre LGPD identificados na pesquisa bibliográfica é prescritiva ou avaliação de conformidade, como os de Piurcosky, Costa, Frogeri e Calegario (2019), Canedo et al. (2021), Menegazzi (2021), Fernandes (2022), Quintanilha e Silva (2023), Ribeiro e Garcés (2023) e Miranda et al. (2024).

Alguns estudam as implicações da lei para profissionais e gestores de TI, como Canedo, Calazans, Bandeira, Costa e Masson (2022), Peixoto et al. (2023), Cavenaghi, Paris, Menegassi, Antunes Neto e Biazotto (2024) e Kanagusku e Lahr (2024), ou para os usuários de TI, como em Cetin (2024). Poucos abordam proteção de dados e segurança da informação, e, quando o fazem, também são avaliativos ou prescritivos (Melo & Mendes, 2023; Neitzke, Mendes, Rivero, Teixeira & Viana, 2023), ou revisam artigos anteriores (Miracle, 2024). Não foram encontrados estudos sobre a percepção de profissionais e gestores de TI sobre a legislação de proteção de dados e os controles de segurança da informação.

Assim, esta pesquisa teve o objetivo de estudar como profissionais de TI percebem as implicações da LGPD nos controles de segurança da informação organizacionais. É relevante saber como profissionais de TI compreendem as implicações da LGPD para a segurança da informação devido à atuação direta desses profissionais com os dados pessoais, bem como a necessidade de proteger os direitos dos titulares desses dados e as questões técnicas e de gestão envolvidas com os requisitos da lei, de forma que este estudo contribui para a aplicação prática da lei para garantir a privacidade e transparência no tratamento dos dados, evitando não conformidades e impactos desnecessários ou desproporcionais da adequação dos controles de segurança da informação aos requisitos da lei. Além disso, esta pesquisa não se limitou a explorar dados sobre a percepção de profissionais técnicos, mas buscou coletar dados também junto aos gestores de TI, o que permitiu cruzar dados de fontes com visões diferentes, ampliando o conhecimento sobre o tema.

Os dados mostram que muitos profissionais técnicos avaliam ter pouco conhecimento sobre a LGPD, mas reconhecem o impacto positivo de treinamentos e divulgação. Embora a infraestrutura tecnológica seja adequada, políticas e processos precisam se ajustar aos requisitos da lei. Esses resultados indicam a compreensão do impacto da LGPD nos controles de segurança da informação e a necessidade de capacitação e conscientização sobre a lei.

Este artigo está organizado em mais cinco seções, além desta introdução. A seção seguinte traz a revisão da literatura, que conduziu à construção do modelo utilizado na pesquisa, apresentado na seção 3. A seção 4 fala dos procedimentos metodológicos utilizados, e a seção 5 apresenta os resultados. A seção 6 é dedicada às considerações finais do trabalho.

2 REVISÃO DA LITERATURA

A informação pode ser entendida como um meio para a construção do conhecimento, ou como dados relevantes para um propósito específico (Drucker, 1988; Allen, 1996), tendo se tornado indispensável para as organizações por ser um ativo estratégico (Le Coadic, 2004).

Nas organizações, a informação pode ser considerada um recurso valioso para o processo decisório, na definição de produtos e serviços, e na elaboração e execução de procedimentos (Davenport & Prussak, 1998), sendo que seu valor está intrinsecamente ligado à tomada de decisão e à lucratividade, o que exige que ela seja completa, confiável e relevante (Stair & Reynolds, 2002).

Reconhecendo a informação como um ativo que precisa ser protegido, Dhillon e Backhouse (2001) explicam que a segurança da informação é a proteção das informações contra ameaças, minimizando riscos e buscando a continuidade das operações organizacionais, tendo como objetivos a preservação da sua confidencialidade, integridade e disponibilidade.

No contexto da segurança da informação, a integridade é a garantia de que a informação não foi alterada de forma não autorizada, acidentalmente ou não, e que suas características originais foram mantidas. A confidencialidade é a garantia de que a informação poderá ser acessada somente por quem estiver devidamente autorizado para isso. Já a disponibilidade é a garantia de que a informação será acessada sempre que necessária pelas pessoas devidamente autorizadas (Lopes, 2012). Sêmola (2014) acrescenta que é necessário manter essas características durante o ciclo de vida da informação.

Para proteger a integridade, confidencialidade e disponibilidade da informação, é preciso adotar controles de segurança da informação (Sêmola, 2014), que, segundo Albuquerque Junior, Santos, Oliveira, Silva e Almeida (2018), podem ser classificados conforme sua finalidade:

- Controles técnicos, que têm o objetivo de limitar o acesso a computadores, sistemas, prédios e salas, ou mudar o ambiente físico que armazena e processa as informações para protegê-las por meios físicos. Inclui mecanismos de controle de acesso, ar-condicionado, alarmes, câmeras, proteção contra incêndio e fumaça, e mecanismos que operam em sistemas computacionais, como antivírus, *firewalls*, correções de vulnerabilidades em sistemas, realização de *backup*, biometria, criptografia e sistemas de detecção de intrusos (Dhillon & Moores, 2001; Björck, 2005; Gorayeb, 2012).
- Controles formais, que são adotados para mudar o comportamento dos indivíduos e da organização através de regras, procedimentos, planos e da conformidade com leis e regulamentos, e que envolvem a definição de funções, papéis, responsabilidades e objetivos, como políticas de segurança da informação, processos e regulamentos internos, além de estruturas organizacionais, como escritório de segurança da informação, equipe de tratamento de incidentes e comitê de segurança da informação (Dhillon & Moores, 2001; Björck, 2005; Sêmola, 2014).
- Controles informais, que pretendem mudar o comportamento dos indivíduos através de ações de treinamento e educação, conscientização e divulgação, a comunicação de

responsabilidades e a promoção de comportamentos adequados (Dhillon & Moores, 2001; Björck, 2005; Sêmola, 2014).

Através dos controles de segurança da informação, é possível proteger dados pessoais que são tratados nos processos organizacionais, que é o objetivo da LGPD. A lei dispõe ainda sobre o consentimento explícito dos titulares dos dados para sua coleta, armazenamento e tratamento, com uma finalidade específica e legítima e com transparência sobre quem vai acessá-los e por quanto tempo serão utilizados, garantindo ao titular o direito de acesso, correção e exclusão do que for incorreto, excessivo ou desnecessário para a finalidade da coleta. Por fim, a LGPD responsabiliza as organizações pelo descumprimento dos seus requisitos e pela adoção das medidas necessárias para garantir a privacidade dos titulares dos dados (Lei n. 13.709, 2018).

Necessária para o livre desenvolvimento da personalidade humana (Doneda, 2021), a privacidade está relacionada à dignidade humana (Cancelier, 2017) e é reconhecida no Brasil como direito fundamental, que protege a vida privada e a intimidade dos indivíduos (Rodotá, 2008). Com o uso dos dados pessoais para fins comerciais, o direito à privacidade envolve o controle e determinação de como esses dados serão processados (Bioni, 2019).

A ampla utilização da tecnologia e o crescente volume de dados gerados e armazenados tecnologicamente desafiam a proteção dos dados pessoais (van den Hoven, 2008), que incluem imagens, comunicações e localização, impactando diretamente na intimidade das pessoas (Corcoran, 2016). Ainda que isoladamente não possam identificar um indivíduo, pode haver cruzamento de dados de forma a permitir sua identificação (Pinheiro, 2020), o que pode ser facilitado pela utilização de tecnologia (Ferreira, 2018). Como agravante, há a possibilidade de dados pessoais sensíveis serem utilizados para discriminação ou controle sobre o indivíduo (Doneda, 2021).

Dados sensíveis são aqueles relacionados a características pessoais ou circunstâncias de um indivíduo, que podem revelar origem étnica, opinião política, crenças religiosas e filosóficas, filiação sindical, dados biométricos, de saúde e genéticos, e dados sobre vida ou orientação sexual, como explicam Quinn e Malgieri (2021). No Brasil, a LGPD (Lei 13.709, 2018) apresenta um conceito semelhante, inclusive quanto à preocupação de que esses dados sejam utilizados para discriminação do indivíduo, como observa Pinheiro (2020), o que explica a razão de serem assim considerados.

A proteção desses dados passa necessariamente pela garantia da privacidade, que no entender de Sheehan e Hoy (2000), diz respeito à consciência do indivíduo sobre seus dados, à possibilidade de escolha sobre como esses devem ser tratados ou divulgados, ao acesso aos seus dados em poder de outros, ao seu direito de recorrer a violações da sua privacidade, e à segurança de que esses dados estão bem guardados.

A privacidade, portanto, está relacionada a confidencialidade, integridade e disponibilidade dos dados e, consequentemente, à adoção de controles de segurança da informação. Entretanto, esses controles não se resumem a recursos tecnológicos, pois incluem processos, práticas, documentos e estruturas organizacionais (Belasco & Wan, 2006; Sêmola, 2014), inclusive porque a privacidade dos dados pessoais é ameaçada não só por vulnerabilidades tecnológicas, mas principalmente pelo comportamento humano (Belasco & Wan, 2006).

Acquisti e Grossklags (2003) reforçam que o comportamento das pessoas que lidam com informações sensíveis pode comprometer sua segurança, enquanto Mitnick e Simon (2003) acrescentam que incidentes que comprometem a segurança dos dados costumam

envolver as pessoas, ainda que estejam relacionados a exploração de falhas tecnológicas e envolvam a utilização de tecnologia.

Para evitar incidentes que comprometam a integridade, disponibilidade e confidencialidade dos dados pessoais, são necessários controles de segurança da informação que envolvem recursos tecnológicos, documentos, estruturas, ações e processos organizacionais, bem como a conformidade com leis e regulamentos externos, como previsto por Herath, Herath e Bremser (2010) e identificados na literatura por Albuquerque Junior et al. (2018) (Tabela 1).

