SemeAd 2024
XXVII Seminários em Administração

05, 06, 07 e 08 de novembro de 2024
ISSN 2177-3866

A COMPREENSÃO DOS PROFISSIONAIS DE TI QUANTO À LGPD E SUAS IMPLICAÇÕES NA SEGURANÇA DA INFORMAÇÃO

NAIRA MARIA DA SILVA DUARTE
ESCOLA DE ADMINISTRAÇÃO DA UFBA

ANTONIO EDUARDO DE ALBUQUERQUE JUNIOR
FUNDAÇÃO OSWALDO CRUZ - FIOCRUZ / INSTITUTO GONÇALO MONIZ - IGM

ERNANI MARQUES DOS SANTOS
UNIVERSIDADE FEDERAL DA BAHIA (UFBA)

Agradecimento à orgão de fomento:
Os autores agradecem à FAPEX, CAPES e CNPq.

A COMPREENSÃO DOS PROFISSIONAIS DE TI QUANTO À LGPD E SUAS IMPLICAÇÕES NA SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

Com o avanço da tecnologia em diversos setores da sociedade, a quantidade de informações disponíveis tem crescido exponencialmente (van den Hoven, 2008). Se o uso disseminado da tecnologia teve impacto sobre as práticas organizacionais e ampliou as possibilidades de transações digitais e, como consequência, o acúmulo de dados gerados nessas transações para análise, por outro lado vem trazendo riscos de abusos na utilização desses dados (Ismail, Malone & Geest, 2019). Isto aumenta a necessidade de medidas para proteger os dados utilizados nessas operações (Herath, Herath, & Bremser, 2010), principalmente devido à possibilidade de comprometimento de transações e pessoas (Marciano, 2006).

A literatura destaca o crescimento no volume e diversidade de dados coletados a partir do uso de recursos tecnológicos, ressaltando os riscos do tratamento inadequado desses dados (Wu et al., 2016; Ismagilova et al., 2020; Kumar & Somani, 2018; Latulipe, Mazumder, & Wilson, 2020; Yao, Chuang, & Hsu, 2018). Diante dessa situação, governos e organizações internacionais começaram a regulamentar a coleta e processamento de dados pessoais (Baumer, Earp, & Payton, 2000; Kitiyadisai, 2005; Lindsay, 2005; Hallinan, Friedewald, & McCarthy, 2012; Bennett et al., 2014; Raminelli & Rodegheri, 2016; Jasserand, 2018; Poullet, 2018; Magalhães & Divino, 2019; Lenert & McSwain, 2020; Zanini, 2020).

Leis e regulamentos internacionais têm mostrado uma crescente preocupação com a proteção dos dados pessoais, exigindo a garantia da integridade das informações, respeito à sua finalidade de uso e o consentimento para utilização, entre outros requisitos (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 foi sancionada em agosto de 2018 e estabeleceu um marco legal para o tratamento desses dados em organizações públicas e privadas, estejam eles em meio digital ou não. Vigente desde setembro de 2020, a lei implica mudanças significativas na gestão de tecnologia da informação (TI) (Ismail, Malone, & Geest, 2019), trazendo também 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 das organizações, ampliando a relevância de compreender seus impactos (Almeida & Soares, 2022). Neste contexto, mostra-se relevante entender a compreensão dos profissionais de TI a respeito das implicações da LGPD para a segurança da informação, tendo em vista a proteção dos direitos dos titulares desses dados.

Assim, a pesquisa que resultou neste artigo teve o objetivo de estudar como profissionais de TI percebem as implicações da LGPD nos controles de segurança da informação organizacionais. A compreensão do profissional de TI sobre a lei é importante para a adequação das organizações às exigências legais a fim de proteger os dados pessoais, 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. Além da importância de ordem prática, esta pesquisa também não se limitou a explorar 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.

2. FUNDAMENTAÇÃO TEÓRICA

A despeito da relevância da informação em diferentes setores da sociedade, seu conceito varia de acordo com o contexto (Capurro & Hjorland, 2007), podendo 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 (Le Coadic, 2004) e sendo considerada um ativo estratégico fundamental (Dias, 2000).

