UNIVERSIDADE FEDERAL DA BAHIA
ESCOLA DE ADMINISTRAÇÃO
NÚCLEO DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO

NAIRA MARIA DA SILVA DUARTE

A COMPREENSÃO DOS PROFISSIONAIS DE TI QUANTO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E SUAS IMPLICAÇÕES NAS ORGANIZAÇÕES - ESTUDO DE CASO SENAC

Salvador
2021

NAIRA MARIA DA SILVA DUARTE

A COMPREENSÃO DOS PROFISSIONAIS DE TI QUANTO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E SUAS IMPLICAÇÕES NAS ORGANIZAÇÕES- ESTUDO DE CASO SENAC

Dissertação apresentada ao PPGA Profissional – Programa de Pós-Graduação em Administração Profissional da Escola de Administração da Universidade Federal da Bahia, como requisito parcial para a obtenção do título de Mestre em Administração.

Orientador: Prof. Dr. Antônio Eduardo de Albuquerque Junior

Salvador
2021

Escola de Administração - UFBA

D812 Duarte, Naira Maria da Silva.
A compreensão dos profissionais de TI quanto à lei geral de proteção de dados pessoais e suas implicações nas organizações: estudo de caso SENAC / Naira Maria da Silva Duarte. – 2021.
179 f. : il.

Orientador: Prof. Dr. Antônio Eduardo de Albuquerque Junior.
Dissertação (mestrado) – Universidade Federal da Bahia, Escola de Administração, Salvador, 2021.

1. Brasil. Lei geral de proteção de dados (2018). 2. SENAC – Estudo de casos. 2. Tecnologia da informação – Medidas de segurança. 3. Proteção de dados. 4. Programas de compliance. I. Universidade Federal da Bahia. Escola de Administração. II. Título.

CDD – 658.478

NAIRA MARIA DA SILVA DUARTE

A COMPREENSÃO DOS PROFISSIONAIS DE TI QUANTO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E SUAS IMPLICAÇÕES NAS ORGANIZAÇÕES - ESTUDO DE CASO SENAC

Dissertação apresentada ao curso de Mestrado Profissional em Administração do Núcleo de Pós-Graduação em Administração da Escola de Administração da Universidade Federal da Bahia, como requisito parcial para a obtenção do título de Mestre em Administração.

Salvador, 08 de novembro de 2021

Banca Examinadora:

_____
Prof. Dr. Antônio Eduardo de Albuquerque Junior – Orientador
Doutor em Administração – Universidade Federal da Bahia

_____
Prof. Dr. Adriano Santos Rocha Silva
Doutor em Administração – Universidade Federal de Sergipe

_____
Prof. Dr. Ernani Marques dos Santos
Doutor em Administração – Universidade Federal da Bahia

Salvador
2021

Dedico as minhas filhas Isadora, Isabelle,
muito amadas, e ao meu PAI
Claudemiro Duarte Filho, “meu herói e
orientador dos pilares da minha vida:
Honestidade, Integridade, Amor e Família”.

“Não existe um caminho para a felicidade.
A felicidade é o caminho”

Mahatma Gandhi

AGRADECIMENTOS

A Deus, luz na minha vida, que está sempre na minha jornada e possibilitou a chegada até aqui.

As minhas filhas, Isadora e Isabelle, que me apoiaram incondicionalmente e me ajudaram a superar as limitações e os desafios que o mestrado apresentou; sem esse acolhimento, não seria possível chegar a este resultado. Gratidão a elas que são os meus tesouros e a razão do meu viver.

A minha irmã, Claudia Duarte, que assumiu o leme do meu lar e o conduziu diariamente com muito amor com minhas filhas; e aos meus Pais, Claudemiro Duarte Filho (meu exemplo de Ser Humano), Laurita Duarte e Vera Marta da Silva, que me deram total apoio mesmo nos momentos de ausência, *stress* e cansaço. Eles acreditaram que eu seria capaz de superar os desafios.

Aos demais familiares, meu eterno agradecimento por fazerem parte de minha vida e estarem sempre ao meu lado.

À Marina Almeida, amiga e diretora do SENAC, que me inspira, me motiva e me aconselha, seja no aspecto pessoal e/ou profissional, minha eterna gratidão e amizade.

À amiga Ana Rita Andrade, idealizadora do mestrado para a Instituição SENAC Bahia, meus agradecimentos e carinho eterno.

Às amigas Andreia Nunes, Isabela Luduvice e Italany Barbosa, por fazerem parte da corrente do bem e dos apoios essenciais nos momentos difíceis na conquista dos créditos necessários para chegar até aqui. A vocês, realizações e conquistas.... Contem sempre comigo. Obrigada!

Aos demais amigos da turma do INFMG que foram parceiros e fizeram com que os dias fossem de crescimento, de aprendizagem e de forte laço de amizade – obrigada aos amigos conquistados.

Ao meu Mestre e Orientador, Antônio Eduardo de Albuquerque, que foi muito importante na construção deste trabalho, agradeço por ter permitido minha livre escrita e por ter lido as versões do trabalho sempre com atenção, além de ter dado sugestões valiosas para enriquecê-lo. Grata por ter ficado à disposição para atender a tempo e a hora, com gentileza e paciência, e ~~sobre~~ sob sua orientação foi possível realizar um trabalho que me deu muito orgulho. Gratidão

por acreditar que eu seria capaz. Quando estava pronta para desistir, me conduziu ao caminho da fundamentação teórica e ali encontrei a felicidade de superar meus próprios desafios.

Aos demais mestres que contribuíram na consolidação do conhecimento acadêmico e foram essenciais na formação que o mestrado me proporcionou, expandindo minhas percepções e quebrando paradigmas quanto à docência.

Aos colegas e amigos Gestores de TI do SENAC que participaram das pesquisas e contribuíram com seu tempo e sugestão para a construção da cartilha e do roteiro que foram incluídos no trabalho. Gratidão pela parceria e pelo trabalho de construção de conhecimento que sempre compartilhamos.

A minha equipe de trabalho – Getin (Gerência da Tecnologia da Informação) – que possibilitou as ações práticas que implementamos na gestão, meu carinho e gratidão.

Agradeço a Deus por cada curva percorrida para chegar aqui. Obrigada a cada uma dessas pessoas que estiveram comigo, percorrendo a estrada do conhecimento. Encontramos a felicidade do acolhimento e o saber de muitos que somaram nesta jornada.

Eternamente grata.

"A felicidade não está no fim da jornada, e sim em
Cada curva do caminho que percorremos para
Encontrá-la."
(Autor Desconhecido)

Pai,
Obrigada pela caminhada que realizamos,
E, o ensinamento que deixastes em cada curva do meu caminho.
(Em memória)

DUARTE, Naira Maria da Silva. A compreensão dos profissionais de TI quanto à lei geral de proteção de dados pessoais e suas implicações nas organizações – Estudo de Caso - SENAC. 2021. Orientador: Antônio Eduardo de Albuquerque Junior. 179 f. il. Dissertação (Mestrado em Administração) – Escola de Administração, Universidade Federal da Bahia, Salvador, 2021.

RESUMO

A evolução tecnológica tem como premissas aproximar países e sociedades, facilitar a comunicação, reduzir as distâncias e aproximar as diferenças culturais. No entanto, a coleta e manipulação de dados por meio de recursos tecnológicos tornam possível o uso indevido e abusivo por parte das pessoas e organizações. A vulnerabilidade das informações é uma questão social. Sendo assim, requer um controle maior nas políticas de segurança da informação. Contudo, os controles atuais não são suficientes para evitar os abusos que o mundo digital proporciona. Nos ambientes cada vez mais conectados, os controles e as regulamentações legais são essenciais para evitar as arbitrariedades que o uso excessivo das informações pode gerar para as organizações e/ou indivíduos. Considerando a utilização desmedida da informação, os países instituíram leis e direitos que fundamentam o uso e controle dos dados pessoais coletados. No Brasil, os requisitos da Lei 13.709 de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), envolvem diferentes mudanças de abordagem nas medidas de segurança da informação de uma organização. Sujeitas às exigências da Lei, as organizações públicas, privadas e paraestatais precisam considerar essas mudanças em sua infraestrutura tecnológica e na segurança da informação, além de outras medidas de controles, através de políticas de segurança da informação para assegurar a proteção dos dados pessoais, visando o direito à privacidade de seus clientes, empregados, parceiros e fornecedores, ainda, considerando que a adequação à Lei baseia-se em pessoas, processos e tecnologias. O adequar das Organizações quanto às exigências legais como instrumento de controle e monitoramento dos dados pessoais requer medidas restritivas da Política da Segurança da Informação. Para tal, é necessário verificar a compreensão dos profissionais de TI quanto à gestão de riscos no uso inadequado dos dados e os novos papéis e as responsabilidades que a Lei define, a transparência, a disseminação do conhecimento nas organizações, as regulamentações e os tratamentos das informações, observando as questões éticas dos profissionais de TI, no que diz respeito à privacidade dos dados pessoais sobre sua guarda e responsabilidade. Este trabalho tem como objetivo identificar como os profissionais de TI compreendem as exigências da LGPD e suas implicações para as organizações, além da necessidade de adoção de controles de segurança da informação. Assim, foram aplicadas pesquisas quantitativas e qualitativas, através de questionário *Survey*, com aproximadamente 70 gestores de TI do SENAC a nível Brasil, avaliando os impactos da LGPD nos controles dos dados nas suas organizações. Após a tabulação e análises estatísticas da pesquisa, os resultados foram apresentados em um Grupo Focal, mediado no formato virtual através da ferramenta *Teams*, com a participação de 16 Gestores Estratégicos de TI do SENAC de 7 Estados do Brasil, quando foram expostas as opiniões e considerações referentes ao resultado da pesquisa aplicada. No final desse trabalho, com os diagnósticos consolidados, foram realizadas as avaliações, considerando os pressupostos da pesquisa na qual evidenciou-se que a compreensão e a conscientização dos profissionais de TI são relevantes para as adequações exigidas na Lei, quanto à segurança da informação nas organizações. O trabalho expôs os possíveis impactos, além das oportunidades que a Lei 13.709/2018 poderá gerar na Governança da Tecnologia da Informação (GTI) e os controles da Segurança da Informação (SI), no que visa às mitigações, aos riscos e à redução das vulnerabilidades dos dados pessoais tratados nas organizações.

Palavras-chave: Segurança da Informação. Proteção dos Dados. Lei. Conformidade.

DUARTE, Naira Maria da Silva. The understanding of IT professionals regarding the general law of protection of personal data and its implications in organizations – Case Study - SENAC. 2021. Advisor: Antônio Eduardo de Albuquerque Junior. 179 f. il. Dissertation (Master in Administration) – School of Administration, Federal University of Bahia, Salvador, 2021.

ABSTRACT

Technological evolution is based on bringing countries and societies closer together, facilitating communication, reducing distances and bringing cultural differences closer together. However, the collection and manipulation of data through technological resources make possible the misuse and abuse by people and organizations. Information vulnerability is a social issue. Therefore, it requires greater control over information security policies. However, current controls are not enough to prevent the abuses that the digital world provides. In increasingly connected environments, legal controls and regulations are essential to avoid the arbitrariness that excessive use of information can generate for organizations and/or individuals. Considering the excessive use of information, countries have instituted laws and rights that underlie the use and control of collected personal data. In Brazil, the requirements of Law 13.709 of 2018, known as the General Law for the Protection of Personal Data (LGPD), involve different changes in approach to an organization's information security measures. Subject to the requirements of the Law, public, private and parastatal organizations need to consider these changes in their technological infrastructure and information security, in addition to other control measures, through information security policies to ensure the protection of personal data, aiming the right to privacy of its customers, employees, partners and suppliers, also considering that compliance with the Law is based on people, processes and technologies. The adaptation of the Organizations regarding the legal requirements as an instrument of control and monitoring of personal data requires restrictive measures of the Information Security Policy. For this, it is necessary to verify the understanding of IT professionals regarding risk management in the inappropriate use of data and the new roles and responsibilities that the Law defines, transparency, the dissemination of knowledge in organizations, regulations and the treatment of information, observing the ethical issues of IT professionals, with regard to the privacy of personal data on their custody and responsibility. This work aims to identify how IT professionals understand the requirements of the LGPD and its implications for organizations, in addition to the need to adopt information security controls. Thus, quantitative and qualitative researches were applied, through a Survey questionnaire, with approximately 70 IT managers from SENAC in Brazil, evaluating the impacts of the LGPD in the data controls in their organizations. After tabulation and statistical analysis of the survey, the results were presented in a Focus Group, mediated in a virtual format through the Teams tool, with the participation of 16 Strategic IT Managers from SENAC from 7 States of Brazil, when opinions and considerations regarding the result of the applied research. At the end of this work, with the consolidated diagnoses, the assessments were carried out, considering the assumptions of the research in which it was evident that the understanding and awareness of IT professionals are relevant to the adjustments required by Law, regarding the security of information in organizations. The work exposed the possible impacts, in addition to the opportunities that Law 13.709/2018 may generate in Information Technology Governance (GTI) and Information Security (IS) controls, with a view to mitigating, risking and reducing vulnerabilities of personal data processed in organizations.

Keywords: Information Security. Data Protection. Law. Compliance.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ACM	Association for Computing Machinery
AEPD	Autoridade Europeia para a Proteção de Dados
ANPD	Autoridade Nacional de Proteção de Dados
APF	Administração Pública Federal
ART	Artigo
CF	Constituição Federal
CN	Conselho Nacional
CNC	Confederação Nacional do Comércio
CPL	Conceitos e Processos Legais
FC	Federação do Comércio
GDPR	Regulamento Geral Sobre a Proteção de Dados
GRC	Governança, Riscos e Conformidade
GRH	Gestão de Recursos Humanos
GTI	Gestão da Tecnologia da Informação
IND	Indicadores das Pesquisas
IGSF	Índice da Gestão da Segurança Formal
IGST	Índice da Gestão da Segurança Técnico
IGSI	Índice da Gestão da Segurança Informal
ICIF	Índice do Controle da Informação Formal
ICIT	Índice do Controle da Informação Técnico
ICII	Índice do Controle da Informação Informal
ICIRPF	Índice do Controle da Informação Responsabilidade e Penalidades Formal
ICIRPT	Índice do Controle da Informação Responsabilidade e Penalidade Técnica

ICIRPI	Índice do Controle da Informação Responsabilidade e Penalidade Informal
IIOF	Índice dos Impactos e Oportunidades Formal
IIOT	Índice dos Impactos e Oportunidades Técnica
IIOI	Índice dos Impactos e Oportunidades Informal
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
LMC	Lei Marco Civil
LP	Lei da Privacidade
MP	Medida Provisória
MPDFT	Ministério Público do Distrito Federal e dos Territórios
OECD	Organização para a Cooperação Econômica e Desenvolvimento
PET	*Privacy Enhancing Technology*
PSI	Política de Segurança da Informação
SENAC	Serviço Nacional de Aprendizagem Comercial
SESC	Serviço Social para o Comércio
SI	Sistema da Informação
TAC	Termo de Ajustamento de Conduta
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação

SUMÁRIO

1 INTRODUÇÃO

Com a utilização de recursos tecnológicos nos mais diversos segmentos da sociedade, as informações à disposição de indivíduos e organizações vêm crescendo exponencialmente (VAN DEN HOVEN, 2018). Como observado por Ismail, Malone e Van Geest (2019, p. 50-52), o uso de tecnologia para essa finalidade tem impactado e mudado diferentes práticas nas organizações. Neste contexto, ao tempo em que a utilização de dispositivos móveis e mídias sociais facilita o acúmulo e análise de dados e a realização de negócios digitais, possibilita também abusos na utilização desses mesmos dados. O uso das informações sem a aplicação de controles adequados vem provocando incidentes que comprometem não só a segurança das transações organizacionais, mas, também, das pessoas envolvidas nos diferentes processos internos das organizações (MARCIANO, 2006). As ocorrências de incidentes que podem comprometer as informações tratadas nas organizações reforçam a necessidade de medidas voltadas para controlar os dados utilizados nas operações organizacionais (HERATH; HERATH; BREMSER, 2010).

Wu et al. (2016) destacam que houve um crescimento no volume e na diversidade dos dados coletados através do uso das mídias sociais, dados esses que podem ser facilmente analisados e manipulados. A despeito de possibilitarem novas oportunidades de negócio, diferentes estudos evidenciam os riscos associados ao uso desses dados sem a aplicação dos controles adequados (ISMAGILOVA et al., 2020; KUMAR; SOMANI, 2018; LATULIPE; MAZUMDER; WILSON, 2020; YAO; CHUANG; HSU, 2018).

Considerando a necessidade de proteger os dados e a continuidade das operações organizacionais, os profissionais de TI devem garantir a integridade das informações, respeitando sua finalidade de uso, o que passa pelo respeito às exigências legais, inclusive, pelo consentimento quanto à sua utilização. Contudo, dados vêm sendo expostos devido a falhas em sistemas ou nos processos organizacionais. Mulholland (2018) cita três casos que reforçam esse argumento: o primeiro trata do vazamento de dados relativos ao comportamento sexual de doadores de sangue; o segundo caso trata da coleta de dados relativos ao uso de brinquedos sexuais pelo fabricante de forma automática e sem o consentimento das pessoas; e o terceiro caso trata do uso de dados de cidadãos chineses pelo Estado para identificar seu grau de fidelidade ao regime político do país. Em um artigo mais antigo, Foxman e Kilcoyne (1993), citam o comércio ilegal de dados de 1(um) milhão de eleitores nos Estados Unidos, devido a controles de segurança da informação ineficientes. Já Poullet (2018) cita o caso recente do uso

de dados de usuários do *Facebook* de forma não consentida para identificar e manipular preferências políticas e intenções de voto.

Esses casos ilustram como o direito à privacidade vem sendo considerado uma das questões éticas mais importantes na era da informação, como previra Mason (1986). Para contrapor a facilidade de armazenamento, de processamento e de acesso a dados sobre as pessoas, diferentes países restringiram o acesso às características, às ideias, às impressões, aos movimentos, aos comportamentos, às comunicações e às preferências dos indivíduos, dados cuja manipulação pode ser realizada de maneira massiva com o uso de recursos tecnológicos (MOORE, 2001).

Iniciativas voltadas para a proteção de dados pessoais foram foco de diferentes estudos científicos (BAUMER; EARP; PAYTON, 2000; BERGKAMP, 2002; KITIYADISAI, 2005; HALLINAN; FREIDEWALD; McCARTHY, 2012; LIMA; MONTEIRO, 2013; BHAIMIA, 2018; JASSERAND, 2018; POULLET, 2018; TIKKINEN-PIRI; ROHUNEN; MARKKULA, 2018; MENDES, LAURA SCHERTEL; DONEDA DANILO, 2019; BLUM, RENATO OPICE; SCHUCH, SENA, 2019), o que evidencia a relevância do tema no contexto atual.

No Brasil, a proteção de dados pessoais era tratada em diferentes leis e decretos, sem que houvesse, no entanto, um marco legal específico para essa finalidade, até que houve a sanção da Lei nº 13.709, em 14 de agosto de 2018. Conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), o documento dispõe sobre o tratamento de dados pessoais por pessoas ou organizações públicas, privadas ou paraestatais, estejam esses dados em formato digital ou não, e está vigente desde setembro de 2020.

Considerando que os dados são cada vez mais processados em ambientes digitais, a criação de mecanismos legais que visam a sua proteção trouxe para os profissionais de TI a necessidade de agirem com mais prudência quanto à sua manipulação, o que pede a adoção de medidas adequadas às responsabilidades trazidas pela Lei. Desta forma, esses profissionais ficaram responsáveis por mapear e determinar a extensão desses dados para implantar controles de proteção, documentar seu uso e limitar os danos provocados por incidentes que possam afetá-los (ISMAIL MALONE E VAN GEEST, 2019).

Com aprovação da LGPD, o trabalho de profissionais de TI de organizações públicas, privadas e paraestatais sofreu implicações que vão além da preocupação com questões técnicas de Tecnologia da Informação (TI). A Lei estabeleceu uma série de papéis e necessidades de segurança da informação, e para que as organizações estejam em conformidade com seus

requisitos, é necessário não somente o conhecimento sobre a Lei, mas também sobre como essas exigências legais vão afetar suas atividades, os processos internos de TI nas organizações e os ambientes computacionais onde os dados são processados.

A adequação da Lei 13.709/2018 nas organizações deve ser observada segundo três pilares: a guarda, a responsabilidade e a privacidade. Assim, sistemas de processamento de dados pessoais devem ser criados para servir ao homem e, portanto, devem respeitar seus direitos individuais e sua liberdade (MORGADO, 2019). Em outras palavras, esse processamento deve ser legal e justo aos indivíduos, sendo uma questão ética relevante (MASON, 1986).

O direito à privacidade se transformou ao longo dos anos, e, atualmente, tem sofrido grande influência da tecnologia. O fluxo de informações é muito grande e impacta diretamente na privacidade dos indivíduos, haja vista que há uma exposição imensa e descontrolada da vida privada e da intimidade. Sendo assim, os dados pessoais passam a ter um valor para a sociedade da informação, que é essencial para a economia digital.

No cenário de transformação digital e de adequações a LGPD, é fundamental que os profissionais de TI tenham a compreensão dos processos e das tecnologias que podem transformar a gestão da TI em todas as áreas das organizações. Neste contexto, a compreensão desses profissionais para os possíveis impactos e riscos que as organizações tão expostas com a vigência da lei 13.709/2018 passa a ser uma questão indispensável para que eles possam aplicar medidas de controle no que se refere ao uso de dados pessoais para assegurar o direito à privacidade e garantir o livre desenvolvimento da pessoa humana.

Este trabalho estuda a TI sobre a temática da Segurança da Informação, o que pode colaborar para o efetivo controle e proteção de dados pessoais, e como os profissionais de TI estão percebendo as mudanças na gestão de TI nas organizações, considerando a relevância da Segurança da Informação e a LGPD.

1.1 QUESTÃO DE PESQUISA

Diante do exposto, este trabalho tem como questão de pesquisa: Como os profissionais de TI compreendem as implicações da Lei Geral de Proteção de Dados (LGPD) para as organizações, quanto à adoção de controles na segurança da informação?

1.2 JUSTIFICATIVAS

O tema “a compreensão do profissional de TI quanto a percepção da LGPD” abordado nesta dissertação fomenta o interesse tanto no meio acadêmico quanto entre gestores públicos, privados e de paraestatais, uma vez que o respeito à Lei Geral de Proteção de Dados Pessoais é compulsório e suas exigências afetam as organizações que atuam em diferentes áreas e de qualquer tamanho. No entanto, a abordagem da compreensão do profissional de TI sobre a Lei, ainda é um assunto pouco discutido no meio acadêmico, mesmo que pese ter sido sancionada em agosto de 2018. Em pesquisas bibliográficas preliminares, foram identificados poucos estudos sobre segurança da informação em organizações paraestatais, sendo este termo entendido, conforme Carvalho (2016, p. 686), como se tratando de ente privado que não integra a administração pública direta ou indireta, mas que exerce atividades de interesse público sem finalidade lucrativa, atuando paralelamente com o Estado no 3º setor, não sendo, portanto, ente governamental e nem organização empresarial. Diante das obrigações criadas pela LGPD, também para essas organizações que implicam em revisões de tecnologias e políticas de segurança da informação, justifica-se a realização desta pesquisa, vez que amplia o conhecimento sobre o tema nesse contexto.

Ainda que a LGPD seja recente, a preservação e a garantia da confiabilidade dos dados são objetivos da estrutura de governança da TI, dos procedimentos e da Política de Segurança da Informação organizacional, como também, as responsabilidades dos profissionais de TI em assegurar a integridade dessas informações. A recente obrigatoriedade de atender a seus artigos reforça não só a necessidade, mas também a tempestividade da realização deste estudo, que visa obter a percepção do profissional de TI sobre os impactos da LGPD nas organizações.

A LGPD suscita interesses a respeito das suas implicações, de seus impactos e de suas oportunidades, tanto para as organizações quanto para os profissionais de TI, uma vez que enseja mudanças na estrutura organizacional e em seus processos de TI, para facilitar o acesso e assegurar aos indivíduos o tratamento dos seus dados pessoais, buscando garantir o direito à privacidade e afastando vulnerabilidades e riscos. De acordo com Sêmola (2014), as informações estão sujeitas a vulnerabilidades que estão em todas as partes de uma organização, o que evidencia a relevância do estudo e justifica sua realização.

Para atender aos requisitos da Lei 13.709/2018 que promove a eficiência na rastreabilidade, na transparência e no controle do tratamento dos dados pessoais pelas organizações, é necessário atentar para as boas práticas da segurança da informação, que, como

entendem Cooper (2009) e Dhillon e Backhouse (2000), visam à confidencialidade, à disponibilidade e à integridade das informações. Assim, para fomentar a aplicação prática da LGPD, é necessário ampliar a compreensão a respeito das suas implicações sobre a segurança da informação nas organizações, bem como, a compensação dos profissionais de TI tem um papel sistêmico na aplicação das medidas de conscientização e de eficácia.

A LGPD foi sancionada para assegurar a privacidade e a transparência no tratamento dos dados pessoais. Segundo Freedman (1987), a privacidade e o direito às informações pessoais passam a ter um novo significado em consequência da sofisticação da tecnologia, sua capilaridade, seu poder de transformação e da possibilidade de comercialização de dados pessoais, o que reforça a necessidade de realizar este estudo. Da mesma forma, os requisitos da Lei podem exigir que mudanças significativas sejam realizadas, na aplicação de tecnologias e nos processos relacionados à segurança da informação, fato que reforça a importância da compreensão do profissional de TI, uma vez que ele é o agente de transformação nos processos da TI de uma organização, o que se mostra como uma justificativa de ordem prática para o estudo

Como a LGPD se revela especialmente importante para garantir os direitos fundamentais de liberdade e de privacidade frente aos interesses comerciais e financeiros, o estudo se mostra relevante e justificado também para a sociedade como um todo.

Por fim, ao considerar as mudanças provocadas pela LGPD para a segurança da informação e para os profissionais de TI, este estudo pode trazer avanços para a área temática de Sistemas de Informação, o que justifica a sua realização também para a Administração como área de conhecimento científico.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Este trabalho tem como objetivo geral identificar como os profissionais de TI percebem a adequação dos controles de segurança da informação nas organizações quanto às exigências da LGPD. Para isto, pretende-se realizar uma pesquisa *Survey* com os profissionais de TI, considerando a participação dos Diretores, dos Gerentes, dos Coordenadores e dos Analista do SENAC que atuam nos 27 Estados do Brasil, onde os resultados foram apurados e tratados através de métodos estatísticos. No momento seguinte, foram convidados alguns Diretores,

Gestores e Coordenadores de TI do SENAC, que atuam estrategicamente, que participaram do Grupo Focal, a fim de colaborarem com as análises dos resultados obtidos na referida pesquisa, como também, apresentaram suas considerações quanto aos pontos abordados e o entendimento deste trabalho.

1.3.2 Objetivos Específicos

Para alcançar o objetivo geral, os objetivos específicos devem cobrir aspectos do problema da pesquisa, como entende Gil (2009). Assim, os seguintes objetivos específicos foram estabelecidos para este estudo:

a) Identificar os controles de segurança da informação adotados pele SENAC;

b) Relacionar os controles técnicos, formais e informais de segurança da informação adotados pelo SENAC aos requisitos da LGPD;

c) Identificar a percepção dos profissionais de TI quanto aos impactos dos requisitos da LGPD sobre os controles de segurança da informação adotados nas organizações;

d) Propor medidas necessárias de adequação dos controles de segurança da informação adotados aos requisitos da LGPD.

1.4 ESTRUTURA DA DISSERTAÇÃO

Esta dissertação foi organizada em sete capítulos, além das referências utilizadas no trabalho. Esta introdução traz a questão-problema, as justificativas, os objetivos da pesquisa e a estrutura da dissertação. O próximo capítulo apresenta a fundamentação teórica do trabalho, abordando a Informação, a Privacidade, os Conceitos de Dados Pessoais e Dados Pessoais Sensíveis, a Segurança da Informação e a Garantia a Proteção dos Dados, Mecanismos de Controle de Dados Pessoais sobre a ótica da segurança da informação, Leis de Proteção de Dados Pessoais no Cenário Internacional e a Lei Geral de Proteção de Dados Pessoais no Brasil. O terceiro capítulo versa sobre os pressupostos e o modelo da pesquisa. O quarto capítulo trata do modelo, do desenho da pesquisa, dos procedimentos metodológicos, dos dados da organização e dos participantes, dos procedimentos de coleta de dados – pesquisa *Survey*, do

tratamento dos dados – grupo focal - e análise de dados. No quinto capítulo são mostrados: a apresentação e análise dos dados, a análise parcial da pesquisa *Survey*, as análises estatísticas descritivas dos indicadores, a matriz de correlação geral dos indicadores, a apresentação da análise de dispersão do indicador da gestão de segurança por cargo, o resultado do grupo focal e a análise geral dos resultados. No sexto capítulo é apresentada a discussão dos pressupostos da pesquisa e no sétimo capítulo vêm as considerações finais, a conclusão e as recomendações para pesquisas futuras.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 INFORMAÇÃO

A informação permeia vários segmentos e atividades, como as ciências, a realização de procedimentos técnicos, o comércio e os processos organizacionais, resultando em seu uso crescente na vida social, cultural, política e econômica da sociedade moderna. Para tal, vários conceitos são atribuídos à informação, e pode ser compreendida como meio para a construção do conhecimento através da troca de mensagens entre dois agentes (ALLEN, 1996; MACHLUP; MANSFIELD, 1983), ou como o dado dotado de relevância e propósito (DRUCKER, 1988), de maneira que esse conceito pode variar com o contexto em que o termo é aplicado (CAPURRO; HJORLAND, 2007). Independentemente do conceito, Le Coadic (2004) argumenta que a informação se tornou um produto e é considerada como um componente essencial para as organizações. Neste sentido, a informação adquiriu um caráter estratégico e pode ser o principal ativo de uma organização, como entende Dias (2000). Marciano (2006) cita que Shannon (1948) apresenta a informação como um elemento mensurável sobre a perspectiva do emissor e do receptor desta informação. Para Henessy e Babcock (1998), o valor da informação é como um elemento modificador das incertezas rumo a variabilidade conhecida. De acordo com Marciano (2006), anteriormente reconhecida por seu papel como redutora de incertezas, a informação é cada vez mais vista como um recurso transformador do indivíduo e da sociedade, cabendo-lhe o papel essencial no contexto socioeconômico vigente, não por acaso denominado de Era da Informação.

A informação no contexto organizacional configura-se como um valor de recursos econômicos primordiais, pois é um elemento de poder no campo do processo decisório, onde vem sendo utilizada não só para a definição de produtos e serviços, como também, para estabelecer desempenhos, definição de processos e procedimentos, entre outros, e quanto mais pertinente for uma informação, maior é o seu valor. Para Davenport e Prussak (2002), o conhecimento é valioso, pois "corresponde a informação com um contexto, um significado, uma interpretação". Corroborando, Stair (2002) considera que o valor da informação está diretamente relacionado à tomada de decisão e com foco na lucratividade e deve ser: completa, econômica, flexível, confiável, relevante, simples e verificável. Neste contexto, a informação deixou de ser um recurso segmentado e/ou singular para ser o recurso organizacional. Já para Moresi (2000), a informação pode ter valores diferentes para pessoas diferentes, podendo assumir também valores diferentes para uso e para troca.

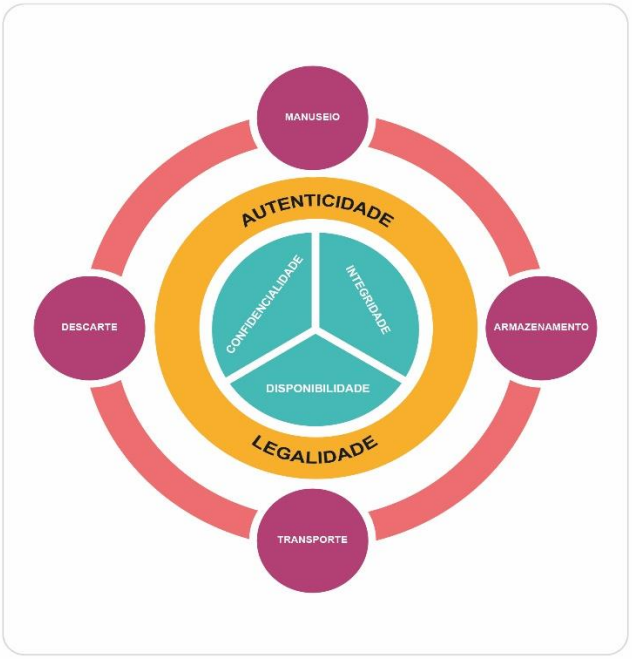
As normas NBR ISO/IEC 27002 e NBR ISO 27001:2013, da Associação Brasileira de Normas Técnicas (ABNT, 2013), afirmam que a informação é um ativo que, como qualquer outro ativo importante, pode ser essencial para o cumprimento da missão de uma organização e, por este motivo, necessita ser protegida. As normas explicam também que a segurança da informação é a proteção da informação contra vários tipos de ameaças, a fim de garantir a continuidade do negócio, minimizando os riscos e maximizando o retorno sobre investimentos e as oportunidades de negócio. Além disso, as normas estabelecem como objetivo da segurança da informação a preservação da confidencialidade, da integridade e da disponibilidade da informação, com o que concordam Dhillon e Backhouse (2000).

Nesse sentido, a integridade é a garantia de que a informação manterá suas características originais estabelecidas pelo seu proprietário, garantindo que não haja alteração não autorizada (LOPES, 2012), visando à garantia da sua exatidão contra mudanças não autorizadas, sejam acidentais ou intencionais (COOPER, 2009). A disponibilidade da informação é a garantia de que a informação poderá ser acessada sempre que seus legítimos usuários precisarem. Já quanto à confidencialidade da informação, o objetivo é garantir que será acessada apenas por quem estiver legitimamente autorizado para evitar sua divulgação indevida (COOPER, 2009; LOPES, 2012).

Considerando a temporalidade da informação e sua integridade, Sêmola (2014) alerta sobre a importância de estar atento a todos os momentos do ciclo de vida da informação, como ilustra a figura 1 que estabelece como princípios da segurança da informação a autenticidade e a legalidade da informação. Floridi (2010), por sua vez, destaca a importância de uma gestão eficiente do ciclo de vida da informação (figura 2). Nota-se que o ciclo de vida da informação apresentado por Sêmola (2014) é finalizado com a etapa de manuseio da informação. O mesmo acontece com o modelo de Floridi (2010), porém este autor apresenta a possibilidade de reciclar e eliminar a informação, ou seja, é uma decisão que pode direcionar para a preservação da informação pela reciclagem, o que difere de Sêmola (2014) que prevê o descarte da informação, assim que o tempo de guarda for concluído.

Neste trabalho, a informação é admitida como conhecimento, sendo este um dado dotado de valor, segundo Davenport e Prussak (2002), ou dotado de relevância e de propósito, conforme Drucker (1988). Como todo ativo que tem valor, a informação precisa ser protegida e é o elemento a ser protegido por medidas de segurança da informação (FONTES, 2006; SÊMOLA, 2014). Neste sentido, o profissional de TI deve compreender o valor da informação e suas responsabilidades na garantia do cumprimento da Lei nº 13.709/2018.

Figura 1 – Ciclo de Vida da Informação na Segurança da Informação



Fonte – Adaptado de Sêmola (2014)

Figura 2 – Ciclo de Vida da Informação – Modelo de Floridi

Fonte – Adaptado de Floridi (2010)

2.2 PRIVACIDADE

O desenvolvimento da TI aumentou a disponibilidade de recursos tecnológicos digitais nos diversos segmentos da sociedade, mas também facilitou a exposição dos dados pessoais. Desta forma, foi necessário regulamentar as diretrizes que assegurem a proteção desses dados e, consequentemente, a privacidade das pessoas. Observa-se a ligação entre a proteção de dados pessoais com a privacidade, fato que deve ser contextualizado considerando a evolução social e tecnológica.

O conceito de privacidade teve origem na sociedade feudal no início da disposição das habitações em cidades com a ascensão da burguesia, que passou a proteger sua propriedade e sua própria intimidade. Segundo Rodotá (2008), a privacidade não era uma experiência natural de cada indivíduo, mas sim um privilégio de um grupo específico, decorrente do direito da propriedade. Somente no final do século XIX, a privacidade é desassociada do direito à propriedade, passando para o direito a inviolabilidade da intimidade, que foi destaque no artigo "*The Right to Privacy*", de Warren e Brandeis, publicado na Harvard Law Review, em 1890. Os autores defenderam a criação e proteção de novos direitos, considerando a transformação que a sociedade sofreu (NAVARRO, 2011).

O conceito de privacidade esteve ligado a questões jurídicas, com o entendimento de que é essencial para a realização da pessoa humana e do livre desenvolvimento de sua personalidade (DONEDA, 2020). Após as duas Guerras Mundiais, o direito à privacidade do indivíduo é reforçado pela necessidade de proteção do homem em sua essência, fundamentado na dignidade humana. A forma como a privacidade passou a ser compreendida se tornou determinante na construção do indivíduo como ser, no desenvolvimento de sua personalidade e na sua inserção na sociedade (CANCELIER, 2017).

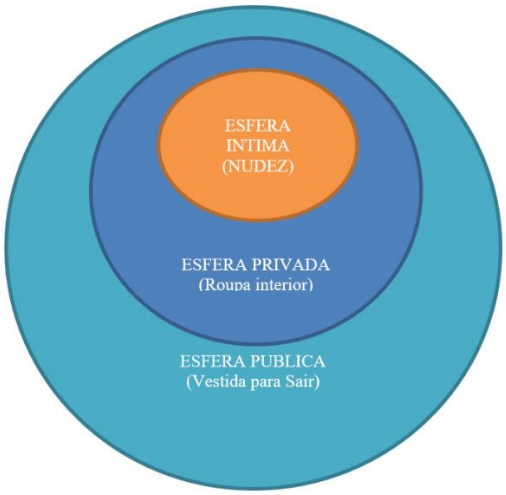
Esse entendimento resultou em leis em diferentes países. No Brasil, a privacidade é reconhecida como direito fundamental pela Constituição Federal de 1988, bem como pelo Código Civil de 2002, mas em ambos os casos o termo é referido como vida privada e intimidade e como a proteção das escolhas pessoais. Rodotá (2008, p. 15) expande esse entendimento ao defender que o direito à privacidade é "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular". Bioni (2019) corrobora com o entendimento de que a privacidade está relacionada à capacidade dos indivíduos de controlar e determinar como são usados seus dados.

Para Doneda (2020), a privacidade deve ser compreendida como um espaço de liberdade com condições de desenvolvimento da própria personalidade, livre de qualquer tipo de controle social. Já Sheehan e Hoy (2000) entendem que a privacidade está relacionada a garantias quanto à proteção e uso dos dados pessoais, enquanto Paesani (2014) complementa que privacidade envolve o direito do indivíduo à autodeterminação da informação, que seria a faculdade de controlar o uso que terceiros fazem dos seus dados pessoais e o direito de corrigir erros em cadastros e bancos de dados. Fica claro, portanto, que privacidade envolve o controle dos dados pessoais pelos indivíduos, o que ganha relevância diante da possibilidade de uso abusivo, manipulação e exposição de dados pessoais. Xu *et al*. (2008) complementam que o conceito de privacidade depende do contexto em que o termo é aplicado e varia conforme experiências vividas pelos indivíduos.

A exposição de dados pessoais pode envolver imagens, comunicações pessoais, localização, associações em grupos e experiências vividas por indivíduos, o que põe em risco sua intimidade (CORCORAN, 2016). A introdução de novas tecnologias e de formas de usá-las pede atenção para esse fenômeno (PAESANI, 2014), pois vulnerabilidades existentes e a exposição de dados em ambiente digital podem afetar o direito à privacidade.

Para explicar a privacidade, Hummann (2016) propõe três dimensões de controle e exposição de dados: a esfera pública, que trata de ausência de restrições de acesso ou uso dos dados; a esfera privada, onde os dados são controlados através da imposição de algumas restrições, limitando quem tem acesso; e a esfera íntima, onde os dados são totalmente protegidos e o acesso só ocorre com o pleno consentimento do indivíduo (figura 3).