Tabela 1
Exemplos de controles técnicos, formais e informais de segurança da informação

Tipo	Exemplos
Técnicos	Redundância de dados; Segregação de redes de computadores; Redundância de peças e equipamentos; Prevenção contra códigos maliciosos; Controle de acesso lógico; Transmissão e armazenamento seguro de dados; Autenticação forte; Redundância de equipamentos; Controle de acesso físico; Proteção ambiental
Formais	Política de segurança da informação; Comitê de segurança da informação; Regulamentos internos de segurança da informação; Processos e procedimentos de segurança da informação; Equipe de tratamento de incidentes de segurança da informação; Escritório de segurança da informação; Processo de análise e avaliação de riscos; Classificação de informações; Sistema de gestão de segurança da informação; Revisão da política de segurança da informação
Informais	Programas de treinamento de profissionais de TI; Programas de treinamento de usuários de TI; Campanhas de divulgação de regulamentos e da política de segurança da informação; Campanhas de conscientização

Fonte: adaptado de Albuquerque Junior et al. (2018).

A LGPD exige a revisão dos controles de segurança da informação nas organizações, impactando gestão, política, estrutura e tecnologia. A política de segurança da informação deve definir papéis, responsabilidades e estruturas, como comitê de segurança, equipe de tratamento de incidentes e escritório de segurança (Doherty & Fulford, 2006; Lopes, 2012; Sêmola, 2014). Assim, ela e os controles associados precisam ser ajustados conforme a LGPD, que estabelece processos e responsabilidades para proteger dados pessoais, como o encarregado de dados, que monitora a conformidade, promove conscientização, coordena incidentes e interage com a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e com os titulares dos dados (Lei n. 13.709, 2018).

Os princípios da LGPD (Lei n. 13.709, 2018) – finalidade do tratamento dos dados, livre acesso do titular aos seus dados, transparência sobre como e por quem os dados serão tratados, segurança e qualidade dos dados, não discriminação do titular em decorrência do tratamento dos dados, responsabilização de quem coleta, armazena e trata os dados, e consentimento do titular – demandam ajustes na política de segurança da informação ou a criação de uma específica para dados pessoais, mesmo sem exigência explícita na lei.

A Lei n. 13.709 (2018) impacta a análise e avaliação de riscos previstas na política de segurança da informação, como propõe Sêmola (2014), pois são atividades que devem considerar a privacidade e proteção de dados. Embora não sejam assuntos comumente relacionados a segurança da informação, a lei requer consentimento dos titulares dos dados antes da coleta, processamento ou compartilhamento e prevê sanções pelo descumprimento de seus requisitos, com impacto em políticas e processos internos.

Para cumprir a LGPD quanto ao controle de acesso e proteção dos dados pessoais, pode ser necessário que as organizações adaptem criptografia, *firewalls* e *backup*, que dependem dos profissionais de TI. Porém, esses profissionais focam mais em controles técnicos do que em conscientização, processos, políticas e regulamentos (Albuquerque Junior & Santos, 2015). Outros autores abordam a possibilidade de requisitos técnicos serem priorizados em detrimento da conformidade legal (Tikkinen-Piri, Rohunen & Markkula, 2018; Solove, 2008). Mas as organizações precisam também de profissionais de TI capacitados para a lei, apesar de haver uma carência de mão-de-obra com conhecimento a respeito da LGPD (Rocha, Fontes & Machado, 2023). Uma compreensão limitada a respeito dos impactos da lei sobre a segurança da informação pode levar à não conformidade e sanções da ANPD.

A importância de os profissionais de TI compreenderem e estarem preparados para a LGPD é observada por Rocha, Fontes e Machado (2023) e Kanagusku e Lahr (2024), enquanto Chiles, Behr, Farias e Corso (2013) já haviam destacado a conscientização e o treinamento desses profissionais para que se tenha conformidade com a lei, pois reduzem a falta de compreensão e a resistência às mudanças. Isto faz necessário promover uma abordagem que considere tanto aspectos técnicos quanto não técnicos da proteção de dados pessoais.

Cabe ressaltar que as ações de capacitação, se não forem suficientes e contínuos, podem não resultar nas mudanças comportamentais esperadas nem na cultura organizacional, apesar de provocarem uma familiaridade com as leis (Maddali, 2024; Sher, Talley, Yang & Kuo, 2017).

O alinhamento entre cultura organizacional e conformidade regulatória tem sido identificado como um dos principais desafios para implementação efetiva de normas de proteção de dados (Silva & Antunes Neto, 2023; Georgiadis & Poels, 2022). Kitiyadisai (2005) e Custers e Ursic (2016) reforçam a ideia de que a internalização dos princípios de privacidade exige medidas formais e informais, indo além da mera adequação técnica.

3 PROPOSIÇÕES E MODELO DE PESQUISA

As adequações que a LGPD impõe às organizações alcançam estrutura organizacional, processos, políticas, regulamentos e recursos tecnológicos, bem como mudanças no comportamento das pessoas que lidam com esses dados. As possíveis implicações da LGPD na segurança da informação organizacional podem ser categorizadas em três áreas principais, conforme classificação de Albuquerque Junior et al. (2018):

- Implicações Formais: incluem alterações na política de segurança da informação, nos regulamentos internos, nos processos, nas estruturas organizacionais e nos procedimentos relacionados à segurança da informação. Isso pode envolver revisões da política de segurança da informação e de regulamentos internos, mudanças nos processos de análise de riscos, criação ou mudanças nos comitês e equipes de segurança da informação, bem como a definição de responsabilidades individuais e coletivas para garantir conformidade com a LGPD.
- Implicações Técnicas: abrangem mudanças no funcionamento de dispositivos tecnológicos e a implementação de novos sistemas de segurança da informação tendo em vista os requisitos da LGPD. Isso inclui soluções de redundância de dados e de segregação e monitoramento de redes e repositórios de dados, além de mudanças em controles de acesso lógico e físico.
- Implicações Informais: envolvem ações de treinamento e conscientização de usuários e profissionais de TI da organização sobre a LGPD. Isso inclui divulgação dos requisitos da lei, mudanças nos regulamentos e políticas de segurança da informação, além de promover comportamentos éticos no tratamento de dados pessoais.

Como a LGPD trata da privacidade, que é um tema que contém interseções com a segurança da informação, e devido ao fato de a segurança da informação estar intimamente ligada à atuação dos profissionais de TI, sua compreensão quanto aos impactos da LGPD sobre a segurança da informação é relevante para o sucesso da adequação da organização aos requisitos desta lei.

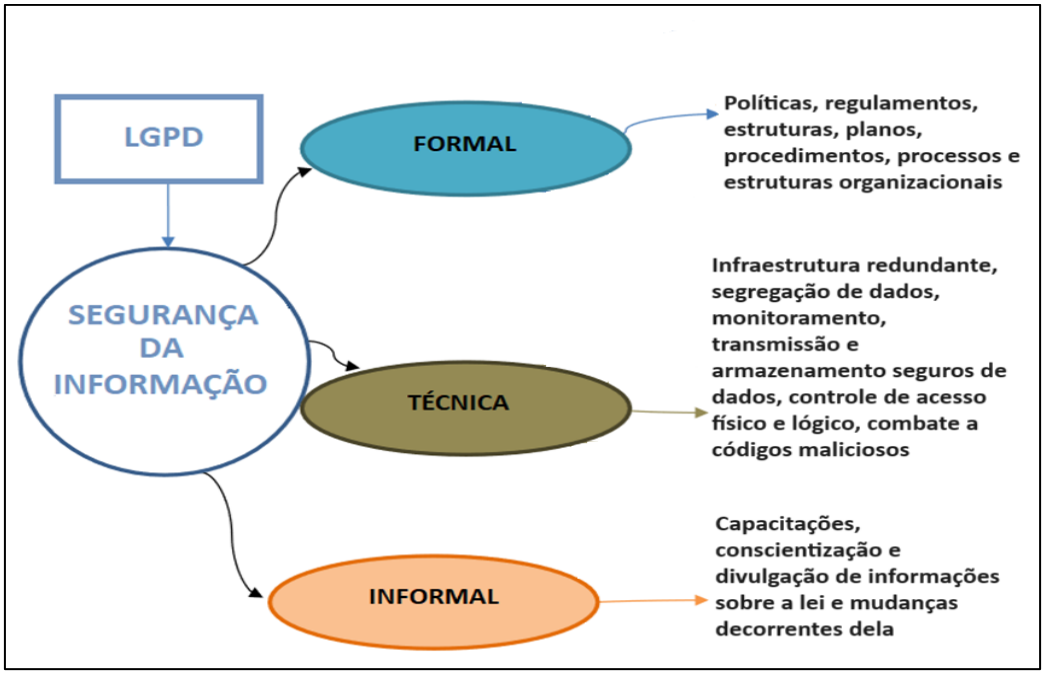
As possíveis implicações, que podem ser de ordem técnica, formal ou informal, podem exigir adequações em controles técnicos de segurança da informação existentes ou implantação de novos controles, ou mudanças na gestão, processos, procedimentos e estruturas organizacionais de TI da organização, e em mudanças nos papéis e responsabilidades dos profissionais de TI, o que pede ações de divulgação, treinamento e conscientização.

Desta forma, as proposições teóricas desta pesquisa destacam a compreensão por parte dos profissionais de TI a respeito das implicações da LGPD sobre a segurança da informação:

- Proposição 1: os profissionais de TI compreendem as necessidades de realizar adequações na tecnologia visando à conformidade aos requisitos da LGPD quanto à segurança da informação.
- Proposição 2: os profissionais de TI compreendem os impactos sobre os processos e a gestão de segurança da informação para atender às necessidades de proteção de dados pessoais segundo a LGPD.
- Proposição 3: os profissionais de TI conhecem as implicações da LGPD sobre os papéis e responsabilidades das pessoas da área de TI com relação à proteção de dados pessoais.