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).

As normas NBR ISO/IEC 27002:2022 e NBR ISO 27001:2022, da Associação Brasileira de Normas Técnicas ([ABNT], 2022a; 2022b), reconhecem a informação como um ativo que precisa ser protegido e 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, com o que concordam Dhillon e Backhouse (2001).

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 (Cooper, 2009; Lopes, 2012). À necessidade de garantir a integridade, disponibilidade e confidencialidade da informação, Sêmola (2014) acrescenta a preocupação com sua autenticidade e legalidade e o acompanhamento dessas características durante seu ciclo de vida, que, segundo Floridi (2010), precisa ser gerenciado de forma eficiente, permitindo que seja reciclada ou eliminada quando for possível e não for mais necessária.

Para proteger a integridade, confidencialidade e disponibilidade da informação, é necessário adotar controles de segurança da informação (Fontes, 2006; Sêmola, 2014), que, segundo Albuquerque Junior, Santos, Oliveira, Silva e Almeida (2018), podem ser classificados a depender da sua finalidade:

a) Controles técnicos, que têm o objetivo de limitar o acesso a prédios, salas, computadores e sistemas, ou mudar o ambiente físico no qual as informações são armazenadas e processadas 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, 1999; Dhillon & Moores, 2001; Björck, 2005; Gorayeb, 2012).
b) 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).
c) 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 desses controles, a segurança da informação pode proteger dados pessoais que são tratados nos processos organizacionais, que é justamente o objetivo da LGPD. A lei dispõe sobre a necessidade de consentimento explícito dos titulares dos dados para que possa haver sua coleta, armazenamento e tratamento, e determina que os dados só podem ser coletados para uma finalidade específica e legítima, com transparência sobre quem vai acessá-los e por quanto tempo serão utilizados, e 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 cumprimento 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 pela legislação vigente, que protege a vida privada e a intimidade dos indivíduos (Rodotá, 2008). Sendo os dados pessoais utilizados pelas organizações para fins comerciais, o direito à privacidade envolve o controle e determinação do uso desses dados (Bioni, 2019; Paesani, 2014).

A ampla utilização da tecnologia e o crescente volume de dados gerados e armazenados desafiam a proteção dos dados pessoais (van den Hoven, 2008), pois esses dados digitais 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 a identificação (Pinheiro, 2020), o que pode ser viabilizado com a utilização de recursos tecnológicos que facilitam sua análise, manipulação e transmissão (Ferreira, 2018). Como agravante, há a possibilidade de os dados pessoais serem sensíveis e poderem ser 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, além de dados que permitam discriminação do indivíduo, como discutido por 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), visto que a privacidade e integridade dos dados pessoais são ameaçadas não só por vulnerabilidades tecnológicas, mas principalmente pelo comportamento humano (Whitman, 2003; 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 esses incidentes e garantir 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 pela ABNT (2022a) e por Höne e Eloff (2002) e Herath, Herath e Bremser (2010). Os controles de segurança da informação foram identificados na literatura por Albuquerque Junior et al. (2018) (Quadro 1).

A introdução da LGPD trouxe a necessidade de revisar os controles de segurança da informação adotados nas organizações, pois seus requisitos poderão trazer diferentes impactos na gestão, política, estrutura, recursos tecnológicos e demais controles adotados. Como a política de segurança da informação organizacional deve indicar os papéis e responsabilidades dos indivíduos e as estruturas organizacionais necessárias, como o comitê de segurança da informação, equipe de tratamento de incidentes e escritório de segurança da informação (Höne & Eloff, 2002; Doherty & Fulford, 2006; Lopes, 2012; Sêmola, 2014), é natural que tanto ela quanto os demais controles que são adotados seguindo suas orientações sejam

alterados em decorrência da LGPD, que aborda também processos, procedimentos, princípios, ações e papéis que precisam ser criados ou alterados para que se tenha proteção dos dados pessoais. A lei trata de uma política de retenção de dados e das responsabilidades de grupos e pessoas, como o encarregado de tratamento de dados pessoais, para orientar as questões de privacidade e proteção de dados na organização, coordenar as respostas aos incidentes que envolvam dados pessoais e lidar com a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e com os titulares dos dados, inclusive sobre a ocorrência desses incidentes, bem como monitorar a conformidade da organização e realizar ações de conscientização, divulgação e treinamento sobre o tema (Lei n. 13.709, 2018).