Figura 3 – Teoria das Esferas de Heinrich Hubmann



Fonte: Medium

Sheehan e Hoy (2000) propõem cinco princípios para a privacidade: a consciência do indivíduo sobre os dados a seu respeito e do uso que é feito deles; a possibilidade de escolha sobre como esses dados serão usados ou divulgados; a garantia de que o indivíduo terá acesso aos seus dados em posse de outro indivíduo ou organização; a segurança de que esses dados serão guardados por que está de posse deles; e o direito de recorrer sempre que houver uma violação da sua privacidade e para corrigir erros nos seus dados. A observação desses princípios garantiria, assim, o controle do indivíduo sobre seus dados.

No entanto, a tecnologia vem trazendo uma dificuldade crescente para garantir que esses princípios sejam respeitados. Os dados vêm sendo gerados e armazenados em larga escala e o volume de dados cresce de forma exponencial (COUPOFY, 2016; VAN DEN HOVEN, 2008), o que aumenta a responsabilidade das organizações que guardam e manipulam esses dados (MOREIRA, 2001), exigindo cautela e um comportamento ético por parte das pessoas que trabalham nessas organizações (FONTES, 2016).

2.3 CONCEITOS DE DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

Na sociedade da informação, as pessoas utilizam constantemente dispositivos de comunicação para lazer, trabalho ou outras situações da vida cotidiana. Com eles, acessam constantemente sistemas de informação hospedados e mantidos por diferentes atores. Como consequência, os dados gerados nesse processo são armazenados em um ou mais bancos de dados que ficam em locais difusos e desconhecidos dessas pessoas, esses dados podem ser armazenados “na nuvem”[1].

Dados pessoais podem ser de grande diversidade, como: números de documentos, endereço profissional, cor de pele, município e estado de nascimento, hábitos de compras, religião, situação financeira, escola e universidade em que estudou, formação e profissão, além[2] de nome, sobrenome, número de telefone e endereço residencial. Pinheiro (2020) entende que, ainda que isoladamente não permitam identificar uma pessoa, isso pode acontecer através do cruzamento desses dados. De acordo com Ferreira (2018), mecanismos muitas vezes automáticos podem ser usados para análise, manipulação e transmissão desses dados para outras

[1] Associação Brasileira de Normas e Técnicas (ABNT) traduziu o conceito de *cloud computing* (processamento na nuvem) criado pela International Organization for Standardization (ISO) como “um paradigma para habilitar o acesso, via rede, a um grupo escalável e elástico de recursos, físicos ou virtuais, com auto provisionamento e administração sob demanda”. (ABNT NBR ISO/IEC 17788:2015)

organizações, o que facilita a realização do cruzamento desses dados e a identificação e exposição do indivíduo ao qual se referem.

Esses são considerados dados pessoais sensíveis, conforme o art. 5º, inciso II da Lei 13.709/2018, que explica que são dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização religiosa, filosófica ou política, dado sobre a saúde ou vida sexual, além de dados genéticos ou biométricos, que permitem a identificação do seu proprietário. Pinheiro (2020) reforça esse entendimento classificando dados pessoais sensíveis como aqueles relativos a atributos da personalidade do ser humano e suas escolhas particulares. Para Bioni (2019), dados sensíveis compreendem um tipo de dados pessoais em razão de o seu conteúdo oferecer vulnerabilidade relacionada à possibilidade de discriminação.

Doneda (2010, p. 191) procurou ampliar a questão relativa à proteção de qualquer dado pessoal, e não somente do dado sensível, justificando que qualquer dado pessoal é passível de possibilitar a discriminação ou o controle sobre o indivíduo, diminuindo sua liberdade de escolha. No entanto, o autor destaca que os dados sensíveis merecerem uma proteção diferenciada, visto que têm maior potencial para prejudicar o titular devido à má utilização – e por este motivo são considerados “sensíveis” em relação aos demais.

O art. 8.1 da Diretiva 95/46/CE do Parlamento europeu proíbe o processamento dos dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, o pertencimento a sindicatos, assim como o tratamento de dados relativos à saúde ou à sexualidade, considerando o descumprimento um ato passível de condenações criminais. Para evitar que ocorra, a norma prevê o controle prévio por parte das autoridades de controle, como a verificação da pertinência do tratamento dos dados para coibir excessos.

Pinheiro (2019) conceitua o tratamento de dados como toda operação realizada com algum tipo de manuseio desses dados. O autor entende como tratamento a coleta, a produção, a recepção, a classificação, a utilização, o acesso, a edição, a modificação, a reprodução, a transmissão, a distribuição, o processamento, o arquivamento, o armazenamento, a eliminação, a avaliação ou o controle, a comunicação, a transferência, a difusão ou a extração. Neste sentido, Frazão (2019) expressa preocupação sobre como são tratados os dados pessoais e evidencia a necessidade de garantir os direitos fundamentais de liberdade, de privacidade e de livre desenvolvimento da personalidade da pessoa natural. A autora destaca as reflexões e ponderações sobre a possibilidade de as organizações poderem discriminar ou manipular as opiniões das pessoas através do tratamento desses dados, possibilidade evidenciada por Foxman

e Kilcoyne (1993), Mulholland (2018) e Poullet (2018). Torna-se relevante adotar medidas que garantam a proteção dos dados pessoais sensíveis.

2.4 A SEGURANÇA DA INFORMAÇÃO E A GARANTIA DA PROTEÇÃO DOS DADOS PESSOAIS

Para além da tecnologia, através da implementação de normas, procedimentos, diretrizes e regras de segurança da informação, é possível estabelecer controles que auxiliam na proteção dos dados pessoais (ABRAHÃO, 2003).

Sêmola (2014) define a segurança da informação com a área do conhecimento dedicada à proteção dos ativos de TI. Para Mandarini (2004), a segurança da informação visa à proteção das informações e os investimentos realizados pelas organizações para controlar e combater às ameaças existentes às informações, minimizando riscos e maximizando os investimentos em TI. Para isto, é preciso entender que as ameaças podem estar em todas as partes de uma organização e que a segurança envolve também as pessoas, e não somente a tecnologia, completa Sêmola (2014).

Não sendo uma questão puramente técnica, mas também organizacional e social (BELASCO; WAN, 2006; LUO et al., 2011; MITNICK; SIMON, 2003; SÊMOLA, 2014), é necessária uma preocupação com as organizações e os profissionais de TI quanto ao sigilo de dados pessoais no âmbito dos seus sistemas de informação. Chang e Ho (2006) consideram essenciais também questões como privacidade, vulnerabilidade, risco e confiança

A relevância da política de segurança da informação está no estabelecimento dos critérios de confiança e dos controles dos riscos que mitigam as ameaças de vazamento acidental ou intencional. Neste sentido, é necessária uma preocupação com as organizações e os profissionais de TI quanto ao sigilo de dados pessoais no âmbito dos seus sistemas de informação. Os mecanismos de proteção, técnicos ou não, são a maneira de se manter a informação sob sigilo, uma vez que a sociedade está cada vez mais *on-line* e as informações dos indivíduos mais disponíveis para as organizações. Tal situação tem aumentado a preocupação com a privacidade de informações tanto para as pessoas, para a comunidade científica e para as organizações (MARTORELL; NASCIMENTO; GARRAFA, 2016).

As informações podem ser expostas, tornadas inacessíveis ou corrompidas, devido a incidentes naturais ou não, como incêndios, inundações, tremores de terra e tumultos urbanos,

e que podem estar ou não relacionados diretamente às informações. Há ainda a possibilidade de incidentes relacionados às ações ou omissões de pessoas de fora ou de dentro das organizações e que podem ser intencionais ou não. Independentemente da intencionalidade ou do agente causador, esses incidentes podem também expor ou corromper informações sensíveis (BELASCO; WAN, 2006; WHITMAN, 2003). Estas possibilidades apontam para os riscos relacionados ao comportamento humano. Acquisti e Grossklags (2003) estudaram o comportamento das pessoas quanto à segurança da informação e concluíram que, apesar da existência de mecanismos tecnológicos para proteger a informação, nem sempre é possível ter a segurança da informação. Segundo os autores, este fenômeno é uma decorrência do chamado *fator humano* da segurança da informação, segundo o qual o comportamento das pessoas que lidam diretamente com informações sensíveis pode comprometer sua segurança. Pfleeger (1997) concorda ao sustentar que os investimentos em segurança da informação devem considerar três segmentos: pessoas, tecnologia e processos.

Considerando o fato de não se ter controles eficazes quanto aos riscos decorrentes de ações humana no uso de tecnologia (BELASCO; WAN, 2006; LUO et al., 2011; MITNICK; SIMON, 2003), há o aumento da importância de se utilizar meios para mudar o comportamento das pessoas com relação à segurança da informação e privacidade. Para Fontes (2016), isso é possível através de ações de conscientização, treinamentos, procedimentos, políticas, normas e orientações.

A necessidade de estabelecer controles que busquem adequar o comportamento humano reforça a complexidade dos processos internos de segurança da informação nas organizações. Soma-se a isto a necessidade de garantir a conformidade aos regulamentos e leis (HÖNE; ELOFF, 2002).

A utilização de controles de segurança da informação, visando à proteção de dados pessoais passa, indispensavelmente, pela aplicação de medidas para garantir os três princípios da segurança da informação: integridade, disponibilidade e confidencialidade. Essas medidas envolvem processos organizacionais e tecnologias (HERATH; HERATH; BREMSER, 2010), bem como uma preocupação com a conformidade legal (ALBUQUERQUE JUNIOR *et al.*, 2018; HÖNE; ELOFF, 2002), que evidencia sua complexidade e aumenta sua relevância no contexto organizacional. A conformidade com requisitos legais é um dos objetivos indiretos da segurança da informação, como previsto na norma NBR ISO IEC/27002 da ABNT (2013), e está estritamente ligada à necessidade de atender aos requisitos da legislação que trata da proteção de dados pessoais.

Segundo Doneda (2006), a proteção de dados pessoais transforma a concepção contemporânea de proteção da privacidade, deixando de "dar vazão somente a um imperativo de ordem individualista" – o direito de ser deixado sozinho e a não intrusão –, passando a "ser a frente onde irão atuar vários interesses ligados à personalidade e às liberdades fundamentais da pessoa humana" (DONEDA, 2006, p. 30). Para Bioni (2019), a proteção de dados pessoais tem sido compreendida como o direito de o indivíduo ter autodeterminação sobre suas informações pessoais, fazendo com que o cidadão emita autorizações e controle o fluxo dos seus dados pessoais.

Segundo Whitman (2003), as ameaças para a segurança da informação podem ser classificadas em categorias que incluem erros ou falhas tecnológicas (*software* e *hardware*), obsolescência dos ativos de TI, vazamento de informações por espionagem, vandalismo, sabotagem e ou extorsão (atos humanos intencionais) e por força da natureza. No entanto, Belasco e Wan (2006) classificam as ameaças à segurança da informação em três tipos: técnicas, que necessitam da tecnologia; humanas, que estão relacionadas com a ética e o comportamento humano; e naturais, provocadas por elementos da natureza (Quadro 1).

Quadro 1 – Classificação de Ameaças

TIPOS	EXEMPLOS
Técnicas	Códigos maliciosos, ataques e acessos não autorizados por hackers e terroristas, negação de serviços, abusos praticados por usuários internos ou externos, boatos e sondagem de informações utilizando recursos tecnológicos.
Humanas	Visualização inadvertida de informações sensíveis, sabotagem de dispositivos físicos, terrorismo e roubo de informações ou documentos.
Naturais	Gelo, fogo, terremoto, tornado e tempestade.

Fonte: Belasco e Wan (2006).

Deve haver a compreensão não só de gestores e de profissionais de TI, mas também de gestores das organizações, de que a proteção de dados pessoais passa pela implementação de controles que atendam às necessidades técnicas e de comportamento humano, bem como de formalização desses controles nos processos e na estrutura organizacional (ALBUQUERQUE JUNIOR; SANTOS, 2015).

2.5 MECANISMOS DE CONTROLE DE DADOS PESSOAIS SOBRE A ÓTICA DA SEGURANÇA DA INFORMAÇÃO

A informação é reconhecida como um ativo de valor que pode trazer vantagens competitivas, destacam Fortes (2016) e Sêmola (2014). Para Jimene (2020), a sociedade está vasta por conexão pela *internet*, e como consequência, as informações vêm sendo cada vez mais expostas. A autora reforça que essa exposição indevida das informações pode ocasionar prejuízos diversos decorrentes de ataques cibernéticos, de fraudes digitais, de vazamento de informações e de concorrência desleal, dentre outras causas, podendo comprometer a competitividade organizacional.

De acordo com Bioni (2019), as informações pessoais são necessárias para a economia na sociedade informacional. Como as informações são fluidas, o fluxo informacional se tornou mais complexo e dificultou o exercício do controle dos dados pessoais por parte dos seus titulares.

Considerando a informação como um ativo de valor e o indivíduo cada vez mais vulnerável no ambiente digital conectado, é relevante o desenvolvimento de mecanismos e de controles para a segurança da informação. Para Mandarini (2004), a segurança da informação deve ser responsável por proteger informações sensíveis, e essa proteção pode prevenir fraudes e assegurar a integridade dos dados armazenados e processados por uma organização.

Segundo Jimene (2020), a segurança da informação tem o foco na necessidade de proteger dados pessoais, não sendo um processo novo. Para colaborar com essa afirmação, Machado (2014, p. 23) expõe o conceito de segurança da informação de forma bem simples e didática: “a segurança da informação é uma maneira de proteger os sistemas de informação e a sociedade contra diversos ataques, mantendo documentos e arquivos dentro dos princípios de confidencialidade, integridade e disponibilidade”. De acordo com Jimene (2020), os profissionais de TI das organizações devem utilizar de medidas técnicas, tecnológicas e administrativas que possibilitem a proteção de dados pessoais de acessos, para evitar incidentes e o uso ilícito das informações. Nesse sentido, a autora complementa que podem ser utilizadas medidas não só técnicas ou tecnológicas, mas também administrativas.

Reforçando a necessidade de ter maior controle sobre dados pessoais, Bioni (2019) argumenta que dois conceitos podem ser considerados: a expressão *Privacy by Design*, que põe a proteção dos dados pessoais no centro do desenvolvimento de produtos e serviços; e *Privacy Enhancing Technology* (PET), que é um conjunto de medidas tecnológicas voltado para

manutenção da privacidade através da eliminação ou redução do uso de dados pessoais desnecessários em sistemas de informação. Trata-se de uma mudança na forma de desenvolver e implementar tecnologias e sistemas de informação com um foco na proteção dos dados pessoais, o que pode contribuir, consideravelmente, para a conformidade das organizações com os requisitos da legislação voltada para esse tema, envolvendo recursos tecnológicos, processos administrativos e o comportamento das pessoas

Nesse sentido, Björck (2005) entende que controles de segurança da informação podem ser normas, estruturas organizacionais, processos organizacionais, programas de treinamento e conscientização, planos, estratégias e a Política de Segurança da Informação organizacional, que têm como objetivos conscientizar e alterar o comportamento dos indivíduos formalmente (estabelecendo metas, obrigações e responsabilidades) e informalmente (capacitando e conscientizando). Para o autor, são controles de segurança da informação também tecnologias implantadas nos ambientes computacionais das organizações, como controles de acesso lógico e físico, antivírus, soluções de *backup*, biometria, criptografia, *firewalls*, monitoramento de ambientes críticos, proteção contra desastres naturais, bloqueios e alarmes, além do uso de ambientes seguros e salas cofre.

Esses controles de segurança da informação podem ser classificados de diferentes maneiras (BJÖRCK, 2005; YEH; CHANG, 2007; SÊMOLA, 2014), podendo ser por sua finalidade, aproximação com a tecnologia ou pelas características que buscam afetar na organização. A classificação proposta por Dhillon (1999) tem por base o que esses controles buscam afetar na organização:

a) Controles técnicos: visam à limitação do acesso a prédios, salas, computadores e sistemas (DHILLON, 1999; DHILLON; MOORES, 2001), incluindo mecanismos que operam em sistemas computacionais e controlam o acesso lógico, como antivírus, *firewalls*, correções de vulnerabilidades de sistemas existentes, realização de *backup*, uso de biometria, criptografia sistemas de detecção de intrusos (BELASCO; WAN, 2006; SENTHILKUMAR; ARUMUGAM, 2011; GORAYEB, 2012), além dos controles que visam à proteção das informações por meios físicos, como soluções de controle de acesso físico, alarmes e proteção contra fogo (BJÖRCK, 2005).

b) Controles formais: buscam afetar a organização e as pessoas por meio de regras e conformidade da organização com leis e procedimentos. Esses controles envolvem a definição de funções, de responsabilidades, de planos, de objetivos

e de papéis, como o Sistema de Gestão de Segurança da Informação, a Política de Segurança da Informação, o Escritório de Segurança da Informação e a equipe de tratamento de incidentes (DHILLON; MOORES, 2001; KILLCRECE et al., 2003; MANDIA; PROSISE; PEPE, 2003; FARN; LIN; FUNG, 2004; BJÖRCK, 2005; CASEY, 2005; MARTINS; SANTOS, 2005; PARK; JANG; PARK, 2010; MANOEL, 2014; SÊMOLA, 2014).

c) Controles informais: visam afetar a organização e as pessoas promovendo o conhecimento e a conscientização através de ações de treinamento e educação em segurança da informação (BJÖRCK, 2005), envolvendo a comunicação de responsabilidades e a promoção de comportamentos (DHILLON; MOORES, 2001), bem como a realização de treinamentos e ações de conscientização e divulgação (DHILLON; MOORES, 2001; SÊMOLA, 2014).

Neste trabalho foi utilizada a tipologia de Dhillon (1999) para classificar os controles de segurança da informação identificados em diferentes trabalhos na literatura sobre o tema (Quadro 2). Para este autor, a adoção de controles isolados e o foco em ações específicas devem ser evitados. Ao invés disso, deve-se considerar o contexto organizacional e outros controles que devem ser adotados em conjunto. Sveen, Torres e Sarriegi (2009) acrescentam que há uma interdependência entre os diferentes tipos de controles de segurança da informação, de forma que controles técnicos dependem de controles formais e informais, enquanto controles formais dependem de controles informais, como ações de conscientização e educação e do apoio das tecnologias implantadas para reforçar comportamentos adequados.

Conforme corrobora Jimene (2020), os mecanismos de controle voltados para os dados pessoais devem seguir as diretrizes, as regras e as políticas definidas pela área de segurança da informação, segundo as características, as categorias e os critérios de classificação dos dados coletados e manipulados. Assim sendo, controles técnicos devem considerar as possíveis exposições dos dados dos indivíduos a diferentes vulnerabilidades, segundo Bioni (2019). Os Profissionais de TI devem observar as Leis que tutelem sob a manipulam dados pessoais, e as quais, podem ter implicações em controles formais, informais e técnicos para as organizações.

Além disso, a interdependência entre controles formais, técnicos e informais suscita que requisitos da LGPD podem ter implicações que vão além de questões administrativas e comportamentais.

Quadro 2 – Tipos de Medidas Técnicas, Formais e Informais

CATEGORIAS	TIPOS E EXEMPLOS
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 periódica da Política de Segurança da Informação.
Técnicas	Redundância de dados; Segregação e monitoramento de redes de computadores; Redundância de peças de equipamentos; Prevenção contra códigos maliciosos; Controle de acesso lógico; Transmissão e armazenamento seguros de dados; Autenticação forte; Redundância de equipamentos; Controle de acesso físico; Proteção ambiental.
Informais	Treinamento de profissionais de TI; Treinamento de usuários de TI; Divulgação de regulamentos e da Política de Segurança da Informação; Ações de conscientização.

Fonte: elaborado por Albuquerque Junior (2018) com base em Dhillon e Moore (2001), Farn, Lin e Fung (2004), Björck (2005), Belasco e Wan (2006), Juels (2006), Doherty e Fulford (2006), Thorpe (2006), Panko (2006), Park, Jang e Park (2010), Gorayeb (2012), ABNT (2013), Casey (2005), Martins e Santos (2005), Manoel (2014) e Sêmola (2014).

2.6 LEIS DE PROTEÇÃO DE DADOS PESSOAIS NO CENÁRIO INTERNACIONAL

Desde a introdução da ideia de sociedade da informação na década de 1970, (CASTELLS, 2016; MATTELART, 2001), houve um avanço acelerado na utilização da TI e um reposicionamento da informação para o centro da vida em sociedade. Esse movimento aconteceu, principalmente, através da ampla utilização de dispositivos tecnológicos nos mais diversos aspectos da vida cotidiana. Com isso, recursos tecnológicos passaram a coletar dados muitas vezes sem que seu usuário soubesse disso ou sem conhecer a finalidade dessa coleta de dados, e a manipulação desses dados pode ser feita também utilizando recursos tecnológicos (MOORE, 2001).

Como consequência disso, governos e organizações internacionais passaram a regulamentar e restringir a coleta e processamento de dados pessoais (BAUMER; EARP;

PAYTON, 2000; BERGKAMP, 2002; BHAIMIA, 2018; HALLINAN; FREIDEWALD; McCARTHY, 2012; JASSERAND, 2018; KITIYADISAI, 2005; LIMA; MONTEIRO, 2013; LINDSAY, 2005; POULLET, 2018; TIKKINEN-PIRI; ROHUNEN; MARKKULA, 2018). Nesse contexto, o Conselho da Europa buscou a proteção dos dados pessoais através de diretrizes que uniformizaram o tratamento desses dados na Diretiva nº 95/45/EC (MORGADO, 2009). Essa preocupação fez com que a proteção de dados pessoais deixasse de ser uma decisão puramente ética ou de gestão para e se tornar uma obrigação legal na União Europeia. Essa iniciativa foi tomada também de forma isolada por diferentes países, muitos dos quais antes da própria União Europeia.

Na Alemanha, foi criada, em 1977, uma lei que protege contra a utilização abusiva dos dados pessoais (ZANINI, 2020). Chamada localmente de *Bundesdatenschutzgesetz*, ou simplesmente BDSG, a Lei trata dos direitos e deveres de organizações públicas e privadas que coletam e processam dados pessoais (GEIGER, 2003).

Outra lei que se destaca por ser uma das primeiras a tratar de proteção de dados pessoais é a *Australian Privacy Act*, ou Lei de Privacidade Australiana, que desde 1988 traz os princípios de privacidade e regula todas as organizações públicas e privadas quanto ao uso e divulgação de dados pessoais, bem como direitos do titular dos dados e regras aplicáveis à manutenção da qualidade desses dados, além de transparência e anonimato, complementando outras leis referentes ao tema para regiões e setores específicos (LINDSAY, 2005).

Na América Latina, destaca-se a Lei nº 25.326/2000, que trata da proteção de dados pessoais na Argentina, considerado o primeiro país do continente a abordar o tema. Essa Lei determina que a coleta de dados pessoais só pode ser realizada mediante autorização dos indivíduos e se aplica a pessoas e organizações que lidam com esse tipo de informação no país, dando aos titulares poder de decisão sobre suas bases e criando obrigações para as pessoas e organizações que as manipulam, além de criar órgãos para supervisão da proteção desses elementos referenciais e sanções para quem a descumprir (RAMINELLI; RODEGHERI, 2016).

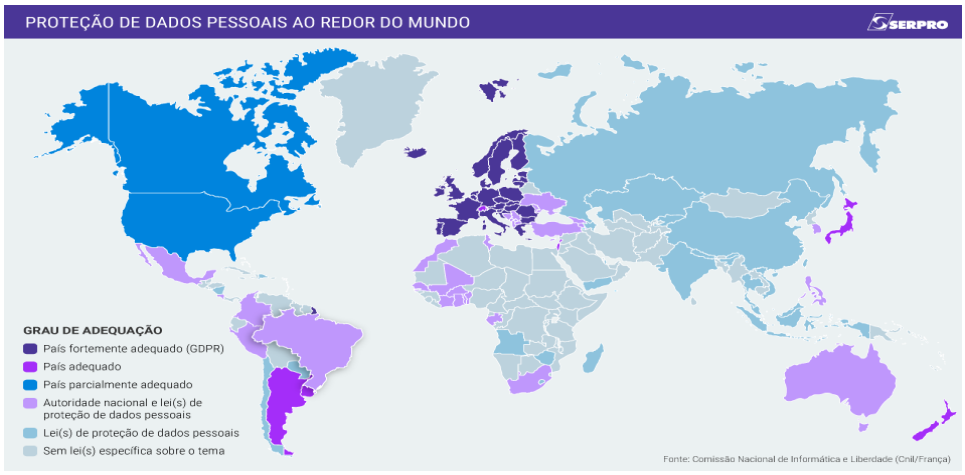
A partir do final da década de 1990 e, principalmente, após a década de 2000, foram publicadas diversas leis que tratam do assunto em diferentes países, como no Canadá (BENNETT; PARSONS; MOLNAR, 2014), no México, na Colômbia (MAGALHÃES; DIVINO, 2019), nos Estados Unidos (LENERT; MCSWAIN, 2020) e no Reino Unido (MORGADO, 2009), tanto em uma única lei quanto em leis esparsas. Essas leis trazem, de forma geral, princípios para nortear o tratamento dos dados pessoais, garantias para os titulares dos dados e obrigações para as organizações e pessoas que lidam com esses dados.

No entanto, possivelmente o mais importante reforço para a regulamentação da proteção dos dados pessoais no mundo foi a já citada legislação da União Europeia. Esta Lei de 1995 determina que o processamento dos dados pessoais seja justo para os indivíduos, e os dados pessoais processados sejam adequados, relevantes e não excessivos para os propósitos aos quais se destinam. Além disso, deve estar claro para o titular quais dados serão coletados, para que finalidade e por quanto tempo eles serão usados, sempre com o consentimento do indivíduo (MORGADO, 2009).

Embora haja diferenças significativas entre as leis internacionais que tratam da proteção de dados pessoais, elas costumam ter pontos em comum, como: a necessidade das organizações realizarem avaliações de impactos para as pessoas cujos dados serão tratados; a criação de escritórios para tratar de questões de privacidade nas organizações; a transparência quanto ao que será feito com os dados, além da criação de autoridades nacionais para tratar do tema (CUSTERS et al., 2018). Em geral, há um entendimento de que esses dados não devem ser armazenados por mais tempo do que o necessário, e, ainda, da proibição do processamento de dados que revelem origem racial ou étnica, posições políticas, crenças religiosas e filosóficas, associação a sindicato, estado de saúde e estilo de vida sexual. Para que o processamento desses dados seja legal, deve ser feito com o consentimento do indivíduo e deve ser necessário para a realização de algumas atividades específicas, como, por exemplo, a realização de alguma atividade de interesse público (MORGADO, 2009).

Vários países no mundo já estão adequados total ou parcialmente às leis de proteção de dados pessoais, com destaque para os europeus (figura 4). Inspirada na legislação europeia, a LGPD brasileira foi publicada em agosto de 2018 e determina regras para captação, armazenamento e compartilhamento de dados pessoais no Brasil, prevendo procedimentos que as organizações precisarão adotar para impedir abusos quanto ao tratamento de dados pessoais (RUARO; GLITZ, 2019).

Figura 4 – Mapa de Adequação a Lei de Proteção de Dados no Mundo



Fonte: Extraído do site da SERPRO – Fonte: Comissão Nacional de Informática e Liberdade (CNI/França)

A adequação à LGPD brasileira, seja em organizações públicas, privadas ou paraestatais, deveria ter acontecido entre sua sanção em 2018 e 2020, quando todas as sanções previstas deveriam entrar em vigor. Entretanto, o início da vigência de parte dos seus requisitos foi adiado para agosto de 2021, o que pode ter atrasado o processo de adequação nas organizações. Atualmente, o cenário é híbrido, como demonstrado na linha do tempo na figura 5.

Figura 5 – Cenário Linha do Tempo da Lei Geral de Proteção de Dados no Brasil

Fonte: Extraído do site da SERPRO

2.7 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Antes de ser sancionada a LGPD, já havia no Brasil e em outros países a discussão sobre a importância dos dados pessoais e, consequentemente, sobre sua proteção, em especial, devido

à ocorrência de incidentes relacionados à ampla utilização de recursos tecnológicos para coletar, armazenar e processar dados (BENNETT, 1997; BOFF; FORTES, 2014; DONEDA, 2010; ESS, 2008; GELLMAN, 1997; VAN DEN HOVEN, 2008; LIMA; MONTEIRO, 2013; RINDFLEISCH, 1997; RUARO *et al*., 2015; RUARO; RODRIGUEZ, 2010; SCHWARTZ, 2004). A inspiração para esses regulamentos de proteção de dados pessoais a partir dos anos 1990 vem do desenvolvimento do modelo de negócios da economia digital, como as facilidades de utilização de bases de dados internacionais, incluindo dados pessoais, o que foi proporcionado pelos avanços tecnológicos e pela globalização (PINHEIRO, 2019)

Para aumentar o escopo de proteção que a legislação anterior trazia aos dados pessoais, a LGPD apresentou conceitos e requisitos mais apropriados à realidade atual, com ampla utilização de tecnologia. Oficialmente, nomeada Lei nº 13.709, de 14 de agosto de 2018 (BRASIL, 2018), a LGPD regulamenta o uso dos dados pessoais nas organizações, incluindo o tratamento realizado por meio de seus recursos tecnológicos, também aborda as análises realizadas para atender a seus processos internos e pelas pessoas que lidam com eles (OLIVEIRA et al., 2019).

O texto da LGPD é voltado para a proteção da liberdade e da privacidade e dispõe sobre o livre desenvolvimento da personalidade dos indivíduos, sendo aplicada a qualquer operação, independentemente do meio utilizado ou do local onde se encontra a organização ou os dados, desde que sejam tratados ou coletados no Brasil, e seu tratamento esteja relacionado a algum serviço ou produto oferecido no país, ou os dados sejam referentes a indivíduos localizados no território brasileiro (BRASIL, 2018). Por isso, os dados pessoais armazenados em nuvens públicas e privadas localizadas fora do Brasil também terão que cumprir as exigências da LGPD (PINHEIRO, 2019).

Para assegurar a proteção de dados pessoais, a Lei supracitada define vários termos utilizados no seu texto e traz obrigações para as organizações públicas e privadas. Abaixo estão os principais termos definidos pela lei (BRASIL, 2018):

- Dado pessoal: dado relacionado a pessoa natural identificada ou identificável;
- Dado pessoal sensível: dado pessoal de origem racial ou étnica, ou sobre saúde, vida sexual, ou dados genéticos ou biométricos, ou envolvendo convicção religiosa, filosófica ou política;
- Banco de dados: conjunto estruturado de dados pessoais, independentemente de onde esteja estabelecido ou se em suporte eletrônico ou físico;

- Documento: unidade de registro de informações, independentemente do seu suporte ou formato;
- Tratamento: qualquer operação realizada com dados pessoais, incluindo coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, modificação, comunicação, transferência, difusão ou extração;
- Tratamento da informação: ações referentes a produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação da informação;
- Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- Controlador: aquele a quem competem as decisões sobre tratamento de dados pessoais, podendo ser organização pública ou privada, ou mesmo uma pessoa natural;
- Operador: pessoa ou organização que realiza o tratamento de dados pessoais em nome do controlador.

No contexto da LGPD, tratamento pode ser qualquer tipo de operação envolvendo dados pessoais, inclusive, o armazenamento e a manutenção destes em um banco de dados. Já titular é a pessoa sobre a qual os dados se referem, e o principal interessado na proteção deles. O controlador e o operador são os agentes responsáveis pelo tratamento desses dados: o primeiro é o responsável pela tomada de decisões, e o segundo, pelas ações realizadas para o tratamento. Assim como os regulamentos internacionais, a lei brasileira deixa clara a necessidade do consentimento do titular dos dados pessoais e a imposição de restrições de acesso de pessoas estranhas, o que é de responsabilidade do controlador e do operador (BRASIL, 2018).

No entendimento de Cots e Oliveira (2018), ao proteger o direito fundamental à privacidade, a LGPD protege as pessoas que são suscetíveis às condições do ambiente. Atenta à nova realidade de utilização de dados pessoais pelas organizações, a lei protege a livre iniciativa, mostrando que há uma atenção aos negócios que dependem desses dados, e dispensa a exigência do consentimento para os dados tornados manifestamente públicos pelo titular, resguardados outros direitos decorrentes. Ao mesmo tempo, garante que a utilização de dados

pessoais para fins de pesquisa científica, produção artística e investigação jornalística seja possível, desde que suas regras sejam respeitadas.

Além de trazer definições e regras a serem observadas, a LGPD contém também uma série de princípios que norteiam seu texto e o tratamento de dados pessoais e que, portanto, devem ser observados por organizações e indivíduos (BRASIL, 2018):

- Respeito à privacidade;
- Autodeterminação informativa;
- Liberdade de expressão, informação, comunicação e opinião;
- Inviolabilidade da intimidade, da honra e da imagem;
- Desenvolvimento econômico, tecnológico e a inovação;
- Livre iniciativa, livre concorrência e defesa do consumidor; e
- Direitos humanos, livre desenvolvimento da personalidade, dignidade e o exercício da cidadania pelas pessoas naturais.

Para Peixoto (2020), com a vigência da Lei, alguns de seus aspectos jurídicos começam a ser debatidos à luz do Marco Civil da *Internet* e, sobretudo, com o Código de Defesa do Consumidor (CDC). Ainda para o autor, a legislação é categórica: todos os dados tratados por pessoas jurídicas de direito público e privado, cujos titulares estejam no território nacional, ou a sua coleta se deu no país, ou ainda que tenha por finalidade a oferta de produtos ou serviços no Brasil, devem estar preparadas. Assim, não se trata de uma opção, mas de uma obrigação das organizações a adequação às normas brasileiras de proteção de dados pessoais.

As transações realizadas no ambiente virtual, atualmente, fazem parte do dia a dia das pessoas. Portanto, é preciso garantir os direitos das pessoas no mundo digital da mesma forma que esses direitos são garantidos no mundo real. Nesse sentido, é importante destacar que a LGPD não protege somente os dados pessoais nos meios digitais (PINHEIRO, 2019).

Segundo Peixoto (2020), para manter negócios com os países europeus, as organizações serão obrigadas a garantir que suas políticas de tratamento de dados estejam em conformidade com as leis de proteção de dados pessoais sob o risco de penalidades, além da perda de clientela, do valor de marca e da credibilidade no mercado internacional. Desta forma, a LGPD terá efeitos nacionais e internacionais, na medida em que os dados pessoais forem coletados em território nacional ou por aquisição de produto e serviço para indivíduos no território nacional.

O autor acrescenta que a LGPD terá um impacto dos mais significativos que uma legislação nacional já alçou. As medidas a serem tomadas para a proteção dos dados pessoais vêm sendo e serão debatidas em diferentes áreas, como na cibersegurança, no meio jurídico, na economia e no meio social, pois são evidentes o crescimento do tráfego digital, os riscos de ataques e os vazamentos de dados que podem afetar praticamente toda atividade pública e privada num país. Ainda segundo o autor, é cada vez mais frequente a exposição de dados em larga escala, o que mostra as fragilidades de sistemas e protocolos, inclusive, por parte de quem deveria fiscalizar a segurança das operações: o Estado.

A LGPD prevê uma série de diretrizes e obrigações quanto ao tratamento dos dados, de modo que os titulares possam controlar e requerer o acesso a eles a qualquer momento, independente de irregularidades. Ao receberem um requerimento do titular, a resposta às demandas tem de ser dada em até 15 dias (VALENTE, 2020). Segundo Peixoto (2020), os negócios terão impactos profundos em virtude da LGPD, cabendo às organizações se protegerem de eventuais penalidades e resguardarem-se da opinião pública negativa decorrente da não adaptação – o que seria uma demonstração de pouca confiabilidade, já que não conseguem garantir a proteção de seus bancos de dados. Como exemplos de vazamento de dados e prejuízo para a imagem da organização, é possível destacar os casos da Netshoes, Banco Inter e da empresa de crédito Boa Vista, todos ocorridos no Brasil (PEIXOTO, 2020).

Valente (2020) destaca que, no caso do Poder Público, a Lei dispensa o consentimento no tratamento de dados para políticas públicas previstas em leis, em regulamentos e em contratos. É permitido também o uso compartilhado de dados por entes públicos, desde que respeitados os princípios previstos na Lei. Uma obrigação é que cada órgão informe as hipóteses de tratamento de dados, incluindo a base legal, a finalidade e os procedimentos empregados para tal. No entanto, Peixoto (2020) relata que uma das ações mais imediatas em caso de exposição e vazamento é comunicar a Autoridade Nacional de Proteção de Dados (ANPD) em prazo razoável a ser definido pela própria autoridade.

A Lei traz um conjunto de sanções previstas para o caso de violação, como: advertência, com possibilidade de medidas corretivas; multa de até 2% do faturamento com limite de até R$ 50 milhões; bloqueio ou eliminação dos dados pessoais relacionados à irregularidade, suspensão parcial do funcionamento do banco de dados e proibição parcial ou total da atividade de tratamento (VALENTE, 2020). Peixoto (2020) concorda e menciona que já existem empresas que trabalham com certificação de *sites* empresariais e institucionais, atestando que estes estão em conformidade com LGPD.

Uma vez que a LGPD aborda a coleta, o armazenamento, o processamento e a transmissão dos dados utilizados pelas organizações para os mais diversos fins, e tem como foco principal a privacidade dos seus titulares, é evidente a necessidade de discutir a Lei, tendo em vista a segurança da informação, como argumentam Silveira (2021), Neves et al. (2021) e Rocha et al. (2019).

2.8 IMPLICAÇÕES DA LGPD NA SEGURANÇA DA INFORMAÇÃO DAS ORGANIZAÇÕES

Como a Lei prevê a implantação de medidas preventivas e corretivas, tanto técnicas quanto não técnicas, caberá às organizações adequarem seu parque tecnológico e seus regulamentos, suas políticas, seus processos e suas estruturas organizacionais, além de promover ações de conscientização e educação adequadas. Nesse sentido, organizações que têm responsabilidades definidas, estruturas organizacionais criadas, documentos elaborados e publicados, como prevê a literatura (ALBUQUERQUE JUNIOR; SANTOS, 2015; MANDARINI, 2004; SÊMOLA, 2014), podem, hipoteticamente, se adaptar com mais facilidade aos requisitos da LGPD.

Desta forma, por prever responsabilidades e funções dentro das organizações, a LGPD pode exigir mudanças na estrutura interna das organizações, mas aquelas que já contam com estruturas organizacionais de segurança da informação podem enfrentar menos dificuldades para se adequarem às exigências da Lei, enquanto outras organizações podem sofrer impactos mais significativos para atender aos seus requisitos.

Na literatura sobre o tema, há um entendimento de que a busca pela conformidade com requisitos legais é uma razão pelas quais as organizações adotam medidas de segurança da informação (ALBUQUERQUE JUNIOR et al., 2018). Assim, a criação de estruturas organizacionais que lidam com políticas e regulamentos internos de segurança da informação ou a realização de mudanças em estruturas organizacionais existentes para fins de conformidade com a LGPD pode acontecer. Organizações que já contam com um setor e um comitê de segurança da informação, equipes de tratamento de incidentes e gestor de segurança da informação, como orienta Sêmola (2014), podem precisar adequar essas estruturas e papéis organizacionais às novas exigências legais, mas podem também estar mais propensas a adotar medidas mais adequadas às suas necessidades, como controle de acesso, autenticação de usuários, criptografia, procedimentos documentados, entre outras medidas de natureza física,

técnica ou administrativa (ALBUQUERQUE JUNIOR; SANTOS, 2015; MANDARINI, 2004).

Neste contexto, embora haja um entendimento de que a segurança da informação é um elemento essencial na gestão das organizações (CHANG; HO, 2006), os requisitos da Lei de proteção de dados poderão ter diferentes impactos nas organizações, pois estão diretamente relacionados à forma como a segurança da informação é gerida e com as políticas e controles adotados em cada organização.

A política de segurança da informação é um documento que fundamenta e orienta as medidas de segurança da informação em uma organização, servindo de base para as demais ações (LOPES, 2012). Como explica Almeida (2000), políticas ou diretrizes são planos gerais de ação que estabelecem e orientam de maneira genérica a tomada de decisão. De acordo com Sterne (1991), a política de segurança da informação contém regulamentos, regras e práticas que determinam como deve ser a gestão da segurança da informação, a proteção de dados e a distribuição de recursos para essa finalidade em uma organização.