O modelo conceitual da pesquisa (Figura 1) apresenta a relação entre a LGPD, a segurança da informação e os impactos formais, informais e técnicos. A dimensão Formal inclui as alterações nos controles formais, que incluem políticas, regulamentos, estruturas, planos, procedimentos e processos organizacionais para operacionalizar as atividades relacionadas à LGPD. Na dimensão Técnica, estão as mudanças nos controles técnicos, incluindo redundância na infraestrutura tecnológica, segregação de dados sensíveis, implementação de *firewalls*, além de recursos para realização de *backup* e recuperação de dados. Já na dimensão Informal estão ações de treinamento e conscientização, campanhas de divulgação e práticas educacionais para promover o conhecimento e comportamentos conforme os requisitos da lei.

Figura 1
Modelo conceitual da pesquisa



Com base na bibliografia consultada, no modelo conceitual e nas proposições da pesquisa, foi elaborado o quadro analítico (Tabela 2) utilizado para operacionalizar o estudo, com os indicadores associados às dimensões da pesquisa, o que permitiu elaborar o instrumento de coleta dos dados.

Tabela 2
Tabela analítica da pesquisa

Dimensão	Indicadores
Técnica	RD – Redundância de ativos de TI para atender à necessidade de disponibilidade dos dados; SM – Segregação e monitoramento de redes e repositórios para garantir confidencialidade e integridade dos dados; CA – Aplicação de controles de acesso em recursos de TI e ambientes físicos para proteção dos dados; TA – Tecnologias aplicadas a transmissão e armazenamento seguros de dados; PC – Tecnologias voltadas para combate a códigos maliciosos.
Formal	RP – Responsabilidades para tratamento de dados pessoais formalmente definidas; EO – Alterações nas estruturas organizacionais para adequação à LGPD; PS – Inclusão de diretrizes ou criação de política de segurança da informação para adequação à LGPD; PP – Alterações e criação de planos, procedimentos e processos de segurança da informação para atender à LGPD; CM – Participação de equipes multidisciplinares no atendimento aos requisitos da LGPD.
Informal	TR – Realização de capacitações sobre LGPD e proteção de dados; CN – Ações voltadas para conscientização sobre LGPD e proteção de dados; DV – Ações de divulgação de informações sobre LGPD e planos, políticas, regulamentos e mudanças decorrentes da implantação dos seus requisitos.

Assim, na dimensão Técnica há o indicador *RD – Redundância de ativos de TI para atender à necessidade de disponibilidade dos dados*, voltado para a identificação de *hardware* e *software* voltados para garantir a disponibilidade desses dados, e o indicador *SM – Segregação e monitoramento de redes e repositórios para garantir confidencialidade e integridade dos dados*, para identificar a separação entre recursos voltados para processos e operações que não envolvem dados pessoais daqueles que envolvem. Tem também o

indicador *CA – Aplicação de controles de acesso em recursos de TI e ambientes físicos para proteção dos dados*, para identificar evidências de uso de recursos para controle de acesso físico e lógico de pessoas que lidam com dados pessoais, e *TA – Tecnologias aplicadas a transmissão e armazenamento seguros de dados*, que visa à identificação da aplicação de tecnologias voltadas para o sigilo de dados em transmissão ou armazenados. E tem o indicador *PC – Tecnologias voltadas para combate a códigos maliciosos*, para identificar soluções para proteger os dados contra códigos maliciosos.

A dimensão Formal tem cinco indicadores: *RP – Responsabilidades para tratamento de dados pessoais formalmente definidas*, que trata da formalização das responsabilidades para tratamento de dados pessoais na organização; *EO – Alterações em estruturas organizacionais para adequação à LGPD*, para identificar estruturas organizacionais alteradas em função de exigências da LGPD; *PS – Inclusão de diretrizes ou criação de política de segurança da informação para adequação à LGPD*, que trata da criação ou de alterações na política de segurança da informação; *PP – Alterações e criação de planos, procedimentos e processos de segurança da informação para atender à LGPD*, que indica a criação ou alteração de planos, processos e procedimentos para atender à lei; e *CM – Participação de equipes multidisciplinares no atendimento aos requisitos da LGPD* para identificar grupos multidisciplinares criados ou que receberam a responsabilidade para tratar da LGPD e seus requisitos na organização.

Já a dimensão Informal tem o indicador *TR – Realização de capacitações sobre LGPD e proteção de dados*, para identificar ocorrência de treinamentos sobre LGPD na organização, o indicador *DV – Ações de divulgação de informações sobre LGPD e planos, políticas, regulamentos e mudanças decorrentes da implantação dos seus requisitos*, para identificar ações de divulgação relacionadas à LGPD, e o indicador *CN – Ações voltadas para conscientização sobre LGPD e proteção de dados*, que permite identificar se houve na organização ações de conscientização das pessoas sobre a lei.

4 METODOLOGIA

Este estudo de caso descritivo utiliza múltiplos métodos de pesquisa para estudar o comportamento de uma organização com base em dados secundários obtidos em um levantamento realizado anteriormente e em dados coletados em um grupo focal realizado durante o desenvolvimento desta pesquisa. Com isto, trata-se de um estudo de métodos mistos com desenho explicativo sequencial (Creswell & Plano Clark, 2013), pois os dados quantitativos foram utilizados para embasar e aprofundar a discussão qualitativa posterior, ainda que o levantamento não tenha sido realizado especificamente para atender a este estudo. A integração dos dados foi feita durante a interpretação dos dados qualitativos.

Para a fundamentação teórica, foi realizada uma pesquisa bibliográfica em artigos, livros, teses e dissertações de diferentes bases de dados, incluindo Scielo, Portal de Periódicos CAPES, Spell, Google Scholar e Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), além de periódicos e anais de eventos científicos principalmente das áreas de Administração, Tecnologia da Informação e Ciência da Informação.

Os dados quantitativos foram coletados durante o ano de 2021 através de um levantamento *online* realizado por uma organização que atua em todos os estados brasileiros no ramo da educação profissional. A organização estava passando por um processo de adequação de seus processos internos tendo em vista a conformidade com a LGPD, o que a qualificou para a utilização dos seus dados nesta pesquisa.

Como o levantamento não teve como finalidade obter dados para esta pesquisa, o formulário utilizado incluía questões que não serviam à finalidade do estudo ora apresentado. Assim, embora o formulário utilizado no levantamento tivesse 23 perguntas, 13 delas exploravam temas organizacionais mais amplos que, embora relevantes para um projeto maior, extrapolavam o escopo desta pesquisa. Foram mantidas, portanto, apenas as 10 perguntas diretamente alinhadas às dimensões e indicadores apresentados no Quadro 2, garantindo foco e coerência com os objetivos do estudo.

Participaram do levantamento 64 profissionais de TI de 70 possíveis respondentes (91,4%), incluindo diretores, gerentes, coordenadores e analistas que atuaram em questões estratégicas de TI, o que inclui a adequação da organização aos requisitos da LGPD. Os dados referentes às respostas dadas para as 10 perguntas consideradas foram analisados utilizando o programa *Statistical Package for Social Sciences* (SPSS) versão 20.

As 10 perguntas estavam organizadas em quatro blocos temáticos no formulário utilizado no levantamento, que foram mantidos para fins de análise dos dados. O Bloco I, com cinco perguntas, buscava informações sobre o respondente: sexo, idade, função que exerce e tempo de experiência profissional, além do conhecimento que o respondente julga ter sobre a LGPD. Todas as perguntas do bloco foram de múltipla escolha, exceto a última, que tinha uma escala de três pontos (1-Baixo conhecimento; 2-Médio conhecimento; 3-Alto conhecimento).

Do Bloco II, foram mantidas duas perguntas sobre o quanto os respondentes compreendem a necessidade de adequação tecnológica da organização aos requisitos da LGPD, o que está relacionado à dimensão Técnica. A primeira pergunta questionava o quanto o respondente compreendia a necessidade de atualização dos recursos tecnológicos de segurança da informação. As respostas constavam em uma escala de cinco pontos (1 – Nenhuma compreensão; 2 – Pouca compreensão; 3 – Compreensão razoável; 4 – Muita compreensão; 5 – Plena compreensão). A segunda pergunta questionava como o respondente entende estar atualizada a infraestrutura de TI quanto à LGPD, e as respostas estavam em uma escala de três pontos (1 – Não atende; 2 – Atende parcialmente; 3 – Atende plenamente).

Do Bloco III, foi utilizada apenas uma pergunta do formulário, sobre o impacto na dimensão Informal da segurança da informação: “Como você avalia o impacto das ações de treinamento e divulgação sobre segurança da informação no contexto da LGPD na cultura organizacional?” As respostas estavam em uma escala de três pontos (1 – Impacto baixo, não participou ou não sabe responder; 2 – Impacto médio; 3 – Impacto alto).

O Bloco IV abordava os impactos das exigências da LGPD na dimensão Formal e teve duas perguntas analisadas neste estudo. A primeira questionou o quanto as diretrizes da política de segurança da informação estão adequadas às exigências da LGPD, e as respostas estavam em uma escala de três pontos (1 – Baixa adequação; 2 – Média adequação; 3 – Plena adequação). A segunda tratou da percepção sobre a adequação das normas e procedimentos internos de segurança da informação à LGPD. As respostas também estavam em uma escala de três pontos (1 – Baixa adequação; 2 – Média adequação; 3 – Plena adequação).

A coleta de dados qualitativos ocorreu em um grupo focal realizado com gestores de TI da organização. Foram convidados a participar 16 pessoas, entre gerentes, coordenadores e diretores com experiência e envolvimento nas ações e mudanças envolvendo a LGPD na organização, dos quais sete confirmaram a participação e receberam por correio eletrônico os dados do levantamento quantitativo. O roteiro de discussão foi elaborado com base nos resultados da análise dos dados quantitativos.