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 sestão 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

Quadro 1 - Exemplos de controles técnicos, formais e informais de segurança da informação.
Adaptado de Albuquerque Junior et al. (2018)

A lei traz também princípios da proteção de dados pessoais, como o respeito à finalidade do tratamento dos dados, o livre acesso do titular aos seus dados e a transparência sobre como e por quem os dados serão tratados, a garantia da segurança e qualidade dos dados, a garantia de não discriminação decorrente do tratamento dos dados, a responsabilização das pessoas e organizações que coletam, armazenam e tratam dados pessoais, assim como o consentimento por parte dos titulares dos dados para que eles sejam coletados, armazenados e tratados (Lei n. 13.709, 2018). Esses requisitos, por si só, ensejam a elaboração de uma política de tratamento de dados pessoais, ou a alteração da política de segurança da informação organizacional, embora não sejam explicitamente tratadas na LGPD.

Atividades de análise e avaliação de riscos recomendadas na literatura (Fontes, 2006; Sêmola, 2014) e previstas na política de segurança da informação (ABNT, 2022a) podem ser afetadas pela LGPD, que prevê a avaliação de riscos de privacidade e proteção de dados e requisitos específicos para o processamento de dados sensíveis, itens pouco abordados pela literatura sobre segurança da informação.

Procedimentos para a obtenção do consentimento dos titulares dos dados antes da coleta, processamento ou compartilhamento, para realizar correções, acessos, exclusões ou limitações, e para informar aos titulares dos dados como ocorrerá a coleta, processamento e utilização dos seus dados pessoais, e sanções para violações, incluindo advertências, multas e suspensão parcial das atividades de tratamento de dados, como previsto na Lei n. 13.709 (2018), também são novidades ao se tratar de segurança da informação.

Algumas organizações podem ter uma adaptação mais rápida aos requisitos da LGPD, como aquelas que possuem políticas, regulamentos e estruturas de segurança da informação estabelecidas, como comitês e gestores de segurança da informação, como proposto por Sêmola (2014). No entanto, será necessário ajustar essas estruturas e papéis organizacionais para atender aos requisitos da lei.

Para garantir o controle de acesso e proteger os dados conforme a nova lei, as organizações podem precisar de atualizações tecnológicas ou adaptações em sistemas de criptografia, *firewalls* e *backup*, que

dependem da atuação dos profissionais de TI da organização. No entanto, é importante reconhecer que os profissionais de TI tendem a focar mais em medidas técnicas de segurança da informação do que em aspectos organizacionais e de conscientização (Albuquerque Junior & Santos, 2015). Uma compreensão limitada desses profissionais quanto aos impactos da LGPD sobre a segurança da informação organizacional pode resultar em não conformidade com a lei e sanções por parte da ANPD.

A conscientização e o treinamento dos profissionais e usuários de TI são relevantes para que se tenha essa conformidade com a LGPD, pois tendem a reduzir a falta de compreensão e a resistência às mudanças necessárias (Chiles, Behr, Farias, & Corso, 2013), o que faz necessário promover uma abordagem equilibrada que considere tanto aspectos técnicos quanto não técnicos da proteção de dados pessoais.