Por ser uma orientação geral, a política de segurança da informação determina as demais medidas a serem adotadas, devendo ser respaldada pelo alto escalão de gestores e deve demonstrar o comprometimento deles com a segurança da informação, como destacam Sêmola (2014) e a norma da ABNT (2013). Para Williams (2001), a política de segurança da informação é considerada um fator de sucesso para a promoção da cultura organizacional em prol da segurança da informação.

Entre as razões pelas quais a política de segurança da informação é útil para as organizações, Lopes (2012) observou o seguinte na literatura: demonstra as iniciativas organizacionais de segurança da informação (SÁ-SOARES, 2005); esclarece o quanto é importante a segurança da informação para a organização (HÖNE; ELOFF, 2002); indica o que deve ser protegido e como isso deve ser feito (KING; DALTON; OSMANOGLU, 2001); guia a escolha e implantação de controles adequados para a organização (BARMAN, 2001); contribui para que comportamentos adequados sejam adotados na organização (LEE, 2001). Laureano (2005) concorda que uma política de segurança da informação descreve o que está sendo protegido e por que, complementando que o documento define as prioridades de segurança da informação e seu custo, permite também estabelecer um acordo explícito sobre o valor da segurança da informação entre diferentes áreas da organização, respaldando decisões da área responsável pela segurança da informação, dando a essa área autoridade e possibilidade de alcançar um melhor desempenho.

O conteúdo de uma política de segurança da informação pode incluir uma definição de segurança da informação (FORCHT; AYERS, 2001; HÖNE; ELOFF, 2002), responsabilidades para os agentes envolvidos (DOHERTY; FULFORD, 2006; HÖNE; ELOFF, 2002; PATRICK, 2001), necessidade de ações de educação, conscientização e treinamento (FORCHT; AYERS, 2001), princípios organizacionais de segurança da informação (HÖNE; ELOFF, 2002), gestão da continuidade das operações e recuperação de desastres (FORCHT; AYERS, 2001; DOHERTY; FULFORD, 2006), punições e consequências para quem descumprir a política (HÖNE; ELOFF, 2002; DOHERTY; FULFORD, 2006), bem como referências a outros documentos, como leis, normas, políticas, procedimentos e processos organizacionais, além de um texto que declare o compromisso dos gestores e o alinhamento da política com as estratégias e objetivos da organização (HÖNE; ELOFF, 2002). Com uma nova lei que trata diretamente da proteção de dados pessoais, entende-se que, no mínimo, essa referência precisa ser incluída na política de segurança da informação. Além disso, estruturas organizacionais, funções e responsabilidades criadas para atender às determinações da LGPD precisam também estar previstas na política. Dessa forma, sendo a política de segurança da informação um dos elementos que compõem e ao mesmo tempo orienta a segurança da informação de uma organização, é, possivelmente, um dos aspectos que serão afetados pela LGPD.

Além da política de segurança da informação, outros documentos internos orientam o comportamento das pessoas quanto à proteção dos dados em uma organização, como regulamentos internos e planos de continuidade do negócio e recuperação de desastres (ALBUQUERQUE JUNIOR; SANTOS, 2015), que a complementam e facilitam a operacionalização das medidas técnicas adotadas. Com a LGPD, tanto em sua decorrência direta quanto pelas alterações realizadas na política de segurança da informação, esses documentos, que são complementares à política, precisarão também ser adequados, bem como poderá haver a necessidade de outros serem criados.

Para que haja controle de acesso a dados e para garantir que esses dados não sejam corrompidos, perdidos ou acessados indevidamente, as organizações podem necessitar de atualizações tecnológicas, como sistemas ou algoritmos voltados para anonimização e soluções de criptografia de dados, *firewalls* para proteger dados pessoais de acessos indevidos, antivírus, sistemas de *backup*, sistemas de detecção e prevenção de intrusos e sistemas seguros de gerenciamento de bancos de dados, entre várias outras possibilidades de controles técnicos observados na literatura (BELASCO; WAN, 2006; DHILLON, 1999; SENTHILKUMAR;

ARUMUGAM, 2011; GORAYEB, 2012). A adequação à LGPD também poderá implicar em adquirir novas tecnologias para a segurança da informação.

Com os recursos tecnológicos atuais, os dados vêm sendo processados e armazenados principalmente em bancos de dados, em sistemas de informação e em computadores para serem consultados e analisados posteriormente. Para proteger esses dados, a literatura recomenda a adoção de diferentes controles técnicos de segurança da informação.

Embora a segurança da informação não deva ser tratada com uma visão puramente técnica ou tecnológica (DOHERTY; ANASTASAKIS; FULFORD, 2009; FRANGOPOULOS; ELOFF; VENTER, 2008; SILVA; STEIN, 2007), a adoção de controles de segurança da informação costuma ser responsabilidade da área de TI das organizações (ALEXANDRIA, 2012). Teixeira e Armelin (2019) reforçam que os Profissionais de TI têm a responsabilidade e a obrigação de adotar medidas previstas para a proteção dos dados. Além disso, o desenvolvimento e a manutenção dos sistemas de informação são responsabilidade dos profissionais de TI, de maneira que se espera que esses profissionais tenham acesso privilegiado aos dados coletados, armazenados e tratados nas organizações, a depender do trabalho que desenvolvam. Como consequência, os profissionais de TI podem vir a ser identificados e responsabilizados como operadores de dados pessoais, um dos papéis definidos na LGPD.

Esta realidade faz com que a adequação das organizações à LGPD passe por ações de conscientização e pela capacitação desses profissionais a respeito da Lei e de como proteger os dados pessoais, bem como sobre novos recursos tecnológicos que precisam ser implementados nos processos organizacionais, além dos ajustes na política e nos regulamentos internos de segurança da informação; este deve ser um comportamento ético dos profissionais de TI. A relevância de ações para adequar o comportamento das pessoas em prol da segurança da informação é reforçada por trabalhos científicos sobre o tema (DAMASCENO; RAMOS; PEREIRA, 2015; KLEIN; LUCIANO, 2016), sendo o treinamento um dos meios abordados em estudos científicos como forma de mudar uma percepção negativa das pessoas sobre uma nova tecnologia (FRESNEDA, 1998), de reduzir a resistência à implantações (CASTILHO; CAMPOS, 2007; VASCONCELOS; PINOCHET, 2002) e de reduzir falhas na sua utilização (CHILES et al., 2013), o que pode refletir em resultados mais positivos com a implantação de novas tecnologias de segurança da informação para atender à LGPD, reforçando a necessidade de treinamento e conscientização das pessoas que têm papéis-chave no tratamento de dados pessoais.

Contudo, os profissionais de TI, devido a sua visão mais técnica, costumam manter um foco na adoção de controles de segurança da informação que impliquem em ações que envolvam recursos técnicos e físicos, em detrimento da necessidade de realizar mudanças nas estruturas e processos organizacionais e de realizar ações de treinamento, conscientização e divulgação (ALBUQUERQUE JUNIOR; SANTOS 2015). Soma-se a isto o fato de que esses profissionais costumam ser responsáveis pela maioria (senão todas) as ações de segurança da informação realizadas na maioria das organizações.

3 PRESSUPOSTOS E MODELO DE PESQUISA

A LGPD está relacionada diretamente à proteção dos dados pessoais para evitar que o uso desses dados por pessoas e organizações seja abusivo no sentido de prejudicar o direito das pessoas à privacidade. Para isto, a Lei exige uma série de adequações na estrutura e nos processos organizacionais, quanto às políticas, aos regulamentos e às medidas internas e externas para a segurança da informação, além de adequações no comportamento ético das pessoas que lidam com dados pessoais.

Como a segurança da informação costuma ser responsabilidade dos profissionais de TI de uma organização, sua compreensão quanto aos impactos da LGPD é relevante para o sucesso da adequação da organização aos requisitos desta nova legislação.

Conformidade com a Lei envolve, portanto, a compreensão desses profissionais sobre as implicações em todas as dimensões em que elas se apresentam. Com base na literatura consultada, os impactos da LGPD sobre as organizações podem ser classificados em três categorias:

- Impactos Formais: alterações na política de segurança da informação e em regulamentos internos sobre o assunto, mudanças em processos e procedimentos internos que envolvem segurança da informação, como revisões periódicas na política de segurança da informação, processos de análise e avaliação de riscos e classificação de informações, mudanças no Comitê de Segurança da Informação, no Escritório de Segurança da Informação e na equipe de tratamento de incidentes para adequação à LGPD. Pode envolver ainda mudanças no Sistema de Gestão de Segurança da Informação e na definição de responsabilidades individuais e colegiadas, bem como em planos, procedimentos organizacionais de segurança da informação e outros processos internos para adequação à LGPD.
- Impactos Técnicos: alterações no funcionamento de dispositivos técnicos (*hardware* ou *software*) ou a implantação de novos dispositivos de segurança da informação para realizar redundância de dados e equipamentos, segregação e monitoramento de redes de computadores, prevenção contra códigos maliciosos, controle de acesso lógico, transmissão, processamento e armazenamento seguros de dados, autenticação forte, controle de acesso físico e proteção ambiental para proteção de dados pessoais.

- Impactos Informais: realização de ações de treinamento de profissionais de TI e usuários da organização a respeito da LGPD, divulgação dos requisitos da LGPD e das mudanças em regulamentos, em processos e na política de segurança da informação, decorrentes da Lei, além de ações de conscientização sobre a LGPD no sentido de que as pessoas adotem comportamentos éticos e legais no tratamento de dados pessoais.

A categorização dos impactos da LGPD permitiu estabelecer tanto as dimensões de análise (Técnica, Formal e Informal) para estudar a compreensão dos profissionais de TI quanto os pressupostos teóricos desta pesquisa, que são abordados a seguir.

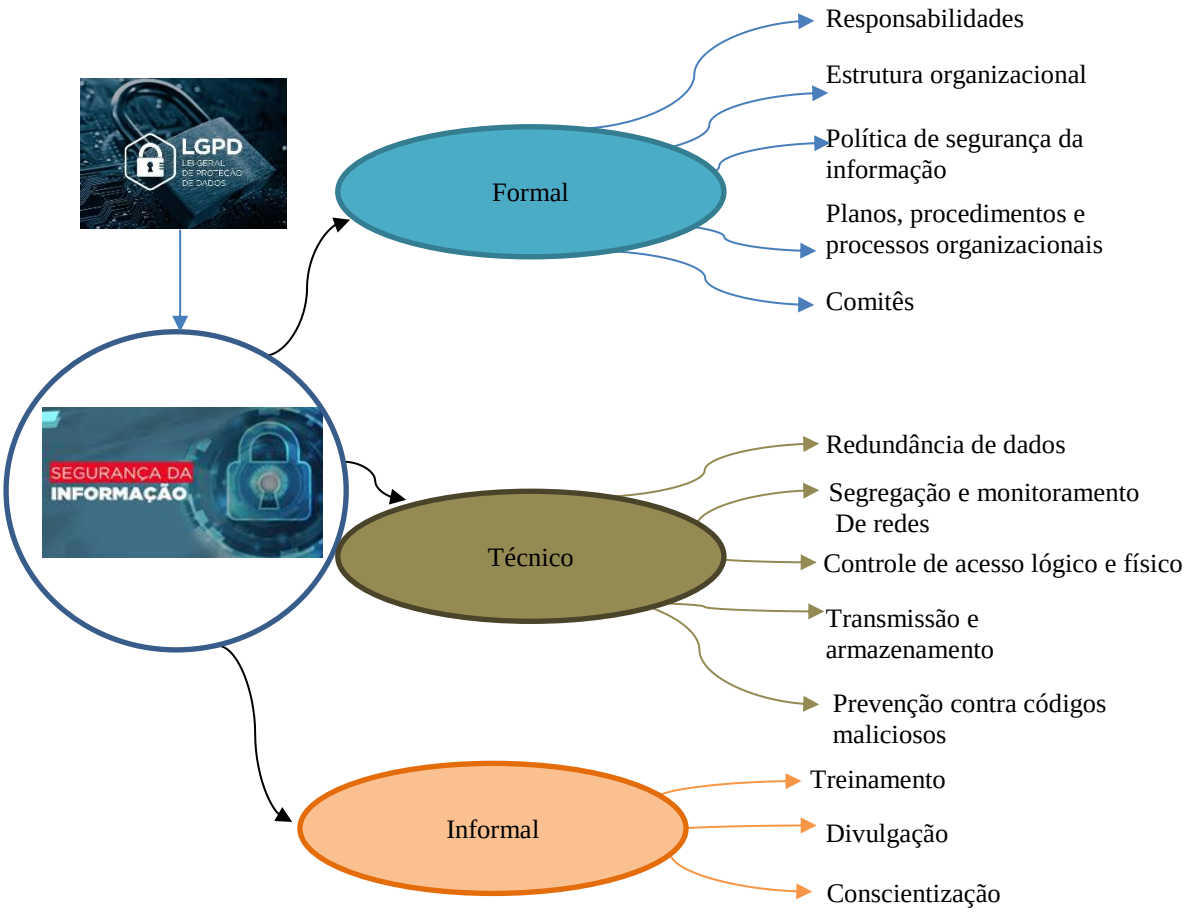
3.1 PRESSUPOSTOS DE PESQUISA

Os pressupostos desta pesquisa estão relacionados à compreensão dos Profissionais de TI quanto aos requisitos da LGPD e seus impactos na gestão da organização, no ambiente computacional e no comportamento de cada uma das pessoas que lidam com dados pessoais.

- Pressuposto 1: Compreendem as necessidades e realizar as adequações na tecnologia, visando à conformidade aos requisitos.
- Pressuposto 2: Compreendem os impactos e as mudanças na gestão da TI para atender às necessidades de proteção de dados.
- Pressuposto 3: Conhecem as implicações da LGPD sobre os papéis e responsabilidades da área de TI e dos usuários.

Com base nesses pressupostos e nas dimensões de pesquisa, foi elaborada a figura 6, que apresenta a relação entre as dimensões e seus componentes, formando o modelo conceitual da pesquisa.

Figura 6 – Modelo Conceitual



Fonte: Elaborado pela autora (2021) com base no modelo de Dhillon e Moore (2001).

A figura 6 apresenta os princípios da segurança da informação que são: a integridade, a disponibilidade e a confidencialidade que podem estar diretamente associadas à privacidade da LGPD. Considerando as diretrizes norteadoras da lei que diz que as informações deverão ser disponibilizadas a qualquer momento que seu titular requisitar, pode relacioná-la ao pilar de disponibilidade (acesso direto ao dado pelo seu titular de forma transparente); a integridade pode ser relacionada à informação que deverá estar intacta, conforme foi autorizado para o seu uso (o dado não poderá ser manipulado e alterado sem o consentimento do titular) e a confidencialidade, a qual podemos relacioná-la à privacidade, considerando que só terá acesso à informação mediante ao consentimento (as informações são públicas através de consentimento).

Na dimensão formal, são consideradas as medidas que requeiram alterações nas políticas, nas normas, nos regulamentos, nos planos, nos procedimentos e nos processos organizacionais, especialmente, de médio e longo prazos, a fim de garantir investimentos

necessários, contratações, treinamentos e a implantação de infraestrutura para a operacionalização das novas atividades que estejam relacionados à LGPD.

Para tal, os critérios e as diretrizes, sejam técnicos e ou operacionais, da política de Segurança da Informação devem seguir o princípio da segurança recomendada pela lei. O comitê de Segurança da Informação possibilita as deliberações quanto às diretrizes que asseguram confiabilidade das informações, as ações que visam mitigar os riscos da TIC, avaliam e gerenciam os incidentes de segurança da informação, assim como as medidas estratégicas que possibilitam que a área da TI opere em alto grau na proteção da segurança da informação e aplicação das melhores práticas na governança da PSI. Os Regulamentos internos, processos e procedimentos para a segurança da informação possibilitam o cumprimento das deliberações que são aprovadas no comitê, e eles permitem os controles e as rastreabilidades das ocorrências sistêmicas nos incidentes e nas avaliações dos impactos, nas revisões periódicas das medidas adotas para a segurança da informação.

Neste contexto, a equipe responsável pela gestão da segurança da informação deve considerar as normas, as diretrizes e os princípios que fundamentam o pleno controle da integridade, da confiabilidade e da disponibilidade da informação.

Na dimensão técnica recomenda medidas de tratamento que assegurem a integridade, a disponibilidade e a confiabilidade das informações, as quais, segundo a Lei, podem ser acessados pelos titulares dos dados e pelos agentes da organização que têm autorização de manipulá-los. A segurança da informação pode ser obtida através da redundância na infraestrutura tecnológica que é essencial para a alta disponibilidade nos processos organizacionais, em que essa metodologia consiste na duplicação de componentes críticos para o funcionamento dos serviços, visto que, caso aconteça uma falha sistêmica no primeiro componente, o segundo assume o processamento. Assim sendo, a interrupção passa despercebida e evita a perda de dados. As redundâncias podem ser aplicadas com fontes de energia alternativas, múltiplos locais de armazenamento de dados e outros dispositivos. O princípio da segregação integrada da infraestrutura técnica possibilita o isolamento físico e lógico para garantir a qualidade das informações de processamento.

Essa ação permite que seja dado tratamento adequado a informações sensíveis sem atrapalhar atividades relacionadas a outros tipos de dados reduz os controles desnecessários e atende ao princípio do Livre Acesso. O controle e a verificação de usuários são indispensáveis para o processo de monitoramento que permite proteger as informações através de permissões de acesso aos vários recursos tecnológicos.

Para controlar o acesso de usuários internos e externos, possibilitam a identificação de incidentes, o uso indevido dos dados pessoais e a realização de consultas aos registros para verificação e identificação de responsabilidades.

O plano de recuperação, assim como a política de backup é medida que diminui os danos causados por uma falha sistêmica e/ou um ataque nas bases de dados. Providências como essas asseguram as informações que são de extrema importância, e a preservação é mantida fora do alcance de pessoas que não estejam autorizadas. Para tal, o controle de acesso deve atender a política de segurança com autenticações fortes, como também, a aplicação de programas que efetuem a prevenção contra códigos maliciosos.

Na dimensão informal, as providências são dotadas, para proporcionar o conhecimento das leis, o desenvolver da conscientização de todos da organização quanto os princípios, as diretrizes e as responsabilidades na adequação da LGPD para a cultura organizacional. A eficiência dessas providências é obtida através de treinamentos, seja para a equipe técnica, operacional ou de usuários. Com aplicação de campanhas e políticas de divulgação, cumprindo os requisitos da LGPD, os colaboradores devem entender, compreender e aplicar as ações de adequação da Lei que resultaram em mudanças e investimentos, sejam nas dimensões técnicas ou formais.

Para tal, as dimensões foram consideradas como mecanismo de controle e de avaliação quanto à governança e aos riscos de TI, os quais devem ser considerados: o porte, a complexidade e o grau de dependência quanto os processos organizacionais; neste contexto o profissional de TI deverá definir critérios ao Sistema da Informação para adequar as diretrizes da LGPD, bem como, o nível de risco inerente às suas atividades operacionais, gerenciais e administrativas que a Lei incide nas organizações.

A partir dessas dimensões e componentes, foi elaborado o Quadro Analítico (Quadro 3), que consolida as perspectivas e inclui os indicadores que permitem operacionalizar a pesquisa.

Quadro 3 – Quadro Analítico

Categoria	Perspectivas	Indicadores
Formal	Responsabilidade	Mudanças nas responsabilidades dos agentes envolvidos no tratamento de dados pessoais.
	Estrutura Organizacional	Novas estruturas organizacionais – DPO, Controlador e Operador.
		Alterações em estruturas organizacionais existentes.
	Políticas de Segurança da Informação	Novas diretrizes relacionadas à LGPD incluídas na política de segurança da informação.
		Política de segurança da informação criada em decorrência da LGPD.
	Planos, Procedimentos e Processos organizacionais	Alterações em planos, procedimentos e processos.
		Novos planos, procedimentos e processos.
	Comitês	Participação de equipes multidisciplinares nas avaliações quanto as adequações para LGPD.
Técnica	Redundâncias	Implementar ativos de TI paralelos para atender à segurança da informação nas bases e ambientes computacionais.
	Segregação e monitoramento	Separar e monitorar as atividades passíveis de serem controladas pela LGPD e as não controladas.
	Controle de acesso lógico e físico	Validar os acessos aos ambientes e as informações.
	Transmissão e armazenamento	Controlar as transmissões e os armazenamentos dos dados.
	Prevenção contra códigos maliciosos	Aplicar medidas de proteção aos dados.
Informal	Treinamento	Capacitar técnicos e usuários.
	Conscientização	Ações, campanhas e artefatos voltados para a conscientização.
	Divulgação	Ações de divulgação de informações da LGPD.
		Divulgação de regulamentos, planos e políticas internas.

Fonte: Elaborado pela autora (2021) com base no modelo de Dhillon e Moore (2001).

4 MÉTODO

O trabalho de pesquisa enquadra-se como aplicada, tendo em vista sua característica de contribuir para fins práticos, ou seja, aplicar ou utilizar os resultados para solucionar problemas que ocorrem na realidade (MARCONI; LAKATOS, 2007).

Quanto à abordagem metodológica, este estudo é quantitativo e qualitativo, pois tem o propósito de analisar e interpretar dados, observando a opinião dos participantes quanto às implicações da Lei, embora utilize métodos de coleta de dados quantitativos.

Quanto aos objetivos, a pesquisa é descritiva. De acordo com Gil (2009), os estudos descritivos objetivam descrever as características de determinada população ou fenômeno, ou estabelecer relações entre variáveis. Sendo assim, a pesquisa procurou descrever os impactos que a Lei trata para as organizações.

O estudo envolveu também a realização de pesquisa bibliográfica, que, segundo Gil (2009), é desenvolvida a partir de material já publicado, composto principalmente de artigos, de periódicos, de livros e, ainda, de material disponível na Internet, evidenciando, inclusive, a relevância do tema na literatura, conforme Quadro 4:

Quadro 4 – Método e Objetivos

Método	Objetivos
Survey	Obter as informações quantitativas sobre a percepção dos profissionais de TI a respeito da adequação das suas organizações à LGPD. A pesquisa será aplicada para os Diretores, Gerentes, Coordenadores e Avalista todos da área de TI dos Regionais.
Grupo Focal	Aferir qualitativas sobre os resultados da *Survey*, em que deverão ser consideradas as ponderações sobre o tema, através da reunião com os diretores e gerentes que participaram do processo de análise.

Fonte: Elaborado pela autora (2021).

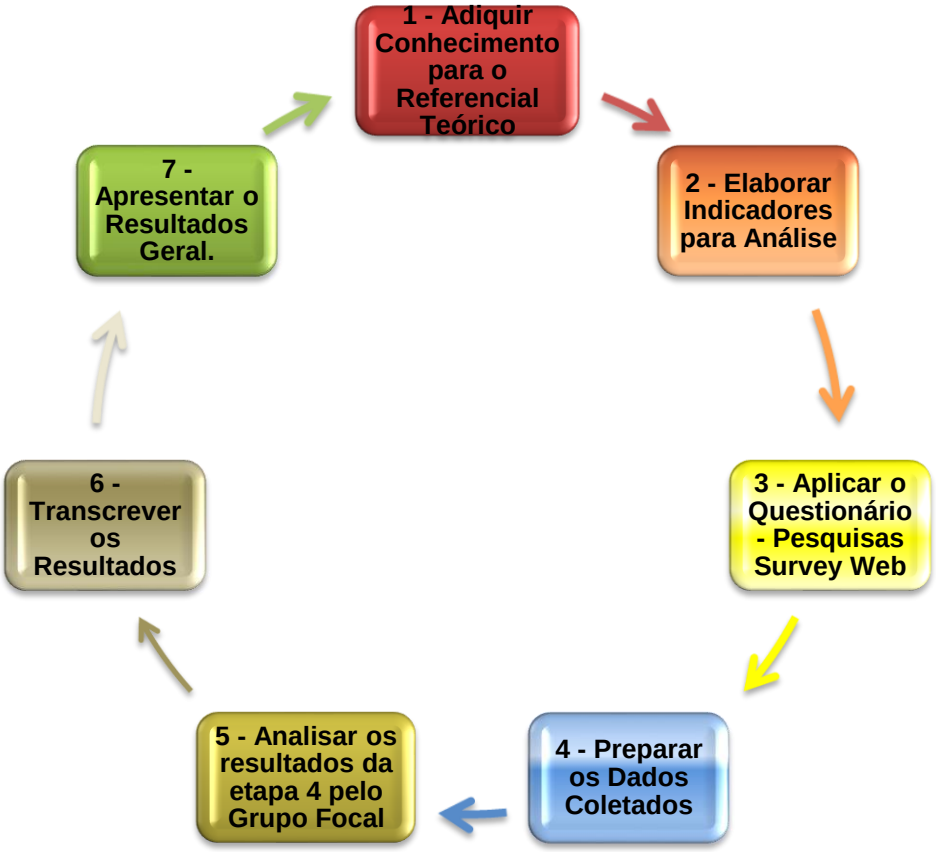
4.1 DESENHO DA PESQUISA

A pesquisa envolveu uma ampla revisão bibliográfica que aconteceu durante todo o processo de construção, de definição do tema apresentando, de justificativas e de objetivos. A construção dos instrumentos de pesquisa é resultado da definição de um modelo de pesquisa que, por sua vez, foi idealizado com base nessa pesquisa bibliográfica. A aplicação dos instrumentos de pesquisa resultou na coleta de dados quantitativos e qualitativos, que foram categorizados com base no modelo de pesquisa e analisados, a fim de identificar a percepção dos participantes quanto às implicações da LGPD sobre a segurança da informação nas organizações.

A consecução da pesquisa, representada na figura 7, envolveu as seguintes etapas:

- Etapa 1: Adquirir conhecimento sobre o tema para o referencial teórico, consolidando no modelo que foi utilizado na parte empírica da pesquisa.
- Etapa 2: Identificar indicadores necessários para a operacionalização da pesquisa e construir os instrumentos de pesquisa.
- Etapa 3: Aplicar o questionário da pesquisa através de *Survey web*.
- Etapa 4: Tratar os dados coletados, classificar e consolidar a análise das pesquisas, observando a conformidade aos resultados com os preceitos da fundamentação teórica.
- Etapa 5: Preparar o grupo focal e tratar os resultados coletados, classificados e analisados, observando a exposição e considerações dos participantes.
- Etapa 6: Transcrever os resultados obtidos na pesquisa s*urvey* e no Grupo Focal para fundamentar, quantitativa e qualitativamente, os resultados do estudo.
- Etapa 7: Apresentar os resultados obtidos.

Figura 7 – Desenho da pesquisa.



Fonte: Elaborada pela autora (2021).

A pesquisa envolveu a realização de Survey Web, com a aplicação de um questionário para os Profissionais de TI (Analistas, Coordenadores, Gerentes e Diretores) do SENAC. No qual, Wright (2005), uma pesquisa Survey web tem as vantagens pela agilidade proporcionada pelos recursos de TI, além do custo baixo e da alta taxa de resposta, como destacam Ilieva et al. (2002).

A análise dos dados coletados na *Survey* envolveu a classificação desses dados em blocos conceituais, baseados no modelo da pesquisa, o que envolve o agrupamento das respostas obtidas de acordo com os indicadores das dimensões teóricas – codificação temática, conforme Gil (2009) e Flick (2009).

A análise dos dados coletados no grupo focal seguiu as orientações de Iervolino e Pelicione (2001, p. 119), que propõem duas formas de se proceder: através do sumário etnográfico e da codificação dos dados via análise de conteúdo. O primeiro assenta-se "nas citações textuais dos participantes do grupo", enquanto o segundo enfatiza a "descrição

numérica de como determinadas categorias explicativas aparecem ou estão ausentes das discussões e em quais contextos isto ocorre". Os métodos citados não são excludentes entre si, podendo ser combinados em um só momento de análise.

No Apêndice B apresenta-se um quadro com os autores, suas referências e as abordagens teóricas que foram utilizadas e citadas nesta dissertação.

4.2 PROCEDIMENTOS METODOLÓGICOS

Para este trabalho, realizou-se uma pesquisa bibliográfica através de artigos, livros, dissertações publicadas e anais de eventos científicos, revistas especializadas e *websites* sobre os temas abordados. Foram consultadas as bases de dados *Scielo*, Portal CAPES, Spell, *Google Scholar* e Biblioteca Digital de Teses e Dissertações (BDTD) do Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT), além de diferentes repositórios institucionais de diferentes universidades. Foram consultados também os anais dos seguintes eventos científicos: Encontro da Associação Nacional de Pós-Graduação e Pesquisa em Administração (ANPAD), *International Conference on Information Systems and Technology Management* (CONTECSI), Seminários em Administração (SemeAd), Encontro Nacional de Engenharia de Produção (ENEGEP), Encontro Nacional de Pós-Graduação e Pesquisa em Ciência da Informação (ENANACIB), todos com participação de pesquisadores das áreas de Sistemas de Informação, de Ciência da Informação, de Engenharia de Produção e de Administração, áreas de conhecimento aderentes aos temas abordados no estudo.

Considerando os aportes bibliográficos, foram elaboradas duas pesquisas, sendo: uma quantitativa e outra qualitativa, ambas com o objetivo de avaliar o modelo de pesquisas aplicado neste trabalho sobre os pressupostos relacionados à compreensão dos profissionais de TI quanto à adequação da LGPD e seus impactos na gestão da segurança da informação.

Na aplicação da pesquisa s*urvey*, as perguntas foram realizadas com objetividade, no sentido de aferir as variáveis que se pretendia, conforme observa Gil (2002). Para a análise dos dados, foi utilizada a análise de conteúdo, seguindo as recomendações de Bardin (1977), quanto à classificação dos dados transcritos, a fim de identificar evidências condizentes com os indicadores da pesquisa. O Quadro 2 apresenta um resumo de cada uma das abordagens

metodológicas utilizadas e os objetivos de cada uma delas, juntamente com suas técnicas de coleta de dados.

O Grupo Focal foi realizado na modalidade remotamente, mediadas consoante a metodologia. Segundo Krueger (2009) e Morgan (2010), este método é relevante, pois avalia as abordagens críticas que são apontadas e observadas nos questionários, nos quais as investigações se baseiam em questões e respostas. Ponderando o potencial da avaliação do Grupo Focal, através da análise e discussão crítica dos conteúdos resultantes da pesquisa aplicada, observa-se sua eficiência, uma vez que o resultado é fundamentado por múltiplos pontos de vistas, assim como a influência emocional no processo, considerando a interpretação dos resultados da pesquisa. Portanto, este processo possibilita o diálogo com os participantes e poderá conduzir a novos *insights*, os quais, segundo Yin (2015, p.136), pode-se começar a análise, observando os dados e procurando padrões, *insights* e conceitos promissores, o que significa que podemos "brincar" com os dados e aforar a própria estratégia.

Os métodos aplicados foram classificados, considerando a natureza qualitativa e quantitativa, os perfis dos profissionais de TI que participaram das pesquisas de acordo com o quadro 04, apresentados anteriormente, e a construção dos questionamentos sobre cinco temas correlacionadas ao estudo que norteou o plano de pesquisa, conforme demonstra a tabela 1.

Tabela 1 – Quantidades de perguntas e possibilidades de resposta para os temas abordados.

Nº de Perguntas	**Temas abordados na Pesquisa**	**Possibilidades de Respostas**
11	**Segurança da Informação** - Identificar como os profissionais de TI vêm as adequações da LGPD.	5
4	**Política de Segurança** - Verificar como os profissionais de TI identificaram os impactos que a LGPD.	5
4	**Controle de Dados** - Diagnosticar se os profissionais de TI evidenciam a mudança dos controles das informações sobre sua responsabilidade e penalidades;	5
4	**Governança de TI** - Considerar os possíveis impactos e as oportunidades que a Lei pode gerar para os profissionais de TI.	5

Fonte: Elaborado pela autora (2021)

4.3 DADOS DA ORGANIZAÇÃO E DOS PARTICIPANTES

O plano de pesquisa deste trabalho foi aplicado na organização paraestatal SENAC - Serviço Nacional de Aprendizagem Comercial, que é instituição de direito privado criada em 1946, subordinada à Confederação Nacional do Comércio (CNC). Fundada em junho de 1945, por Alexandre Marcondes Filho, então ministro do Trabalho da Indústria e do Comércio, por meio de uma portaria especial destinando-a a promover a difusão e o aperfeiçoamento do ensino comercial no país. No mesmo ano, foi criada a Confederação Nacional do Comércio (CNC), órgão sindical patronal máximo do comércio no Brasil, com a função de empenhar-se na criação do SENAC. Portanto, teve sua regulamentação para o ensino comercial e fixava direitos e deveres de comerciantes e comerciários, através do Decreto-Lei, de nº 8.622 – com a seguinte EMENTA[3]: Dispõe sobre a aprendizagem dos comerciários, estabelece deveres dos empregadores e dos trabalhadores menores relativamente a essa aprendizagem e dá outras providências.

O SENAC possui uma rede de escolas próprias distribuídas por diversos pontos do país e se mantém com a contribuição arrecadada de todos os estabelecimentos comerciais vinculados à CNC, correspondente a 1% do montante pago por cada uma dessas empresas ao conjunto de seus empregados. A Instituição possui uma administração nacional e diversas administrações regionais. Seu órgão dirigente máximo, o Conselho Nacional, é composto pelo presidente da CNC, pelos representantes do Ministério do Trabalho e pelos representantes dos diversos conselhos regionais. O primeiro presidente do seu Conselho Nacional foi João Daudt de Oliveira.

Os 70 participantes nas pesquisas aplicadas foram Profissionais de TI do SENAC, sendo Analistas, Coordenadores, Gerentes e Diretores. Os critérios por esses profissionais, considerou a experiência, o tempo de atuação nas questões técnicas e tecnológicas, na governança de TI, nas diretrizes estratégicas, nas ações inovadoras, nos projetos nacionais e regionais, e, liderando e sendo liderados para a construção de uma educação profissional de qualidade voltada para o futuro do trabalho, os quais, tiveram suas identificações anonimizadas através da ferramenta SAFE TEXT e os mesmos foram identificados por letras, conforme Tabelas 2 e 3.

[2] Publicada no Diário Oficial da União - Seção 1 - 12/1/1946, Página 542 (Publicação Original).

Tabela 2 – Dados dos Perfis dos Participantes da *Survey*

Sexo	Faixa Etária	Cargo/Função	Experiência Profissional Anos de Organização
19 – Feminino	0 – Entre 18 e 25 anos	20 - Analista de TI	12 – Entre 1 e 5 anos
	14 – Entre 26 e 35 anos	7 - Coordenador de TI	11 – Entre 6 e 10 anos
	18 – Entre 36 e 45 anos	28 - Gerente de TI	12 – Entre 11 e 15 anos
45 – Masculino	24 – Entre 46 e 55 anos	9 - Diretor de TI	8 – Entre 16 e 20 anos
	8 – Acima de 55 anos		21 – Acima de 20 anos

Fonte: Elaborada pela autora (2021)

Tabela 3 – Dados dos Participantes do Grupo Focal

Gestores	Sexo	Faixa Etária	Cargo/Função	Anos de Organização
A	Masculino	Entre 36 e 45 anos	Diretor	Entre 11 e 15 anos
B	Masculino	Entre 36 e 45 anos	Diretor	Entre 16 e 20 anos
C	Masculino	Entre 46 e 55 anos	Gerente	Entre 16 e 20 anos
D	Feminino	Entre 46 e 55 anos	Gerente	Acima de 20 anos
E	Masculino	Entre 46 e 55	Coordenador	Acima de 20 anos
F	Masculino	Acima de 55 anos	Gerente	Acima de 20 anos
G	Masculino	Entre 36 e 45 anos	Gerente	Entre 16 e 20 anos

Fonte: Elaborada pela autora (2021)

Os questionários foram enviados para 70 profissionais de TI do SENAC, através do *Google Forms*, distribuídos entre: 05 Diretores de TI, 24 Gerentes de TI, 12 Coordenadores de TI, 34 Analistas. No entanto, 62 participantes responderam à pesquisa aplicadas integralmente, sendo: 04 Diretores de TI, 19 Gerentes, 10 Coordenadores e 29 Analistas. Por tanto, 08 Profissionais de TI não participaram sendo: 01 Diretor, 05 Gestores e 02 Coordenadores.

Os dados foram coletados, remotamente, seguindo as orientações descritas no Apêndice E, e foram classificados em cinco blocos para evidenciar os indicadores construídos, conforme apresentado no quadro 04 (seção 3.1), os quais, devem estar relacionados com os objetivos e os pressupostos para fundamentar o plano de pesquisa deste trabalho.

Para o Grupo Focal, foram convidados, através da plataforma *Microsoft Teams*, 16 Profissionais de TI do SENAC, sendo: 02 Diretores de TI, 04 Gerentes de TI e 01 Coordenador de TI, a escolha desses participantes teve como critério a atuação direta deles nas ações estratégicas do SENAC. Os demais participaram sem expor diretamente suas reflexões sobre o tema.

Os dados foram coletados, através da gravação da reunião de forma remota, seguindo o roteiro e as orientações descritas no Apêndice F. Para tal, foram utilizados os resultados estáticos da pesquisa *Survey*, os quais atenderam aos objetivos e os pressupostos do plano de pesquisa deste trabalho.

4.4 PROCEDIMENTOS DE COLETA DE DADOS

Apresenta-se, nesta subseção, os métodos utilizados para a pesquisa *survey* e para o Grupo Focal.

4.4.1 Procedimentos de coleta de dados – pesquisa *survey*

A coleta dos dados da pesquisa realizada com os profissionais do SENAC, conforme a tabela 2, já apresentada, teve como premissa obter informações específicas quanto à percepção desses profissionais, considerando o entendimento da segurança da informação e a adequação da LGPD na organização. Utilizou-se uma ferramenta de modelagem de dados, *software Statistical Package for Social Sciences* (SPSS), versão 20.0, para apuração da pesquisa *Survey*, foram aplicados filtros e tabulações para que os resultados tivessem relevância estatística.

As coletas dos dados foram classificadas em cinco blocos. Em cada um deles foi utilizada uma escala *Likert* de cinco pontos para identificar o nível de compreensão dos profissionais de TI: (1) - Nenhum, (2) - Pouco, (3) - Razoavelmente, (4) - Muito e (5) - Plenamente.

Para todos os blocos, com exceção do bloco – I, foram utilizados 28 parâmetros para mensurar as variáveis e avaliar as dimensões da compreensão dos profissionais de TI sobre as implicações da LGPD na segurança da informação. Os parâmetros foram distribuídos em três dimensões de análise: técnica, formal e informal.

Deste modo, o plano de pesquisa foi descrito sobre a abordagem qualitativa, considerando as tendências, as atitudes e as opiniões dos participantes, a partir dos resultados estatísticos, que foram analisados e calculados sob as probabilidades das variações de percentagens, das médias, da moda, das correlações, dos desvio-padrão e da margem de erro, para os blocos de II a IV.

As estruturas dos blocos foram categorizadas seguindo as dimensões de análise (Técnica, Formal e Informal) para coletar dados segundo as distribuições, atentando aos seguintes objetivos: Bloco I - identificar o perfil dos profissionais de TI que participaram da pesquisa, coletando informações sobre sexo, idade, função que exerce na organização, tempo de atuação na organização e a compreensão que julgam ter sobre a LGPD. No Bloco II - identificar como os profissionais de TI veem as adequações da LGPD quanto ao tratamento dos dados pessoais sobre a políticas de segurança da informação. Nas perguntas constavam nove parâmetros relacionados à Gestão de Segurança da Informação: GST – Gestão da Segurança Técnico, GSF – Gestão da Segurança Formal e GSI – Gestão da Segurança Informal. Para o Bloco III - verificar como os profissionais de TI identificaram os impactos que a LGPD incide na Política da Segurança da Informação, considerando os controles das informações nas organizações. Constam seis parâmetros relacionados ao Controle das Informações: CIT – Controle da Informação Técnico, CIF – Controle da Informação Formal e CII – Controle da Informação Informal. No Bloco IV - diagnosticar se os profissionais de TI evidenciam a mudança dos controles das informações sobre sua responsabilidade e as penalidades associadas. Constam seis parâmetros relacionados ao Controle da Informação quanto às Responsabilidades e às Penalidades: CIRPT – Controle da Informação Responsabilidade Penalidade Técnico, CIRPF – Controle da Informação Responsabilidade Penalidade Formal e CIRPI – Controle da Informação Responsabilidade Penalidade Informal. No Bloco V - considerar os possíveis impactos e as oportunidades que a lei poderá trazer para os profissionais de TI. Constam sete parâmetros relacionados aos Impactos e Oportunidades para os Profissionais de TI: IOT – Impactos Oportunidades Técnico, IOF – Impactos Oportunidades Formal e IOI – Impactos Oportunidades Informais.