Como a pesquisa foi desenvolvida durante o período de isolamento social da pandemia de Covid-19, a reunião do grupo focal aconteceu remotamente, utilizando o programa *Microsoft Teams*, o que permitiu sua gravação para análise posterior, tendo sido moderado pelo anfitrião. A reunião seguiu orientações de Morgan (2010) e Krueger e Casey (2015), iniciando com a apresentação dos resultados descritivos do levantamento realizado junto aos profissionais de TI da organização, com o intuito de fomentar o diálogo entre os participantes.

Os dados qualitativos obtidos com o grupo focal foram analisados conforme recomendam Iervolino e Pelicione (2001) para análise de conteúdo por codificação temática e sumário etnográfico, o que permitiu a análise dos assuntos relacionados à compreensão da LGPD e seus impactos na segurança da informação. A análise foi guiada pelas categorias analíticas apresentadas no Quadro 2. A integração dos dados qualitativos e quantitativos foi conduzida por meio de exibição conjunta, através da comparação entre os dados obtidos nas duas abordagens metodológicas para cada dimensão analisada.

5 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Os dados do levantamento mostram que, dos 64 participantes, 70% são homens, 37% tinham entre 46 e 55 anos à época em que foi realizada a pesquisa, enquanto 28% tinham entre 36 e 45 anos, 22% tinham 26 e 35 anos, e 13% tinham mais que 55 anos. Desse total, 44% atuavam como gerentes, 31% como analistas de sistemas, 14% como diretores, e 11% como coordenadores de TI. Apenas 13% dos respondentes tinham entre 16 e 20 anos de experiência profissional, enquanto 19% tinham entre 1 e 5 anos, 19% entre 11 e 15 anos, 16% tinham entre 6 e 10 anos, e 33% com mais de 20 anos. Os dados estão na Tabela 3.

Tabela 3
Dados dos participantes

Faixa etária (anos)	%
26 – 35	22
36 – 45	28
46 – 55	37
Mais de 55	13
Gênero	**%**
Masculino	70
Feminino	30
Função	**%**
Analista de sistemas	31
Gerente	44
Coordenador	11
Diretor	14
Experiência profissional (anos)	**%**
1 – 5	19
6 – 10	16
11 – 15	19
16 – 20	13
Mais de 20	33

A análise dos dados quantitativos mostrou que 45% dos respondentes consideraram ter pouco conhecimento sobre a LGPD, enquanto 11% declararam ter pleno conhecimento (Tabela 4). Esse resultado já sinaliza a necessidade de a organização intensificar ações de conscientização e treinamento para aumentar a compreensão interna sobre a lei e reduzir a resistência às mudanças necessárias, como observam Chiles et al. (2013).

Tabela 4
Conhecimento dos profissionais de TI sobre LGPD

Nível de conhecimento autodeclarado	%
Alto conhecimento	11
Médio conhecimento	44
Baixo conhecimento	45

Nas respostas relativas à dimensão Informal, 59% dos participantes avaliaram o impacto das ações de treinamento e divulgação sobre segurança da informação na LGPD como alto, e 38% como médio em resposta à pergunta "Como você avalia o impacto das ações de treinamento e divulgação sobre segurança da informação no contexto da LGPD na cultura organizacional?". Esses resultados refletem a aceitação das mudanças tecnológicas e organizacionais necessárias para a conformidade com a lei.

Na dimensão Formal, os dados indicam a necessidade de ajustes nas normas, procedimentos e política de segurança da informação. Na pergunta "O quanto as diretrizes da política de segurança da informação da organização estão adequadas às exigências da LGPD?", 50% consideram a adequação baixa e 41%, média. Na pergunta "Como percebem a adequação das normas e procedimentos internos de segurança da informação à LGPD?", 54% apontam baixa adequação e 44%, média. Os resultados reforçam a importância de fazer revisões na política e nos regulamentos de segurança da informação, já que orientam as demais ações.

Já na dimensão Técnica, 53% declaram compreender a necessidade de atualizar os recursos tecnológicos de segurança da informação, considerando aqueles que responderam ter plena compreensão e muita compreensão. Para 60%, a infraestrutura existente atende plenamente à LGPD, enquanto 39% acreditam que atende parcialmente, indicando a necessidade de mudanças, como atualização de *hardware*, *software* e redundância de dados. Os resultados mostram que a organização investiu na adequação da infraestrutura e em ações de conscientização, embora muitos profissionais afirmem não conhecer a lei o suficiente. Os esforços sobre política, procedimentos e processos internos foram considerados limitados, evidenciando a necessidade de ajustes em controles formais, que orientam normas, estruturas organizacionais e demais controles técnicos e informais. A Tabela 5 traz os dados quantitativos referentes às perguntas relacionadas às dimensões de análise do estudo.

Tabela 5
Dados quantitativos

Impacto das ações de treinamento e divulgação sobre LGPD	%
Impacto alto	59
Impacto médio	38
Impacto baixo, não participou ou não sabe responder	3
Adequação das diretrizes da política de segurança da informação à LGPD	**%**
Alta adequação	9
Média adequação	41
Baixa adequação	50
Adequação das normas e procedimentos internos de segurança da informação à LGPD	**%**
Alta adequação	2
Média adequação	44
Baixa adequação	54
Compreensão sobre a necessidade de atualizar recursos tecnológicos de segurança da informação	**%**
Plena compreensão	8
Muita compreensão	45

Compreensão razoável	42
Pouca compreensão	3
Nenhuma compreensão	2
Atualização da infraestrutura de TI existente quanto à LGPD	%
Atende plenamente	60
Atende parcialmente	39
Não atende	1

Os participantes do grupo focal (chamados de Gestor 1, Gestor 2, Gestor 3, Gestor 4, Gestor 5, Gestor 6 e Gestor 7) são seis homens e uma mulher da área de TI da organização, sendo quatro gerentes, dois diretores e um coordenador. Três participantes tinham entre 36 e 45 anos de idade, três tinham entre 46 e 55 anos, e um tinha mais de 55 anos à época da pesquisa. Um dos participantes tinha entre um e cinco anos de experiência, três tinham entre 16 e 20 anos, e três tinham mais de 20 anos na área de TI.

O moderador questionou inicialmente aos gestores participantes do grupo focal se os resultados do levantamento refletem a realidade daquele momento de adequação dos controles internos pelo qual a organização estava passando, e todos declararam entender que sim. Após serem questionados a respeito da sua participação em treinamentos sobre a LGPD, todos confirmaram ter participado e três acrescentaram ainda estarem estudando para aumentar a conformidade da organização, demonstrando a necessidade de mudanças em controles das dimensões Formal e Informal, enquadradas nos indicadores *PP – Alterações e criação de planos, procedimentos e processos de segurança da informação para atender à LGPD* e *TR – Realização de capacitações sobre LGPD e proteção de dados*.

Sobre os processos da organização, o Gestor 1 citou que os problemas de adequação são resultantes da autonomia das subunidades descentralizadas, pois a gestão central de TI não pode exigir mudanças nos processos descentralizados para atender aos requisitos da lei. O gestor acrescentou que foi criado um comitê multidisciplinar para tratar das adequações técnicas em toda a organização, pois as atividades atingem todas as áreas e isto pede uma abordagem multidisciplinar, sendo uma evidência do indicador *CM – Participação de equipes multidisciplinares no atendimento aos requisitos da LGPD*. Outra evidência deste indicador foi trazida pelo Gestor 7, que referiu ser necessário que todas as subunidades descentralizadas da organização criem "comitês multidisciplinares para tratar de segurança da informação, privacidade e conformidade com a LGPD" no âmbito local.

Foi citada pelo Gestor 1 a criação de um escritório permanente cujo responsável exercerá as atividades de encarregado de proteção de dados pessoais, e que funcionará como o comitê de privacidade e proteção de dados. Essas evidências estão relacionadas aos indicadores *RP – Responsabilidades para tratamento de dados pessoais formalmente definidas* e *EO – Alterações nas estruturas organizacionais para adequação à LGPD*.

O Gestor 2 destacou que, apesar de haver um encarregado de proteção de dados, a organização não possui um responsável pelo controle de acesso e pode precisar de um em cada subunidade devido à descentralização da organização, alinhando-se ao indicador *RP – Responsabilidades para tratamento de dados pessoais formalmente definidas*. O Gestor 4 enfatizou a importância de definir essa responsabilidade e criar um comitê geral para a LGPD, pois a lei impacta todas as áreas da organização. O Gestor 3 ressaltou a necessidade de dedicação dos profissionais de TI à conformidade, reforçando esse indicador na dimensão Formal. O Gestor 1 apontou a urgência de identificar e classificar os processos que utilizam dados pessoais conforme prioridade e risco, evidenciando o indicador *PP – Alterações e*

criação de planos, procedimentos e processos de segurança da informação para atender à LGPD.

O Gestor 7 acrescentou que foram criados na sua subunidade grupos de trabalho para mapeamento de processos e riscos, revisão de permissões de acessos, contratos, política de segurança, procedimentos e regulamentos internos de privacidade, ações associadas a *PS – Inclusão de diretrizes ou criação de política de segurança da informação para adequação à LGPD*, e *PP – Alterações e criação de planos, procedimentos e processos de segurança da informação para atender à LGPD*.

Ao falar do desenvolvimento do sistema *Enterprise Resource Planning* (ERP) para a organização, o Gestor 2 citou a necessidade de autorização para tratamento de dados para que os profissionais de TI possam trabalhar, o que está relacionado ao indicador *PP – Alterações e criação de planos, procedimentos e processos de segurança da informação para atender à LGPD*, para definir como será a obtenção da autorização para os profissionais de TI lidarem com os dados, e *RP – Responsabilidades para tratamento de dados pessoais formalmente definidas*, ambos da dimensão Formal.