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):

a) 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.
b) Implicações Técnicas: abrangem mudanças no funcionamento de dispositivos tecnológicos e a implementação de novos sistemas de segurança da informação tendo em vista a proteção dos dados pessoais com base nos requisitos da LGPD. Isso inclui redundância de dados e equipamentos que não contavam com esses recursos, bem como segregação e monitoramento de redes e repositórios de dados, além de mudanças em controles de acesso lógico e físico.
c) Implicações Informais: envolvem ações de treinamento e conscientização dos profissionais de TI e dos usuários 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 ligado à segurança da informação, e devido ao fato de a segurança da informação estar intimamente ligada às atividades 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. É de se esperar, portanto, que estes profissionais tenham compreensão desses impactos.

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.

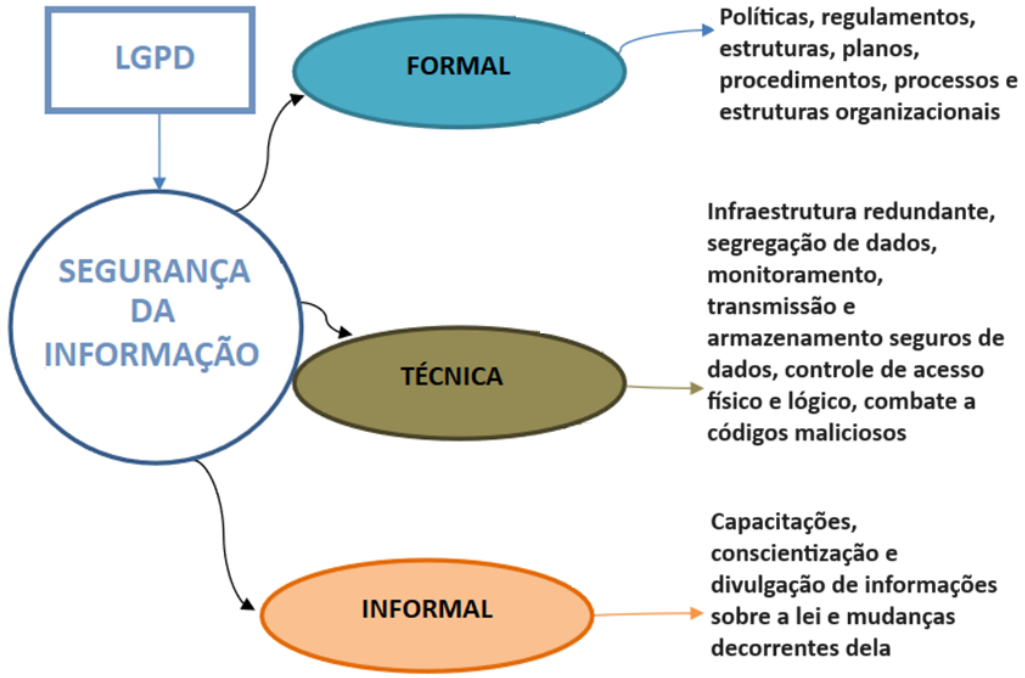

Figura 1 – Modelo conceitual da pesquisa.
Elaboração própria.

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

Assim, na dimensão *Técnica* tem 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.

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

Quadro 2 – Quadro analítico da pesquisa.
Elaboração própria.

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. MÉTODO

Este estudo de caso com objetivo descritivo utiliza múltiplos métodos de pesquisa para estudar o comportamento de uma organização com base em dados de um levantamento realizado em um estudo anterior e em dados coletados em um grupo focal realizado posteriormente. Para a fundamentação teórica deste trabalho, foi realizada uma pesquisa bibliográfica abrangente 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 anais de eventos e periódicos científicos relevantes para diferentes áreas de conhecimento, mas principalmente Administração, Tecnologia da Informação e Ciência da Informação.

Os dados quantitativos foram coletados durante o ano de 2021 através de um levantamento realizado em 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 dados nesta pesquisa.