Com a finalidade de realizar a análise estatística dos dados dos blocos, cujas respostas obtidas foram agrupadas de acordo com as médias das respostas dos 28 parâmetros das

dimensões teóricas, foi criado um índice através das médias de cada dimensão dos quatro blocos de respostas, de modo que foram calculados.

4.4.2 Procedimentos de coleta de dados – grupo focal

A coleta dos dados da pesquisa qualitativa, através da metodologia Grupo Focal, possibilitou um processo dinâmico na análise dos dados, os quais foram obtidas pela interação do grupo que participou da pesquisa. Também foi possível uma contextualização problema sobre o tema, mediante os resultados apresentados originados do cenário resultante da pesquisa *Survey*. A atividade em grupo possibilitou aos participantes explorarem seus pontos de vista, a partir de reflexões sobre as implicações da LGPD na segurança da informação, considerando as dimensões de análise: técnica, formal e informal.

O Grupo Focal foi realizado com os profissionais do SENAC de níveis estratégicos, conforme a tabela 3, apresentada anteriormente, foi gravada através da plataforma *Microsoft Teams e share point*, e, posteriormente, transcrita. O processo contou com um mediador que apresentou o roteiro que seria aplicado, o tempo de duração de cada participante, cujas respostas deveriam apresentar as reflexões e considerações quanto aos resultados da pesquisa *Survey* e a relevância desta para o SENAC.

A metodologia seguiu as observações indicadas por Iervolino e Pelicione (2001, p. 119) que propõem duas formas de se proceder a análise: através do sumário etnográfico e da codificação dos dados, via análise de conteúdo. O primeiro assenta-se “nas citações textuais dos participantes do grupo”, enquanto o segundo enfatiza a “descrição numérica de como determinadas categorias explicativas aparecem ou estão ausentes das discussões e em quais contextos isto ocorre”. Os métodos citados não são excludentes entre si, podem ser combinados em um só momento de análise. Desta forma, o Grupo Focal foi preparado seguindo as sete etapas, conforme mostra o Quadro 5:

Quadro 5 – Etapas para a preparação do Grupo Focal

Etapas	**Descrição**
1. Selecionar da equipe	Convidar os profissionais de TI do SENAC, um moderador e um relator.
2. Confirmar participantes	Confirmar a participação dos Diretores, Gerentes e Coordenadores de TI do SENAC que atuam estrategicamente na Instituição.
3. Duração da atividade	Estimar 2 horas total, sendo 15 minutos para a apresentação dos resultados e 10 minutos para cada participante.
4. Elaborar roteiro de discussão	Descrito no Apêndice B
5. Condução da reunião	Agendar o ambiente na Plataforma *Teams*. O mediador fará o esboço, a finalidade e o formato da discussão no começo da reunião.
6. Registrar a reunião	Será gravado, e em paralelo anotações realizadas pelo redator.
7. Analisar os resultados	Após a reunião foi preenchido o relatório – roteiro do grupo focal e compartilhados com os participantes para validação e aprovação.

Fonte: Elaborado pela autora (2021) com base em Iervolino e Pelicione (2001).

Os participantes têm mais de 15 anos de atuação na área da Tecnologia da Informação e estão atuando diretamente nas ações estratégicas do SENAC, sendo este o motivo pelo qual foram escolhidos a participarem do Grupo Focal. Vale ressaltar que todos eles contribuíram e complementaram a pesquisa com reflexões relevantes quanto a contextualização do tema e da pesquisa aplicada.

4.5 PROCEDIMENTOS DE ANÁLISE DOS DADOS

A análise dos dados da pesquisa *Survey* foi realizada através da ferramenta de modelagem de dados, *software Statistical Package for Social Sciences* (SPSS) versão 20.0, o teste de *Kolmogorov-Smirnov* e a análise de *Boxsplot.* Através de aplicação de filtros e tabulações, os dados foram organizados em gráficos de probabilidades que facilitaram a construção dos resultados quantitativos.

Segundo Field (2009), nessa etapa faz-se necessário preparar os dados e realizar alguns testes para verificar se estes estão normalmente distribuídos. A partir da caracterização preliminar da amostra, analisou-se a forma de distribuição da variável. Para isso, utilizou-se o teste de *Kolmogorov-Smirnov*, que segundo Bruni (2019, p.167) avalia se os valores de uma amostra podem ser considerados como provenientes de uma população com determinada

distribuição teórica. De acordo com o nível de significância obtido, foi possível atestar a normalidade da amostra. Ressalta-se que o valor definido para a significância dos testes analisados foi de 5%. Deste modo, os resultados encontrados nos testes estatísticos realizados nesta pesquisa podem ser considerados corretos ao nível de confiança de 95%. Posteriormente, os 12 índices foram analisados, através da análise de correlação para quantificar a força da relação entre os índices, e a análise de *Boxsplot* para representação da dispersão dos dados obtidos em cada índice. Através da mediana, foi possível calcular a tendência central das respostas dos participantes.

Após a análise estatística, os resultados foram analisados à luz do referencial teórico para delinear as considerações finais em relação aos resultados encontrados na pesquisa *Survey*.

A análise dos dados apurados durante o Grupo Focal não teve um tratamento estatístico envolvido para a modelagem de dados, pois essa pesquisa é de natureza qualitativa, fato que implica na análise dos resultados obtidos pela pesquisa *survey,* também sobre uma abordagem qualitativa, visando organizar as informações para que elas possam revelar com o máximo de objetividade e isenção quanto as questões apresentadas aos profissionais de TI do SENAC sobre o roteiro apresentado. Segundo Gatti (2005) e Morgan (1988).

O processo de análise ocorreu remotamente pela plataforma *Microsoft Teams*, sincronicamente à coleta dos dados. No entanto, a atividade não teve um caráter hipotético, pois as informações foram refletivas sobre os dados quantitativos da 1ª pesquisa aplicada ao grupo de profissionais de TI do SENAC. Colaborando com o método, Silva (2008, p. 29) diz que "[...] as investigações qualitativas se têm preocupado com o significado dos fenômenos e processos sociais, levando em consideração as movimentações, crenças, valores, representações sociais e econômicas, que permeiam a rede de relações sociais. "

Flick (2009) comenta que o Grupo Focal deve envolver todos os participantes. Estes devem ter opinião própria, específica sobre o tema tratado nessa dinâmica e toda experiência subjetiva dos participantes deve ser explorada. O principal objetivo da técnica do Grupo Focal é trabalhar atitudes, sentimentos, crenças, experiências e reações de uma forma em que não seria possível com outro método, por exemplo, com questionários, ou com reunião direta.

Após a atividade, os resultados foram aferidos à luz do referencial teórico, para em seguida delinear as considerações finais.

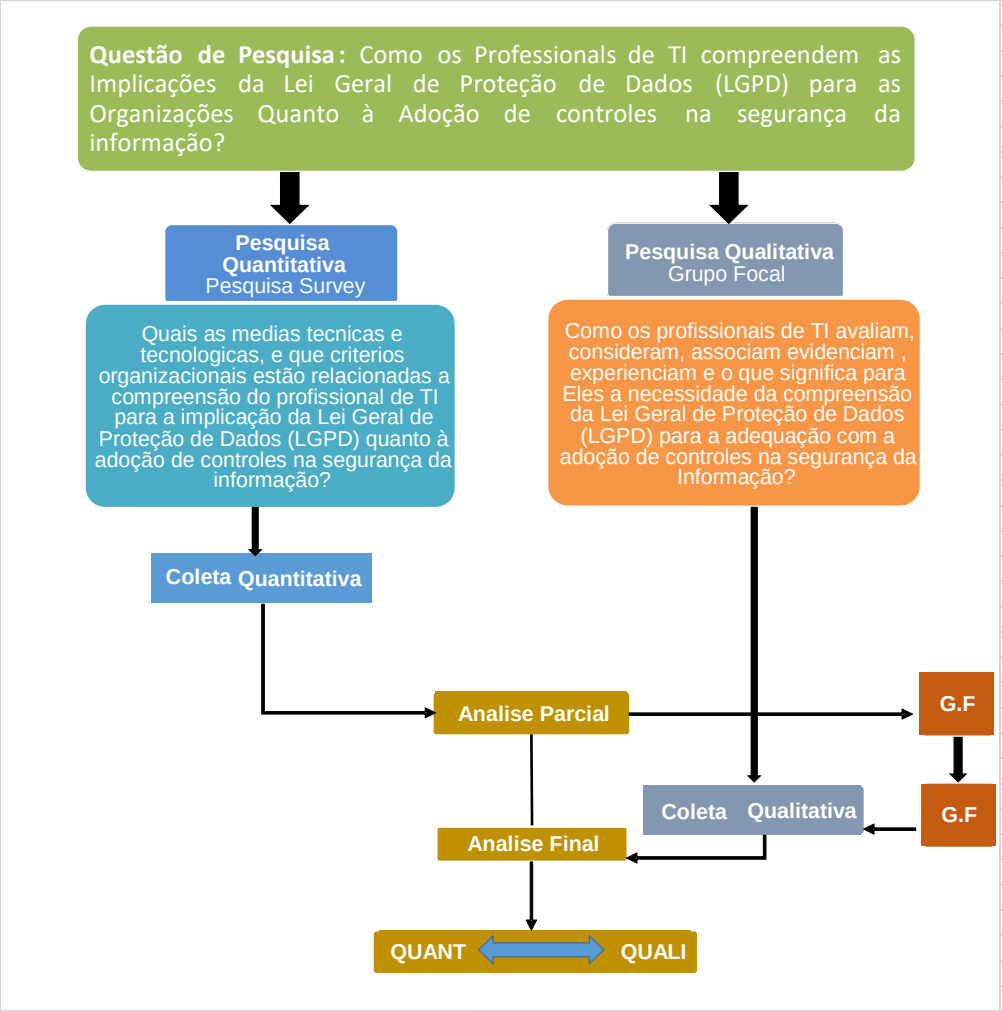
5 APRESENTAÇÃO E ANÁLISE DOS DADOS

Neste trabalho, conforme já abordado nos procedimentos metodológicos, a metodologia aplicada combinou as abordagens quantitativas e qualitativas, com o propósito de analisar e interpretar dados, observando na pesquisa e na opinião dos participantes do grupo focal, considerando o objetivo central deste trabalho – Como os profissionais de TI compreendem as implicações da Lei Geral de Proteção de Dados (LGPD) para as organizações quanto à adoção de controles na segurança da informação? Portanto, utilizou-se dois métodos de pesquisa, por considerar que o resultado de uma abordagem poderá aprimorar a interpretação dos dados com análise por uma segunda fonte.

A análise dos dados das pesquisas quantitativa e qualitativa seguiram o planejamento e as etapas definidas no desenho de pesquisa, conforme a figura 8. Para colaborar com a abordagem mista de método, os autores Cooper; Schindler (2016) e Yin (2015) consideram a coleta de dados a partir de múltiplas fontes, de forma coerente com estudos de casos múltiplos. A pesquisa envolveu a realização de *Survey Web*, que aplicou questionários e reunião com participantes-chave da mesma organização. Segundo Wright (2005), uma pesquisa *Survey web* tem vantagens pela agilidade proporcionada pelos recursos de TI, além do custo baixo e da alta taxa de respostas, como destacam Ilieva et al. (2002). Considerando a análise dos dados qualitativa e quantitativamente, pode-se notar que a aplicação dos dois métodos possibilita a integração dos dados que resultam em informações que poderão apoiar a organização mutuamente.

Nesta pesquisa, adotou-se estrategicamente que os dados qualitativos e quantitativos teriam o mesmo peso. A fundamentação teórica adotada para os pressupostos relacionados à Segurança da Informação.

Figura 8 – Diagrama das pesquisas Quantitativa e Qualitativa



Fonte: Elaborado pela autora (2021)

A pesquisa quantitativa foi composta por 70 profissionais de TI do SENAC. Os critérios definidos estavam diretamente relacionados com a experiência profissional e a função que exerciam. Desta forma, foram excluídos os profissionais de TI de nível técnico e auxiliares.

Para a pesquisa foi enviado o questionário, através da plataforma *Microsoft Forms*, para 70 e-mails, dos quais 64 profissionais de TI do SENAC preencheram o *Forms*, e 6 não retornaram. Portanto, o percentual dos participantes ficou em 91.4%. Os quais foram observados, que 70% são do sexo masculino e 30% feminino, no critério para a faixa etária 37% estão entre 46 e 55 anos, 28% estão entre 36 e 45 anos, 22% estão entre 26 e 35 anos e 13% estão acima dos 55 anos. Para o perfil área de atuação a composição foi: 44% para

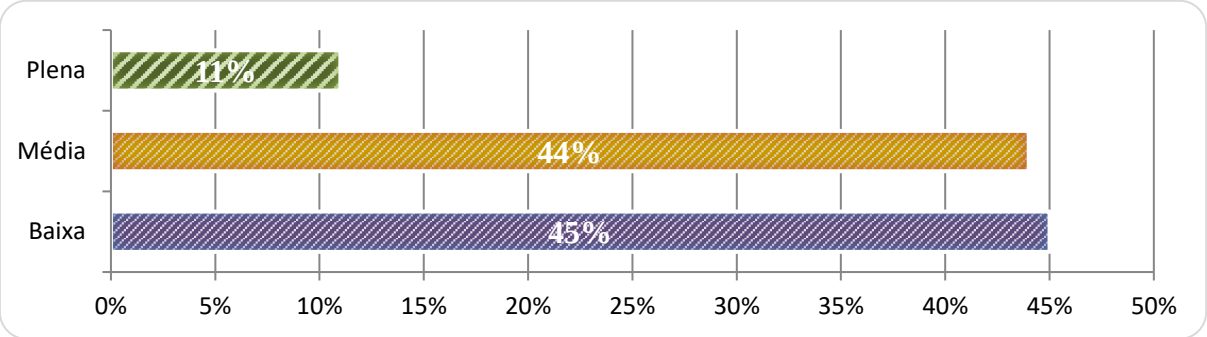
Gerentes, 31% para Analista de Sistema, 14% para Diretor e 11% como Coordenadores de TI. Na análise experiência profissional observou-se que 33% estão acima de 20 anos, 19% estão entre 11 e 15 anos, 19% estão entre 1 e 5 anos e 13% estão entre 16 e 20 anos de experiências, consoante Tabela 2, na subseção 4.3.

Para a 1ª etapa do Grupo Focal, contou-se com a participação de 16 Profissionais de TI, onde 07 deles receberam o resultado da pesquisa *survey* e o roteiro da reunião, os demais receberam apenas o *link* de acesso a plataforma *Teams*, os quais, participaram como ouvintes.

5.1 ANÁLISE PARCIAL DA PESQUISA *SURVEY*

O primeiro indicador, observado na pesquisa *Survey* mostrou que a percepção quanto à compreensão da Lei e seus impactos na organização demostra que 45% dos profissionais de TI do SENAC consideraram que o seu conhecimento quanto a LGPD está abaixo do recomendado, 44% afirmam estar com o nível de conhecimento mediano e 11% declaram ter plenamente o conhecimento da LGPD e os possíveis impactos que ela poderá trazer para a organização, conforme Gráfico 1 abaixo.

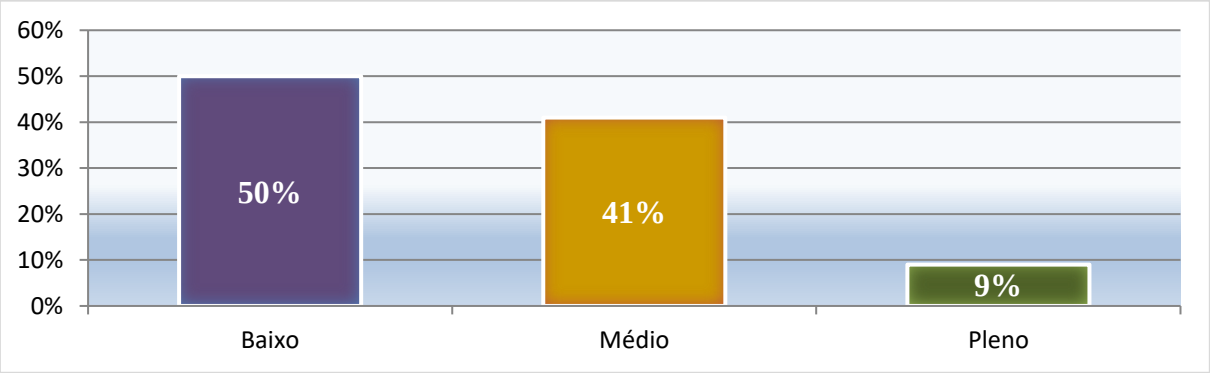
Gráfico 1 - Auto percepção quanto ao conhecimento sobre a LGPD.



Fonte: Elaborado pela autora (2021) através da extração dos dados da pesquisa *survey*.

No indicador “diretrizes para a Política da Segurança da Informação” (PSI), observou-se que os critérios adotados na política da segurança da informação, de acordo com as normas ISO/IEC 27001/27002 e recomendados pela SGSI do SENAC, estão com 50% abaixo do recomendado, 41% estão mediamente de acordo com as normas e 9% afirmam que estão plenamente conforme os padrões de controle e segurança, conforme Gráfico 2. Os critérios adotados na Política de Segurança da Informação são requisitos fundamentas para a adequação da LGPD.

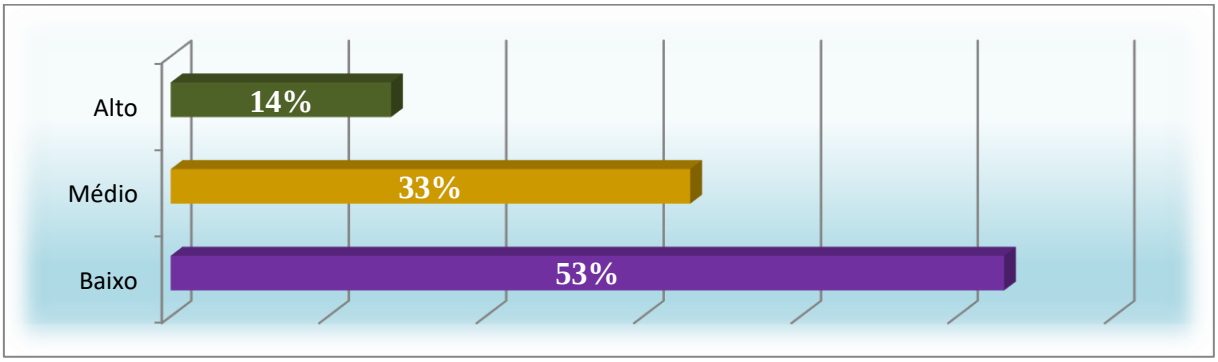
Gráfico 2 – Impacto da Política da Segurança da Informação



Fonte: Elaborado pela autora (2021) através da extração dos dados da pesquisa *survey*.

O indicador "gestão da tecnologia da informação – controle da informação", indica que: 53% estão com os controles da segurança da informação (CSI) abaixo da recomendação e os impactos poderão ser muito significativos, 33% classificaram que os controles atendem as recomendações acima da média e os impactos são pouco significativos, e 14% indicaram que os controles atendem as recomendações e os impactos serão pouco prováveis, pois os controles atuais seguem a NBR ISO 27003:13 (vide Gráfico 3).

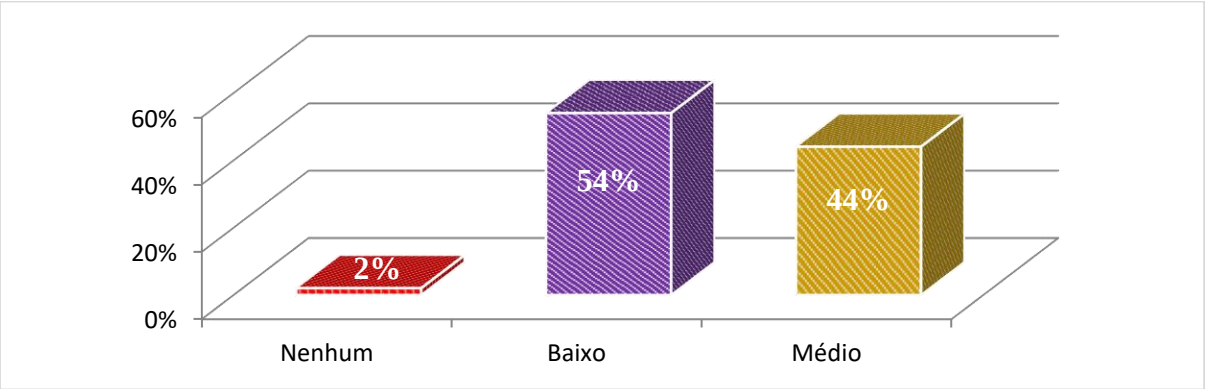
Gráfico 3 – Gestão da tecnologia da informação – Controle da informação



Fonte: Elaborado pela autora (2021) através da extração dos dados da pesquisa *survey*.

No indicador "controles gerais da informação na organização", os profissionais apresentaram que: 54% dos controles para as normas e os procedimentos para as informações estão abaixo dos padrões recomendamos na SGSI, 44% classificam que os controles das informações estão no nível aceitável, enquanto 2% afirmaram que não existe nenhum padrão para os controles da informação – normas e procedimentos, como informado no gráfico 4.

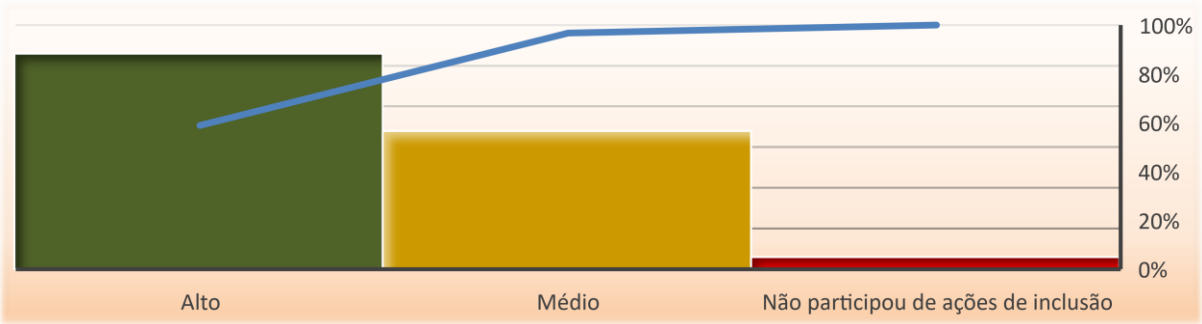
Gráfico 4 – Controles gerais da informação na organização



Fonte: Elaborado pela autora (2021) através da extração dos dados da pesquisa *survey*.

No indicador quanto as "ações para a inclusão na cultura organizacional quanto a Segurança da Informação no contexto da LGPD", 59% consideraram que as iniciativas de divulgação, de treinamento e de capacitação foram muitos eficazes, 38% dos profissionais determinaram que os programas adotados foram razoáveis e 3% afirmaram que não tiveram participação em nenhuma ação sobre os temas relacionados à esta legislação, como é retratado no gráfico 5.

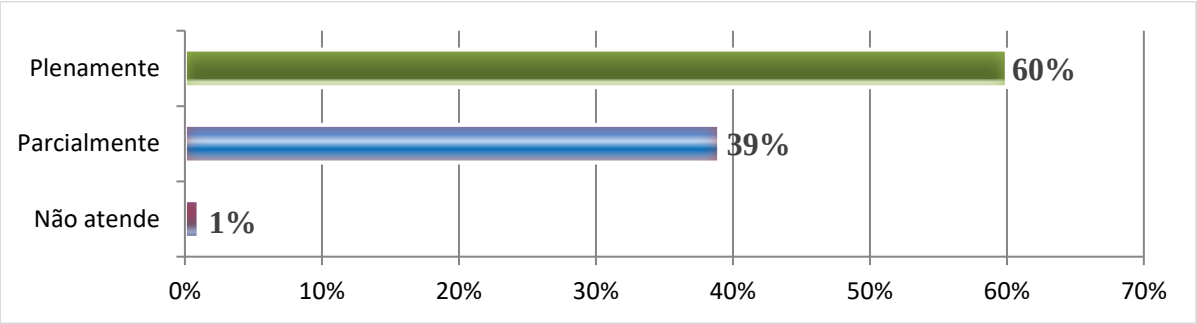
Gráfico 5 – Ações para a inclusão na cultura organizacional quanto a Segurança da Informação no contexto da LGPD.



Fonte: Elaborado pela autora (2021) através da extração dos dados da pesquisa *survey*.

No indicador "infraestrutura organizacional para atender a lei", os participantes consideraram que o SENAC vem investido na atualização técnica e tecnológica, os quais refletem no gráfico 6, com percentuais de 60% para plenamente atualizado, 39% em fase final de adequação e somente 1% ainda não atendem aos requisitos de atualização da infraestrutura de TI, como se pode notar no Gráfico 6.

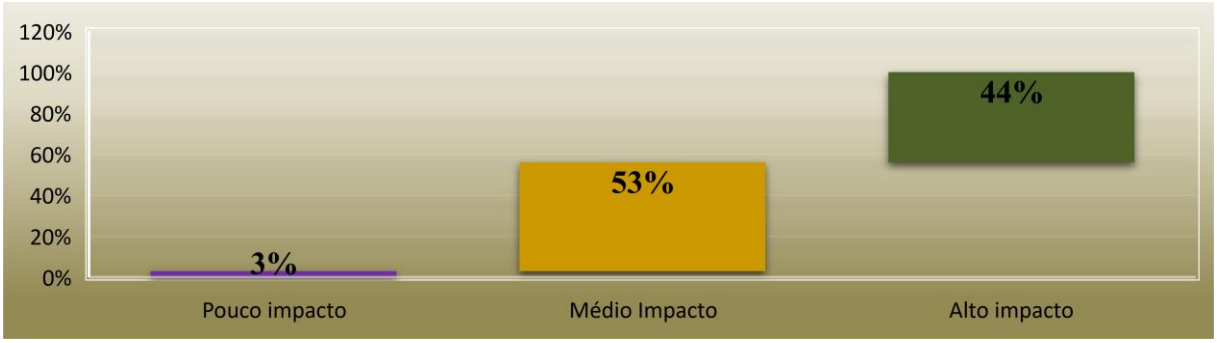
Gráfico 6 – Infraestrutura organizacional para atender a lei em sua organização



Fonte: Elaborado pela autora (2021) através da extração dos dados da pesquisa *survey*.

Na perspectiva do indicador "impacto da LGPD para a organização", observa-se que: 53% indicam que os impactos serão medianos, 44% identificaram que a lei poderá gerar impactos significativo e somente 3% consideraram que os possíveis impactos serão poucos, como é apresentado no Gráfico 7.

Gráfico 7 – Impacto da LGPD para a organização.



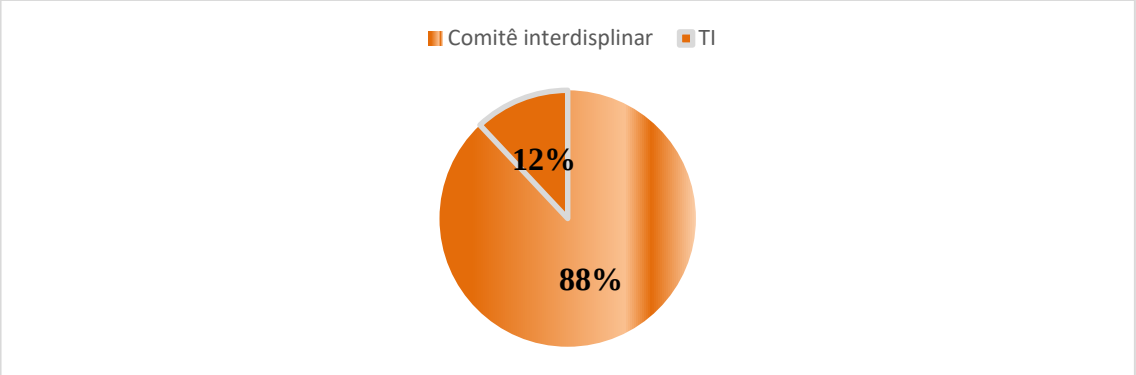
Fonte: Elaborado pela autora (2021) através da extração dos dados da pesquisa *survey*.

A pesquisa evidencia que a compreensão da Lei pelos Profissionais de TI está em assimilação, pois 50% dos profissionais questionados ainda não têm conhecimentos relevantes sobre a Lei. Um destaque identificado na pesquisa é o conhecimento, considerado crucial para que ocorra o processo de transformação da cultura, ou seja, a adequação da organização, atendendo aos três pilares: Pessoas, Tecnologia e Processos, considerando os critérios da LGPD.

Os gestores destacaram a importância da participação efetiva nas diversas áreas do SENAC – Diretoria, Administrativo, Financeiros, TI, RH, Jurídico, Marketing, Planejamento, e Educacional – no intuito de aplicar a abrangência da Lei em seus processos e porque é

necessário um controle efetivo e eficiente sobre os dados em todas áreas, considerando que o conhecimento e as responsabilidades de cada área são essências para o processo de adequação da LGPD no SENAC; destaca-se, também, a necessidade do acompanhamento efetivo pelo gestor das áreas, que deverá orientar, auxiliar e auditar a TI nas etapas da adequação. Interessante evidenciar que a adequação à LGPD terá 88% de atividades relacionadas as demais áreas e 12% ficarão sob a responsabilidade da TI, conforme Gráfico 8 abaixo.

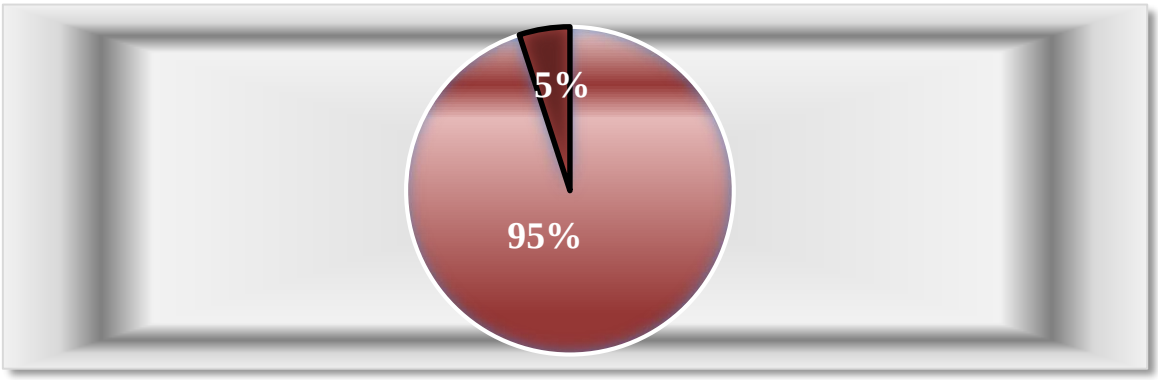
Gráfico 8 – Preferência de distribuição de atividades entre as áreas.



Fonte: Elaborado pela autora (2021) através da extração dos dados da pesquisa *survey*.

Fortalecendo o padrão de ações multidisciplinares no processo de adequação da Lei, os gestores, em sua maioria, consideraram que as medidas tecnológicas e as mudanças sistêmicas serão as mais simples neste processo. Todavia, a cultura organizacional deverá adequar-se, tanto no quesito da privacidade dos direitos individuais, como os indivíduos em relação à sociedade digital. No Gráfico 9, nota-se que 95% dos participantes já participaram de treinamentos sobre a LGPD e 5% estão estudando profundamente o tema. Fato que, salienta a importância de se capacitar para obter o conhecimento o qual é fundamental para o processo de adequação da lei para as organizações.

Gráfico 9 – Participação em treinamentos sobre a LGPD



Fonte: Elaborado pela autora (2021) através da extração dos dados da pesquisa *survey*.

Todos os gestores enfatizaram a importância da pesquisa e como o tema tem muitas questões a serem estudas, bem como, que os resultados refletiram o momento de adequação pelo qual a Instituição está passando. O sucesso da adequação da organização à Lei, no entendimento dos participantes, depende de três paliares: Pessoas, Tecnologia e Processos.

Depois da análise descritiva, foi analisada a correlação entre os indicadores das dimensões técnica, formal e informal. Em seguida, foi analisada a relação entre todos os doze índices e foi feita a análise de *Boxsplot* para representação da dispersão dos dados obtidos sobre os cargos dos respondentes, a saber: analistas, coordenadores, gerentes e diretores.

Os resultados encontrados corroboram com o aparato conceitual sobre a importância da Gestão da Segurança da Informação nas organizações e com a aplicação de medidas para assegurar a integridade e a confiabilidade das informações para fins de adequação à LGPD.

Ficou evidente também, a partir dos dados, a compreensão dos Profissionais de TI de que as diretrizes da LGPD para a gestão de TI facilitam as adequações técnicas, formais e informais. Os indicadores que mediram a compreensão determinaram a relação de eficiência na aplicação de medidas técnicas que possibilitam a aplicação das melhores práticas para garantir processos e serviços críticos de TI, determinando a disponibilidade de sistemas, de redes e de dados, e, consequentemente, a confiabilidade quanto aos controles de segurança da informação.

5.2 ANÁLISE ESTATÍSTICA DESCRITIVA DOS INDICADORES

Os dados evidenciaram que o indicador que apresentou maior média e mediana, simultaneamente, foi o IIOT – “indicador de Impactos e Oportunidades na dimensão Técnica”, e a menor média e mediana foi para o indicador IGST – “indicador da Gestão de Segurança na dimensão Técnica”. As médias variaram entre 4,1719 e 2,6758; a variação observada indica que os profissionais de TI, em média, identificaram o nível de impacto e as oportunidades que a LGPD poderá incidir sobre a organização, assim como na gestão de TI as possíveis mudanças operacionais são muito percebidas, pois, atingiram quase o ponto máximo da escala indicada. A menor média observada na tabela ficou para a gestão da segurança da informação que apresentou o menor ponto da escala indicada, o que evidencia a necessidade de as organizações aplicarem medidas mais eficientes neste aspecto (Tabela 4). Segundo Almeida (2010, P.156), “Ainda que se perceba a necessidade de implementá-la, em geral não há clareza sobre o que

deve ser protegido e sobre como fazê-lo". O autor defende o uso de uma ontologia para definir a informação no ambiente organizacional para a proteção dos dados, para garantir o sucesso na gestão da segurança da informação.

Tabela 4 – Estatísticas Descritivas.

Índices	IGST	IGSF	IGSI	ICIT	ICIF	ICII	ICIRPT	ICIRPF	ICIRPI	IIOT	IIOF	IIOI
Média	2,6758	3,6328	3,1250	3,7188	3,3125	3,5313	3,6797	3,7500	3,4479	4,1719	3,7969	4,0234
Mediana	2,6250	3,6250	3,0000	3,7500	3,0000	4,0000	3,5000	4,0000	3,3330	4,0000	4,0000	4,0000
Mínimo	1,5000	2,5000	1,0000	2,7500	2,0000	1,0000	1,0000	2,0000	1,0000	2,6670	2,0000	1,5000
Máximo	3,7500	5,0000	5,0000	5,0000	5,0000	5,0000	5,0000	5,0000	5,0000	5,0000	5,0000	5,0000

Fonte: Elaborado pela autora (2021) através da extração dos dados da pesquisa *survey*.

No ponto mínimo, apenas o indicar ICIT – "indicador do Controle da Informação na dimensão Técnica" apresentou o nível mínimo 2,7500 mais próximo de 3 entre os mínimos, o que demonstra um ponto de alerta quanto à necessidade de controles mais efetivos para se adequar à LGPD, considerando que a ISO/IEC 27002:2013 entende que controle é a "forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal."

Apenas o indicador IGST – "indicador Gestão de Segurança na dimensão Técnica" apresentou o nível mais próximo de 4, com 3,7500 pontos, sinalizando que as organizações adotaram controles técnicos, corroborado pela NBR ISO/IEC 27.002:2013, que conceitua a segurança da informação como a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio; minimizar os riscos ao negócio; maximizar o retorno sobre os investimentos e as oportunidades que estabelecem como seu objetivo a preservação da confidencialidade, da integridade e da disponibilidade da informação. Sêmola (2014) concorda e acrescenta que a informação é reconhecida como um ativo crítico para a continuidade operacional das organizações.

5.3 MATRIZ DE CORRELAÇÃO GERAL

A matriz de correlação dos indicadores estará avaliando por meio da análise das correlações lineares, entre as variáveis, como elas se comportam nas forças positivas e negativas. Observa-se na Tabela 5 que a maior força de correlação positiva geral entre os índices

(0.793) foram os indicadores Gestão de Segurança (IGSF e IGSI). Seguida pela segunda maior força de correlação positiva geral (0,752), também os índices da Gestão de Segurança (IGST e IGSF) e a terceira (0,750) entre os índices de Controle das Informações (ICIF e ICII). No que comprovam os autores BELASCO; WAN (2006); GORAYEB (2012); MAYNARD; RUIGHAVER (2006); SÊMOLA (2014), a segurança da informação envolve uma série de medidas que vão além de soluções técnicas ou tecnológicas, alcançando os processos internos das organizações, formação de equipes e comitês organizacionais, treinamento de usuários e profissionais de TI, ações de divulgação e conscientização e mudanças de comportamentos dos indivíduos, além da conformidade com requisitos legais.

Tabela 5 – Matriz de Correlação Geral

Coeficientes de correlação, usando todas as observações 1 – 64												
	IGST	IGSF	IGSI	ICIT	ICIF	ICII	ICIRPT	ICIRPF	ICIRPI	IIOT	IIOF	IIOI
IGST	1											
IGSF	,752**	1										
IGSI	,705**	,793**	1									
ICIT	,343**	,329**	,304*	1								
ICIF	,589**	,629**	,578**	,384**	1							
ICII	,559**	,636**	,606**	,243	,750**	1						
ICIRPT	,238	,368**	,298*	,284*	,381**	,311*	1					
ICIRPF	,372**	,353**	,290*	,496**	,295*	,194	,223	1				
ICIRPI	,582**	,516**	,343**	,426**	,366**	,236	,456**	,436**	1			
IIOT	-,290*	-,315*	-,494**	,258*	-,198	-,234	,124	,106	,119	1		
IIOF	,076	,028	-,030	,223	-,034	-,015	,133	,298*	,312*	,396**	1	
IIOI	-,014	-,179	-,163	,271*	,011	,047	,068	,225	,064	,489**	,448**	1

Fonte: Elaborado pela autora (2021) através da extração dos dados da pesquisa *survey*.

Na correlação negativa geral, a 1ª maior força negativa geral entre os índices (-0.494) foi entre os índices IGSI e IIOT, ou seja, quanto maior forem as ações de treinamentos, de divulgações e de conscientização organizacional quanto às medidas adotadas na gestão da segurança da informação, menor serão os impactos técnicos nos processos de monitoramento, contingenciamento e recuperação dos dados. No que demonstra Chiles (2013), ações de treinamento proporcionam a redução de falhas na utilização de novos processos e resultam uma implantação com melhores resultados.

A 2ª maior força de correlação negativa geral (-0,315) foi entre os índices IGSF e IIOT, ou seja, quanto mais forem as medidas formais para os processos, procedimentos, normas, políticas entre outras medidas de *compliance*, menor serão os impactos técnicos nos processos de monitoramento, contingenciamento e recuperação dos dados.

Para a 3ª força negativa (-0,290) entre os índices IGST e IIOT, isto é, quanto mais adotarem adaptações técnicas e tecnológicas para a Gestão da Segurança para os monitoramentos, contingenciamentos, redundâncias entre outras medidas técnicas, tais medidas diminuem os impactos técnicos, diminuindo também as possibilidades de sanções para as organizações, com aplicação de penalidade para os profissionais de TI responsáveis pela gestão das informações.