O Gestor 4 citou a criação e divulgação de uma cartilha sobre a LGPD e a realização de eventos envolvendo diferentes áreas para aumentar a aceitação interna das mudanças que precisam ser realizadas, o que está relacionado ao indicador *DV – Ações de divulgação de informações sobre LGPD e planos, políticas, regulamentos e mudanças decorrentes da implantação dos seus requisitos*. Nas suas palavras, "a mudança da cultura organizacional só é obtida com esclarecimentos e ações de conscientização, divulgação e treinamento" – evidências dos indicadores *CN – Ações voltadas para conscientização sobre LGPD e proteção de dados* e *TR – Realização de capacitações sobre LGPD e proteção de dados*. O Gestor 1 acrescentou ser necessário capacitar os membros da área de TI e de outras áreas que lidam com dados pessoais, reforçando este último indicador da dimensão Informal.

Evidências deste último indicador também foram identificadas nas falas de outros participantes. O processo de desenvolvimento do ERP, como citado pelo Gestor 2, envolve a autorização para tratamento de dados, o que implica na necessidade de profissionais de TI conhecerem as exigências legais e de serem capacitados para a LGPD. O Gestor 3 concordou sobre isto, pois entende que ainda há problemas de conformidade a serem resolvidos e isto depende da capacitação das pessoas.

Comentando sobre o desafio de "garantir a segurança da informação com o compartilhamento dos dados, que perpassam por diferentes setores e processos organizacionais" durante o desenvolvimento de sistemas, o Gestor 2 entende ser necessário implantar "listas de controle de acesso e criptografia para transmissão e armazenamento de dados pessoais", o que traz implicações da dimensão Técnica relativas a *SM – Segregação e monitoramento de redes e repositórios para garantir confidencialidade e integridade dos dados*, *CA – Aplicação de controles de acesso em recursos de TI e ambientes físicos para proteção dos dados*, e *TA – Tecnologias aplicadas a transmissão e armazenamento seguros de dados*, pois envolvem o uso de criptografia, listas de controle de acesso, *firewall* e *software* de monitoramento.

O moderador questionou ao grupo se é possível haver um responsável por controlar os acessos aos dados pessoais em um sistema ERP, pois, ainda que as medidas necessárias de segurança da informação tenham sido implementadas, é possível que câmeras capturem os dados. O Gestor 2 respondeu que há controle de acesso físico e segregação de dados no sistema para reduzir o impacto de um incidente como esse, o que está relacionado aos indicadores *SM – Segregação e monitoramento de redes e repositórios para garantir*

confidencialidade e integridade dos dados e *CA – Aplicação de controles de acesso em recursos de TI e ambientes físicos para proteção dos dados*, ambos da dimensão Técnica.

A conscientização e o papel da TI foram abordados pelo Gestor 5, para quem o sucesso da adequação dos controles de segurança da informação não está na TI, mas nas ações de conscientização, relacionadas ao indicador *CN – Ações voltadas para conscientização sobre LGPD e proteção de dados*. Para o gestor, uma consultoria pode avaliar processos, normas, regulamentos e política de segurança da informação a fim de identificar o que será impactado pela lei e quais são as alterações necessárias, que, no caso, podem estar relacionadas à dimensão Formal, pois aponta para os indicadores *PS – Inclusão de diretrizes ou criação de política de segurança da informação para adequação à LGPD* e *PP – Alterações e criação de planos, procedimentos e processos de segurança da informação para atender à LGPD*.

Foi citada pelo Gestor 3 a hipótese de um titular de dados revogar o termo de consentimento, o que mostra implicações dos requisitos da lei sobre processos, procedimentos e política organizacional de segurança da informação e tratamento de dados, relacionadas aos indicadores *RP – Responsabilidades para tratamento de dados pessoais formalmente definidas*, *PS – Inclusão de diretrizes ou criação de política de segurança da informação para adequação à LGPD* e *PP – Alterações e criação de planos, procedimentos e processos de segurança da informação para atender à LGPD* da dimensão Formal.

As implicações da LGPD sobre controles formais foram comentadas também pelo Gestor 6, cuja fala aponta para os dois últimos indicadores citados anteriormente e a *EO – Alterações nas estruturas organizacionais para adequação à LGPD*. Este participante falou ainda da falta de conhecimento declarada pelos profissionais de TI sobre a lei, ressaltando a necessidade de divulgar as ações da organização, conscientizar o público interno e capacitar os profissionais – implicações relacionadas aos três indicadores da dimensão Informal: *TR – Realização de capacitações sobre LGPD e proteção de dados*, *CN – Ações voltadas para conscientização sobre LGPD e proteção de dados*, e *DV – Ações de divulgação de informações sobre LGPD e planos, políticas, regulamentos e mudanças decorrentes da implantação dos seus requisitos*.

Provocados pelo moderador, os participantes do grupo focal discutiram o impacto da LGPD nos processos que envolvem dados pessoais. Todos os gestores concordaram que a organização deve elaborar um relatório de impacto, conforme a lei, para mapear nesses processos os riscos à privacidade, destacando o indicador *PP – Alterações e criação de planos, procedimentos e processos de segurança da informação para atender à LGPD*. Eles também concordaram que os controles técnicos para mitigar esses riscos incluem sistemas criptografados e repositórios redundantes, alinhados aos indicadores *RD – Redundância de ativos de TI para atender à necessidade de disponibilidade dos dados* e *TA – Tecnologias aplicadas à transmissão e armazenamento seguros de dados*, recursos que os participantes dizem que já existem na organização, mas precisam de adequações.

O Gestor 3 tratou do desrespeito à LGPD e suas consequências, explicando que as penalidades aplicadas pela ANPD podem ir além do prejuízo financeiro e proibir a utilização de um banco de dados se os controles de acesso não forem aplicados, e isto pode pôr em risco as operações organizacionais, uma situação relacionada a um indicador da dimensão Técnica (*CA – Aplicação de controles de acesso em recursos de TI e ambientes físicos para proteção dos dados*), uma implicação da lei em controles técnicos, com o que o Gestor 6 concordou.

No entanto, o Gestor 3 acrescentou que falhas na proteção dos dados pessoais podem levar a penalidades para a organização, mas que essas falhas podem ocorrer inclusive em organizações parceiras: “contratos que envolvem compartilhamento de dados precisam de

cláusulas claras e específicas sobre tratamento de dados pessoais", pois os incidentes nessas parceiras podem levar às penalidades também. A situação apresentada está relacionada ao indicador *RP – Responsabilidades para tratamento de dados pessoais formalmente definidas*, pois os contratos, no entendimento do gestor, devem prever deveres e responsabilidades de ambas as partes sobre os dados pessoais. Está relacionada também à revisão dos processos e procedimentos de contratação, evidência do indicador *PP – Alterações e criação de planos, procedimentos e processos de segurança da informação para atender à LGPD*.

Por fim, o Gestor 3 acrescentou que um incidente em uma subunidade regional pode ser decorrente de falhas em procedimentos, processos, equipamentos ou *softwares*, o que leva a implicações relacionadas mais uma vez ao indicador *PP – Alterações e criação de planos, procedimentos e processos de segurança da informação para atender à LGPD*, e também a *SM – Segregação e monitoramento de redes e repositórios para garantir confidencialidade e integridade dos dados* e *TA – Tecnologias aplicadas a transmissão e armazenamento seguros de dados*, e que "pode prejudicar a continuidade das operações em toda a organização", ensejando adequações no plano organizacional de continuidade do negócio.

A dimensão Técnica mostrou 60 % dos respondentes afirmando que a infraestrutura já atende à LGPD; no grupo focal, gestores reconheceram a adequação da tecnologia, mas salientaram a necessidade de controle de acesso. Esta convergência sugere que a percepção de suficiência técnica coexiste com lacunas específicas de configuração.

Na dimensão Informal, o impacto atribuído aos treinamentos (59 %) contrasta com declarações de baixo conhecimento sobre a lei (45 %), revelando uma primeira impressão positiva, mas o simples fato de a organização ter oferecido treinamentos não significa que os conteúdos tenham sido assimilados ou que tenham sido suficientes, apesar de ser uma necessidade reconhecida por Rocha et al. (2023). Outros estudos, como os de Maddali (2024) e de Sher et al. (2017) reforçam que treinamentos pontuais podem produzir apenas familiaridade superficial com as leis, sendo pouco efetivos se não forem contínuos, aplicados e mensurados com base em resultados comportamentais.

Esses resultados mostram também um descompasso entre a suficiência técnica e necessidade de promover o conhecimento sobre a lei, o que já foi observado em estudos sobre leis de proteção de dados pessoais. Isto pode significar que os profissionais superestimam a conformidade técnica sem dominar os requisitos legais, como descrito na literatura (Tikkinen-Piri et al., 2018; Solove, 2008).

Na dimensão Formal, observam-se divergências relevantes: enquanto a maioria dos respondentes indica baixa adequação das políticas, os gestores relatam a criação de comitês e cartilhas, sinalizando uma fase de transição institucional rumo à conformidade com a LGPD. Alguns sugerem ainda a necessidade de comitês locais específicos para tratar da privacidade.

Os achados do levantamento orientaram o grupo focal, que trouxe tópicos não capturados pelo questionário. A Tabela 6 traz resultados de ambos os conjuntos de evidências. Embora a maioria declare que a infraestrutura de TI está de acordo com a LGPD, parcela expressiva admite conhecimento limitado da lei, o que é reforçado pelos gestores e que compromete essa avaliação que fizeram sobre a adequação da tecnologia. A percepção de suficiência tecnológica pode ocultar necessidades de atualizações e ajustes em controles técnicos de segurança da informação, e os treinamentos oferecidos ainda não se converteram em domínio normativo nem em atualização efetiva de políticas e procedimentos.