O formulário utilizado no levantamento continha 23 perguntas, que foram disponibilizadas através do aplicativo *Microsoft Forms*. Ao todo, foram convidados a participar 70 profissionais de TI da organização, incluindo diretores, gerentes, coordenadores e analistas de TI, que foram escolhidos com base nos critérios de tempo de atuação na organização e envolvimento em questões estratégicas de TI. Desses convidados, 64 enviaram respostas, o que corresponde a 91,4% de participação na pesquisa. Para este estudo, não foram analisadas as respostas às 23 perguntas do formulário, mas somente aquelas que estão diretamente relacionadas ao objetivo deste artigo. Assim, for formulário original, foram consideradas as respostas a 10 perguntas, cujos dados foram analisados utilizando o programa *Statistical Package for Social Sciences* (SPSS) versão 20.

As 10 perguntas estavam organizadas em quatro blocos temáticos, 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 a respeito de o quanto os respondentes compreendem a necessidade de adequação técnica e 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 as organizações atualizarem seus recursos tecnológicos de segurança da informação em decorrência da LGPD. 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 do bloco 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 – 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 pergunta tratou de como os respondentes percebem 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.

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, sendo o moderador o anfitrião da reunião virtual. 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 identificação dos assuntos relacionados à compreensão da LGPD e seus impactos na segurança da informação.

5. APRESENTAÇÃO E ANÁLISE DOS DADOS

Dentre os 64 participantes do levantamento, 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 de 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, e 33% com mais de 20 anos.

A análise dos dados quantitativos mostrou que 45% dos respondentes consideraram ter pouco conhecimento sobre a LGPD, enquanto 11% declararam ter pleno conhecimento. 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, Behr, Farias e Corso (2013).

Ao analisar as respostas relativas à dimensão Informal, os dados mostram que a pergunta “Como você avalia o impacto das ações de treinamento e divulgação sobre segurança da informação no contexto da LGPD na cultura organizacional?” teve 59% das respostas apontando impacto alto, enquanto a percepção de que tiveram impacto médio teve 38% das respostas. Esses resultados estão relacionados à aceitação das mudanças que aconteceram ou futuras, tanto em tecnologia quanto em políticas, procedimentos e processos internos, para que a organização fique em conformidade com a lei.

Para a dimensão Formal, as respostas apontam que a organização precisa realizar mudanças nas normas, procedimentos e política de segurança da informação. Para a pergunta “O quanto as diretrizes da política de segurança da informação da organização estão adequadas às exigências da LGPD?”, 50% dos respondentes têm a percepção de que a política está com suas diretrizes pouco adequadas às exigências da LGPD, e 41% entendem que a adequação é média. Para a pergunta “Como percebem a adequação das normas e procedimentos internos de segurança da informação à LGPD?”, 54% informaram que as normas e procedimentos têm baixa adequação, e 44% percebem que a adequação é média. Esses resultados mostram a necessidade de adequações na política, normas e procedimentos de segurança da informação, principalmente porque a política e os regulamentos orientam as demais ações e controles de segurança da informação das outras dimensões.

Já quanto à dimensão Técnica, 53% entendem que a lei traz a necessidade de atualizar os recursos tecnológicos de segurança da informação. Para 60% dos respondentes, a infraestrutura de segurança da informação da organização atende plenamente aos requisitos da LGPD, enquanto 39% entendem que atende parcialmente, o que aponta a necessidade de atualizar a infraestrutura, que pode envolver implantação e substituição de *hardware* e *software* e redundância que os dados necessitam. Esse resultado evidencia que, na opinião dos respondentes, a organização empreendeu esforços para que a infraestrutura tecnológica atenda às necessidades e teve ações de conscientização, divulgação e treinamento, ainda que pese a percepção de que esses profissionais não conhecem a lei o suficiente. Os respondentes entendem também que houve poucos esforços sobre a política, procedimentos e processos internos, mostrando que há necessidade de adequações em controles formais. Cabe ressaltar que a política de segurança da informação da organização orienta a aplicação de outros controles formais, como normas, estruturas

organizacionais e procedimentos internos, bem como dos controles técnicos e informais.