Observando a matriz geral de correlações entre as variáveis e as dimensões, podemos concluir que: a Gestão da Segurança apresentou os índices mais fortes de toda a pesquisa sobre as observações dos profissionais de TI. Na 1ª força evidencia que os profissionais de TI indicaram que a eficiência da Gestão da Segurança da Informação está relacionada com deliberação de diretrizes, normas, políticas, regras, procedimentos, controles entre outras medidas que asseguram a integração das informações. Contudo, é essencial que essas ações sejam divulgadas, conscientizadas e treinadas, sendo inseridas na cultura da organização.

Na 2ª força é evidenciada novamente que a Gestão da Segurança da Informação determina a relação de eficiência com a aplicação de medidas técnicas que possibilitam o contingenciamento nos componentes críticos, o que possibilita a alta disponibilidade de sistemas, de redes e de dados. Desta forma, o funcionamento de um serviço, a confiabilidade dele é aprimorada, pois, caso aconteça uma falha de qualquer natureza no sistema primário, o sistema secundário assume o controle da operação. O que garante a utilização ininterrupta de serviços e evita a perda de dados. Contudo, é fundamental que as organizações adotem normas, políticas, regras, procedimentos, controles entre outras medidas que favoreçam a confiabilidade e evitem as falhas operacionais. Segundo Tomiatti (2012), fica voltado à governança de TI o papel na criação de controles que permitam que a TI trabalhe da forma mais transparente possível, permitindo que as informações armazenadas em seus sistemas sejam confiáveis, para que as decisões sejam acertadas tanto pela TI quanto pela direção da organização.

Na 3ª força foi abordado o Controle das Informações, que consiste nas adaptações técnicas que possibilitam a disponibilidade sistêmica, a estabilidade e permite o acesso dos usuários de forma segura de ameaças externas e internas, o que, preserva a confidencialidade, a integridade e a disponibilidade da informação. Para tal, as diretrizes de divulgação, de conscientização e de treinamentos quanto aos controles das informações minimizam os riscos de vazamento. Desta forma, Sêmola (2014) afirma que a vulnerabilidade da informação está em toda parte da organização, e, para tal, é básico a conscientização das ações nas organizações.

Considerando a relação das correlações negativas para os índices da Gestão da Segurança Informal, ou seja, quanto menor forem as ações em divulgação, os treinamentos e a conscientização sobre as diretrizes de Controle da Informação, maior serão os impactos na Gestão da Segurança, e isso consequentemente possibilitará uma maior vulnerabilidade nas operações das organizações.

Na segunda análise, a maior força de correlação negativa geral indica que quanto maior forem as aplicações de políticas, de regras, de procedimentos, de medidas de segurança, entre outros que assegurem os controles, as informações na organização, menor serão os impactos nos processos organizacionais, na gestão de TI e na adequação à LGPD.

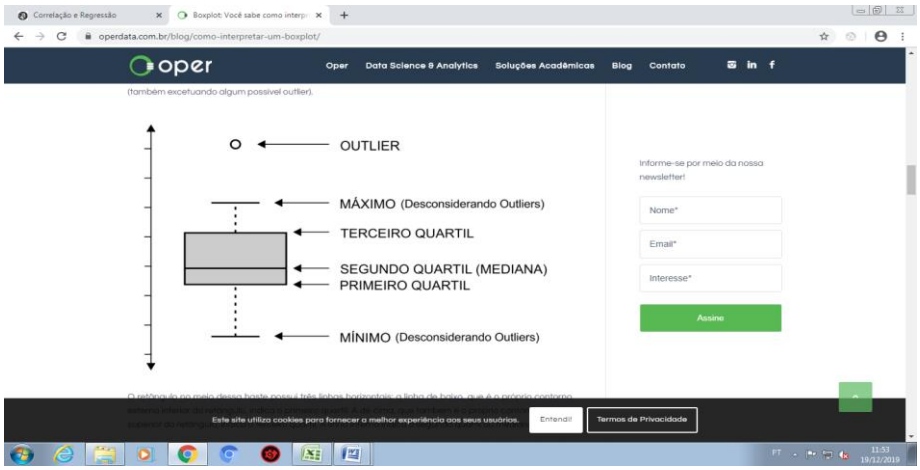
Para a terceira força negativa, quanto maior forem as ações que possibilitem o contingenciamento nos componentes críticos os quais são essenciais para a alta disponibilidade de sistemas, de redes e de dados, menor serão os impactos nas rotinas operacionais.

Conclui-se que, quanto maior for a Gestão da Segurança da Informação, maior será a qualidade da Segurança e menor serão os impactos operacionais, o que poderá resultar em maiores oportunidades profissionais. No entanto, se a Gestão da Segurança da Informação for baixa, maior serão os impactos operacionais e praticamente nenhuma oportunidade profissional.

5.4 APRESENTAÇÃO DA ANÁLISE DE DISPERSÃO DO INDICADOR DA GESTÃO DE SEGURANÇA POR CARGO

A análise de dispersão por cargo teve por base os quatro cargos identificados nos dados, a saber: Analista, Coordenador, Gerente e Diretor. Essa análise foi realizada através da ferramenta *boxsplot*, conforme a Figura 9 que é a exemplificação de como utilizar a ferramenta gráfica que permite visualizar a distribuição e os valores discrepantes (*outliers*) dos dados, fornecendo, assim, um meio complementar para desenvolver uma perspectiva sobre o caráter dos dados. Além disso, o *boxplot* também é uma disposição gráfica comparativa, cujas medidas de estatísticas descritivas com o mínimo, o máximo, o primeiro quartil, o segundo quartil ou a mediana e o terceiro quartil formam o *boxplot*.

Figura 9 – Boxplot – Gráfico de Análise de Dados

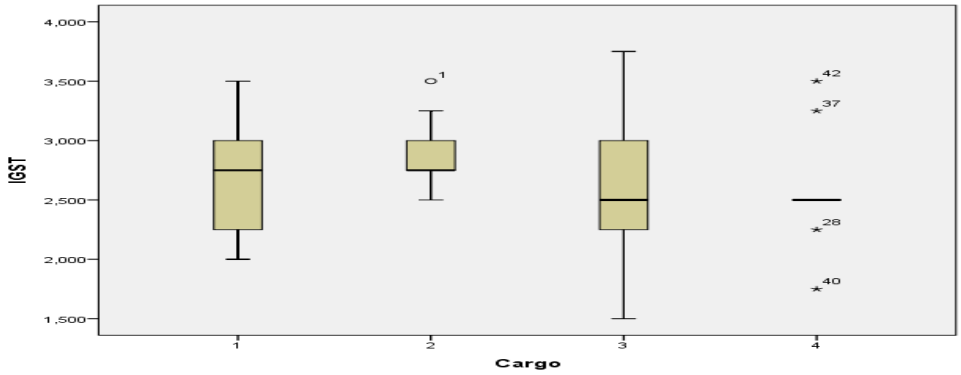


Fonte: *site* operdata.com.br

Observa-se na Figura 10 a dispersão quanto as avaliações do objetivo específico *"Identificar como os profissionais de TI veem as adequações da LGPD quanto ao tratamento dos dados pessoais sobre a políticas de segurança da informação"*. Sob a ótica da fundamentação teórica – Gestão da Segurança na dimensão TÉCNICA, o resultado diagnosticado foi: o cargo Analista (1) apresentou maior dispersão de dados (maior distância entre o primeiro e o terceiro quartil). Já o cargo Coordenador (2) apresenta a maior concentração de respostas, ou seja, a menor dispersão de dados. Sob a perspectiva de conformidade das médias, observa-se que o Analista e o Coordenador apresentaram a maior mediana, entre 2,5 e 3,0, e também maior aproximação com o máximo ideal.

Portanto, o resultado indica que há maior conformidade entre a percepção dos cargos de Gerentes e de Coordenadores de TI. É possível verificar características similares, cuja tendência das respostas foi para uma maior atribuição à Gestão da Segurança da Informação, o que determina a relação de eficiência com a aplicação de medidas técnicas que propiciam o contingenciamento nos componentes críticos, proporcionando uma alta disponibilidade sistêmica. Como resultado, um serviço confiável que reforça a necessidade de uma compreensão técnica nos processos de adequação para os requisitos de segurança da informação da lei 13.709/2018.

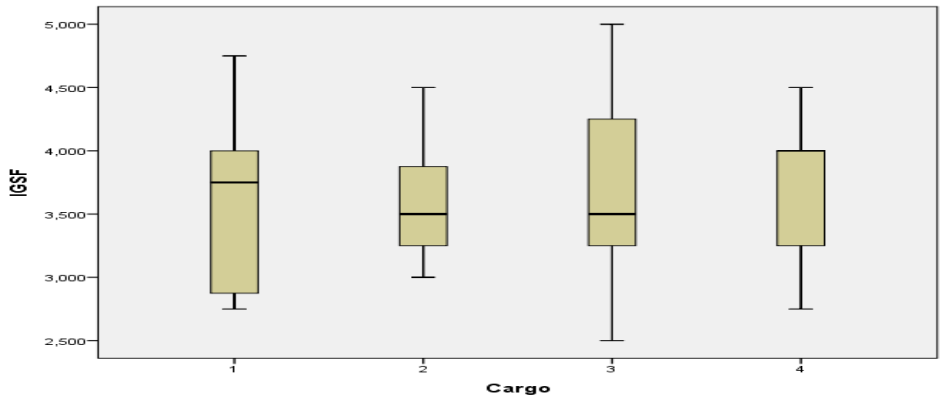
Figura 10 – Distribuição do IGST por Cargo



Fonte: Elaborado pela autora (2021) através da ferramenta *boxsplot*,

Na Figura 11, observa-se a dispersão, quanto ao objetivo específico *"Identificar como os profissionais de TI veem as adequações da LGPD quanto ao tratamento dos dados pessoais sobre a políticas de segurança da informação"*. Quanto à fundamentação teórica – Gestão da Segurança na dimensão FORMAL, a maior dispersão dos dados foi para o Analista (1) (maior distância entre o primeiro e o terceiro quartil). No entanto, Coordenadores (2) apresentam a maior concentração de respostas, ou seja, a menor dispersão de dados. Sob a perspectiva de conformidade das médias, observa-se que o Diretor (4) apresenta a maior mediana, entre 4,0 e 4,5, considerando que há maior disponibilidade da informação para pessoas deste cargo.

Figura 11 – Distribuição do IGSF por Cargo



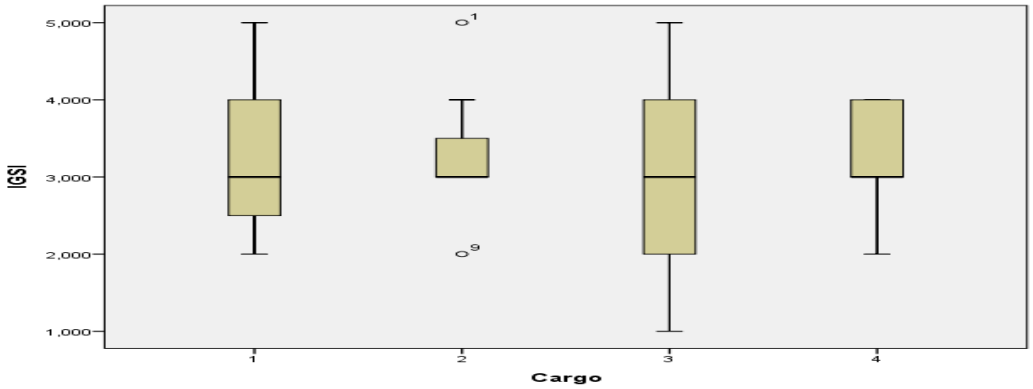
Fonte: Elaborado pela autora (2021) através da ferramenta *boxsplot*,

Diante disso, a segurança da informação envolve uma série de medidas que vão além de soluções técnicas ou tecnológicas, alcançando os processos internos das organizações, a formação de equipes e comitês organizacionais, o treinamento de usuários e profissionais de TI, as ações de divulgação e conscientização, fatos que, evidenciam que quanto maior acesso

às informações, melhores serão as aplicações e compreensões aos processos e procedimentos organizacionais a conformidade com a LGPD.

Na Figura 12, há dispersão quanto ao objetivo específico *"Identificar como os profissionais de TI veem as adequações da LGPD no tratamento dos dados pessoais sobre a políticas de segurança da informação"*. Quanto à fundamentação teórica – Gestão da Segurança na dimensão INFORMAL: a maior dispersão de dados foi do Gerente (3), (maior distância entre o primeiro e o terceiro quartil). Contudo, o Coordenador (2) apresenta a maior concentração de respostas, ou seja, a menor dispersão de dados. Sob a perspectiva de conformidade das médias, observa-se que apresentaram mediana igual a 3,0, e, considerando a pontuação máxima igual a 5 (cinco), portanto, respostas com maior conformidade com o máximo ideal.

Figura 12 – Distribuição do IGSI por Cargo

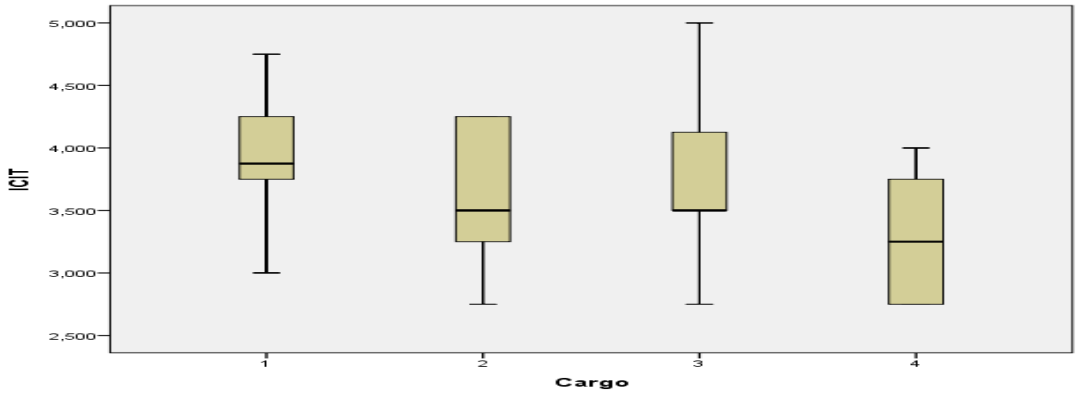


Fonte: Elaborado pela autora (2021) através da ferramenta *boxsplot*,

Assim, fica demonstrado que as ações de treinamentos, de divulgações e a conscientização organizacional quanto às medidas adotadas na gestão da segurança da informação sobre a adequação da LGPD são fundamentais para minimizar os impactos técnicos e os processos organizacionais, fato apontado na pesquisa *Survey* pelos Coordenadores de TI.

Na Figura 13, a maior dispersão dos dados apresentados foi o (2) Coordenador (2) (maior distância entre o primeiro e o terceiro quartil). O Analista (1) apresentou a maior concentração de respostas, ou seja, a menor dispersão de dados. Sob a perspectiva de conformidade das médias, observa-se que o Analista (1) apresenta a maior mediana, entre 3,5 e 4,0, e, considerando a pontuação máxima igual a 5 (cinco), portanto, respostas com maior conformidade com o máximo ideal.

Figura 13 – Distribuição do ICIT por Cargo

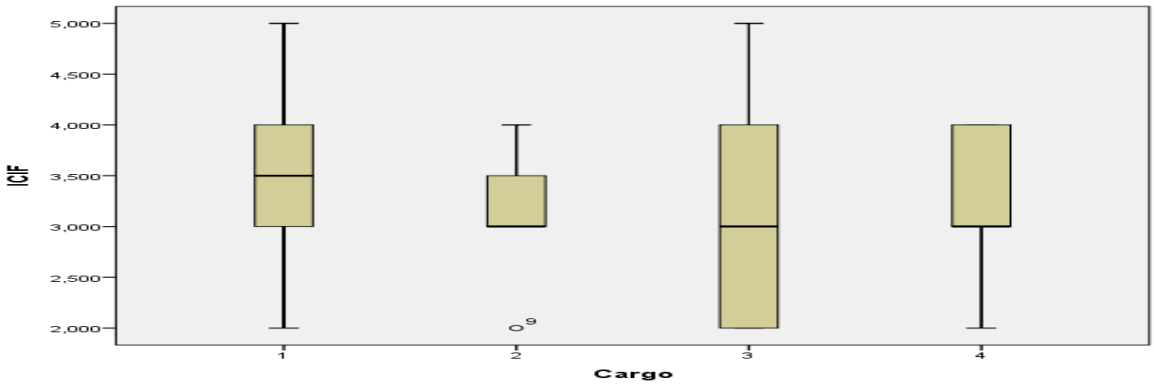


Fonte: Elaborado pela autora (2021) através da ferramenta *boxsplot*,

Este resultado indica que há maior conformidade entre a percepção do Analista, cuja tendência das respostas foi para uma maior atribuição ao Controle da Informação, que determina a aplicação de medidas técnicas nos controles de acesso aos dados, o que proporciona a confiabilidade dos dados. Desta forma, as medidas de controle reforçam as obrigações técnica sobre os requisitos no controle de acesso, conforme a LGPD. O que reforça que o conhecimento sobre as necessidades técnicas para esta conformidade é mais evidenciado pelos analistas, pois estes são os que gerenciam os dados das instituições.

Analisando a Figura 14, a dispersão maior de dados foi do Gerente (3) (maior distância entre o primeiro e o terceiro quartil). No entanto, o Coordenador (2) apresenta a maior concentração de respostas, ou seja, a menor dispersão de dados. Sob a perspectiva de conformidade das médias, observa-se que o Analista (1) apresenta a maior mediana, entre 3,5 e 4,0, e, considerando a pontuação máxima igual a 5 (cinco), portanto, respostas com maior conformidade com o máximo ideal.

Figura 14 – Distribuição do ICIF por Cargo

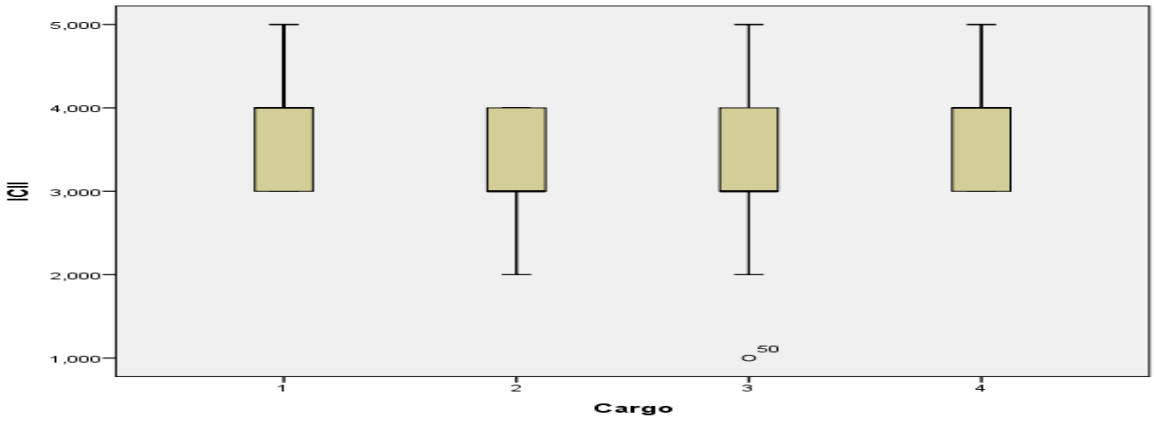


Fonte: Elaborado pela autora (2021) através da ferramenta *boxsplot*,

Consequentemente, o resultado indica que há maior entendimento entre a percepção do Analista, cuja tendência das respostas foi para uma maior atribuição ao Controle da Informação, quanto as políticas, as normas, as regras, os procedimentos, entre outras, na formatação dos regimentos aos controles de acesso às informações, o que proporciona as diretrizes quanto ao uso dos dados. Assim sendo, as diretrizes legais minimizam os impactos dos acessos indevidos. Esses profissionais de TI, portanto, corroboram o pressuposto de que a compreensão sobre a legislação poderá atuar como facilitador da definição de controles formais de segurança da informação.

Observa-se na Figura 15, quanto à dispersão, que todos possuem a mesma dispersão. Sob a perspectiva de conformidade das médias, observa-se que o Analista (1) e o Diretor (4) apresentam as maiores medianas, entre 4,0 e 5,0, e, considerando a pontuação máxima igual a 5 (cinco), portanto, respostas com maior conformidade com o máximo ideal.

Figura 15 – Distribuição do ICII por Cargo



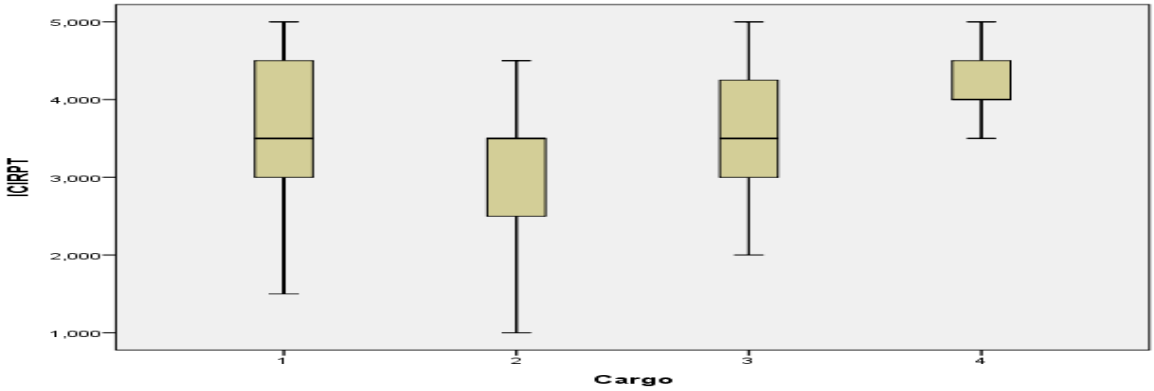
Fonte: Elaborado pela autora (2021) através da ferramenta *boxsplot*,

Desta maneira, destacamos que o resultado demonstrou que todos os cargos pesquisados têm a mesma dispersão de respostas, o que evidencia que as ações de divulgação, comunicação, informação, treinamentos e capacitações quanto ao Controle da Informação até este momento encontram-se em fases diversas. Contudo, os Diretores e Analistas de TI apresentaram as maiores medianas quanto ao Controle da Informação na Dimensão Informal.

Na Figura 16, observa-se que a dispersão de dados foi maior para o Analista (1), (maior distância entre o primeiro e o terceiro quartil). Todavia, o Diretor (4), apresenta a maior concentração de respostas, ou seja, a menor dispersão de dados. Sob a perspectiva de conformidade das médias, observa-se que o Diretor (4) apresenta a maior mediana, entre 4,0 e

5,0, e, considerando a pontuação máxima igual a 5 (cinco), portanto, respostas com maior conformidade com o máximo ideal.

Figura 16 – Distribuição do ICIRPT por Cargo



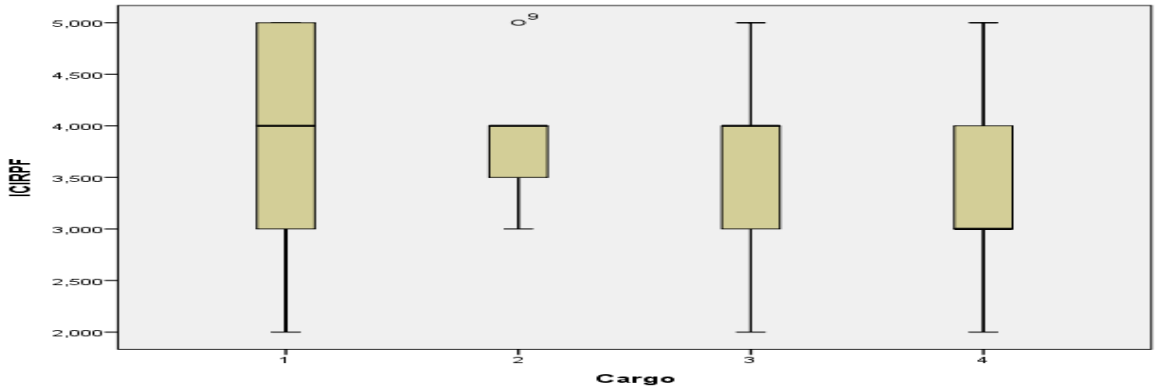
Fonte: Elaborado pela autora (2021) através da ferramenta *boxsplot*,

Assim sendo, a análise dos dados permitiu constatar que o Controle da Informação quanto às Responsabilidades e Penalidades na dimensão técnica apresenta uma dispersão maior por parte dos Analista e os Diretores de TI, os quais tem um entendimento mais uniforme das respostas. Este fato pode ser atribuído ao nível de compreensão que este cargo pode ter sobre as sanções aplicadas pela Lei, o que reforça a exigência da compreensão do profissional de TI quanto ao tema, o qual refletiu-se na maior dispensação das respostas.

Analisando a Figura 17, a maior dispersão de dados foi o Analista (1) (maior distância entre o primeiro e o terceiro quartil). Enquanto o Coordenador (2) apresenta a maior concentração de respostas, ou seja, a menor dispersão de dados. Sob a perspectiva de conformidade das médias, observa-se que o Analista (1) o Coordenador (2), e o Gerente (3) apresentam as maiores medianas, entre 4,0 e 4,5, e, considerando a pontuação máxima igual a 5 (cinco), portanto, respostas com maior conformidade com o máximo ideal.

Nos resultados apresentados para o Controle da Informação quanto às Responsabilidades e às Penalidades na dimensão formal, observa-se que os Analistas têm uma dispersão maior, provavelmente, por sua pouca atuação nos processos de políticas, normas, regulamentos, procedimentos entre outras diretrizes, fato que corrobora com a necessidade de compreensão das diretrizes legais. No entanto, Diretores, Gerentes e Coordenadores de TI apresentam uma regularidade nas respostas, provavelmente, por causa da compreensão sobre os regimentos e normas da lei, o que reforça a exigência da compreensão do profissional de TI quanto ao tema, o qual refletiu-se na maior dispensação das respostas.

Figura 17 – Distribuição do ICIRPF por Cargo



Fonte: Elaborado pela autora (2021) através da ferramenta *boxsplot*,

A Figura 18 mostra que a maior dispersão dos dados ocorreu com o Coordenador (2) (maior distância entre o primeiro e o terceiro quartil). Contudo, o Gerente (3) apresenta a maior concentração de respostas, ou seja, a menor dispersão de dados. Sob a perspectiva de conformidade das médias, observa-se que o Gerente (3) apresenta a maior mediana, entre 3,0 e 4,0, considerando a pontuação máxima igual a 5 (cinco), portanto, respostas com maior conformidade com o máximo ideal.

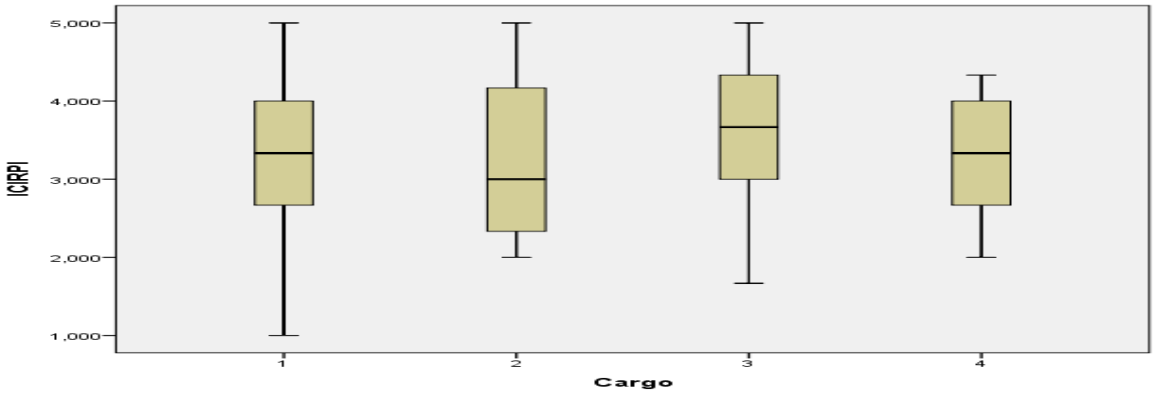
Deste modo, observa-se que o Controle da Informação quanto às Responsabilidades e às Penalidades na dimensão informal apresentou uma dispersão maior por parte dos Coordenadores de TI, e os Gerentes de TI apresentaram uma maior consistência nas respostas, como também, apresentaram a maior mediana, o que comprova que, dos cargos pesquisados, os Gerentes de TI compreendem a indispensabilidade de ações que proporcionam a comunicação, a divulgação, a informação, os treinamentos e as capacitações quanto aos controles das informações que devem ser adotados pela organização.

Na Figura 19, a maior dispersão dos dados apresentou-se no Gerente (3) (maior distância entre o primeiro e o terceiro quartil). Já o Diretor (4) apresenta a maior concentração de respostas, ou seja, a menor dispersão de dados. Sob a perspectiva de conformidade das médias, observa-se que o Analista (1) e o Gerente (3) apresentam a maior mediana, 4,0 e 4,5, considerando a pontuação máxima igual a 5 (cinco), portanto, respostas com maior conformidade com o máximo ideal.

Em suma, o resultado apresentou que os Gerentes foram o cargo que demonstrou maior dispersão nas respostas quanto aos Impactos e Oportunidades sobre a dimensão técnica, e os Diretores de TI maior contração, o que revela que: para os Gerentes as respostas estão

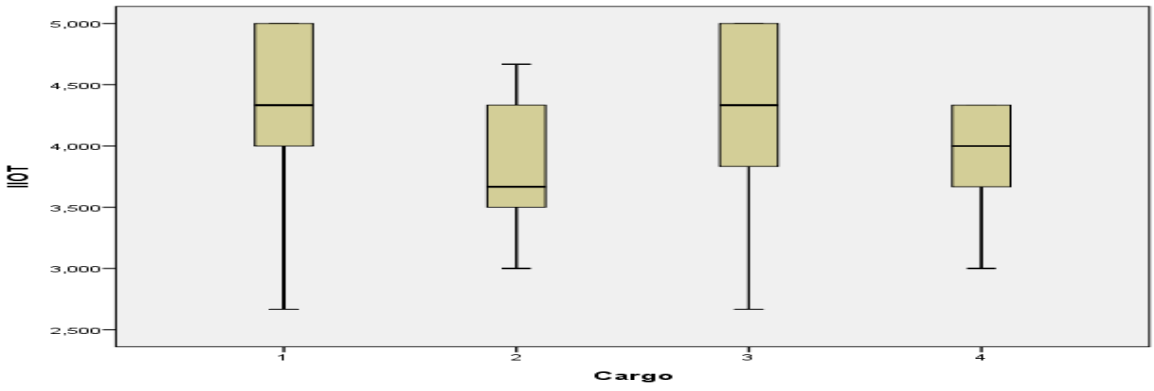
associadas às medidas de mitigações que vêm sendo tratadas nas Instituição, por isso a diversidade de respostas. Contudo, os Diretores de TI conseguem perceber, na sua maioria, os impactos que a Lei estará refletindo nas operações Institucionais. Todavia, os Gerentes e Analistas apresentaram uma maior mediana no que consistem as respostas, o que demonstra que os cargos com uma maior profundidade técnica apresentaram o melhor entendimento quanto aos impactos e as oportunidades que as implantações técnicas e tecnológicas, ou não, poderão representar na adequação à Lei nas Instituições, e, as oportunidades serão em cima dessas medidas técnicas e tecnológica aplicadas.

Figura 18 – Distribuição do ICIRPI por Cargo



Fonte: Elaborado pela autora (2021) através da ferramenta *boxsplot*,

Figura 19 – Distribuição do IIOT por Cargo

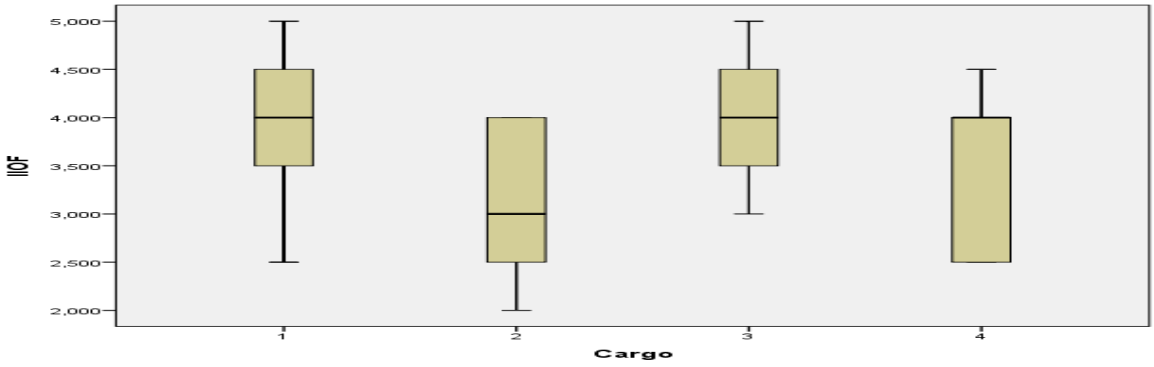


Fonte: Elaborado pela autora (2021) através da ferramenta *boxsplot*,

Analisando a Figura 20, a maior dispersão de dados ocorreu para o Coordenador (2) e Diretor (4) (maior distância entre o primeiro e o terceiro quartil). No entanto, o Analista (1) e o Gerente (3) apresentaram a maior concentração de respostas, ou seja, a menor dispersão de dados. Sob a perspectiva de conformidade das médias, observa-se que o Analista (1) e o Gerente

(3) apresentaram a maior mediana, entre 4,0 e 4,5, considerando a pontuação máxima igual a 5 (cinco), portanto, respostas com maior conformidade com o máximo ideal. Em síntese, os resultados indicam que os Diretores e Coordenadores de TI apresentam a maior dispersão nas respostas quanto aos Impactos e às Oportunidades sobre a dimensão formal, e os Gerentes e Analistas de TI maior contração, as quais revelam que Gerentes e Analistas compreendem que as políticas, as normas, os controles e outras normativas não podem ser dispensadas, pois, a publicação e a obrigação dessas medidas asseguram a eficiência das tratativas técnicas adotadas para mitigar os impactos.

Figura 20 – Distribuição do IIOF por Cargo

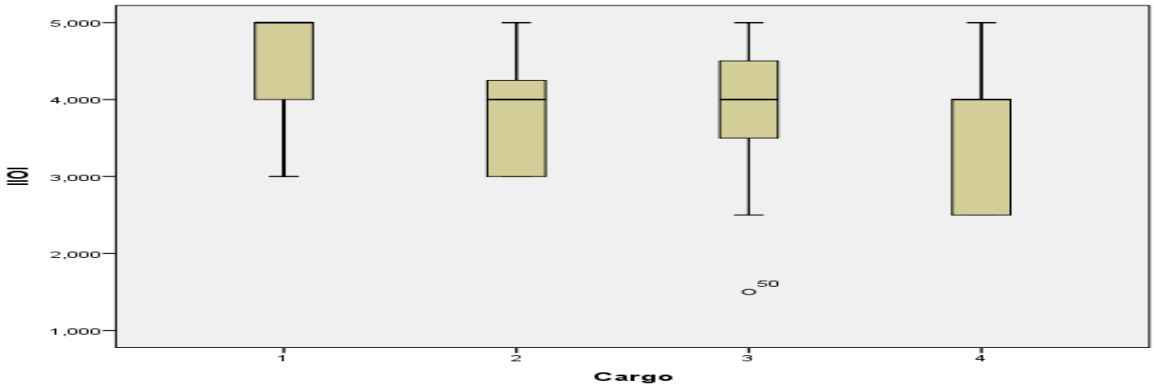


Fonte: Elaborado pela autora (2021) através da ferramenta *boxsplot*,

Na Figura 21, a dispersão dos dados ocorreu com o Diretor (4) (maior distância entre o primeiro e o terceiro quartil). Já o Gerente (3) apresenta a maior concentração de respostas, ou seja, a menor dispersão de dados. Sob a perspectiva de conformidade das médias, observa-se que o Analista (1) apresenta a maior mediana, 5,0, considerando a pontuação máxima igual a 5 (cinco), portanto, respostas com maior conformidade com o máximo ideal.

Os resultados indicam que os Diretores de TI apresentam a maior dispersão nas respostas quanto aos Impactos e Oportunidades sobre a dimensão informal, e os Gerentes de TI maior contração, e assim, pode-se considerar que os Gerentes percebem que a ações adotadas para comunicar os impactos e as oportunidades da Lei, e a compreensão sobre o tema pelos participantes são equivalentes. No entanto, os Diretores apresentaram resultados heterogêneos, o que pode refletir seu nível de compreensão quanto aos impactos e as oportunidades. Todavia, os Analistas apresentaram maior mediana, considerando que o nível de compreensão quanto aos impactos e as oportunidades são plenamente percebidos.

Figura 21 – Distribuição do IIOI por Cargo



Fonte: Elaborado pela autora (2021) através da ferramenta *boxsplot*,

5.5 RESULTADO DO GRUPO FOCAL

A reunião do grupo focal foi realizada em 22 de abril de 2021, tendo início às 17:05 e sendo encerrada duas horas depois, segundo roteiro Apêndice B. Contou com a participação dos gestores estratégicos do SENAC, que avaliaram os resultados da *survey* e, consequentemente, suas percepções sobre o assunto tratado e os possíveis impactos para a organização. A pesquisadora apresentou os resultados da *survey* e recebeu as seguintes contribuições: todos os participantes reconheceram que os resultados refletem a realidade da organização. Também foi unânime que o conhecimento sobre o tema está em construção e que existem muitas lacunas na lei que ainda requerem maiores estudos para a sua aplicação, sendo indispensáveis o conhecimento e a compreensão dos profissionais de TI sobre o tema, bem como a gestão de processos, pessoas e *compliance*, devido ao fato de a Lei abranger critérios e conceitos que excedem a Gestão da Tecnologia da Informação. Além disso, há um entendimento por parte dos participantes de que os requisitos da Lei devem ser observados em toda a organização. No entendimento dos gestores, um comitê multidisciplinar deve ter a responsabilidade de tratar da LGPD na organização, fortalecendo a ideia de que são necessárias ações multidisciplinares em um processo de adequação à Lei. Os gestores também consideraram que os controles tecnológicos e as demais mudanças necessárias são mais simples neste processo. Todavia, quase a totalidade dos gestores julgam que a conscientização organizacional quanto à privacidade é uma obrigação e uma demonstração de respeito aos direitos da sociedade digital. Nas palavras do gestor A "... a conscientização é muito importante para o processo de adequação da organização às exigências da Lei". Colaborando com o gestor A, o gestor D afirmou que "...o processo de adequação a LGPD se intensificou no Regional

após medidas de divulgação e treinamento para todos os níveis da organização...". As considerações contribuem com as ações da dimensão informal.

Todos os gestores participantes do Grupo Focal já participaram de treinamentos sobre a LGPD e os gestores C, F e G estão estudando profundamente o tema. Fato este, que cita a importância de se capacitar para obter o conhecimento, e, consequentemente, melhorar a atuação nos processos organizacionais. Os gestores enfatizaram a importância desta pesquisa e que o tema tem muitas lacunas a serem estudadas, bem como o fato, os resultados refletiram o momento de adequação que a Instituição SENAC está passando, complementando que o sucesso da adequação a qualquer lei depende do esforço e entendimento sobre pessoas, tecnologia e está *compliance*.

Durante a reunião foi possível destacar as considerações do gestor A, que fez uma reflexão sobre a lei no Brasil, as reverberações da GPDR - *General Data Protection Regulation*, que, traduzido, significa "Regulamento Geral de Proteção de Dados", para a proteção de dados pessoais de cidadãos da União Européia (UE) com a LGPD e os principais pilares e fundamentos da lei brasileira. Em seguida apresentou as medidas adotadas nacionalmente pela organização e suas contribuições para as subunidades regionais do SENAC quanto ao tema. Considerou que os resultados apresentados são reflexo da independência e autonomia que cada Departamento Regional tem para a GSI, lembrando que a gestão nacional atua como órgão consultivo. Acrescentou que foi criado um comitê técnico que delibera e trata todas as questões técnicas e tecnológicas nacionalmente, colaborando para o tratamento do tema LGPD.