Os dados mostram também que a organização tem necessidades diversas, como criação de comitês e ações de conscientização e capacitação, que devem vir acompanhados

de uma revisão normativa, além de descentralização de parte das responsabilidades. Treinamentos precisam migrar de eventos pontuais para programas continuados e avaliáveis.

Os resultados evidenciam todos os indicadores das dimensões Informal e Formal, além de quatro da dimensão Técnica, com exceção de *PC – Tecnologias voltadas para combate a códigos maliciosos*. Apesar da aptidão técnica da organização, a conformidade com a LGPD ainda exige ações contínuas de capacitação e revisão dos controles formais, incluindo estrutura organizacional e política de segurança da informação.

Embora a criação de comitês e a elaboração de normas e materiais de conscientização e divulgação, como cartilhas e regulamentos, tenham sido apontadas pelos gestores como medidas relevantes para a conformidade com a LGPD, é necessário considerar sua viabilidade e impacto efetivo. A implementação de comitês requer recursos, definição clara de responsabilidades, engajamento institucional e integração entre subunidades, especialmente em contextos organizacionais descentralizados. Já os materiais de conscientização e educação, para além da sua existência formal, devem ser atualizados, acessíveis e incorporados às rotinas dos profissionais, o que depende de estratégias contínuas de sensibilização e uso efetivo. Sem mecanismos de acompanhamento, essas iniciativas correm o risco de se tornarem ações simbólicas, com baixo alcance prático. Portanto, a eficácia dessas medidas depende da articulação entre estrutura, cultura organizacional e estratégias de gestão da mudança, reforçando a necessidade de avaliações sistemáticas sobre seu impacto.

Tabela 6
Comparação entre os elementos presentes nos dados qualitativos e quantitativos

Gestor	Dados qualitativos	Dados quantitativos
Gestor 1	Reconhece a atualização da infraestrutura tecnológica; Percebe a necessidade de revisar processos e políticas; Menciona necessidade de comitês e escritórios; Trata da autonomia das subunidades e a dificulta a padronização de processos; Trata da necessidade de capacitação.	60% entendem que a infraestrutura é adequada; 50% entendem que a política de segurança da informação é pouco adequada; 45% dos profissionais de TI declaram pouco conhecimento sobre a lei.
Gestor 2	Reconhece a qualidade da infraestrutura tecnológica; Menciona a necessidade de responsáveis pelo controle de acesso em cada subunidade; Destaca que a descentralização exige maior formalização; Trata da formalização da autorização para profissionais de desenvolvimento trabalharem com os dados.	60% entendem que a infraestrutura é adequada; 53% compreendem a necessidade de atualizar recursos tecnológicos; 98% entendem que normas e procedimentos têm média ou baixa adequação.
Gestor 3	Destaca que muitos profissionais não conhecem a lei; Entende que falhas podem levar a sanções da ANPD; Ressalta a necessidade de capacitação; Trata da importância de contratos com terceiros abordarem a proteção de dados pessoais; Necessidade de classificar os processos conforme o risco à privacidade.	45% dos profissionais de TI declaram ter pouco conhecimento sobre a lei; 98% entendem que normas e procedimentos têm média ou baixa adequação.
Gestor 4	Defende a necessidade de ações de conscientização e educação.	59% percebem como alto o impacto das ações de treinamento e divulgação;

		38% percebem esse impacto como médio.
Gestor 5	Reforça a necessidade de ações de conscientização; Sugere a contratação de consultoria externa para mapear processos e normas.	45% dos profissionais de TI declaram ter pouco conhecimento sobre a lei; 59% percebem como alto o impacto das ações de treinamento e divulgação; 98% entendem que normas e procedimentos têm média ou baixa adequação.
Gestor 6	Destaca a falta de conhecimento declarada pelos profissionais de TI; Defende ações de conscientização; Sugere a criação de estruturas organizacionais específicas para tratar de privacidade.	45% dos profissionais de TI declaram ter pouco conhecimento sobre a lei; 59% percebem como alto o impacto das ações de treinamento e divulgação.
Gestor 7	Aborda a criação de comitês e grupos para revisar processos, políticas e acessos; Sugere a formação de grupos de trabalho locais para mapear processos, riscos e permissões de acesso; Sugere a criação de comitês de privacidade locais nas subunidades	50% entendem que a política de segurança da informação é pouco adequada; 98% entendem que normas e procedimentos têm média ou baixa adequação.

5.1 DISCUSSÃO DAS PROPOSIÇÕES DA PESQUISA

Os resultados da pesquisa apontam que os profissionais de TI da organização compreendem as implicações dos requisitos da LGPD sobre a segurança da informação da organização, principalmente sobre a política, processos e procedimentos, além de papéis e responsabilidades quanto à proteção de dados pessoais.

Os participantes entendem que a infraestrutura tecnológica está atualizada devido aos investimentos feitos em segurança da informação, mas ainda há necessidade de adequações na tecnologia para que a organização fique em conformidade. Também os gestores não falam em desatualização tecnológica ou necessidade investimentos nessa área, corroborando com os dados do levantamento, o que dá sustentação empírica à Proposição 1: “os profissionais de TI compreendem as necessidades de realizar adequações na tecnologia visando à conformidade aos requisitos da LGPD quanto à segurança da informação”, o que pode ser explicado pelo foco técnico dos profissionais de TI (Albuquerque Junior & Santos, 2015).

Os resultados mostram que os participantes percebem que a LGPD impôs à organização a necessidade de realizar ações de conscientização, divulgação e principalmente de capacitação, que precisa ser reforçada junto aos profissionais de TI – uma necessidade observada tanto nos dados quantitativos quanto nos qualitativos. A falta de conhecimento dos profissionais de TI sobre a lei pode afetar não só a adequação dos controles técnicos, mas também dos processos que envolvem tratamento de dados pessoais com os quais lidam.

As obrigações trazidas pela LGPD têm ainda implicações em diferentes controles formais. Gestores e profissionais de TI percebem que controles formais estão inadequados às exigências da LGPD, ainda que mudanças já tenham ocorrido, como a criação de comitês e grupos multidisciplinares, pois a lei exige ajustes também na política de segurança da informação para incluir definições referentes à proteção de dados pessoais e aos princípios da lei, além novos papéis e responsabilidades. Como a política orienta a adoção de outros controles (Lopes, 2012; Sêmola, 2014), estruturas organizacionais, processos e procedimentos precisarão ser atualizados ou criados para refletir os requisitos da lei, inclusive para desenvolvimento de sistemas, contratos e acordos com outras organizações, e o atendimento às demandas dos titulares dos dados pessoais. Assim, os dados dão sustentação empírica à

proposição 2: “os profissionais de TI compreendem os impactos sobre os processos e a gestão de segurança da informação para atender às necessidades de proteção de dados pessoais segundo a LGPD”; e à proposição 3: “os profissionais de TI conhecem as implicações da LGPD sobre os papéis e responsabilidades das pessoas da área de TI com relação à proteção de dados pessoais”.

5.2 SÍNTESE DOS ACHADOS

Os dados evidenciam uma organização cuja capacidade tecnológica declarada contrasta com a necessidade de ajustes nas políticas, normas, estruturas e no conhecimento das pessoas que lidam com dados pessoais. Embora 60% dos respondentes considerem a infraestrutura aderente à LGPD e 59% avaliem como elevado o impacto dos treinamentos, 45% admitem ter baixo conhecimento da lei. Há necessidades de adequação em controle de acesso e criptografia, além de políticas e normas que são avaliadas como inadequadas para atender aos requisitos da lei. A criação de comitês e escritórios para tratar de privacidade e a divulgação de cartilhas de divulgação e conscientização, embora relevantes precisam ser operacionalizados considerando escopo, necessidade de recursos, integração entre subunidades descentralizadas e métricas de desempenho. O monitoramento dessas ações é importante para mitigar o risco de se tornarem meramente simbólicos, incapazes de produzir uma mudança comportamental na organização. Enfim, é necessário transformar treinamentos pontuais em programas contínuos e que possam ser avaliados, bem como alinhar a infraestrutura tecnológica a políticas e processos organizacionais. A convergência entre infraestrutura, governança normativa e cultura organizacional poderá assegurar a adesão da organização à LGPD.

Observando-se as três dimensões de análise, emergem diferentes impactos da lei sobre a segurança da informação. Na dimensão Técnica, a percepção de suficiência tecnológica coexiste com necessidades relacionadas a procedimentos. Na dimensão Formal, a baixa adequação das políticas e normas revela que a governança documental não acompanhou a modernização tecnológica, apesar da criação de comitês e escritórios voltados para a proteção de dados pessoais. Já a dimensão Informal mostra que treinamentos são avaliados como impactantes, mas o autodeclarado desconhecimento da LGPD por parte dos profissionais de TI demonstra que a transferência de conhecimento não ocorreu de forma efetiva. Essa assimetria sugere que, sem revisões normativas e programas educacionais permanentes, os controles técnicos operam em um vácuo regulatório e cultural, comprometendo a efetividade da conformidade organizacional.

Além de dar sustentação empírica às proposições teóricas, os resultados confirmam a interdependência entre tecnologia, governança e cultura no processo de adequação à LGPD, convergindo com evidências identificadas na literatura (Rocha et al., 2023; Zainedin, 2025). Esses resultados reforçam a necessidade de estratégias que envolvam investimentos técnicos, governança formal e capacitação continuada para a conformidade da organização com a LGPD.

6 CONSIDERAÇÕES FINAIS

Este estudo teve como objetivo compreender como profissionais de TI percebem as implicações da LGPD nos controles de segurança da informação. A investigação articulou as dimensões Técnica, Formal e Informal relacionadas ao tema. Diante da relevância da proteção dos dados pessoais e do aumento nas transações digitais e da interconexão entre diversas

fontes de dados e sistemas, a LGPD traz a obrigação e necessidade de promover a conscientização e o treinamento de usuários e profissionais de TI. Neste estudo, os dados sobre a percepção dos profissionais de TI a respeito dos impactos da lei sobre os controles de segurança da informação na organização mostram que há uma compreensão de que controles técnicos, formais e informais precisam sofrer adequações aos requisitos da LGPD.