Os sete 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 organizacional, e todos declararam entender que refletem o momento de adequação dos controles internos pelo qual a organização estava passando. Após serem questionados pelo moderador a respeito da sua participação em treinamentos sobre a LGPD, todos confirmaram ter participado e três acrescentaram ainda estarem estudando para adequar processos internos e 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 que seus processos sejam alterados 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*.

Apesar de haver um encarregado de proteção de dados pessoais designado, o Gestor 2 acrescentou que a organização ainda não tem uma pessoa para controlar o acesso aos dados e que talvez seja necessária uma pessoa em cada subunidade devido à descentralização organizacional, sendo uma exigência relativa a *RP – Responsabilidades para tratamento de dados pessoais formalmente definidas*. O Gestor 4 ressaltou ser importante definir essa responsabilidade e criar um comitê geral para tratar da LGPD, pois a lei envolve todas as áreas e processos organizacionais. O Gestor 3 acrescentou ser necessário dedicação dos profissionais de TI à conformidade com a lei, ampliando a relevância desse indicador da dimensão Formal. O Gestor 1 abordou a necessidade de identificar e classificar os processos que utilizam dados pessoais em diferentes níveis de prioridade e os riscos associados, uma evidencia 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, o que está relacionado aos 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*.

O Gestor 2 citou a necessidade de autorização para tratamento de dados para permitir que os profissionais de TI trabalhassem ao falar do desenvolvimento do sistema *Enterprise Resource Planning* (ERP) para a organização, 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 são necessárias para concretizar as demais ações futuras a que estão relacionadas 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, abordado pelo Gestor 2, envolve a autorização para tratamento de dados, como ele citou, 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 citado pelo Gestor 3 a hipótese de um titular de dados revogar o termo de consentimento, o que pede controle e conhecimento por parte da organização. Isto configura 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, que apresentou evidências que apontam para os dois últimos indicadores citados anteriormente e a *EO* –

Alterações nas estruturas organizacionais para adequação à LGPD. Este participante falou ainda da fragilidade que representa a 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*.

Os participantes foram provocados pelo moderador do grupo focal quanto ao impacto da LGPD sobre os processos em que há tratamento de dados pessoais, e todos os gestores disseram entender que a organização deverá elaborar um relatório de impacto, como previsto na lei, para identificar e descrever esses processos e os riscos à privacidade, evidenciando implicações da dimensão Formal, mais especificamente do indicador *PP – Alterações e criação de planos, procedimentos e processos de segurança da informação para atender à LGPD*. Os participantes concordaram também que os controles técnicos que podem ser utilizados para mitigar esses riscos incluem sistemas criptografados e repositórios redundantes, relacionados aos indicadores *RD – Redundância de ativos de TI para atender à necessidade de disponibilidade dos dados* e *TA – Tecnologias aplicadas a transmissão e armazenamento seguros de dados*, recursos que afirmam já existirem na organização e que pedem somente 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 de segurança da informação, com o que o Gestor 6 concordou.

No entanto, o Gestor 3 acrescentou que falhas na proteção dos dados pessoais podem levar a penalidades que afetam toda a organização, e 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.

Com estes resultados, foram identificadas evidências de todos os indicadores das dimensões Informal e Formal, e de quatro indicadores da dimensão Técnica (exceto *PC – Tecnologias voltadas para combate a códigos maliciosos*). Apesar da aptidão técnica da organização, ainda são necessárias ações de sensibilização e capacitação, relacionadas à dimensão Informal, e investimentos na adequação de controles formais, inclusive estruturas organizacionais e na política de segurança da informação, aumentando a conformidade da organização à LGPD.

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 os controles de segurança da informação da organização, mas principalmente sobre a política, processos e procedimentos de segurança da informação, além de seus papéis e responsabilidades quanto à proteção de dados pessoais.

Há um entendimento dos participantes de que a infraestrutura tecnológica está atualizada, refletindo investimentos anteriores em segurança da informação. No entanto, ainda há necessidade de adequações nos recursos tecnológicos para que a organização fique em conformidade com a LGPD. As falas dos gestores não apontam no sentido de 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", resultado pode ser explicado pelo foco dos profissionais de TI em aspectos técnicos de segurança da informação (Albuquerque Junior e Santos, 2015).