Nas reflexões do gestor A, o SENAC também socializa processos e procedimentos para adequação à Lei como a construção da Cartilha Nacional sobre a LGPD, o Termo de Referência para a contratação de Consultoria para realizar avaliação sobre todas as áreas e processos sobre a LGPD. O participante falou ainda da importância da informação e da realização de *workshops* com as áreas administrativas, comercial, financeiras, recursos humanos, jurídico, TI, *marketing*, restaurantes, escolas, Faculdades e EAD do SENAC, aplicando a abrangência da Lei em seus processos e porque é necessário um controle efetivo e eficiente sobre os dados. Sobre o Escritório de Proteção de Dados, ou DPO – *Data Protection Officer* – é o profissional que será o encarregado de cuidar das questões referentes à proteção dos dados da organização, o participante esclareceu que se trata de um Comitê Multidisciplinar, cujas decisões são tomadas em conjunto. Observou também a necessidade de identificar quais processos tratam de dados pessoais e criação de *ranking* por ordem de criticidade, de prioridade e de riscos, bem como a importância de um inventário, visando à identificação de quais são e como estão sendo

armazenados os dados pessoais em meios físicos e digitais, além da base legal para obtenção e armazenamento desses dados.

O participante A apontou a indispensabilidade do mapeamento de vulnerabilidades dos processos quanto ao uso dos dados pela organização e citou a necessidade do acompanhamento pelo gestor da área, que estará dando orientações, auxiliando e auditando a etapa de inventário de dados que será realizada com a área de TI, por meio do relatório de impacto da LGPD na organização, através da DPIA - *Data Protect Impact Assessment* - metodologia adotada pela legislação europeia de proteção de dados pessoais, que consiste na execução de uma avaliação de impacto da proteção dos dados pessoais. Já na LGPD, a metodologia tem o nome de Relatório de Impacto de Proteção de Dados (RIPD), que alertando para o fato que nem todos os controles precisam ser aplicados em decorrência dos altos custos envolvidos, mas que é imprescindível buscar o sigilo das partes das bases de dados que contêm dados pessoais, envolvendo a criptografia, inclusive, dos dispositivos móveis e em toda comunicação por onde trafegam e onde são armazenados esses dados.

Por fim, o gestor A ressalta que é fundamental garantir o conhecimento dos profissionais de TI sobre a LGPD, acrescentando que as adequações necessárias não devem ser atribuídas apenas aos profissionais de TI, pois a Lei tem muitos pormenores que estão além da tecnologia. O gestor A concluiu considerando que o processo de adequação da LGPD está além da TI.

O gestor B salientou que o compartilhamento de dados e a segurança da informação são pontos de atenção que mais preocupam no desenvolvimento dos sistemas, destacando ser este o principal desafio no desenvolvimento de um sistema *Enterprise Resource Planning* (ERP) para a área educacional da organização, projeto cuja responsabilidade para adequação à Lei está sob sua responsabilidade. Salientou sobre as bases legais que possibilitam o SENAC a realizar suas atividades, no entanto, é importante conscientizar os profissionais de TI para não liberação do tratamento de dados sem verificar a disponibilidade dessas bases. Ao ser questionado sobre o papel profissional de TI, responsável pelo controle dos dados, conforme a definição da LGPD, ele explica que ainda não tem uma definição, mas acredita que o controle será por regional.

O gestor C, explicou que as aplicações de penalidades por parte da ANPD em casos de desrespeito à LGPD podem extrapolar o valor financeiro, considerando que uma sanção aplicada poderia comprometer ou suspender a utilização do banco de dados, colocando em risco, inclusive, as operações da organização. Ele exemplificou que o SENAC, por ter uma base de dados única nos sistemas ERP Financeiro e Educacional, se tiver uma ocorrência junto à ANPD, causada por um incidente em uma regional, pode levar toda a organização a uma sanção

de bloqueio, afetando a organização como um todo. O gestor C destacou o que considera um ponto frágil da LGPD, que é o Termo de Consentimento fornecido pelo titular do dado. O participante observou que o titular dos dados tem o direito de revogar o consentimento a qualquer momento, exigindo um controle maior sobre os dados. Ainda, elucidou a necessidade de cláusulas claras nos contratos quanto ao tratamento dos dados com os fornecedores, incluindo deveres e responsabilidade de todas as partes com relação aos requisitos da LGPD, enfatizando a necessidade de registrar os critérios e os procedimentos adotados quanto ao tratamento dos dados nos casos de incidentes, incluindo os de mitigação e comunicação à ANPD. A importância do conhecimento dos profissionais de TI quanto à Lei foi também abordada pelo gestor. No entanto, o gestor ressalta a necessidade de dedicação ao entendimento da Lei, pois tem muitas lacunas ainda a serem estudadas.

O gestor D, relata que o processo de conscientização e aplicação de medidas que regulem as diretrizes da LGPD na organização é fundamental para que as demais etapas da adequação da Lei ocorram com êxito. Confirmou que os resultados obtidos no regional, atualmente, refletem a eficiência e a eficácia dessas medidas educacionais. Ressalta a importante da fala do gestor A quanto ao comitê multidisciplinar para o tratamento das questões diretas e indiretas que envolvam a LGPD. O gestor D dá ênfase ao estudo da Lei, pois ela poderá reverberar por todas as áreas da organização, afirmando que "... a mudança da cultura organizacional só é obtida com esclarecimentos que geram a consciência dos fatos...".

O gestor E, confirmou que os resultados refletem o cenário atual quanto à compreensão que os profissionais de TI da organização têm a respeito da LGPD, além de corroborar com os demais gestores quanto à compreensão de que o desafio da conformidade com a Lei não está com a TI e, sim, com o processo de conscientização organizacional. O gestor destaca que existe um processo de contratação de uma empresa de consultoria para avaliar os processos das áreas administrativa, financeira, RH, TI, jurídico, *marketing*, educacionais e seus processos organizacionais. Só após esta fase, iniciarão as adequações da LGPD, como também, os ajustes necessários à gestão da PSI, aos regulamentos, às políticas e aos controles administrativos. Ressalta que os resultados da pesquisa expressam e evidenciam os pontos de atenção que a gestão da segurança da informação vem apresentado nas pesquisas nacionais.

As considerações do gestor F relatam que os pontos apresentados na pesquisa refletem o momento de inovação e adequação que os regionais estão vivenciando, e que a LGPD só reforma a necessidade de ampliarmos as tratativas que reforçam a melhoria contínua da governança de TI. Corrobora com as preoculpações do gestor C quanto à exposição dos dados

pessoais e aos danos que podem ser gerados pela não adequação à Lei, pois a pesquiva evidencia a fragilidade na percepção dos profissionais quanto ao tema. Destaca que, o fato capacitação e divulgação são essenciais para o processo de adequação e transformação que a Lei trará para todos os profissionais que estiverem envolvidos, como também, lembra que não é só TI. Destacou a importancia da pesquisa e que esta deveria ser apresentada no comitê nacional, como também prover um trabalho com todos os Regionais, parabeniza a pesquisa e o trabalho.

Por fim, o gestor G, argumenta sobre a importância de garantir segurança administrativa e jurídica para as organizações no contexto da LGPD. O participante concordou com todas as observações feitas pelos outros participantes e acrescentou que a Regional onde trabalha também instituiu um conselho e um comitê multidisciplinar de segurança da informação. O comitê é presidido pelo gestor responsável pelo escritório de proteção de dados e é regulamentado por um regimento próprio. Para tratar da LGPD, foram criados oito grupos de trabalho, que atuam no mapeamento de processos, gestão de riscos, gestão de acessos, políticas de privacidade, gestão de contratos, além da criação de regulamentos internos como normas e procedimentos, códigos de éticas para colaboradores, alunos e fornecedores em consonância com os outros participantes. Esse gestor destaca que todos precisam conhecer a LGPD, destacando o papel das pessoas, bem como da tecnologia e da conformidade com a Lei.

Os demais participantes, enviaram comentários por texto, ressaltando a importância das discussões e dos resultados da *Survey.*

5.6 ANÁLISE GERAL DOS RESULTADOS

Na utilização das duas metodologias de pesquisa, quantitativa e qualitativa, é essencial a integração dos dados para que o resultado atenda às premissas apreendidas no trabalho. Para tal, o diagrama dessas pesquisas, orientou as coletas, a análise parcial da pesquisa *Survey*, a análise da reunião e a integração dos resultados.

Diante dos dados obtidos tanto na *Survey* quanto no grupo focal, ficou evidente que os princípios para a adequação da LGPD estão sustentados na conformidade com leis e regulamentos, nas pessoas e na aplicação da tecnologia, o que se coaduna com as dimensões teóricas desta pesquisa: formal, informal e técnica. Os dados evidenciam também que o conhecimento dos profissionais de TI quanto aos requisitos da lei é extremamente relevante para que sejam adotados os devidos controles de segurança da informação.

As evidências apuradas nas pesquisas *Survey* e no Grupo Focal apontam que os profissionais de TI do SENAC são experientes, com mais de 20 anos de atuação na área de TI. No entanto, o fato de terem a experiência não evidenciou ser suficiente para determinar o nível de compreensão da LGPD, pois aproximadamente 50% dos profissionais questionados ainda não têm conhecimentos relevantes sobre a Lei. Todavia, a pesquisa destaca que o conhecimento é considerado como crucial para que ocorra o processo de transformação da cultura, ou seja, a adequação da organização, atendendo aos três pilares: Pessoas, Tecnologia e Processos, considerando os critérios da LGPD. Ainda assim, a percepção quanto às necessidades de mudanças na gestão e na Política da Segurança da Informação contrapõem-se.

O impacto na Política de Segurança da Informação para o SENAC foi considerado como alto, pois 50% entendem que as políticas não estão adequadas, enquanto outros 41% entendem que as diretrizes da política são insuficientes. Ao mesmo tempo, os impactos para a Gestão da Segurança da Informação são evidenciados como baixos, pois 53% entendem que serão brandos os possíveis impactos, e 33% compreendem que os impactos a GSI serão moderados.

Observou-se também a necessidade de implementação de processos mais eficientes quanto aos Controles da Informação no que tange às diretrizes e obrigações da Lei. Este fato é verificado no indicador de percepção quanto à compreensão da LGPD, pois esta requer da gestão de TI do SENAC uma maior atenção para a geração do conhecimento sobre os critérios e diretrizes da Lei. Analistas e Coordenadores de TI evidenciaram, na análise de dispersão, que 50% deles não têm conhecimento necessário sobre as obrigações da Lei. Portanto, os resultados apontam que é primordial a divulgação, a capacitação e o treinamento, como também a adoção de medidas educativas que esclareçam os regulamentos quanto aos impactos da LGPD nos processos do SENAC. Não obstante, os resultados apontam que o maior índice da compreensão sobre a Lei foi identificado entre os ocupantes de cargos de Diretor e Gerente, os quais tiveram maior acesso às ações da LGPD, o que fundamenta a assertiva de que quanto maior o acesso à informação, melhores são as tomadas de decisões.

Nota-se nas apurações dos indicadores para a Gestão da Segurança da Informação que as adequações do SENAC à Lei 13.709/2018 foram consideradas vitais para melhorar o controle e a gestão dos dados, por 92% dos profissionais de TI. Acrescenta-se a isso que 63% entendem que as medidas de controles para a Segurança da Informação, para os acessos aos dados, para a política de *backup*, para a gestão dos riscos e para o contingenciamento nas vulnerabilidades sobre os dados pessoais e os dados pessoais sensíveis na Gestão da Segurança da Informação devem ser considerados, pois ainda são pouco observados na governança. Sustenta-se a

afirmativa que 54% dos participantes reconhecem que o Controle da Informação do SENAC, para atender à LGPD, é um ponto de atenção, apesar das medidas atuais em investimentos técnicos, tecnológicos e em recursos humanos. Buscando a eficiência da GSI do SENAC, 74% dos profissionais de TI consideram a necessidade de ampliação da infraestrutura para atender a contingência da segurança, a segregação das bases de dados – processos para atender o direito do "livre acesso aos dados do titular" - e os ajustes em todas as políticas, regimentos, normas e procedimentos.

Desta forma, constata-se nas pesquisas que é essencial que os profissionais de TI tenham compreensão sobre o processo de adequação à LGPD na Gestão de TI e na atribuição de responsabilidades, bem como sobre as sanções previstas na Lei. Essa importância foi observada sobre as três dimensões de análise: técnica, formal e informal. Os resultados corroboram com a premissa de que essa compreensão determina a eficiência na aplicação de tecnologias e a adoção de outras práticas de proteção de dados e serviços críticos da TI, o que determina a alta disponibilidade de sistemas e a confiabilidade sobre as informações. Com isso, fica clara a relação entre essa compreensão dos profissionais de TI e a adoção de controles técnicos de Segurança da Informação.

Observou-se também que ações de divulgação, comunicação, informação e capacitação de todos os usuários de TI da organização são fundamentais para mitigar os riscos e reduzir os impactos e vulnerabilidades às quais os dados podem estar sujeitos, aumentando a eficiência dos controles para a gestão da Segurança da Informação, através de mudanças de comportamentos dos indivíduos.

Desta forma, os controles informais são positivos para a aplicação de políticas, de normas, de procedimentos, entre outras medidas, além de fomentar a utilização de recursos de TI de forma coerente com a LGPD, facilitando para a gestão de segurança da informação no SENAC, como também, este conhecimento por todas as áreas está auxiliando diretamente a eficiência e a eficácia no processo de adequação à Lei, considerando a atuação interdisciplinar. Os colaboradores do SENAC compreendem indispensáveis as mudanças nos processos relacionadas à gestão de pessoas quanto a sensibilização e conscientização dos dados pessoais, pois são eles que estão em contato com todas as informações do SENAC diariamente, orientando e disciplinando os Colaboradores, os Clientes, os Alunos, os Responsáveis, os Parceiros e os Fornecedores

No entanto, o resultado evidencia a necessidades de ajustes que vão além, alcançando, inclusive, o aprimoramento na Gestão da Segurança da Informação, envolvendo políticas,

processos, procedimentos e regulamentos de novos controles técnicos e a ampliação de ações para mudar o comportamento dos indivíduos, para garantir o controle dos titulares sobre seus dados, a privacidade, o monitoramento e a rastreabilidade sobre o que é feito com os dados pessoais.

Enfim, os conhecimentos dos profissionais de TI sobre a legislação e sobre as necessidades técnicas, normativas e de fomento a comportamentos coerentes vão auxiliar na adequação à LGPD no SENAC.

6 DISCUSSÃO DOS PRESSUPOSTOS DA PESQUISA

A Lei 13.709/2018 traz princípios e diretrizes que visam assegurar às pessoas o direito à privacidade e ao controle do uso dos seus dados pessoais, prevendo consequências para as organizações que descumprirem suas exigências, além dos eventuais danos à reputação da organização. Por este motivo, as organizações não podem subestimar ou negligenciar quanto ao requisito do conhecimento da LGPD pelos profissionais de TI, através de ações de conscientização, de treinamentos e nas reformulações dos procedimentos, das políticas, das normas e das orientações (FONTES, 2016). A lei define claramente os papéis e as responsabilidades desses profissionais e o desconhecimento dela poderá gerar sanções. Cabe ressaltar que a preocupação quanto a relevância do conhecimento e da responsabilidade dos dados pelos profissionais de TI na premissa da Segurança da Informação são abordadas na literatura anterior à LGPD (MOREIRA, 2001), os quais demonstraram argumentações a favor dos investimentos que não se limitam às questões tecnológicas, mas também aos processos organizacionais (PFLEEGER, 1997).

As pesquisas comprovaram que os profissionais de TI percebem a importância da compreensão da Lei, e como a ausência do "conhecimento" poderá impactar nos controles da Segurança da Informação, sendo eles técnicos, formais e/ou informais. O desconhecimento das diretrizes e regras essenciais à adequação da Lei afetará os controles da organização (BJÖRCK, 2005; YEH; CHANG, 2007; SÊMOLA, 2014), o que impossibilitará a conformidade aos requisitos da LGPD.

No contexto da dimensão técnica, para atender aos pilares de Integridade e de Disponibilidade, deverão ser definidas medidas de reforço à infraestrutura, implantando soluções sistêmicas para a proteção dos dados, tais como: implantar instalar sistemas de verificação para detectar alterações nos dados que possam acontecer na rede ou por conta de eventos não ocasionados por interação humana (falhas em equipamentos, pulso eletromagnético etc.); aplicar o código *checksum*[4]; recuperar *backup*, entre outras medidas. Para garantir a eficiência da infraestrutura deve-se criar processos de manutenção ágeis para os *hardwares* e os *softwares*; avaliar as compatibilidades sistêmicas para eliminar os possíveis conflitos tecnológicos; aplicar o processo de uma infraestrutura tecnológica voltada à manutenção e preservação, adotando medidas de: sistema de backup com remoto ou na nuvem; atualizações

[3] *Checksum em inglês* quer dizer checar a integridade de dados enviados por canais com ruídos ou armazenados em diferentes meios por determinado período

periódicas; uso de comunicação compatível com redundância para evitar quedas constantes na conexão; plano de Recuperação de Desastres (RD) que contenha procedimentos e diretrizes para se administrar crises, catástrofes naturais (enchentes, desmoronamentos de terra etc.) e eventos que possam prejudicar os equipamentos (incêndios, blecautes, entre outros). Pressupõe-se que ao adotar as medidas de contingência na infraestrutura aumenta o grau de Confidencialidade.

Nesta perspectiva, notou-se que os controles aplicados no SENAC garantem o ciclo de vida da informação (criar, coletar, guardar, processar, distribuir, usar, descartar e reciclar) na transmissão, no processamento e no armazenamento dos dados de forma segura. Para tanto, os controles deverão atender aos princípios da Segurança da Informação para a LGPD (FLORIDI, 2010), fato evidenciado na pesquisa com 99% dos participantes que afirmam o processo de atualização na infraestrutura, sendo que 60% apontam que estão atendendo às normas de segurança, e 39% reconhecem que estão na fase final de atualização para atender às normas ISO 27001/27002 e a LGPD. Não obstante, 1% indica não ter realizado nenhuma medida de atualização para a infraestrutura. Colaborando com esta abordagem, os participantes do Grupo Focal citaram que o SENAC tem como diferencial a aplicação de medidas técnicas para as atualizações sistêmicas (segregação da base de dados, redundância dos equipamentos, soluções de criptografias e contingência na nuvem) que são ações estratégicas.

Na dimensão formal, que é estar em conformidade com a Lei, deve-se empregar medidas de atualizações, correções, ajuste e exclusões de diretrizes internas e externas que validem as políticas, as normas, os regulamentos, os planos, os procedimentos e os processos organizacionais para que eles estejam de acordo com as leis. Oliveira (2019) destaca a necessidade de atender aos procedimentos legais para a LGPD.

Neste sentido, observou-se apenas a conformidade no que se refere aos critérios legais quanto à adequação para a LGPD, pois o SENAC é uma das entidades do sistema "S" que está sujeita ao controle externo exercido pelo TCU, pelo Ministério Público, pela estrutura do Poder Executivo e pela CGU, ou seja, constata-se a tutela administrativa, que é o poder conferido ao Chefe do Poder Executivo e aos Ministros de Estado de fiscalizar as entidades, sem substituir a gestão interna nem impor decisões hierárquicas, mas sim com o propósito de assegurar a sua própria autonomia. De acordo com o art. 74 da Constituição Federal que prevê a participação colaborativa entre as esferas de poder, atuando de forma sistêmica, com intuito de fiscalizar a eficácia e a eficiência da gestão orçamentária, financeira e patrimonial e apoiar o exercício do controle externo.

Nota-se que o controle interno passa pela fiscalização exercida pelo Conselho Nacional (CN) e pela Comissão de Contas (CC) na elaboração dos orçamentos anuais e culmina nas estruturas internas de comitês de ética, de gerências de governança, de *compliance* e de ouvidorias. Melhor dizendo, há estruturas estabelecidas em Códigos de Ética e em Regulamentos, constituídas por auditorias, órgãos de governança corporativa, corregedorias, ouvidorias, conselhos fiscais e auditorias externas.

Sendo assim, é mais do que evidente que o SENAC está com 100% dos seus controles legais atendidos. Todavia, quando se apura os requisitos de conformidade à dimensão formal, percebeu-se que as adequações ainda estavam em andamento, conforme indicado pelos participantes, em que 53% indicam que os ajustes aos controles internos relacionados a LGPD estão baixos. No entanto, 47% indicam que os controles internos para a adequação da LGPD estão atrasados, sendo: 33% em fase de consolidação e 14% estão plenamente concluídos, segundo a NBR ISO 27003:13. Nesta perspectiva, os participantes do Grupo Focal confirmam a integridade e o compromisso que o SENAC tem quanto aos cumprimentos internos e externos para estar em conformidade as leis.

Para a dimensão informal constata-se o comprometimento em proporcionar oportunidades de formação a todos os Colaboradores, possibilitar o entendimento e o conhecimento sobre a percepção que se deseja. Segundo Albuquerque Junior; Santos (2015), há uma necessidade de realizar ações de treinamento, de divulgação e de conscientização quando existe a necessidade de realizar mudanças nas estruturas e nos processos organizacionais. Para este fim, é necessário treinamento sistemático em todos os níveis, criar campanhas e políticas de divulgação, em que deverá considerar-se todas as medidas adotadas nas dimensões técnicas e formal, para que os Colaboradores tenham o entendimento, a compreensão e a aplicação das ações quanto às mudanças nas estruturas e nos processos organizacionais.

Quanto à aplicabilidade das medidas informais, verificou-se que 59% dos participantes consideraram que as iniciativas de divulgação, de treinamento e de capacitação foram muito eficazes. Entretanto, 38% determinaram que as ações adotadas foram razoáveis, enquanto 3% afirmaram que não participaram de nenhuma programação sobre os temas. Na concepção do Grupo Focal, o SENAC vem investindo em ações educacionais como Programa de Transparência e Unicidade SENAC com trilhas informativas sobre a Lei Geral de Proteção de Dados, com cursos técnicos, publicação e divulgação de cartilhas, investimento em consultoria que auxilie na adequação da Lei entre outras. Deste modo, acredita-se que as medidas

necessárias às adequações da LGPD estão sendo realizadas, contudo, entende-se que muitos profissionais de TI, por ter um caráter predominante técnico, ficam à margem de algumas mudanças.

No 1º pressuposto, procurou-se evidenciar se os profissionais de TI compreendem as necessidades de realizar adequações na tecnologia, visando à conformidade aos requisitos da LGPD quanto à segurança da informação. Para tal, a adequação à LGPD na organização impõe obrigações que estabelecem como objetivo a maior transparência no tratamento e no processamento dos dados pessoais e nos dados pessoais sensíveis, concomitantemente, com o consentimento do titular. Assim, o profissional de TI deverá ter o conhecimento quanto aos requisitos da Lei para realizar as adequações na tecnologia, considerando a segurança da informação. Neste contexto, o profissional deverá ter experiência em leis e práticas de proteção de dados, além do entendimento completo da infraestrutura de TI, do uso da tecnologia, da estrutura técnica e organizacional, a fim de adotar medidas de segurança para proteger os dados, na coleta, no armazenamento, no tratamento e descartados, seguindo o clico de vida dos dados para LGPD, considerando a metodologia *Privacy by Design*.[5]

O Processo de controle à Segurança da Informação envolverá atuação de profissionais de TI, como também, aplicará os critérios legais, os controles internos e externos, através de normas e procedimentos para o tratamento de dados pessoais, possibilitando que a legislação seja cumprida em todos os seus artigos para estar em conformidade. Este processo fomenta a criação da cultura de proteção de dados, por meio de palestra, de *workshop*, de treinamentos e de campanha de divulgação, ou seja, de aplicação de ação de conscientização organizacional. Portanto, na percepção do profissional de TI, será necessário se especializar para entender todos os pontos da legislação. Por outro lado, o desconhecimento das diretrizes e regras essenciais à adequação da Lei afetará os controles da organização (BJÖRCK, 2005; YEH; CHANG, 2007; SÊMOLA, 2014) que impossibilitarão a conformidade aos requisitos da LGPD.

Neste sentido, o profissional de TI deverá compreender as necessidades de realizar adequações na tecnologia, visando à conformidade aos requisitos da LGPD quanto à segurança da informação, exercendo os dois papéis: o primeiro de implementar os requisitos técnicos e tecnológicos para adequar-se aos artigos da Lei que possibilitam o acesso aos dados pessoais a qualquer momento, a execução dos dados e a transparência dos dados para outras Organizações;

[4] *Privacy by Design* é uma expressão em inglês que significa a obrigação de incorporar a privacidade e a proteção de dados pessoais no desenvolvimento de produtos, de serviços, de projetos, de processos, de práticas, de tecnologias e de infraestruturas em todos os projetos organizacionais.

o segundo papel estará relacionado com o profissional que deverá ampliar seus conhecimentos sobre a LGPD, no intuito de reforçar e ampliar as medidas e barreiras que possam mitigar os impactos de vulnerabilidades na Segurança da Informação nas Organizações.

No 2º pressuposto, considerou-se se que os profissionais de TI compreendem os impactos e as mudanças na gestão TI para atender às necessidades de proteção de dados pessoais segundo as diretrizes da LGPD nas organizações. Nesta premissa, é necessário avaliar os impactos oriundos da adequação da LGPD, são os principais desafios que os gestores e os profissionais de TI deverão superar independente de suas percepções, que poderão ocorrer se as medidas essenciais não forem observadas: na infraestrutura, nas técnicas e tecnológicas (nas padronizações e governança da tecnologia da informação), na implementação sistêmica para o controle da informação (sigilo e o livre acesso), nas dificuldades de integrações sistêmicas, na interoperabilidade dos dados e das informações que impactam em investimentos e orçamento da organização. Neste contexto, observou-se na análise de dispersão da pesquisa que o Analista tem maior percepção quanto à aplicação das medidas de Segurança da Informação atribuídas ao Controle da Informação (políticas, normas, regras, procedimentos entre outras na formatação dos regimentos aos controles de acesso às informações, o que proporciona as diretrizes quanto ao uso dos dados) que poderá refletir na redução dos impactos aos acessos indevidos. Somando a esta percepção, o Analista tem pouca atuação nos processos de políticas, normas, regulamentos, procedimentos entre outras diretrizes legais; no entanto, os gestores apresentam uma regularidade na percepção sobre os regimentos e normas da Lei.

Em síntese, os gestores demonstraram maior entendimento quanto aos impactos e às oportunidades, considerando as medidas adotadas para mitigar os desafios que a Lei poderá incidir nas operações organizacionais, que foram evidenciados na pesquisa e aludidos no Grupo Focal. Todavia, os Analistas apresentaram uma maior percepção no que se refere aos impactos e às oportunidades quanto às diretrizes definidas para as implementações técnicas e tecnológicas.

Enfim, os gestores apresentam a maior dispersão quanto aos impactos e às oportunidades sobre as medidas adotadas para os treinamentos, a divulgação, a comunicação e a conscientização organizacional; no entanto, os Analistas indicaram o menor entendimento quanto às ações adotadas para comunicar os impactos e as oportunidades da Lei.

As adequações sistêmicas são essenciais para atender a proteção dos dados e, segundo Machado (2014, p. 23) “[...] a segurança da informação é uma maneira de proteger os sistemas de informação e a sociedade contra diversos ataques, mantendo documentos e arquivos dentro

dos princípios de confidencialidade, integridade e disponibilidade". Portanto, as organizações não podem negligenciar com as operações que envolvam os dados e ou informações de pessoas que estão sobre sua guarda e responsabilidade, segundo Moreira, (2001).

Neste sentido, o profissional de TI deverá compreender os impactos e as mudanças que a adequação da lei fará recair sobre a gestão de TI, e atender as diretrizes de proteção de dados pessoais e dados pessoais sensíveis, tendo em vista a conformidade aos requisitos da LGPD. Colaborando, Jimene (2020) diz que os profissionais de TI das organizações devem utilizar de medidas técnicas, tecnológicas e administrativas que possibilitem a proteção de dados pessoais de acessos, para evitar incidentes e o uso ilícito das informações. Fontes (2006) e Sêmola (2014) destacam a importância da compreensão e da responsabilidade do profissional de TI quanto à segurança da informação.

No 3º pressuposto, percebe-se que os profissionais de TI conhecem as implicações da LGPD sobre os papéis e responsabilidades da área de TI e dos usuários com relação à proteção de dados pessoais. Para avaliar a percepção da responsabilidade e em que papel está inserido o profissional de TI, é necessário atender as obrigações, de transparência no tratamento e no processamento dos dados, e, consequentemente, reduzir os impactos oriundos da adequação da LGPD na organização. É indispensável a realização de ações, de campanhas e de programas de conscientização, de educação e de treinamentos, através de divulgações, de informativos, de comunicações, de cursos e de capacitações técnicas para o êxito das medidas adotadas para atender às dimensões formais e técnicas, empregando medidas de controles para a Segurança da Informação, atendendo especificamente o princípio da responsabilidade e da prestação de contas. Contudo, a percepção dos papeis e responsabilidade só poderão ser entendidos mediante ao pressuposto da mudança organizacional em relação a proteção dos dados, que poderá refletir na conscientização e na sensibilidade no tratado das informações.

Neste contexto, a organização deverá estabelecer objetivos claros e transparentes quanto ao tratamento e ao processamento dos dados pessoais e os dados pessoais sensíveis para que os profissionais de TI tenham ciência de suas responsabilidades. Contudo, os usuários têm que ser sensibilizados quanto à proteção dos dados pessoais, por meio de um plano de implementação e divulgação da LGPD.

Por fim, observou-se nas pesquisas que, aproximadamente, 50% dos profissionais questionados ainda não têm conhecimentos relevantes sobre a lei, fato que compromete o processo de transformação da cultura, ou seja, a adequação da organização atendendo aos três pilares: Pessoas, Tecnologia e Processos e considerando os critérios da LGPD. Outro ponto,

que compromete a conscientização é o índice baixo quanto ao entendimento da Lei por 45% dos participantes. Contudo, 59% dos participantes consideraram que as iniciativas de divulgação, de treinamento e de capacitação foram eficazes, contrapondo a 38% que determinaram que os programas adotados foram razoáveis e 3% afirmaram que não tiveram participação em nenhuma ação sobre os temas relacionados à esta legislação. Conclui-se que, as providências adotadas pelo SENAC para impulsionar o processo de conscientização e sensibilização quanto ao tratamento dos dados pessoais e dados pessoais sensíveis estão medianos, o que refletiu nas pesquisas em que a, aproximadamente, 50% dos profissionais de TI não foram oportunizadas ações que colaborassem com a capacitação sobre a LGPD. Segundo Chiles, (2013) as organizações devem proporcionar “treinamentos” para a redução de falhas na utilização de novos processos para uma implantação com melhores resultados, a serem percebidos pelos profissionais de TI.

A repercussão das pesquisas indica que o trabalho é significativo, pois a conformidade com a Lei depende de diferentes aspectos que extrapolam a compreensão do profissional de TI. Nota-se que a conformidade com a Lei envolve, portanto, a compreensão desses profissionais sobre as implicações em todas as dimensões em que elas se apresentam: nas medidas e impactos formais, técnicos e informais.

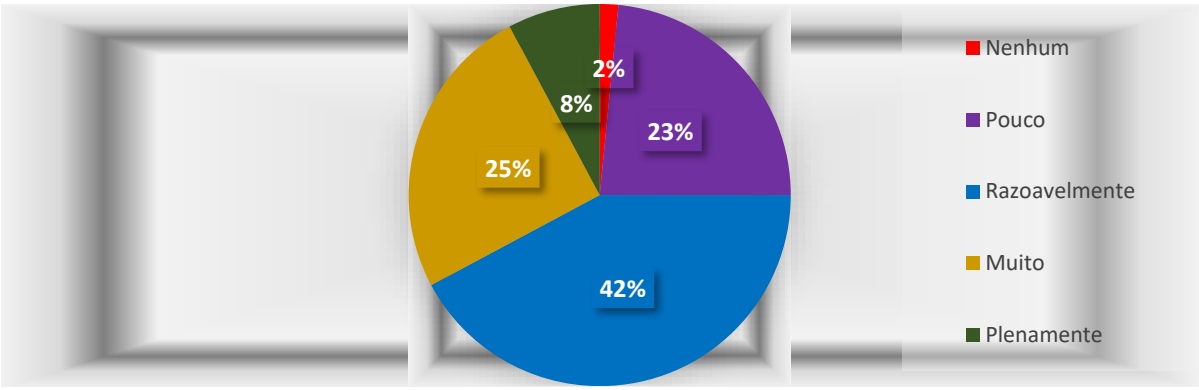
Segundo os resultados obtidos nas pesquisas, considera-se que o profissional de TI do SENAC não tem o entendimento dos desafios quanto à adequação à Lei. No entanto, esses colaboradores sinalizam que as barreiras pela não percepção da Lei estão aquém de processo tecnológicos, elas vão além de aplicação técnica e nas diretrizes organizacional, em que fica evidenciado na pesquisa que 50% dos profissionais de TI não têm o conhecimento sobre a Lei. Os resultados revelaram os pontos de atenção para os controles sobre os dados, para os processos de adequações nas políticas e normas internas e externas, para os procedimentos de controles de eventuais desastres (formal e técnico) e para incentivar as ações de divulgação e capacitação.

Por ser uma Lei, ela é compulsória, pois determina a obrigatoriedade da proteção de dados pessoais e dos dados pessoais sensíveis, com a rastreabilidade quanto ao uso ilegítimo por parte das organizações públicas, privadas e paraestatais. Nota-se que é uma tarefa que impõe desafios, pois observou-se nas pesquisas que o SENAC vem realizando investimentos, atualizações técnicas e tecnológicas, desenvolvendo programas educacionais, e, mesmo assim, os resultados revelam que a organizações não está plenamente adequada para atender os principais artigos da Lei.

Considerando a pesquisa bibliográfica quanto a proteção de dados pessoais e a segurança dos dados nas organizações, notou-se que a compreensão dos profissionais de TI no âmbito da Lei está associada às questões éticas e de responsabilidade ao sigilo, no que se refere às informações sobre sua guarda. Segundo Albuquerque Junior (2015), os comportamentos técnicos costumam manter um foco na adoção de controles de sistemas de informação que implicam em ações e recursos técnicos e físicos, em detrimento de realizar mudanças nas estruturas e processos organizacionais. Fontes (2016) também afirma sobre a responsabilidade ética e a regulamentação dos controles pelos profissionais de TI, reforça a compreensão dos requisitos da LGPD quanto à segurança da informação pelos profissionais de TI.

A pesquisa mostrou que os profissionais de TI compreendem as necessidades de realizar adequações na tecnologia, visando à conformidade aos requisitos da LGPD quanto à segurança da informação. Os dados revelaram que 75% dos participantes compreendem as necessidades de atualizações tecnológicas, sendo que: 42% têm uma compreensão mediana, 25% têm conhecimentos um pouco acima da média e somente 8% têm o pleno conhecimento de como aplicar as medidas para as atualizações técnicas tecnológicas. Contudo, 25% alegam não ter o conhecimento necessário para propor as atualizações tecnológicas para atender as adequações quanto às obrigações técnicas de Segurança da Informação proposta pela Lei, sendo: 23% abaixo da média de compreender de fato as obrigações técnicas e somente 2% indicaram não ter nenhum domínio necessário para atender as recomendações de segurança solicitadas nas diretrizes da Lei, confirme gráfico 10 abaixo.

Gráfico 10 – Adequação Tecnológica para Atender a LGPD

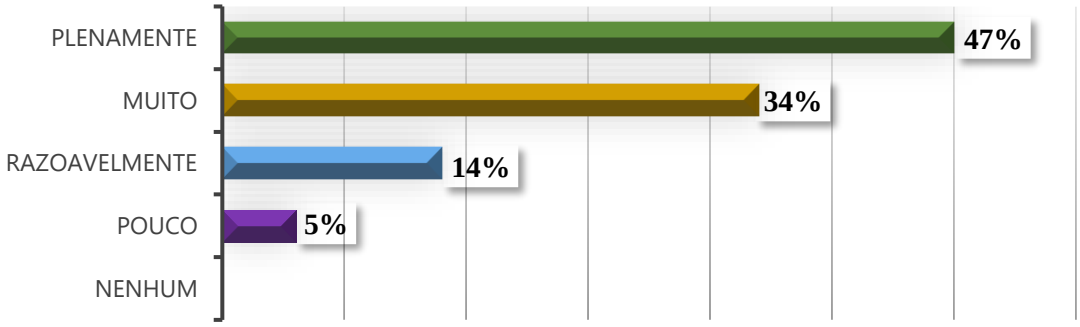


Fonte: Elaborado pela autora (2021)

Na apuração quanto aos impactos e as mudanças na gestão TI para os controles dos dados pessoais, os profissionais de TI do SENAC revelaram que 81% dos participantes compreendem

os impactos e as mudanças que as diretrizes da Lei poderão acarretar à Gestão da TI, sendo 47% que afirmam ter a plena percepção quanto aos impactos da LGPD na governança da TI. Todavia, 34% classificam ter a percepção, contudo, não têm a plena convicção de como poderão ser esses impactos. Porém, 19% classificam os processos de mudança como medianos, sendo que 14% consideram que haverá impactos nas atividades e somente 5% acreditam que não haverá qualquer impacto nas suas atividades diárias, conforme observa-se no gráfico 11.

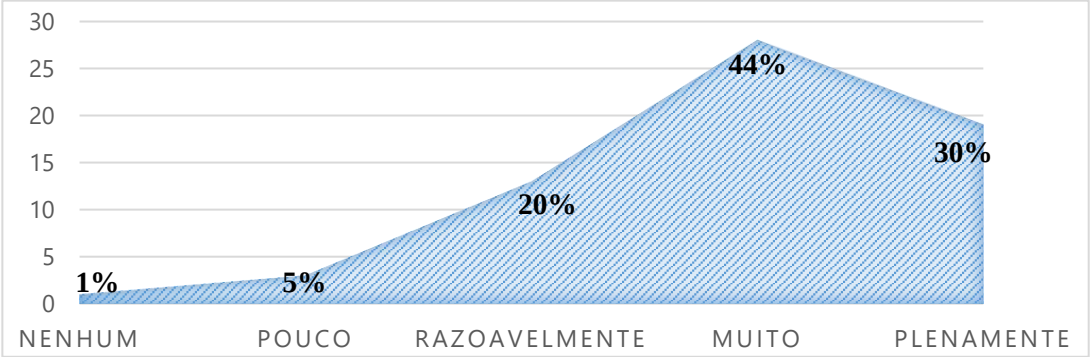
Gráfico 11 – Os Impactos e as Mudanças que LGPD trará para a gestão da TI



Fonte: Elaborado pela autora (2021).

Considerando a abordagem, a responsabilidade que a LGPD poderá propiciar aos profissionais de TI e a compreensão que eles têm nesses aspectos, 74% dos participantes consideram que a Segurança e a Integridade das Informações são de responsabilidade da TI, sendo: 44% deles consideram que os dados estão armazenados nos ambientes computacionais sob a responsabilidade da governança de TI, mas também tem os usuários que são responsáveis pelo seu uso. Assim, 30% atribuem a plena responsabilidade pela integridade dos dados aos profissionais de TI. No sentido inverso, 26% julgam não ser total a responsabilidade da segurança dos dados dos profissionais em questão, sendo: 20% consideram que a responsabilidade pela segurança da informação é 50% do profissional de TI e 50% do usuário. Outros profissionais acreditam que a maior reponsabilidade pela segurança dos dados é do usuário e somente 1% considera que o profissional de TI não tem responsabilidade com a segurança dos dados, conforme nos aponta o gráfico 12.