No entanto, há uma percepção de que pouco precisa ser feito em relação aos controles técnicos, enquanto controles formais precisam sofrer adequações mais contundentes. Mudanças nos controles formais, no entanto, pedem um reforço nos controles informais para aumentar a aceitação das mudanças. Na organização em estudo, a despeito de já terem sido realizadas ações na dimensão Informal, há uma percepção de que são necessárias ainda ações de sensibilização e conscientização sobre o tema.

Os resultados mostram também que, embora os participantes da pesquisa entendam que a organização tem os recursos tecnológicos necessários para atender aos requisitos da lei, mudanças na dimensão Técnica poderão ser necessárias.

Entre os indicadores das três dimensões, apenas *PC – Tecnologias voltadas para combate a códigos maliciosos* (dimensão Técnica) não teve evidências identificadas. Todos os demais apareceram nos dados, com destaque para *PP – Alterações e criação de planos, procedimentos e processos de segurança da informação para atender à LGPD* (dimensão Formal), com 16 evidências, *TR – Realização de capacitações sobre LGPD e proteção de dados* (dimensão Informal), com 12 evidências, e *RP – Responsabilidades para tratamento de dados pessoais formalmente definida* (dimensão Formal), com 7 evidências. A ausência de evidências para *PC – Tecnologias voltadas para combate a códigos maliciosos* não é explicada, mas não indica falta de foco dos profissionais na dimensão Técnica.

Na dimensão Formal, os indicadores menos mencionados foram *CM – Participação de equipes multidisciplinares no atendimento aos requisitos da LGPD* e *EO – Alterações nas estruturas organizacionais para adequação à LGPD*, ambos com três evidências. Na dimensão Informal, *DV – Ações de divulgação de informações sobre LGPD e planos, políticas, regulamentos e mudanças decorrentes da implantação dos seus requisitos* teve apenas duas citações. Já na dimensão Técnica, *RD – Redundância de ativos de TI para atender à necessidade de disponibilidade dos dados* apareceu uma única vez.

Em suma, os dados mostram uma predominância da percepção de que a infraestrutura tecnológica é atualizada, mas persistem pontos sensíveis em controles de acesso e segregação de dados. Além disso, políticas, normas e processos carecem de adaptações para estar de acordo com as exigências da LGPD. Treinamentos foram bem-avaliados, porém não se traduziram em alto nível de conhecimento prático por parte dos profissionais de TI. O fato de treinamentos terem sido oferecidos pode ter gerado uma impressão positiva sobre seus efeitos, ainda que não tenham sido assimilados de maneira suficiente.

As evidências identificadas mostram que os profissionais de TI compreendem parcialmente as implicações da LGPD, especialmente quanto às exigências formais e culturais, o que pode dificultar o avanço da organização em direção à conformidade com a lei e à proteção de dados pessoais.

Do ponto de vista teórico, este trabalho vai além da literatura ao oferecer um modelo com as dimensões Técnica, Formal e Informal da segurança da informação, modelo este que pode ser aplicado a outros contextos, confirmando a relevância de fatores tecnológicos, normativos e de conscientização e educação nesta temática. No plano prático, o estudo desperta a atenção de gestores para a priorização de ajustes em controles formais, como políticas, processos e regulamentos, e em programas de educação e conscientização,

possibilitando que investimentos tecnológicos redundantes ou desnecessários sejam repensados. Ao evidenciar lacunas de conscientização, este trabalho sinaliza caminhos para políticas de capacitação que resguardem os direitos dos titulares dos dados pessoais.

O estudo focou exclusivamente nas percepções de profissionais técnicos e gestores de TI, sendo essa sua principal limitação. Além disso, embora a organização estudada seja complexa e esteja presente em diferentes regiões no Brasil, os resultados não podem ser generalizados, pois a pesquisa foi um estudo de caso único, ficando restrita, portanto, a um único contexto organizacional, o que configura outra limitação do trabalho. Além disso, a análise baseia-se em autodeclarações, que podem ser enviesadas.

Essas limitações impactam a validade dos resultados e a generalização dos achados, com restrições decorrentes da diversidade de percepções sobre a adequação à LGPD, o que limita a validade interna do estudo no que se refere à compreensão organizacional mais ampla. O uso de um estudo de caso único enfraquece a validade externa, impedindo a extrapolação dos resultados para outras organizações com diferentes estruturas, culturas ou mesmo em outras áreas de atuação. Além disso, a natureza autorreferida dos dados pode introduzir vieses ou mesmo superestimar a conformidade, comprometendo a confiabilidade das interpretações. Assim, os achados devem ser compreendidos como indícios contextuais e exploratórios, e não como conclusões generalizáveis. Estudos futuros aplicando outras metodologias, utilizando amostras mais amplas e fazendo triangulação de dados poderão reforçar ou refinar essas conclusões.

Recomenda-se, portanto, expandir a pesquisa para outros grupos, como gestores de outras áreas e usuários de TI, para obter uma visão mais ampla das implicações da LGPD na segurança da informação organizacional. As limitações apontadas ensejam também estudos mais amplos e em outros setores para verificar se profissionais de TI de outras organizações percebem da mesma forma as implicações da LGPD. Outra possibilidade de pesquisa futura é identificar, em organizações que passaram pelo processo de adequação dos controles de segurança da informação aos requisitos da LGPD, os fatores que favoreceram sua adequação e as barreiras enfrentadas, ampliando o conhecimento sobre o tema. Recomenda-se ainda avaliar de forma longitudinal a eficácia das estruturas organizacionais, como comitês multidisciplinares, e das mudanças em controles formais decorrentes do processo de adequação.

REFERÊNCIAS

Acquisti, A.; & Grossklags, J. (2003). Losses, gains and hyperbolic discounting: An experimental approach to information security attitudes and behavior. *Annual Workshop on Economics and Information Security*, College Park, MD, United States of America, 2.

Albuquerque Junior, A. E., & Santos, E. M. (2015). Adoption of Information Security measures in public research institutes. *JISTEM*, 12(2), 289–316. https://doi.org/10.4301/S1807-17752015000200006

Albuquerque Junior, A. E., Santos, E. M., Oliveira, R. C. R., Silva, A. S. R., & Almeida, L. M. (2018). A Adopção de Medidas Formais, Informais e Técnicas de Segurança da Informação e sua Relação com as Pressões do Ambiente Institucional. *RISTI*, 30, 17-33. https://doi.org/10.17013/risti.30.17–33

Allen, B. (1996). *Information Tasks: toward a user-centered approach to information systems*. Orlando: Academic Press.

Almeida, S. C. D., & Soares, T. A. (2022). Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital. *Perspectivas em Ciência da Informação*, 27(3), 26-45. https://doi.org/10.1590/1981-5344/25905

Baumer, D., Earp, J. B., & Payton, F. C. (2000). Privacy of medical records: IT implications of HIPAA. *Computers and Society*, 30(4), 40-47. https://doi.org/10.1145/572260.572261

Belasco, K., & Wan, S.-P. (2006). Online retail banking: security concerns, breaches, and controls. In: Bidgoli, H. (Org.). *Handbook of Information Security: Threats, Vulnerabilities, Prevention, Detection, and Management* (pp. 37-48). New Jersey: John Wiley & Sons, v.1.

Bioni, B. R. (2019). *Proteção de dados pessoais: A função e os limites do consentimento*. Rio de Janeiro: Forense.

Björck, F. J. (2005). *Discovering information security management* [Doctoral thesis, Stockholm University]. Stockholm, Sweden.

Brasil. *Lei n. 13.709*, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF. http://www.planalto.gov.br

Cancelier, M. V. L. (2017). *Infinito particular: Privacidade no século XXI e a manutenção do direito de estar só*. Rio de Janeiro: Lumen Juris.

Canedo, E. D., Ribeiro, V. C., Alarcão, A. P. A., Chaves, L. A. C., Reed, J. N., Mendonça, F. L. L., & Sousa Jr., R. T. (2021). *Challenges regarding the compliance with the General Data Protection Law by Brazilian organizations: A survey*. International Conference on Computational Science and Its Applications, Cagliari, Italy, 21. https://doi.org/10.1007/978-3-030-86970-0_31

Canedo, E. D., Calazans, A. T. S., Bandeira, I. N., Costa, P. H. T., & Masson, E. T. S. (2022). Guidelines adopted by agile teams in privacy requirements elicitation after the Brazilian general data protection law (LGPD) implementation. *Requirements Engineering*, 27, 545–567. https://doi.org/10.1007/s00766-022-00391-7

Casotti, I. J., Ferreira, V. M., Miguel, L. D., Oliveira, A. G., Oliveira, A. K., & Barbosa, F. D. (2024). Garantindo a segurança da informação na era digital: riscos e soluções. *Revista Delos*, 17(60), 01-18. https://doi.org/10.55905/rdelosv17.n60-058

Cavenaghi, M. G. C., Paris, L. R. P., Menegassi, W. J. C., Antunes Neto, J. M. F., & Biazotto, L. H. (2024). Lei Geral de Proteção de Dados e a segurança da informação: Atuação do gestor de tecnologia da informação. *Prospectus*, 6(1), 97-115. https://doi.org/10.5281/zenodo.12718309

Cetin, M. B. (2024). *Evaluating the effects of digital privacy regulations on user trust* [Master Thesis, Vrije Universiteit Amsterdam]. Amsterdam, The Netherlands.

Chiles, W. A. S., Behr, A., Farias, E. S., Corso, K. B. (2013). *Problemas nos processos de adoção de sistemas e tecnologias de informação: estudo de caso em uma autarquia da Prefeitura Municipal de Sant'Ana do Livramento*. Congresso Virtual Brasileiro, 10.