Os resultados desta pesquisa 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. Essa necessidade é 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 percebidas em diferentes controles formais. Gestores e profissionais de TI percebem que controles formais estão inadequados às exigências da LGPD, ainda que algumas mudanças já tenham ocorrido, como a criação de comitês e grupos multidisciplinares, pois a lei exige mudanças 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 os de desenvolvimento de sistemas, contratos e acordos com outras organizações, bem como 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".

6. CONSIDERAÇÕES FINAIS

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 quanto 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.

Dentre o conjunto de indicadores das três dimensões, somente não foram identificadas evidências

referentes ao indicador *PC – Tecnologias voltadas para combate a códigos maliciosos*, da dimensão Técnica. Todos os demais indicadores foram identificados nos dados, com destaque para *PP – Alterações e criação de planos, procedimentos e processos de segurança da informação para atender à LGPD*, indicador da dimensão Formal, com 16 evidências identificadas nas falas dos participantes, *TR – Realização de capacitações sobre LGPD e proteção de dados*, da dimensão Informal, com 12 evidências identificadas, e *RP – Responsabilidades para tratamento de dados pessoais formalmente definida*, também da dimensão Formal, com 7 evidências.

Da dimensão Formal, os indicadores menos identificados nos dados 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 identificadas. Da dimensão Informal, o indicador identificado com menos frequência foi *DV – Ações de divulgação de informações sobre LGPD e planos, políticas, regulamentos e mudanças decorrentes da implantação dos seus requisitos*, que foi citado em dois momentos. Da dimensão Técnica, *RD – Redundância de ativos de TI para atender à necessidade de disponibilidade dos dados* apareceu apenas uma vez.

Este trabalho teve seu foco nas percepções de profissionais de TI, e isto representa uma limitação dos seus resultados. Como consequência, recomenda-se ampliar o estudo para outros grupos de profissionais, o que pode levar a uma compreensão mais ampla a respeito do processo de adequação organizacional às exigências da LGPD. Os resultados encontrados no estudo pedem também uma pesquisa a fim de identificar junto às organizações bem-sucedidas quais foram os fatores que condicionaram sua adequação à LGPD. Outro caminho é identificar junto às organizações de forma geral quais foram as barreiras encontradas.

REFERÊNCIAS

Acquisti, A.; & Grossklags, J. (2003). Losses, gains and hyperbolic discounting: An experimental approach to information security attitudes and behavior. *Proceedings of 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.

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

Capurro, R., & Hjorland, B. (2007). O conceito de informação. *Perspectivas em Ciência da Informação*, 12(1), 148-207.

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. *Anais do 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. *Proceedings of 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

Cooper, M. H. (2009). Information security training: what will you communicate? *Proceedings of Annual ACM SIGUCCS Fall Conference*, St. Louis, MO, United States of America, 37, 217-222.

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. (1999). Managing and controlling computer misuse. *Information Management & Computer Security*, 7(4), 171-175.

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.

Dias, M. A. P. (2000). *Administração de Materiais*. São Paulo: Atlas.

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.

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

Floridi, L. (2010). *Information: A very short introduction*. Oxford: Oxford University Press.

Fontes, E. L. G. (2006). *Segurança da Informação: o usuário faz a diferença*. São Paulo: Saraiva.

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.

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

Höne, K., & Eloff, J. H. P. (2002). Information security policy – what do international information security standards say? *Computers & Security*, 21(5), 402-409.

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*. Cambridge: Cambridge University Press. pp.301-321.

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

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.

Lei n. 13.709, de 14 de agosto de 2018. (2018). *Lei Geral de Proteção de Dados Pessoais*. Brasília, DF.

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.

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

Paesani, L. M. (2014). *Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil*. São Paulo: Atlas.

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

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

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.

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

Whitman, M. E. (2003). Enemy at the gate: threats to Information Security. *Communications of the ACM*, 46(8), 91-95.