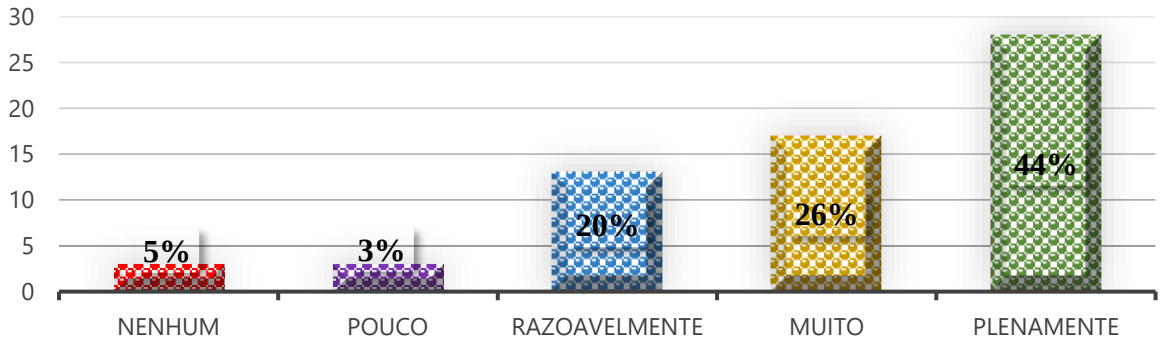
Gráfico 12 – Responsabilidade dos profissionais de TI quanto a Segurança da Informação



Fonte: Elaborado pela autora (2021)

No contexto oportunidade, que a LGPD poderá propiciar aos profissionais de TI, 70% desses profissionais percebem a possibilidade de oportunidades que a adequação poderá proporcionar, sendo: 44% têm a plena convicção nas oportunidades que serão geradas, 25% acreditam que poderão ter oportunidades aceitáveis para os profissionais da área. Contudo, 30% aceitam uma possível oportunidade quanto ao crescimento profissional para os profissionais da TI, sendo: 20% percebem a possível mudança e oportunidade oriundas das adequações da Lei. 5% acreditam que as oportunidades serão imperceptíveis e 5% acreditam não ter nenhuma oportunidade para área de TI, como nos mostra o gráfico 13.

Gráfico 13 – As oportunidades que a LGPD poderá trazer ao Profissional de TI



Fonte: Elaborado pela autora (2021)

Ainda assim, a pesquisa releva que a compreensão do profissional de TI é imprescindível no processo de adequação à Lei na organização, não somente por esta premissa, mas porque os profissionais de TI podem ser a base de mudança que estará gerindo o objetivo central da Lei que é a gestão do tratamento dos dados pessoais, a integridade e as responsabilidades, as quais

incidem diretamente sobre a Gestão da Segurança da Informação, e, consequentemente, sobre a prestação de contas aos ciclo de vida da informação na organização.

Os resultados apontam que a compreensão dos profissionais de TI é relevante, mas o conhecimento desses profissionais não garante que o processo de adequação à lei terá sucesso, com o que corrobora Sêmola (2014) que argumenta que a Gestão da Segurança da Informação envolve uma série de medidas que vão além de soluções técnicas ou tecnológicas, alcançando os processos internos das organizações, formação de equipes e comitês organizacionais, treinamento de usuários e profissionais de TI, ações de divulgação e conscientização e mudanças de comportamentos dos indivíduos, além da conformidade com requisitos legais. No âmbito das competências, os profissionais de TI (gestores, administradores, controladores, analistas e operadores) das organizações deverão observar o tratamento correto para os dados pessoais, aplicando as boas práticas, estabelecendo critérios e condições organizacionais, que envolvem normas, padrões técnicos, política de segurança da informação, procedimentos e processos.

Todavia, a análise dos dados destacou a necessidade de ações de conscientização a respeito da LGPD mais oportunas para os profissionais de TI (Coordenadores e Analistas) do SENAC, de modo que os controles e as medidas de proteção à privacidade dos dados sejam estáveis na organização, consoante Doneda (2020). Pois, o conhecimento, por sua vez, é “um conjunto de declarações organizadas sobre fatos e ideias, apresentando um julgamento ponderado ou resultado experimental que é transmitido a outros por intermédio de algum meio de comunicação” (Castells, 2016). Deste modo, a pesquisa evidencia que o “conhecimento” é um pilar fundamental para na gestão da Segurança da Informação e está dependerá basicamente da capacitação e do entendimento dos profissionais.

7 CONSIDERAÇÕES FINAIS

Nos últimos anos, as organizações vêm investindo estrategicamente em operações inovadoras para produtos e serviços que atendam ao mercado digital, as quais são normalmente respaldadas por recursos tecnológicos sofisticados, por vezes voltados para transações digitais que facilitam a manipulação de dados pessoais, possibilitando interconexões entre diferentes bases de dados. Essas operações podem ser caracterizadas como transações abusivas, bem como expor dados pessoais de forma não autorizada, tanto de modo acidental quanto intencional.

Como consequência, o presente trabalho foi norteado pela temática da Segurança da Informação para analisar a proteção de dados dos indivíduos, tendo como contexto as leis voltadas para essa finalidade ao redor do mundo. A evolução tecnológica possibilita a disseminação e a exposição dos dados pessoais, os quais proporcionam a vulnerabilidade e a fragilidade na privacidade do indivíduo. Diante disso, regulamentar a proteção aos dados pessoais ganhou importância, posto que as informações – e os dados pessoais incluídos – são considerados ativos de valor econômico.

Ainda que tardia, a Lei brasileira insere o País junto aos que já contam com leis que protegem a privacidade dos seus cidadãos. Isso traz possibilidades que extrapolam a preocupação com a segurança da informação, posto que abre o leque de possibilidades de realização de transações comerciais com países que já contam com suas leis de proteção de dados pessoais.

Na perspectiva do cidadão brasileiro, é vital que o Estado, as organizações e toda a sociedade civil estejam cientes de seus direitos e obrigações no que tange à aplicação da LGPD.

Este estudo procurou contribuir, indagando se a compreensão dos profissionais de TI sobre as diretrizes da LGPD poderá facilitar a adequação de organizações paraestatais aos seus requisitos, buscando identificar como a Lei poderá impactar no SENAC. Além de uma pesquisa bibliográfica, este trabalho buscou evidências através da realização de uma *Survey web* e de um Grupo Focal com profissionais e gestores de TI da organização.

O trabalho evidenciou a importância da informação, a necessidade de uma lei para assegurar o direito à privacidade dos titulares dos dados pessoais, a definição dos papéis e a responsabilidade do corpo gerencial das organizações e dos profissionais de TI. Além disso, analisou-se os impactos e as oportunidade que a LGPD impõe à gestão da segurança da

informação e como o profissional de TI compreende este cenário e se esta compreensão facilita a adequação à Lei na Organização.

O tema foi tratado sobre três dimensões: Formal que compreende os controles e ações relacionados à Política de Segurança da Informação, comitês, regulamentos internos e externos, processos e procedimentos organizacionais, e processos de análise e avaliação de riscos; Técnica que são as medidas de prevenção, controles, contingências e redundâncias implementadas através de soluções tecnológicas; e Informal, que são as ações de conscientização, divulgações, comunicação, informação, treinamentos e capacitação técnica, voltadas para mudar o comportamento dos indivíduos.

A fundamentação teórica permitiu a construção de um modelo de pesquisa que considerou as adequações na estrutura técnica e tecnológica, nos processos organizacionais quanto às políticas, às medidas internas e externas para a segurança da informação, além da política de conduta que molda o comportamento ético das pessoas que lidam com dados pessoais. Neste sentido, o profissional de TI deverá entender a Lei e seus desafios nas dimensões quanto às diretrizes da segurança da informação e à responsabilidade no tratamento dos dados. Considera-se o valor da informação, o direto a privacidade, o que são os dados pessoais e sensíveis, a segurança da informação sobre o controle das informações, os mecanismos de controles para esses dados, que normatizações foram sancionais ao redor do mundo e como ela está no Brasil, justificada pela gestão da segurança da informação que está em um dos pilares que amparam a LGPD – *Compliance*, Pessoas e Tecnologia.

Os resultados evidenciaram que os Profissionais de TI do SENAC têm a percepção e a compreensão quanto à necessidade de implementações técnicas e tecnológicas, assim como nas diretrizes organizacionais que vão nortear a adequação da Lei. Nota-se que 81% dos participantes indicaram ter noção quanto aos desafios e riscos que a LGPD trará para a gestão da segurança da informação em todas as dimensões. Dessa forma, 75% revelaram compreender as obrigações fundamentais nas implantações sistêmicas, sejam técnicas e ou tecnológicas, para a adequação da Lei. Entre eles 74% atribuem que a responsabilidade quanto a Integridade, a Conformidade e a Disponibilidade são atribuições da TI sobre a gestão da segurança da informação, ressaltando, assim, a responsabilidade pelo tratamento dos dados. Para 70% desses profissionais, a LGPD poderá oportunizar novas experiências. No entanto, 56% registram ter participado de ações de conscientização e treinamento sobre a lei.

Sobre a abordagem dos líderes de TI que participaram da pesquisa, eles classificaram a adequação à lei como um desafio diretamente ligado a seus ativos, e os maiores riscos

identificados estão diretamente vinculados ao controle sistêmico dos dados, o que visa tornar possível implementações e/ou mecanismos que disponibilizem o acesso a qualquer momento, assim como a exclusão dos dados dos titulares. Este fato requer ajustes técnicos e tecnológicos aos mecanismos de segurança para minimizar os incidentes, em que as observações de alerta para a Gestão de Segurança da Informação foram destacadas e percebidas por todos os gestores.

A pesquisa permitiu constatar que os gestores consideram indispensáveis as mudanças nos processos relacionadas à gestão de pessoas quanto à sensibilização e à conscientização dos dados pessoais, pois são eles que estão em contato com todas as informações do SENAC diariamente, orientando e disciplinando os Colaboradores, os Clientes, os Alunos, os Responsáveis, os Parceiros e os Fornecedores.

Apesar do SENAC possuir amplamente seus controles, suas normas, suas políticas, seus comitês, seus regulamentos entre outros, as medidas de conscientização são cruciais para que o conceito de privacidade seja adotado em toda a cadeia organizacional, além de considerar importante a implementação das ferramentas e dos mecanismos de segurança da informação para proteger contra as ameaças e as vulnerabilidades que os ativos possuem. Segundo Fontes (2011), o processo de Segurança da Informação é um ativo que, por vezes, tornou-se difícil de mensurar do ponto de vista financeiro. Ou seja, o intangível só se torna visível para aqueles que o entendem como essencial para a continuidade da organização.

Todavia, observa-se que o indicador da política de segurança da informação apresentou resultados insuficientes quanto os controles da PSI para as diretrizes e obrigações da LGPD, pois indicaram a necessidade de ajuste e melhorias. Entretanto, avaliaram a gestão PSI atual como eficiente. Contudo, quanto à compreensão das diretrizes e obrigações, alguns profissionais de TI consideram que estão pouco fundamentados. Por isso, faz-se necessária a realização de ações que aumentem a divulgação, a capacitação e os treinamentos, como também, a aplicação de medidas educativas que esclareçam as regras e os possíveis impactos da LGPD na organização. Ainda assim, cabe ressaltar que os participantes não fizeram suas afirmações considerando-as como uma verdade absoluta, pois trata-se de uma percepção individual de cada profissional de TI que participou da pesquisa, e que fortaleceu o objetivo do trabalho que foi avaliar exatamente a sua percepção particular quanto adequação da Lei na organização.

Portanto, observa-se que a "compreensão" do profissional de TI é importante no processo de implementação da Lei que tange à Gestão de TI, as Responsabilidades e as sanções da Lei, conforme as três dimensões consideradas: técnico, formal e informal, apresentadas sobre o

modelo de pesquisa, em que os resultados corroboram com a premissa de que a compreensão do profissional de TI determina a relação de eficiência na aplicação de medidas técnicas que possibilitem as melhores práticas no combate às ações críticas da TI, fato que determina a alta disponibilidade sistêmica, e, consequentemente, a confiabilidade quanto aos controles da informação. Contudo, os profissionais de TI destacaram que a adequação à LGPD está além das diretrizes técnicas e tecnológicas, e que o fator crítico de sucesso para a adaptação à Lei está no uso de equipes multidisciplinares, considerando as medidas de tratamentos aos impactos técnicos, formais e informais.

Conclui-se que os profissionais de TI devem aplicar medidas de segurança da informação eficientes e eficazes no controlar dos dados, para minimizar os riscos provenientes de ameaças e vulnerabilidades quanto ao uso dos dados pessoais (sensíveis e ou não) que as novas tecnologias possibilitam. De acordo com a norma ISO/IEC 27002/2013, "a segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware". No entanto, a adequação à Lei 13.709/2018 está além da compreensão do profissional de TI quanto às diretrizes e controles, ela expõe a necessidade de mudança quanto à exposição e a privacidade do indivíduo com relação a suas informações, no direito de estar, e sendo assim, a Tecnologia é apenas um caminho.

Através deste trabalho foi possível considerar como o entendimento do profissional de TI com relação às proposições da Lei 13.709/2018poderiam contribuir com a adequação das diretrizes e dos princípios da LGPD no SENAC, observando o objetivo da Lei que visa assegurar às pessoas o direito à privacidade e ao controle do uso dos seus dados pessoais, prevendo consequências para as organizações que descumprirem suas exigências.

No decorrer do estudo, a abordagem metodológica foi quantitativa e qualitativa, pois tem o propósito de analisar e interpretar dados, observando a opinião dos participantes quanto às implicações da Lei, cujos resultados podem trazer uma contribuição para a academia e para o SENAC.

Depois de coletar os dados através da pesquisa *Survey* e consolidá-los através da análise estatística para realizar a interpretação dos dados e, concomitantemente, obter as considerações dos resultados por meio da pesquisa e do Grupo Focal, foi possível responder à questão de pesquisa: *"Como os profissionais de TI compreendem as implicações da Lei Geral de Proteção de Dados (LGPD) para as organizações quanto à adoção de controles na segurança da informação?"*.

Observou-se, com isso, que a “compreensão” do profissional de TI é importante no processo de implementação da Lei no que tange à Segurança da Informação, às Responsabilidades e às sanções da Lei, conforme as três dimensões consideradas: técnico, formal e informal apresentadas sobre o modelo de pesquisa, em que os resultados corroboram com a premissa de que a compreensão do profissional de TI determina a relação de eficiência e eficácia na aplicação de medidas técnicas que possibilitem as melhores práticas no combate às ações críticas da TI, fato que determina a alta disponibilidade sistêmica e, consequentemente, a confiabilidade quanto aos controles da informação no SENAC.

O trabalho concebe a Segurança da Informação como indispensável nos processos de automação de uma organização, no controle de segurança e nas adequações legais. Para tal, a compreensão do profissional de TI quanto aos desafios que as implementações poderão acarretar para a gestão de TI é tão importante quanto.

7.1 AÇÕES APLICADAS AO SENAC BAHIA

Através deste trabalho está sendo possível implementar ações que auxiliaram na adequação da organização à LGPD, no SENAC Bahia:

- Palestras sobre a LGPD.
- *Workshop* de conscientização.
- Execução de processos de mapeamento de impactos da LGPD.
- Elaboração de *e-Book* composto de três capítulos:
    - Guia da LGPD
    - Consentimento
    - Resumo da ANPD e os Artigos da LGPD
- Na elaboração dos Relatórios:
    - Avaliação de Impactos – DPIA.
    - Registro de Atividade de Processamento.
    - Registro de violação de dados pessoais.
    - Mapa de Risco e Ações de mitigação.

- Definição e ajustes nas Políticas:
    - Política de Privacidade – Interna e Externo (público).
    - Política de Dados Pessoais.
    - Política de Consentimentos.
    - Política da Segurança da Informação.
    - Política – Código de Conduta.
    - Política de Uso a Internet.
    - Política de e-mail.
    - Política de Uso a Equipamentos.
    - Política dos descartes das Informações.
    - Política de Treinamentos e Divulgação para Adequação da Lei.

Com a aplicação do método da pesquisa, foi possível realizar a aplicação prática quanto à compreensão da Lei e a construção do conhecimento obtido através da fundamentação teórica que balizou o trabalho, além de proporcionar uma aplicabilidade com o conhecimento científico. Como também, está possibilitando a disseminação do conhecimento obtido nas pesquisas aplicadas, através de palestras e *workshop* no SENAC Bahia para mais de 750 colaboradores.

Finalizando o trabalho, observa-se que a utilização de uma amostra com apenas um grupo de uma organização gerou uma limitação na análise da pesquisa, considerando, assim, uma abordagem com a compreensão do profissional de TI somente sobre a ótica do SENAC, não tendo o cruzamento com outras organizações, pois pretendia-se aplicar as pesquisas para os profissionais de TI de organizações públicas, privadas e paraestatais. No entanto, foi aplicada apenas para os profissionais de TI do Senac nos 27 Regionais do Brasil (sendo 26 Estados e no Distrito Federal).

A pesquisa estimava realizar:

- Gerar uma matriz de correlação dos resultados sobre a percepção do Profissional de TI das Organizações (Publica, Privada e Parestatal;
- Apresentar um mapa da percepção da Lei por geolocalização;

- Correlacionar os resultados por: Percepção da lei, Região do Brasil e Nível de escolaridade dos participantes.

Ponderando sobre as limitações percebidas durante a construção deste trabalho, conclui-se que se o fator tempo diante do contexto da pandemia ficou inviável aplicá-la segundo o escopo definido inicialmente.

7.2 RECOMENDAÇÕES PARA PESQUISAS FUTURAS

Considera-se a possibilidade de trabalhos futuros, pois outros impactos na gestão corporativa, oriundas da aplicação da Lei nas organizações, não foram tratadas neste trabalho.

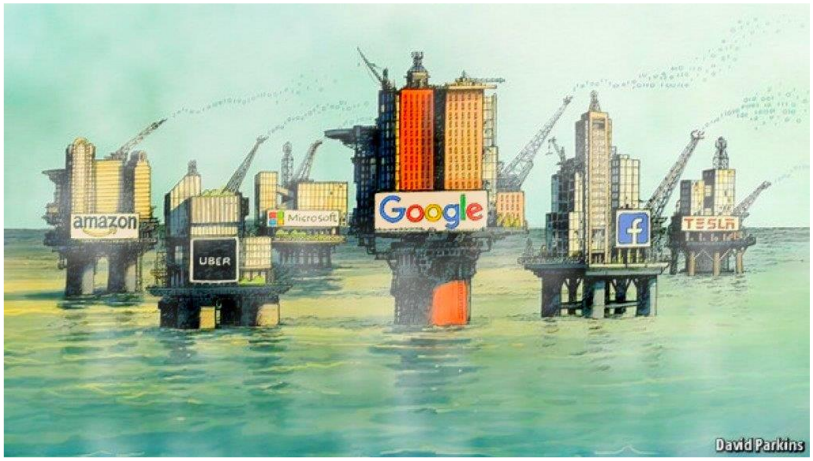
Sugestões de novos trabalhos envolvendo a implementação da LGPD:

- Analisar aplicação de ferramentas adotadas para a adequação da Lei Geral de Proteção.
- Estudo de caso com organizações que tiveram seu negócio transformado pela Lei e os principais impactos deste processo no âmbito da gestão administrativa.
- Aferir os impactos tecnológicos e administrativos na governança da Segurança da Informação.
- Avaliar as possibilidades de reformas acadêmicas quanto a Segurança da Informação, considerando a adequação da Lei 13.709/2018.
- Estudo de caso que considere a transformação do Profissional de TI quanto às responsabilidades técnicas e à gestão administrativa no tocante à privacidade e aos direitos dos titulares de dados.
- Uma abordagem sobre as multiplicidades de papeis e responsabilidades que a LGPD remete: temáticas da Administração, Comunicação e *Marketing*, Econômica, Jurídico, Recursos Humanos e TI.
- Análise das organizações quanto a sua maturidade na aderência à Lei.

Entre outros que possam aprofundar as análises que a vigência da Lei trouxe para as organizações e as mitigações que foram aplicadas no contingenciamento quanto à privacidade das informações pessoais pelas organizações públicas, privadas e paraestatais.

Observando o contexto pesquisado, a gestão de TI é impulsionada pela evolução tecnológica, e o tema sobre a privacidade e os controles na segurança da informação serão constantes, pois as leis sobre o direito à privacidade e a proteção de dados ao redor do mundo encontram-se em desenvolvimento quanto às expectativas dos indivíduos e às necessidades da sociedade cada vez mais digital. Os dados são a nova moeda, mas os profissionais de TI deverão estar atentos às mudanças que este contexto está proporcionando à Tecnologia da Informação nos seus diversos segmentos, o que pode ser observado na Figura 22.

Figura 22 – Ilustração da Informação como fonte de crescimento.



Fonte: *Luís Borges Gouveia*

REFERÊNCIAS

ABRAHÃO, M. S. **A Segurança da Informação Digital na Saúde. Sociedade Beneficente Israelita Brasileira**, 2003. https://www.einstein.br/biblioteca/artigos/131%20132.pdf. Acesso em: 13/06/2019.

ACM, Association for Computing Machinery, Code of Ethics and Professional Conduct, Section 1.7, ACM web page, Downloaded from https://www.acm.org/code-of-ethics.

ACQUISTI, A; GROSSKLAGS, J. Losses, gains and hyperbolic discounting: An experimental approach to information security attitudes and behavior. 2nd Annual Workshop on Economics and Information Security. UC Berkeley. In: CAMP, J. Lewis, S. eds. **The economics of information security**, 2004. Originally presented at the 2003. California.

ALBUQUERQUE JUNIOR, Antonio Eduardo; SANTOS, Ernani M. Adoption of Information Security Measures in public research institutes. **Journal of Information Systems and Technology Management**. Bahia, v.12, n.2, p.289-316, 2015.

ALBUQUERQUE JUNIOR, Antonio Eduardo; SANTOS, Ernani M.; OLIVEIRA, Rodrigo C. R.; SILVA, Adriano S. R.; ALMEIDA, Laercio M. A Adopção de Medidas Formais, Informais e Técnicas de Segurança da Informação e sua Relação com as Pressões do Ambiente Institucional. **RISTI**. Bahia, n. 30, p.17-33, 2018.

ALEXANDRIA, João Carlos S. Picture of Information Security in Public Institutions of Scientific Research in Brazil. In: INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGY MANAGEMENT, 9., 2012. São Paulo. **Proceedings**... São Paulo: TECSI, 2012.

ALLEN, Bryce. **Information Tasks**: toward a user-centered approach to information systems. Orlando: Academic Press, 1996.

ALMEIDA, M. B.; SOUZA, R. R.; CARDOSO, K. Uma proposta de ontologia de domínio para segurança da informação em organizações. **Informação e Sociedade: Estudos**, v. 20, n. 1, p. 155-168, 2010.

ALMEIDA, M.C.B. **Planejamento de bibliotecas e serviços de informação**. Brasília: Briquet de Lemos, p. 5-7, 2000.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2013**: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2013**: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da Segurança da Informação. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17788:2015**: Tecnologia da Informação – Computação em nuvem - Visão geral e vocabulário. Rio de Janeiro, 2015.

BARDIN, L. **Análise de conteúdo** (L. de A. Rego & A. Pinheiro, Trads.). Lisboa: Edições 70, 2006.

BARMAN, Scott. **Writing information security policies. Indianapolis**: New Riders, 2001.

BAUMER, D., J.B. EARP and F.C. PAYTON. "**Privacy of Medical Records**: IT Implications of HIPAA". In: Ethics, Computing, and Genomics: Moral Controversies in Computational Genomics, ed. Herman T. Tavani, Jones & Bartlett Publishers, vol. 2,p. 137-152, 2005.

BELASCO, Kent; WAN, Siaw-Peng. Online retail banking: Security concerns, breaches, and controls. In: BIDGOLI, Hossein (Org.). **Handbook of Information Security**: threats, vulnerabilities, prevention, detection, and management. New Jersey: John Wiley & Sons, vol.1, p.37-48, 2006.

BENNETT, Colin J; PARSONS, Christopher A.; MOLNAR, Adam. Real and Substantial Connections: Enforcing Canadian Privacy Laws Against American Social Networking Companies. **Journal of Law, Information and Science**. Columbia Britanica. v.23, n.1, 2014.

BENNETT, C.; RAAB, C. The Adequacy of Privacy: the European Union Data Protection Directive and the North American Response. **The Information Society: an international journal**, v.13, n.3, p. 245-264, 1997.

BERGKAMP, L. **"Corporate governance and social responsibility: A new sustainability paradigm"**. European Environmental Law Review, May, 136-152.

BHAIMIA, S. The General Data Protection Regulation: the Next Generation of EU Data Protection. In: **Legal Information Management**. Cambridge. vol. 18(01)

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a Função e os Limites do Consentimento. 2ª ed. Rio de Janeiro: Forense, 2019.

BJÖRCK, Fredrik J. Institutional Theory: A new perspective for research into IS/IT security in organisations. In: HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 37., 2004, Big Island. **Proceedings**… Big Island: HICSS, 2005.

BLUM, Renato M. S. Opice. GDPR – General Data Protection Regulation: destaques da regra europeia e seus reflexos no Brasil. **Revista dos Tribunais**, São Paulo, v. 107, n. 994, p. 205-221, 2018.

BOFF, Salete Oro; TEIXEIRA, Adam H. **Energias Renováveis**: políticas públicas de fomento às inovações tecnológicas. Curitiba: Multideia, 2014.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado, 1988.

BRASIL. Decreto n º 9.690, de 23 de janeiro de 2019. Altera o Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a **Lei n º 12.527**, de 18 de novembro de 2011 - Lei de Acesso à Informação. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF,

24 jan. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9690.htm. Acesso em: 17/11/2019.

BRASIL. Decreto nº 9.716, de 26 de fevereiro de 2019. Revoga dispositivos do Decreto n º 9.690, de 23 de janeiro de 2019, que altera o Decreto nº 7.724, de 16 de maio de 2012, que regulamenta **a Lei nº 12.527**, de 18 de novembro de 2011 - Lei de Acesso à Informação. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 27 fev. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9716.htm#art1. Acesso em: 17/11/2019.

BRASIL. **Decreto nº 99.710**, de 21 de novembro de 1990. Promulga a Convenção sobre os Direitos da Criança. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 22 nov. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d99710.htm. Acesso em: 12/06/2020.

BRASIL. **Lei nº 8.069**, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências**.** Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 16 jul. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 16/06/2020.

BRASIL**. Lei nº 10.406**, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 14/06/2020.

BRASIL. **Lei nº 12.527**, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 18 nov. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 10/06/2020.

BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11/06/2020.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 09/11/2019.

BRASIL**. Lei nº 13.853**, de 08 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 09 jul. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 20/11/2019.

BRASIL. **Medida provisória nº 869**, de 27 de dezembro de 2018. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 28 dez. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 08/11/2019.

BRUNI, Adriano Leal. **SPSS aplicado à pesquisa Acadêmica**. 1. ed., São Paulo: Atlas, 2009.

BUENO, Samara Schuck. **Regulação do Tratamento de Dados Pessoais e Contribuições ao Combate do Abuso do Poder Econômic**o. 2019. Dissertação (Mestrado em Direito Político e Econômico) – Universidade Presbiteriana Mackenzie, São Paulo, 2019.

CANCELIER, Mikhail Vieira de Lorenzi. **Infinito Particular**: privacidade no século XXI e a manutenção do direito de estar só. Rio de Janeiro: Lumen Juris, 2017.

CAPURRO, Rafael; Briger Hjorland: Annual Review of Information Sciencie and Technology, ed. Blaise Cronin, V.37, Cap. 8, P 343-411 – **Perspectivas em Ciências da Informação**. Berlin, v.12, n.1, p. 148-207, jan./abr. 2007.

CARVALHO, Matheus. **Manual de direito administrativo**. 2ª ed., Salvador: JusPODIVM, p. 686-690, 2016.

CASEY, Eoghan. Case study: network intrusion investigation – lessons in forensic preparation. **Digital Investigation**. Washington v. 2, n. 4, p. 254-260, 2005.

CASTELLS, M. **Sociedade em Rede**. 17° Ed. São Paulo: Paz & Terra, 2016.

CASTILHO, Janaina Hunch; CAMPOS, Ronaldo Ribeiro de. O fator humano e a resistência à mudança organizacional durante a fase de implantação do sistema de informação: estudo de caso em uma empresa implantadora de tecnologia. **Interface Tecnológica**. v.4., n.1, 2007. Disponível em: http://www.fatectq.edu.br/interfacetecnologica/volume4/artigo13.pdf Acesso em: 16/09/2021.

CGU.**CGU.0517.2019**. https://www.gov.br/cgu/pt-br/acesso-a-informação/institucional/eventos/anos/anos-anteriores/2017/5-anos-da-lei-de-acesso/arquivos/mesa-3-danilo-doneda.pdf/view. Acesso em: 05/10/2020.

CHOU, Shin-Yi; LIU, Jin-Tan; HAMMITT, James K. National Health Insurance and technology adoption: evidence from Taiwan. **Contemporary Economic Policy**, Western Economic Association International v.22, n.1, p.26-38, 2004. Disponível em: http://homepage.ntu.edu.tw/~ntuperc/docs/publication/2004_22_Liu.pdf

COOPER, Donald R.; SCHINDLER, Pamela S. **Métodos de pesquisa em Administração**. 12ª ed. Porto Alegre: AMGH, 2016.

COOPER, Michael H. Information security training: what will you communicate? In: ANNUAL ACM SIGUCCS FALL CONFERENCE, 37., 2009, St. Louis. **Proceedings**… ACM, p.217-222, 2009.

CORCORAN, P. **A privacy framework for the Internet of Things Published** in: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), 2-14 Dec. 2016, DOI: 10.1109/WF-IoT.2016.7845505 2016 IEEE, Reston, VA, USA, 2016. NATIONAL UNIVERSITY OF IRELAND GALWAY. Downloaded on March 28,2021 at 19:14:01 UTC from IEEE Xplore.

COTS, Márcio; OLIVEIRA , Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada**. São Paulo: Thomson Reuters Brasil, 2018.

COUPOFY. **Mobile Commerce Will Grow Twice As Fast As eCommerce in 2017** (Infographic). 2016. Disponível em: https://www.coupofy.com/blog/infographics/mobile-commerce-will-grow-twice-as-fast-as-ecommerce-in-2017-infographic> Acesso em: 11 nov. 2020

CHANG, S. E.; HO, C. B. Organizational factors to the effectiveness of implementing information security management. . **Industrial Management & Data Systems**. Taiwan. v. 106, n. 3, p. 345-361, 2006.

CHILES, Wilians Anderson S.; BEHR, Ariel; FARIAS, Everton S.; CORSO, Kathiane B. 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. In: CONGRESSO VIRTUAL BRASILEIRO – ADMINISTRAÇÃO, 2013. Porto Alegre. **Anais.**.. Porto Alegre, 2013.

CUSTERS, Bart; DECHESNE, Francien; SEARS, Alan M.; TANI, Tommaso; VAN DER HOF, Simone. A Comparision of Data Protection Legislation and Policies Across the EU. **Computer Law & Security Review**, v. 34, n. 2, p. 234-243, 2018. -> falta informar o local Disponível em:<https://daneshyari.com/article/preview/6890515.pdf> Acesso em 16/06/2021

DAMASCENO, Larissa M. S.; RAMOS, Anatália S. M.; PEREIRA, Fernando A. M. Fatores que Influenciam a Predisposição em Seguir uma Política de Segurança da Informação em uma Instituição de Ensino Superior. **Revista de Gestão e Projetos**, v.6, n.3, 2015. Disponível em: <https://periodicos.uninove.br/gep/article/view/9624/4369>. Acesso em 16/06/2021

DAVENPORT, T. H**.: Ecologia da informação:** porque só a tecnologia não basta para o sucesso da informação. Tradução Bernadete Siqueira Abrão. São Paulo: Futura, 2002.

DIAS, Marcos Aurélio P. **Administração de Materiais**. 4. ed. São Paulo: Atlas, 2000.

DOHERTY, Neil F.; ANASTASAKIS, Leonidas; FULFORD, Heather. The information security policy unpacked: **A critical study of the content of university policies**. International Journal of Information Security Management, v.29, n.6, p.459-457, 2009. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.468.6238&rep=rep1&type=pdf. Acesso em 16/06/2021

DOHERTY, Neil F.; FULFORD, Heather. Aligning the information security policy with the strategic information systems plan. **Computers & Security**, v.25, n.1, p.55-63, 2006. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.468.6238&rep=rep1&type=pdf. Acesso em 16/06/2021

DONEDA, Danilo. **Da privacidade a proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

DONEDA, D. **Privacidade e transparência no aceso à informação públic**a. Prenssas Universitárias de Zaragoza, 2010. Disponível em: http://www.egov.ufsc.br/portal/sites/defaults/lefis11-09.pdf. Acesso em: 01/10/2020.

DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Ed. RT, 2020.

DHILLON, Gurpreet S; BACKHOUSE, James. Information System Security Management in the new millennium. **Communications of the ACM**, v. 43, n. 7, p. 125-128, 2000. Disponível https://go.gale.com.ps/i.do?id=GALE%7CA63635271&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00010782&p=AONE&sw=w&userGroupName=anon%7Ed2eca566>. Acesso em 16/09/2021.

DHILLON, Gurpreet S. Current directions in IS security research: towards socioorganizational perspectives. **Information Systems Journal**, v. 11, n. 2, p. 127-153, 2001. Disponível em: <http://130.18.86.27/faculty/warkentin/SecurityPapers/Robert/DhillonBackhouse2001_ISJ_11_1_review_paper.pdf> Acesso em: 16/09/2021.

DHILLON, Gurpreet S. Managing and controlling computer misuse. **Information Management & Computer Security**, v.7, n.4, p.171-175, 1999. Disponível em: http://130.18.86.27/faculty/warkentin/SecurityPapers/Robert/Others/Dhillon1999_IMCS7_4_ManageComputerMisuse.pdf Acesso em: 16/09/2021.

DRUCKER, Peter. The coming of the new organization. **Harvard Business Review**. Boston, v.68, n. 6, p. 45-53, Jan./Feb. 1988.

EARP, J.B., A.I. Antón, L. Aiman-Smith, W. Stufflebeam. Examining Internet Privacy Policies within the Context of User Privacy Values. **IEEE Transactions on Engineering Management**, 52(2), p. 227-237, May 2005.

FERREIRA, Afonso José. Profiling e algoritmos autónomos: um verdadeiro direito de não sujeição. In.: **Anuário da Proteção de Dados**. Lisboa, p. 35-43, 2018.

FERREIRA, Júlio Marinho. **As Rede Sociais, a Exposição e a Manipulação de dados na Internet**: Os perfis falsos e o Catfish. In: I ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, novembro de 2017. Anais eletrônicos [...] Disponível em: <redegovernanca.net.br/public/conferebces/1/Anais_REDE_2017>. Acesso 22/09/2020.

FIELD, A. **Descobrindo a estatística usando o SPSS**. 2. ed. São Paulo: Artmed, 2009.

FLICK, Uwe. Introdução à pesquisa qualitativa. 3. ed. Porto Alegre: Artmed, 2009.

FLORIDI, L. **Information: A very Short Introduction**. 10 ed. Local: Oxford University Press INC, 2010.

FONTES, Edison. **Clicando com Segurança**: tratando as questões atuais da proteção da informação na Organização e na família. Rio de Janeiro: Brasport, p. 257, 2011.

FONTES, Edison L. G. **Segurança da Informação**: o usuário faz a diferença. São Paulo: Saraiva, 2006.

FORTES, B. Vinícius B. **Os Direitos de Privacidade e a Proteção de Dados Pessoais na internet**. Rio de Janeiro: Lumen Juris, 2016.

FORTES, V. B.; BOFF, S. O. **A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental**: perspectivas de construção de um marco regulatório para o Brasil Sequência: Estudos Jurídicos e Políticos, 20 jun. 2014.

FORCHT, Karen A.; AYERS, Walter C. **Developing a computer security policy for organizational use and implementation**. Journal of Computer Information Systems, v. 41, n. 2, p. 52-57, 2001.

FOXMAN, Ellen R.; KILCOYNE, Paula. **Information Technology, Marketing Practice, and Consumer Privacy**: Ethical Issues. Journal of Public Policy & Marketing, 1993. Research Article. Disponível em: https://doi.org/10.1177/074391569501200111.

FRANGOPOULOS, Evangelos D.; ELOFF, Mariki M.; VENTER, Lucas M. **Social Aspects of Information Security**. In: ISSA INNOVATIVE MINDS CONFERENCE, 2008, Johannesburgo. Proceedings... Johannesburgo: ICSA, 2008.

FRAZÃO, Ana. **Fundamentos da Proteção dos Dados Pessoais**: Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

FRAZÃO, Ana. **Nova LGPD: principais repercussões para a atividade empresarial**. A primeira parte de uma série sobre o tema. Disponível em Acesso abril/2020

FREEDMAN, W. **The Right of Privacy in the Computer Age**. Westport: Quorum Books, 1987.

FRESNEDA, Paulo Sérgio V. Transformando organizações públicas: a tecnologia da informação como fator propulsor de mudanças. Revista do Serviço Público, v. 49, n. 1, p. 71-91, 1998.

FRIEDEWALD, M., Raabe, O. **Ubiquitous computing**: An overview of technology impacts. Telematics and Informatics. P. 55-65, 2012.

GATTI, B. A. **Grupo focal na pesquisa em ciências sociais e humanas**. Brasilia: Liber Livro, 2005.

GEIGER, Jutta. The Transfer of Data Abroad by Private Sector Companies: Data Protection Under the German Federal Data Protection Act. **German Law Journal**, v.4, n.8, p.747-757, 2003.

GIL, Antonio C. **Como elaborar projetos de pesquisa**. 6ª ed. São Paulo: Atlas, 2018.

GIL, Antonio **C. Estudo de caso**. São Paulo: Atlas, 2009.

GOUVEIA, Luis Manuel Borges. **"Sociedade da Informação – Notas de contribuição para uma definição operacional"**, novembro de 2004; disponível em: Im@ufp.pt,http://ufp.pt/~Lmbg

GORAYEB, Diana M. C. **Gestão de Continuidade de Negócios aplicada ao ensino presencial mediado por recursos tecnológicos**. 2012. 153f. Dissertação (Mestrado em Engenharia Elétrica) – Universidade de São Paulo, São Paulo, 2012.

HALLINAN, D., FRIEDEWALD, M., MCCARTHY, P. **Citizens' Perceptions of Data Protection and Privacy**, Computer Law and Security Review, vol. 28, n. 3, p. 263-272, 2012.

HENDERSON, C. Sandra; SNYDER, A. **Charles Personal information privacy**: implications for MIS Managers - Department of Management, College of Business, Auburn University, 415 W. Magnolia, Auburn AL 36849, USA Received 23 April 1998; revised 14 January 1999; accepted 20 March, pp. 213-220, 1999.

HENESSY, David A.; BABCOCK, Bruce A. **Information, flexibility, and value added**. Information Aconomics and Policy, v.10, n.4, p.431-449, 1998.

HERATH, Tejaswini; HERATH, Hemantha; BREMSER, Wayne G. Balanced Scorecard implementation of Security strategies: a framework for IT Security Performance Management. **Information Systems Management**, v.27, n.1, p.72-81, 2010.

HÖNE, Karin; ELOFF, Jan H. P. Information security policy – what do international information security standards say? **Computers & Security**, v.21, n.5, p.402-409, 2002.

HUBMANN, H. **Das Persönlichkeitsrecht**. Keip: 250, a 2., veränd. u. erw … 936, r, v, |a BR 1540 b Rechtsphilosophie, k Theologie und k Allgemeines, k Rechtstheologie, Rechtsphilosophie, (DE-627)127075288X |0 (DE-625) rvk/15777: 0 (DE-576)20075288X. 936, r, v, a PD 6060, 2016.

IERVOLINO, S. A.; PELICIONE, M. C. A utilização do grupo focal como metodologia qualitativa na promoção da saúde. **Revista da Escola de Enfermagem da USP**, v.35, n.2, p. 115-21, 2001.

ILIEVA, J.; BARON, S.; HEALEY, N.M. Online surveys in marketing research: Pros and cons. **International Journal of Market Research**, v. 44, n. 3, p. 361-376, 2002.

ISMAGILOVA, E., Hughes, L., Dwivedi, Y. K., & Raman, K. R. (2019b). Smart cities: Advances in research—An information systems perspective. **International Journal of Information Management**, 47, p. 88–100, 2019.