Le Coadic, Y. F. (2004). Princípios científicos que direcionam a ciência e a Tecnologia da Informação digital. *Transinformação*, 16(3), 205-213.

Corcoran, P. M. (2016). *A privacy framework for the Internet of Things*. IEEE World Forum on Internet of Things, Reston, VA, United States of America, 3, 13-18. https://doi.org/10.1109/WF-IoT.2016.7845505

Creswell, J. W., & Plano Clark, V. L. (2013). *Pesquisa de métodos mistos*. Porto Alegre: Artmed.

Custers, B., & Ursic, H. (2016). Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *International Data Privacy Law*, 6(1), 4-15.

Davenport, T. H., & Prusak, L. (1998). *Ecologia da informação: porque só a tecnologia não basta para o sucesso na era da informação*. São Paulo: Futura.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, 11(2), 127-153.

Dhillon, G., & Moores, S. (2001). Computer crimes: theorizing about the enemy within. *Computers & Security*, 20(8), 715-723.

Doherty, N. F.; & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security*, 25(1), 55-63.

Doneda, D. (2021). *Da privacidade à proteção de dados pessoais*. São Paulo: Editora Revista dos Tribunais.

Drucker, P. (1988). The coming of the new organization. *Harvard Business Review*, 68(6), 45-53.

Fernandes, M. A. S. (2022). *Repositório seguro e o impacto gerado pela Lei Geral de Proteção de Dados Pessoais (LGPD)* [Dissertação de Mestrado, Universidade de Brasília]. Brasília, Brasil.

Ferreira, A. J. (2018). Profiling e algoritmos autónomos: um verdadeiro direito de não sujeição. *Anuário da Proteção de Dados 2018*, 35-43.

Georgiadis, G., & Poels, G. (2022). Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data

analytics context: a systematic literature review. *Computer Law & Security Review*, 44, 105640. https://doi.org/10.1016/j.clsr.2021.105640

Gorayeb, D. M. C. (2012). *Gestão de Continuidade de Negócios aplicada ao ensino presencial mediado por recursos tecnológicos* [Dissertação de Mestrado, Universidade de São Paulo]. São Paulo, Brasil.

Haddara, M., Salazar, A., & Langseth, M. (2023). Exploring the impact of GDPR on big data analytics operations in the e-commerce industry. *Procedia Computer Science*, 219, 767-777. https://doi.org/10.1016/j.procs.2023.01.350

Hallinan, D., Friedewald, M., & McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer Law & Security Review*, 28(3), 263-272. https://doi.org/10.1016/j.clsr.2012.03.005

Herath, T., Herath, H., & Bremser, W. G. (2010). Balanced Scorecard implementation of security strategies: a framework for IT security performance management. *Information Systems Management*, 27(1), 72-81.

van den Hoven, J. (2008). Information technology, privacy, and the protection of personal data. In: van den Hoven, J., & Weckert, J. *Information technology and moral philosophy* (pp.301-321). Cambridge: Cambridge University Press.

Iervolino, S. A., & Pelicione, M. C. (2001). A utilização do grupo focal como metodologia qualitativa na promoção da saúde. *Revista da Escola de Enfermagem da USP*, 35(2), 115-121. https://doi.org/10.1590/s0080-62342001000200004

Ismail, S., Malone, M. S., & Geest, Y. V. (2019). *Organizações Exponenciais. Por que elas são 10 vezes melhores, mais rápidas e mais baratas que a sua (e o que fazer a respeito)*. Rio de Janeiro: Alta Books.

Jasserand, C. (2018). Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680? *Computer Law & Security Review*, 34(1), p.154-165. https://doi.org/10.1016/j.clsr.2017.08.002

Kanagusku, A. R. A, & Lahr, M. V. (2024). A LGPD e Seus Desafios aos Profissionais da Área de Tecnologia da Informação. *Journal of Technology and Information*, 4(3). https://doi.org/10.5281/zenodo.14215584

Kitiyadisai, K. (2005). Privacy rights and protection: foreign values in modern Thai context. *Ethics and Information Technology*, 7, 17–26. https://doi.org/10.1007/s10676-005-0455-z

Krueger, R. A., & Casey, M. A. (2015). *Focus groups: A practical guide for applied research*. Los Angelis: Sage.

Lopes, I. M. (2012). *Adopção de políticas de segurança de sistemas de informação na administração pública local em Portugal* [Tese de Doutoramento, Universidade do Minho]. Braga, Portugal.

Maddali, R. (2024). AI-powered data security frameworks for regulatory compliance (GDPR, CCPA, HIPAA). *IJETRM*, 8(4), 393-403.

Melo, K. Y. V. S., & Mendes, G. A. (2023). Information security in small companies: Preparation of the security booklet. *Research, Society and Development*, 12(5), e7612541304. https://doi.org/10.33448/rsd-v12i5.41304

Menegazzi, D. (2021). *Um guia para alcançar a conformidade com a LGPD por meio de requisitos de negócio e requisitos de solução* [Dissertação de Mestrado, Universidade Federal de Pernambuco]. Recife, Brasil.

Miracle, N. O. (2024). The importance of network security in protecting sensitive data and information. *IJRIAS*, 9(6), 259-270. https://doi.org/10.51584/IJRIAS.2024.906024

Miranda, I. C. Z., Souza, C. H. M., Ramos, M., Lélis, E. C., Arima, C. H., & Galegale, N. V. (2024). Avaliação da conformidade de empresas à LGPD: Uma pesquisa com profissionais de tecnologia da informação. *Revista Humanidades e Tecnologia*, 9, 68-90.

Mitnick, K. D., & Simon, W. L. (2003). *Mitnick – A arte de enganar – ataques de hackers: controlando o fator humano na Segurança da Informação*. São Paulo: Makron Books.

Morgan, D. L. (2010). Reconsidering the role of interaction in analyzing and reporting focus groups. *Qualitative Health Research*, 20(5), 718-722. https://doi.org/10.1177/1049732310364627

Mulholland, C. S. (2018). Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, 19(3), 159-180. https://doi.org/10.18759/rdgf.v19i3.1603

Neitzke, C., Mendes, J., Rivero, L., Teixeira, M., & Viana, D. (2023). Enhancing LGPD compliance: Evaluating a checklist for LGPD quality attributes within a government office. *Brazilian Symposium on Software Quality*, Brasilia, DF, Brazil, 22. https://doi.org/10.1145/3629479.3629497

Peixoto, M., Ferreira, D., Cavalcanti, M., Silva, C., Vilela, J., Araújo, J., & Gorschek, T. (2023). The perspective of Brazilian software developers on data privacy. *Journal of Systems and Software*, 195 (2023), 111523. https://doi.org/10.1016/j.jss.2022.111523

Pinheiro, P. P. (2020). *Proteção de dados pessoais: comentários à Lei 13.709/2018 (LGP)*. São Paulo: Saraiva.

Piurcosky, F. P., Costa, M. A., Frogeri, R. F., & Calegario, C. L. L. (2019). A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. *Suma de Negocios*, 10(23), 89-99. https://doi.org/10.14349/sumneg/2019.v10.n23.a2

Poullet, Y. (2018). Is the general data protection regulation the solution? *Computer Law & Security Review*, 34(4), 773-778. https://doi.org/10.1016/j.clsr.2018.05.021

Quinn, P., & Malgieri, G. (2021). The difficulty of defining sensitive data—The concept of sensitive data in the EU Data Protection Framework. *German Law Journal*, 22, 1583-1612. https://doi.org/10.1017/glj.2021.79

Quintanilha, F. S., & Silva, V. B. (2023). O processo de adequação à Lei Geral de Proteção de Dados: Um estudo de caso em uma empresa do segmento da saúde. *Revista de Ciências Empresariais da UNIPAR*, 24(1), 162-186. https://doi.org/10.25110/receu.v24i1-009

Ribeiro, J.P., & Garcés, L. (2023). *Especificação de requisitos de design de software para sistemas de IoT conforme a LGPD: Resultados de aplicação em um sistema de assistência para pacientes com Diabetes Mellitus*. Simpósio Brasileiro de Computação Aplicada à Saúde (pp. 37-42). SBC.

Rocha, R. L., Fontes, S. V., Machado, T. F. (2023). A segurança da informação nas organizações: um estudo sobre o impacto da Lei Geral de Proteção de Dados Pessoais na gestão. *RECH*, 7(2), 463-483.

Rodotá, S. (2008). *A vida na sociedade de vigilância: a privacidade hoje*. Rio de Janeiro: Renovar.

Sêmola, M. (2014). *Gestão da segurança da informação: uma visão executiva*. Rio de Janeiro: Campus.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, 19(1), 62-73.

Sher, M.-L., Talley, P. C., Yang, C.-W., & Kuo, K.-M. (2017). Compliance with electronic medical records privacy policy: an empirical investigation of hospital information technology staff. *Inquiry*, 54, 1-12. https://doi.org/10.1177/0046958017711759

Silva, B. E., & Antunes Neto, J. M. F. (2023). Segurança da informação de encontro às conformidades da LGPD em cartórios e serventias extrajudiciais. *Prospectus*, 5(2), 567-631. https://doi.org/10.5281/zenodo.10065058

Solove, D. J. (2008). *Understanding privacy*. Cambridge: Harvard University Press.

Stair, R. M., & Reynolds, G. W. (2002). *Princípios de sistemas de informação: uma abordagem gerencial*. Rio de Janeiro: LTC.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34, 134-153. https://doi.org/10.1016/j.clsr.2017.05.015

Zainedin, L. (2025). O impacto da Lei Geral de Proteção de Dados (LGPD) na segurança pública. *Brazilian Journal of Development*, 11(3), 01-22. https://doi.org/10.34117/bjdv11n3-001