ISMAGILOVA, Elvira; HUGHES, Laurie; RANA, Nripendra P.; DWIVEDI, Yogesh K. Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. **Information Systems Frontiers**, doi: 10.1007/s10796-020-10044-1, 2020.

ISMAIL, S., Malone, M. S., & Geest, Y. V. **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. 2019

JASSERAND, C. **Acesso da aplicação da lei aos dados pessoais originalmente coletados por entidades privadas**: faltam as salvaguardas dos titulares dos dados na diretiva 2016/680 Computer Law & Security Review, 34 (1), p. 154–165, 2018.

Jen YEH Q and Ting CHANG AJ. **Threats and countermeasures for information system security**: a crossindustry study. Inf Man 2007; 44: 480–491.

JIMENE, Camilla do Vale. Da importância da segurança da informação para adequação à LGPD. In: BLUM, Renato Opice (Org.). **Proteção de dados**: desafios e soluções na adequação à lei. Rio de Janeiro: Forense, 2020.

KILLCRECE, G., Kossakowski K.P., Ruefle, R., and Zajicek, M. (October 2003). State of the Practice of Computer Security Incident Response Teams (CSIRTS), Technical Report CMU/SEI-2003-TR-001, ESCTR-2003-001.

KING, Christopher M.; DALTON, Curtis E.; OSMANOGLU, T. Ertem. **Security architecture**: design, deployment, and operations. Berkeley: McGraw-Hill, 2001.

KITIYADISAI, Krisana. **Privacy rights and protection**: foreign values in modern Thai context. Ethics and Information Technology, 7, p. 17-26, 2005.

KLEIN, Rodrigo H.; LUCIANO, Edimara M. What Influences Information Security Behavior? A Study With Brazilian Users. **JISTEM**, v.13, n.3, p.479-496, 2016.

KRUEGER, R. A. & Casey, M. A. **Focus groups**: A pratical guide for applied research. 4th Ed. Thousand Oaks, California: Sage, 2009.

KUMAR, Sunil; SOMANI, Vikas. Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. **IJSART**, v.4, n.4, 0.125-129, 2018.

LATULIPE, Celine Audrey Rorrer, and Bruce Long. Longitudinal data on flipped class effects on performance in CS1 and retention after CS1. In: Proceedings of the 49th ACM Technical Symposium on Computer Science Education, pages 411–416. ACM, 2018.

LATULIPE, Celine; MAZUMDER, Syeda F.; WILSON, Rachel K. W. Security and Privacy Risks Associated With Adult Patient Portal Accounts in US Hospitals. **JAMA Internal Medicine**, v.180, n.6, p.845-849, 2020.

LAUREANO, M. A. P. **Gestão de Segurança da Informação**. 2005. 130 p. Disponível em: http://www.mlaureano.org/aulasmaterial/gst/apostilaversao2. Acesso em: 20/05/2020.

LE COADIC, Y. F. **Ciência da Informação**. Brasília: Briquet de Lemos livros, p.119, 1999.

LE COADIC, Y. F. **Princípio Científicos que Direcionam a Ciência e a Tecnologia da Informação digital**. Transformação, Campinas, V. 16, n. 3, p. 205-213, 2004.

LEE, R. Daniel. **Developing effective information systems security policies**. Bethesda: SANS Institute, 2001.

LENERT, Leslie; MCSWAIN, Brooke Y. Balancing Health Privacy, Health Information Exchange, and Research in the Contexto of the COVID-19 Pandemic. **Jamia**, v. 27, n. 6, p. 963-966, 2020.

LIMA, Caio Cesar Carvalho; MONTEIRO, Renato Leite. **Panorama brasileiro sobre a proteção de dados pessoais**: discussão e análise comparada. ATOZ – Novas Práticas em Informação e Conhecimento. Curitiba, v. 2, n. 1, p. 60-76, 2013.

LINDSAY, David F. An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law. Melbourne University Law Review, v.29, n.1, p.131-178, 2005.

LOPES, Isabel M. **Adoção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal**. 2012. 437f. Tese (Doutorado em Tecnologias e Sistemas de Informação, Engenharia e Gestão de Sistemas de Informação) – Universidade do Minho, Braga, 2012.

LUO, Xin; BRODY, Richard; SEAZZU, Alessandro; BURD, Stephen. Social Engineering: the neglected human factor for Information Security Management. **Information Resources Management Journa**l, v.24, n.3, p.1-8, 2011. -> falta informar o local

MACHADO, Felipe Nery Rodrigues. **Segurança da Informação**: princípios e controle de ameaças. 1. ed. São Paulo: Érica, 2014.

MACHLUP, Fritz; MANSFIELD, Una. Semantic quirks in studies of information. In: MACHLUP, Fritz; MANSFIELD, Una (Orgs.). **The study of information: interdisciplinary messages**. New York: John Wiley, p.641-671, 1983. -> falta informar o local

MAGALHÃES, Rodrigo A.; DIVINO, Sthéfano B. S. A Proteção de Dados da Pessoa Jurídica e a Lei 13.709/2018: Reflexões à Luz dos Direitos da Personalidade. **Scientia Iuris**, v.32, n.2, p.74-90, 2019.

MANDARINI, M. **Segurança Corporativa Estratégica**. São Paulo: Usina do Livro, 2004.

MANDIA, Kevin; PROSISE, Chris; PEPE, Matthew. Incident response & computer forensis. New York: **McGraw-Hill**, 2a.ed., 2003.

MANOEL, Sergio S. **Governança de Segurança da Informação**: como criar oportunidades para seu negócio. Rio de Janeiro: Brasport, 2014.

MARCIANO, J. L. P. **Segurança da Informação – uma abordagem social**. Brasília, 2006.

MARCONI, M. de A.; LAKATOS, E. M. **Metodologia do trabalho cientifico**: procedimentos básicos, pesquisa bibliografia, projeto e relatório, publicações e trabalhos científicos. 6. ed. São Paulo: Atlas, 2006.

MARCONI, M.; LAKATO, E. **Metodologia Cientifica**, 2ª edição, São Paulo, editora Atlas, 1991.Não aparecem

_____; MARCONI, **Fundamentação da Metodologia Cientifica**. 6. Ed. São Paulo: Atlas, 2007.

MASON, R.O. Four ethical issues of the information age, **MIS Quarterly** 10(1), pp. 04-12, 1986.

MARKKULA, Jouni; ROHUNEN, Anna; TIKKINEN-PIRI, Christina. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. **Computer Law & Security Review**, [S.L.], vol. 34, n. 1, p. 134-153, 2018.

MARTINS, A. B.; SANTOS. C.A.S. **"Uma Metodologia para implantação de um Sistema de Gestão de Segurança da Informação"**. Revista de Gestão e Tecnologia e Sistema de Informação. v. 2, n. 2, pp. 121-136, 2005.

MARTORELL, Leandro Brambilla; NASCIMENTO, Wanderson Flor do; GARRAFA, Volnei. **Redes sociais, privacidade, confidencialidade e ética**: a exposição de imagens de pacientes no facebook. Interface Comunicação, Saúde, Educação, v. 20, n. 56, p. 13-23, 2016.

MASON, Richard O. Four ethical issues of the information age. **MIS Quart**. Vol. 10, n.1, p. 4-12, 1986.

MATTELART, A. **História da Sociedade da Informação**. São Paulo: Loyola, 2001.

MAYNARD, Sean B.; RUIGHAVER, Anthonie B. What makes a good information security policy: a preliminary framework for evaluating security policy quality. In**: ANNUAL SECURITY CONFERENCE**, 5., 2006. Las Vegas. Proceedings… Las Vegas: Information Institute, 2006.

McCARTHY, N. K.. **Resposta a Incidentes de Segurança em Computadores**: Planos para Proteção de Informação em Risco. Porto Alegre: Bookman, 2013

MEDIUM. Disponível em: https://www.google.com/url?sa=i&url=https%3A%2F%2Fmedium.com%2Finternet-das-coisas%2Fseguran%25C3%25A7a-01-privacidade-vs-confidencialidade-c0bae58b2375&psig=AOvVaw0RHXKO1tAJtEPJvn7We7VV&ust=1631305246080000&source=images&cd=vfe&ved=0CAkQjhxqFwoTCPCOw9_b8vICFQAAAAAdAAAAABAD. Acesso em: 08 de set. 2021

YAO, Mei-Ling; CHUANG, Ming-Chen; HSU, Chun-Cheng. The Kano model analysis of features for mobile security applications. **Computers & Security**, v.78, p.336-346, 2018.

MENDES, Laura Schertel. **A Lei Geral de Proteção de Dados Pessoais**: um modelo de aplicação em três níveis. In: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscila

(Coord.). Lei Geral de Proteção de Dados – Caderno Especial. São Paulo: Revista dos Tribunais, p. 35-56, 2019.

MNISTERIO DA DEFESA – Disponível em: https://www.gov.br/defesa/pt-br/acesso-a-informação/lei-geral-de-proteção-de-dados-pessoais-lgpd. Publicado em 03/09/2020, atualizado em 12/04/2021.

MITNICK, Kevin D.; SIMON, William L. Mitnick – **A arte de enganar - Ataques de hackers**: controlando o fator humano na Segurança da Informação. São Paulo: Makron Books, 2003.

MOORE, A. The GDPR & Managing Data Risk For Dummiesfont R, Symantec Special Edition. **Chichester, West Sussex**: John Wiley & Sons, Ltd., 2018.

MOORE, Gary C.; BENBASAT, Izak. Development of an instrument to measure the perceptions of adopting an Information Technology innovation. **Information Systems Research**, v.2, n.3, p.192-222, 2001.

MOREIRA, N. S. **Segurança Mínima: Uma visão corporativa da Segurança da Informação**, Rio de Janeiro: Axcel Books, 2001.

MORESI, Eduardo Amadeu, **Delineando o Valor do Sistema de Informação de uma Organização**. Ciência da Informação, v. 29, n.1, 2000.

MORGADO, L. F. **O cenário internacional de proteção de dados pessoais**. Necessitamos de um Código Brasileiro. Âmbito Jurídico, Rio Grande, XII, n. 65, jun. 2009. Disponível em: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leituea&artigo_id=6336. Acesso em: 19 nov. 2019.

MORGAN, D.L. **Focus groups as qualitative research**. London: Sage, 1988.

MORGAN, D. L. Reconsidering the role of interaction in analyzing and reporting focus groups. **Qualitative Health Research**, 20 (5), p. 718-722, 2010.

MULHOLLAND, Caitlin Sampaio. **Dados Pessoais Sensíveis e a Tutela dos Direitos Fundamentais**: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/2018). Revista de Direitos e Garantias Fundamentais, Vitória, v. 19, n. 3, set.-dez. p. 150-180, 2018.

NAVARRO, Ana Maria Neves de Paiva Navarro. LEONARDOS, Gabriela. **Privacidade Informacional**: origem e Fundamentos no Direito Norte-Americano. Disponível em www.publicadireito.com.br, acesso em 20 ago, 2019.

NAVARRO, Ana Maria Neves de Paiva. **O Direito Fundamental à Autodeterminação Informativa**. Departamento de Pós-Graduação TESE, UFRJ, LETACI. Rio de Janeiro, 2011.

NAVARRO, Ana Maria Neves de Paiva. O direito fundamental à autodeterminação informativa. In: XXI Congresso Nacional do CONPEDI. Direitos Fundamentais e Democracia II. Florianópolis: **FUNJAB**, 2012. p. 410-438. Anais [...] Disponível em: Acesso em: 20/042019.

NEVES, Denise L. F.; PAVANI, Guilherme C.; SALES, Rafael Marcos; LOPES, Tatiana S. A. **A Segurança da Informação de Encontro às Conformidades da LGPD**. Processando o Saber, v.13, p.186-198, 2021.

OLIVEIRA, Ana Paula; ZANETTI, Dânton; LIMA, Flávio S.; SAMPAIO, Themis O. **Lei Geral de Proteção de Dados Brasileira na Prática Empresarial**. Revista Jurídica da Escola Superior de Advocacia da OAB-PR, v.4, n.1, p.172-200, 2019.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. Disponível em: http://www.oecd.org/. Acesso em: 19/11/2019.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS NO BRASIL. Disponível em: https://nacoesunidas.org/. Acesso em: 19/11/2019.

PAESANI, Liliana Minardi. **Direito e Internet**: Liberdade de Informação, Privacidade e Responsabilidade Civil. 7. ed., São Paulo: Atlas, 2014.

PARK, Cheol-Soon; JANG, Sang-Soo; PARK, Youg-Tae. A study of effect of Information Security Management System [ISMS] certification on organization performance. **International Journal of Computer Science and Network Security**, v.10, n.3, p.10-21, 2010.

PATRICK, Walter F. **Creating an information systems security policy**. Bethesda: SANS Institute, 2001.

PEIXOTO, Erick Lucena Campos; EHRARDT Marcos Júnior. **Os Desafios da Compreensão Do Direito À Privacidade No Sistema Jurídico Brasileiro em Face das Novas Tecnologias**. Revista, atualizada e modificada do artigo intitulado "Breves notas sobre a ressignificação da privacidade", publicado na Revista Brasileira de Direito Civil – RBDCivil, v. 16, p. 35-56, 2018 - Revisado em 2020, nº 2, 389-418.

PEIXOTO, Erick Lucena Campos; EHRARDT Marcos Júnior. **Os Desafios da Compreensão Do Direito À Privacidade No Sistema Jurídico Brasileiro em Face das Novas Tecnologias**. Revista, atualizada e modificada do artigo intitulado "Breves notas sobre a ressignificação da privacidade", publicado na Revista Brasileira de Direito Civil – RBDCivil, nº 2, p. 389-418, 2020.

PEREIRA, F. L; JACOBSEN, A., MARTINA, J. E.; LENGLER, F. R. **A importância da inovação na gestão de processos administrativos da Universidade Pública, por meio da implementação da Tecnologia de Certificação Digital**. Revista da UNIFEBE, Brusque, v. 1, n. 21, p. 1-23, 2017

PFLEEGER, Charles P. **Security in computing**. 2a Edition. Prentice Hall, 1997.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais**: Comentários à Lei 13.709/2018 (LGP). 2. ed. São Paulo: Saraiva, 2020.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais:** comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva, 2019

PORTAL DA TRANSPARÊNCIA DA CONTROLADORIA GERAL DA UNIÃO. Defesa Nacional. 2020. Disponível em: http://www.portaltransparencia.gov.br/funcoes/05-defesa-nacional?ano=2020. Acesso em: 10/03/2021.

RAMINELLI, Francieli P.; RODEGHERI, Letícia B. **A Proteção de Dados Pessoais na Internet no Brasil**: Análise de Decisões Proferidas pelo Supremo Tribunal Federal. Cadernos do Programa de Pós-Graduação em Direito, v.11, n.2, p.89-119, 2016.

RINDFLEISCH, A., Heide, J.B. **Transaction cost analysis: past, present and future implications**. Journal of Marketing, 61, p. 30–54, 1997.

ROCHA, Camila P.; CARNEIRO, Ana Valéria S.; MEDEIROS, Marcus Vinícius B.; MELO, Alexandre. Segurança da Informação: **A ISO 27001 como ferramenta de controle para LGPD**. Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará, v.2, n.3, p.78-97, 2019.

RODOTÁ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

RUARO, Regina Linden; RODRIGUEZ, Daniel Pinheiro**. O Direito à Proteção de Dados Pessoais na Sociedade de Informação**. Direito, Estado Sociedade, n. 36, jan/jun. 2010.

RUARO, Regina L.; GLITZ, Gabriela P. C. **Panorama Geral da Lei Geral de Proteção de Dados Pessoais no Brasil e a Inspiração no Regulamento Geral de Proteção de Dados Pessoais Europeu**. Repats, v.6, n.2, p.340-356, 2019.

RUARO, Regina Linden. **Direito Fundamental à Liberdade de Pesquisa Genética e à Proteção de Dados Pessoais**: os princípios da prevenção e da precaução como garantia do direito à vida privada. Revista do direito público. Londrina, v. 10, n. 2, p. 9-38, 2015. Disponível em: http://www.uel.br/revistas/uel/index.php/direitopub/article/view/22298/16895. Acesso em: 30/11/2020.

SÁ-SOARES, Filipe. **Interpretação da Segurança de Sistemas de Informação segundo a Teoria da Ação**. 2005. Tese (Doutorado em Tecnologias e Sistemas de Informação) – Universidade do Minho, Braga, 2005.

SCHMITT, Cristiano Heineck. **Consumidores hipervulneráveis: a proteção do idoso no mercado de consumo**. São Paulo: Atlas, 2014, p. 55-70.

SCHUNK, Giuliana Bonanno. **Contratos de longo prazo e dever de cooperação**. São Paulo: Almedina, 2016.

SCHWARTZ, P. Property, **Privacy, and Personal Data. Harvard Law Review**, 117, 2057-2128, 2004.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva**. 2. ed. Rio de Janeiro: Campus, 2014.

SENA, Samara Rodrigues. **A Proteção de Dados Pessoais de Crianças no Ordenamento Jurídico Brasileiro**. Revista Caderno Virtual. Brasília: IDP, nº 44, v. 2, abr/jun, 2019.

SENADO FEDERAL (Brasil). **Comissão de MP que muda Lei de Proteção de Dados Pessoais aprova plano de trabalho**. Senado Notícias, Brasília, 03 abr. 2019. Disponível em: https://www12.senado.leg.br/noticias/materias/2019/04/03/comissao-de-mp-que-muda-lei-de-protecao-de-dados-pessoais-aprova-plano-de-trabalho. Acesso em: 08/11/2019.

SENADO FEDERAL (Brasil). **Lei que cria Autoridade Nacional de Proteção de Dados é sancionada com vetos**. Senado Notícias, Brasília, 09 jul. 2019. Disponível em: https://www12.senado.leg.br/noticias/materias/2019/07/09/lei-que-cria-autoridade-nacional-de-protecao-de-dados-e-sancionada-com-vetos. Acesso em: 20/11/2019.

SENADO FEDERAL (Brasil). **Sancionada com vetos lei geral de proteção de dados pessoais**. Senado Notícias, Brasília, 15 out. 2018. Disponível em: https://www12.senado.leg.br/noticias/materias/2018/08/15/sancionada-com-vetos-lei-geral-de-protecao-de-dados-pessoais. Acesso em: 19/11/2019.

SENTHILKUMAR, P.; ARUMUGAM, S. **Policy verification, validation and troubleshooting in distributed firewalls**. International Journal of Computer Science and Information Security, v.9, n.10, p.135-137, 2011.

SEPRO. Mapa da proteção de dados. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/mapa-da-protecao-de-dados-pessoais. Acesso em: 20/09/2020.

SILVA, A. C. R. de. **Metodologia da pesquisa aplicada a contabilidade**: orientações de estudos, projetos, artigos, relatórios, monografias, dissertações e teses. 2. ed. São Paulo: Atlas, 2008.

SILVA, Denise R. P.; STEIN, Lilian M. **Segurança da Informação**: uma reflexão sobre o componente humano. Ciências & Cognição, v.10, pp. 43-56, 2007.

SILVEIRA, Suzana Aparecida. **Segurança da Informação e Proteção de Dados Pessoais**: Estudo de caso e proposta de governança para serviços de saúde. São José dos Campos, 2021. 218f. Dissertação (Mestrado em Inovação Tecnológica) - Departamento de Ciência e Tecnologia, Universidade Federal da São Paulo, São José dos Campos, 2021.

SHANNON, Claude E. A mathematical theory of communication. **The Bell Systems Technical Journal**, v 27., p.379-423, 1948.

SHEEHAN, Kim B.; HOY, Mariea G. Dimensions of privacy concern among online consumers. **Journal of Public Policy & Marketing**, v.19, n.1, p.62-73, 2000.

SOMANI, G. M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya. Ddos attacks in cloud computing: issues, taxonomy, and future directions. **Computer Communications**, 107:30–48, 2018.

STAIR, R. M.; REYNOLDS, G. W. **Sistemas de informação**: uma abordagem gerencial. X ed. Rio de Janeiro: editora, 2002

STERNE, Daniel F. On the buzzword 'security policy'. In: **IEEE COMPUTER SOCIETY SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY**, 2, 1991. Oakland. Proceedings... Oakland: IEEE, 1991.

SVEEN, F.O.; TORRES, J.M.; SARRIEGI, J.M. Blind **Information Security Strategy. International Journal of Critical infrastructure Protection**, v.2, p. 95-109, 2009.

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de Dados Pessoais Comentada Artigo por Artigo**. 1. ed. Salvador: Juspodivm, 2019.

TIKKINEN-PIRI, C., Rohunen, A., Markkula, J.: UE **Regulamento Geral de Proteção de Dados: Alterações e implicações para empresas de coleta de dados pessoais**. Comput. Law Secur. p. 128-148, 2018.

TOMIATTI, T. S. **Governança de TI.** Trabalho de Conclusão de Curso (Graduação) - Faculdade de Tecnologia de São Paulo, São Paulo. 2012. Disponível em: http://www.fatecsp.br/dti/tcc/tcc00048.pdf. Acesso em: 25 abr. 2021.

UNIÃO EUROPEIA. **Diretiva 95/46/CE**, de 24 de outubro de 1995. Disponível em: Acesso em: 10 dez. 2019

UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados (RGPD)** 2015/679/CE, de 27 de abril de 2016. Disponível em: Acesso em: 10 dez. 2019.

UNITED NATIONS HUMAN RIGHTS. **Universal Declaration of Human Rights**. 1948. Disponível em: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por. Acesso em: 19/11/2019.

VALENTE, Victor Augusto Estevam. Imprensa, jornalismo digital e Direito Penal: aspectos materiais e processuais. Salvador: **Jus PODIVM**, 2020.

VAN DEN HOVEN; HANCKE, Gerhard P. **Practical Comparison between** COAP and MQTT-Sensor to Server level. In: 2018 Wireless Advanced (WiAd). IEEE, p.1-6. 2018.

VAN DEN HOVEN Jeroen, John Weckert. **Information Technology and Moral Philosophy**. Cambridge Studies in Philosophy and Public Policy, 2008.

VASCONCELOS, Isabella F. G.; PINOCHET, Luiz Hernan C. Poder, tecnologia e controle burocrático: uma análise crozeriana em uma empresa de informática paranaense. In: ENCONTRO DE ESTUDOS ORGANIZACIONAIS, 2., 2002. Recife. **Anais.**.. Rio de Janeiro: ANPAD, 2002.

WHITMAN, Michael E. Enemy at the gate: threats to Information Security. **Communications of the ACM**, v.46, n.8, p.91-95, 2003.

WILLIAMS, P. Information security governance. **Information Security Technical Report**, v. 6, n. 3, p. 60-70, 2001.

WILSON, Piers. Positive perspectives on cloud security. **Information Security Technical Report**, n.16, p. 97-101, 2011.

WRIGHT, K. B. Researching internet-based populations: advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services. **Journal of Computer-Mediated Communication**, v. 10, n. 2, 2005.

WU, J. et al. The research of design based on social commerce. **International Journal of Social Science Studies**, v. 3, p. 157-165, 2016.

XU, Heng; DINEV, Tamara; SMITH, H. Jeff; HART, Paul. **Examining the Formation of Individual's Privacy Concerns**: Toward an Integrative View. In: INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS, 29., 2008. Paris. Proceedings... Atlanta: AIS, 2008.

YIN, Robert K. **Estudo de Caso**: Planejamento e Métodos. 5. ed. Porto Alegre: Bookman, 2015.

YVES, Poullet. **Computer Law & Security Review:** The International Journal of Technology Law and Practice. Steve Saxby, Vol. Issue 4, Editor´s Foreword –CLSR 1985-2018, p. 773-778, 2018.

ZANINI, Leonardo E. A. A Tutela dos Direitos da Personalidade na Alemanha. **Interfaces Científicas – Direito**, v.8, n.2, p.266-283, 2020.

GLOSSÁRIO

AGENTES DE TRATAMENTO – o controlador e o operador.

AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS – Controla o tratamento dos dados pessoais, a fim de garantir o cumprimento das regras de privacidade, a aconselha as instituições e os organismos da UE sobre todos os aspetos do tratamento dos dados pessoais, das políticas e da legislação neste domínio, processa queixas e conduz inquéritos, monitoriza as novas tecnologias suscetíveis de ter um impacto em matéria de proteção de dados e trabalha com as autoridades nacionais dos países da UE para garantir coerência na proteção de dados.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS – órgão responsável por fiscalizar as empresas em casos de denúncias de vazamento de dados.

ANONIMIZAÇÃO – utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

ASSESSMENT – realizar um assessment em uma empresa significa compreender as suas práticas atuais de proteção de dados, o que a LGPD está solicitando e, onde a empresa não atende a estas solicitações.

AUTORIDADE NACIONAL – órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

BANCO DE DADOS – conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

BLOQUEIO – suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

CMMI - é uma sigla na língua inglesa para *Capability Maturity Model Integration*, algo que pode ser traduzido

COMPLIANCE – Deve estar em conformidade com atos, normas e leis, para seu efetivo cumprimento.

CONSENTIMENTO – manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

CONTROLADOR – pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

DADO ANONIMIZADO – dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

DADO PESSOAL SENSÍVEL – dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

DPO – DATA PROTECTION OFFICER - ENCARREGADO DE DADOS – descrito na LGPD como "Encarregado" é pessoal responsável pela conformidade do tratamento dos dados que circulam na empresa e, é este profissional que responde a Agência Nacional de Proteção de Dados.

DPIA - *Data Protection Impact Assessment* – traduzindo para o português, Relatório de Impacto de Proteção de dados (RIPD).

ELIMINAÇÃO – exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

ENCARREGADO – pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

GAPS - é um termo em inglês que significa um distanciamento; afastamento, separação, uma lacuna ou um vácuo.

JOB DESCRIPTION - Uma descrição do trabalho ou JD é uma narrativa escrita que descreve as tarefas gerais ou outras tarefas relacionadas e responsabilidades de um cargo.

KPIs - KPI é a sigla para o termo em inglês *Key Performance Indicator*, que significa indicador-chave de Desempenho. Esse indicador é utilizado para medir o desempenho dos processos de uma empresa e, com essas informações, colaborar para que alcance seus objetivos.

LGPD – Lei Federal nº 13.709/2018 – Lei Geral de Proteção de dados pessoais.

LAI - lei de acesso à informação (Lei Federal nº 12.527/11).

MARCO CIVIL DA INTERNET - Lei n° 12.965/2014 - é uma legislação que inovou diversos aspectos da regulamentação das atividades das empresas relacionadas ao ambiente digital.

OKRs - Objetivos e resultados chave é um sistema para definição e rastreamento de objetivos e seus resultados.

OPERADOR – pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

ORGANIZAÇÃO PÚBLICA – define como o poder de gestão do Estado, no qual inclui o poder de legislar e tributar, fiscalizar e regulamentar, através de seus órgãos e outras instituições; visando sempre um serviço público efetivo. A administração se define através de um âmbito institucional-legal, baseada na Constituição, leis e regulamentos.

ORGANIZAÇÃO PRIVADA – define com a gestão privada, é uma empresa cujo proprietário é uma pessoa natural ou jurídica.

ORGANIZAÇÃO PARAESTATAL – define como gestão de entidades paraestatais, são entidades privadas que realizam atividades de interesse coletivo, sem fins lucrativos que

recebem incentivos de entidades públicas. A distinção entre as entidades do Poder Público e das empresas privadas é denominado Terceiro Setor.

ÓRGÃO DE PESQUISA – órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

PMBOK - O guia *Project Management Body of Knowledge* (PMBOK) é um conjunto de práticas na gestão de projetos organizado pelo instituto PMI e é considerado a base do conhecimento sobre gestão de projetos por profissionais da área.

PMI - O *Project Management Institute* é uma organização sem fins lucrativos que tem o objetivo de disseminar as melhores práticas de gerenciamento de projetos em todo o mundo.

PRIVACY BY DEFAULT – Incorporar mensagens de privacidade dos dados pessoais em todos os sistemas ou aplicativos de tratamento de dados pessoais. Estas mensagens são disponibilizadas e de fácil acesso para os usuários. Resumindo, toda arquitetura e operacionalidade do sistema ou da prática do negócio devem ser centradas na privacidade do usuário.

PRIVACY BY DESIGN - é a metodologia que garante que ao tratar dados pessoais a empresa será proativa na proteção dos dados pessoais e com funcionalidade total, além de garantir que os dados serão protegidos em todo círculo, com aplicação dos conceitos de visibilidade e transparência respeitando acima de tudo a privacidade do usuário.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS – documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

ROPAS - *Record of Processing Activities* - Um ROPA é um registro das atividades de processamento de uma organização que envolvem dados pessoais.

TITULAR – pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

TRANSFERÊNCIA INTERNACIONAL DE DADOS – transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

TRATAMENTO – toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

USO COMPARTILHADO DE DADOS – comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

UTM – *Unified Threat Management* (UTM) - tradução livre para o português Gerenciamento Unificado de Ameaças, foi inicialmente desenvolvida para defesa de redes corporativas com centenas de equipamentos ou com informações críticas a serem protegidas.

APÊNDICE A – Questionário para a pesquisa *Survey*

SEGURANÇA DA INFORMAÇÃO – Lei Geral de Proteção de Dados

Prezado,

Meu nome é Naira Maria da Silva Duarte, Gerente de Tecnologia da Informação do SENAC – BA. Sou aluna do MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO da UNIVERSIDADE FEDERAL DA BAHIA (UFBA).

Estou realizando esse levantamento de dados como etapa final da pesquisa para a construção da dissertação de mestrado cujo título é A COMPREENSÃO DOS PROFISSIONAIS DE TI QUANTO A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E SUAS IMPLICAÇÕES NAS ORGANIZAÇÕES, tendo como objetivo geral identificar como os profissionais de TI percebe, a adequação dos controles de segurança da informação nas organizações quanto às exigências da LGPD.

O objetivo desta pesquisa é dimensionar o nível de compreensão da LGPD para esses profissionais.

O questionário é anônimo, os nomes dos respondentes não serão divulgados na pesquisa e os dados obtidos serão utilizados apenas em âmbito acadêmico. A indicação do perfil deve-se unicamente à necessidade de qualificação e quantificação dos respondentes enquanto sujeitos da pesquisa. Tais dados são importantes para dar credibilidade ao estudo.

Gentileza responder o questionário até 26/01/2021.

Agradeço a sua participação!

TERMO DE CONSENTIMENTO

( ) Declaro que, após ter sido devidamente esclarecido pelo pesquisador, **CONSINTO** que os dados sejam utilizados e os resultados obtidos sejam apresentados e publicados em eventos e artigos científicos.

( ) Declaro que, após ter sido devidamente esclarecido pelo pesquisador, **NÃO consinto** que os dados sejam utilizados e os resultados obtidos sejam apresentados e publicados em eventos e artigos científicos.

Caso opção foi **não consentimento**, pesquisa será concluída após sinalizar está opção – Obrigada!

Caso opção foi **consentimento**, observe a nota explicativa a seguir – Obrigada!

NOTA EXPLICATIVA

A pesquisa está composta de:

Bloco I – Informações gerais das participantes.

Bloco II – Gestão da Segurança.

Bloco III – Controle das Informações.

Bloco IV – Controle das Informações quanto à Responsabilidade e a Penalidade.

Bloco V – Impactos e Oportunidades para os Profissionais de TI.

Totalizando 32 perguntas que podem variar segundo ranger de respostas:

1 – Nenhuma – ação adotada.

2 – Pouca – ação adotada.

3 – Media – ação adotada até 50%

4 – Bom – ação adotada entre 51% a 90%

5 – Plenamente – ação adotada acima de 90%.

BLOCO I – INFORMAÇÕES GERAIS

1. Identifique o cargo ou função que melhor se adequa ao que você faz na organização onde trabalha.

( ) Analista

( ) Coordenador

( ) Gerente

( ) Diretor

2. Quanto tempo trabalha na sua organização?

( ) 1 a 5 anos

( ) 6 a 10 anos

( ) 11 a 15 anos

( ) 16 a 20 anos

( ) Acima de 20 anos

3. Qual a sua faixa de idade?

( ) 18 a 25 anos

( ) 26 a 35 anos

( ) 36 a 45 anos

( ) 46 a 55 anos

( ) Acima de 55 anos

4. Qual seu sexo?

( ) Feminino

( ) Masculino

BLOCO II – GESTÃO DA SEGURANÇA

5. Identifique como você classifica a sua compreensão sobre a LEI 13.709/2018 – LGPD quanto ao controle de segurança da informação.

1 2 3 4 5

Não adequada ( ) ( ) ( ) ( ) ( ) plenamente adequada

6. Indique como você classifica o quanto a sua organização está adequada à LGPD quanto à necessidade de tecnologias de segurança da informação.

1 2 3 4 5

Não adequada ( ) ( ) ( ) ( ) ( ) Plenamente adequada

7. Indique como você classifica o quanto sua organização está adequada em relação às configurações que precisam ser feitas em tecnologias de segurança da informação para atender aos requisitos da LGPD.

1 2 3 4 5

Não adequada ( ) ( ) ( ) ( ) ( ) Plenamente adequada

8. O quanto sua organização tem controle sobre os dados pessoais em comparação com os requisitos da LGPD?

1 2 3 4 5

Nenhum controle ( ) ( ) ( ) ( ) ( ) Total controle

9. Como você classifica sua responsabilidade no tratamento de dados pessoais?

1 2 3 4 5

Nenhuma ( ) ( ) ( ) ( ) ( ) Total responsabilidade

10. O quanto você considera adequadas as estruturas organizacionais de TI e segurança da informação em sua organização para atender aos requisitos da LGPD?

1 2 3 4 5

Não adequada ( ) ( ) ( ) ( ) ( ) Plenamente adequada

11. A organização em que trabalha tem uma política de segurança da informação?

( ) Sim

( ) Não

12. Como você classifica o desenvolvimento de uma política de segurança da informação para a sua organização?

1 2 3 4 5
Não ( ) ( ) ( ) ( ) ( ) Plenamente desenvolvida

13. O quanto a política de segurança da informação está adequada aos requisitos da LGPD em sua organização?

1 2 3 4 5
Não adequada ( ) ( ) ( ) ( ) ( ) Plenamente adequada

14. Quanto sua organização já criou ou alterou dos planos, dos regulamentos e das políticas organizacionais para estar em conformidade com a LGPD?

1 2 3 4 5
Nenhuma alteração ( ) ( ) ( ) ( ) ( ) Muita alteração

BLOCO III – CONTROLE DAS INFORMAÇÕES

15. Qual foi o impacto da LGPD sobre a política de segurança da informação de sua organização?

1 2 3 4 5
Nenhum impacto ( ) ( ) ( ) ( ) ( ) Alto impacto

16. Como classifica os controles que são aplicados na política ou nos ativos de informação em sua organização?

1 2 3 4 5
Nenhuma efetividade ( ) ( ) ( ) ( ) ( ) Muita efetividade

17. Como você identifica o impacto que os usuários poderão causar às medidas de segurança da informação, considerando a não aplicação dos controles de proteção dos dados em sua organização?

1 2 3 4 5
Nenhum impacto ( ) ( ) ( ) ( ) ( ) Alto impacto

18. Como classifica o controle dos dados sensíveis hoje na organização em que você trabalha?

1 2 3 4 5
Nenhum controle ( ) ( ) ( ) ( ) ( ) Total controle

19. Como classifica as medidas de controle das informações de sua organização, considerando os possíveis vazamentos ou ataques cibernéticos?

	1	2	3	4	5	
Nenhum controle	( )	( )	( )	( )	( )	**Total controle**

BLOCO IV – CONTROLE DAS INFORMAÇÕES QUANTO À RESPONSABILIDADE / PENALIDADE

20. Em sua organização, qual o nível de responsabilização dos profissionais de TI por vazamentos de dados?

	1	2	3	4	5	
Nenhuma	( )	( )	( )	( )	( )	**Total responsabilização**

21. Em sua organização, qual o nível de aplicação de penalidades que são atribuídas aos profissionais de TI por vazamento de informações?

	1	2	3	4	5	
Nenhuma penalidade	( )	( )	( )	( )	( )	**Plena penalidade**

22. Qual a sua percepção quanto às mudanças no controle da organização sobre os dados para garantia da privacidade?

	1	2	3	4	5	
Nenhuma mudança	( )	( )	( )	( )	( )	**Alta mudança**

23. Como você identifica se a divulgação está sendo adequada quanto às penalidades para o descumprimento da lei?

	1	2	3	4	5	
Nenhuma divulgação	( )	( )	( )	( )	( )	**Alta divulgação**

24. Como classifica as medidas adotadas por sua organização para disseminação da LGPD, considerando a eficiência de fato?

	1	2	3	4	5	
Nenhuma eficiência	( )	( )	( )	( )	( )	**Alta eficiência**

25. Identifique o quanto de capacitação já foi aplicado na sua organização.

	1	2	3	4	5	
Nenhuma capacitação	( )	( )	( )	( )	( )	**Alta capacitação**

BLOCO V – IMPACTOS E OPORTUNIDADES PARA OS PROFISSIONAIS DE TI

26. Como classifica as possíveis mudanças operacionais que a lei 13.709/2018 - LGPD poderá dispor para os profissionais de TI na empresa em que você trabalha?

1 2 3 4 5
Nenhuma mudança ( ) ( ) ( ) ( ) ( ) Alta mudança

27. Qual o impacto da implantação da LGPD para as atividades de gestão de TI em sua organização?

1 2 3 4 5
Nenhum impacto ( ) ( ) ( ) ( ) ( ) Alto impacto

28. Identifique o nível de impacto que a LGPD poderá incidir na sua organização.

1 2 3 4 5
Nenhum impacto ( ) ( ) ( ) ( ) ( ) Alto impacto

29. Quanto as funções - DPO (Data Protection Officer ou "Encarregado de dados") quem responde pela segurança dos dados na organização e, o Operador - toda pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador, podem mudar a gestão da segurança da informação na sua organização?

1 2 3 4 5
Nenhuma mudança ( ) ( ) ( ) ( ) ( ) Alta mudança

30. Como você identifica as competências existentes quanto à segurança da informação pelos profissionais de TI em sua organização?

1 2 3 4 5
Nenhuma competência ( ) ( ) ( ) ( ) ( ) Alta competência

31. Como você identifica a necessidade de desenvolvimento técnico dos profissionais de TI da sua organização para se adequar aos requisitos da LGPD?

1 2 3 4 5
Nenhuma necessidade ( ) ( ) ( ) ( ) ( ) Alta necessidade

32. Como você, enquanto profissional de TI, visualiza as oportunidades que a LGPD poderá proporcioná-lo no processo de encarreiramento?

1 2 3 4 5
Nenhuma ( ) ( ) ( ) ( ) ( ) Alta oportunidade

Agradeço a participação.
Naira Duarte
https://docs.google.com/forms/d/1bdDH_Sfq7VUWMPLFsnChO91Gou5CfHbD1HDz30XhZC8/edit

APÊNDICE B – Roteiro para o Grupo Focal

Roteiro do Grupo Focal – 1ª etapa
Roteiro e Envio dos resultados da Pesquisa Survey

SEGURANÇA DA INFORMAÇÃO – Lei Geral de Proteção de Dados

Prezado,

Meu nome é Naira Maria da Silva Duarte, Gerente de Tecnologia da Informação do SENAC – BA. Sou aluna do MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO da UNIVERSIDADE FEDERAL DA BAHIA (UFBA).

Estou realizando o resultado da pesquisa aplicada em janeiro de 2021 junto aos profissionais de TI do SENAC, que teve como objetivo o levantamento de dados como etapa final da pesquisa para a construção da dissertação de mestrado cujo título é A COMPREENSÃO DOS PROFISSIONAIS DE TI QUANTO A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E SUAS IMPLICAÇÕES NAS ORGANIZAÇÕES, tendo como objetivo geral identificar como os profissionais de TI percebe, a adequação dos controles de segurança da informação nas organizações quanto às exigências da LGPD.

O objetivo desta reunião é considerar os resultados obtidos quanto o nível de compreensão da LGPD percebidas por esses profissionais.

A atividade será transcrita anonimizada, os nomes dos participantes não serão divulgados na pesquisa e os dados obtidos serão utilizados apenas em âmbito acadêmico.

TERMO DE CONSENTIDO

( ) Declaro que, após ter sido devidamente esclarecido pelo pesquisador, CONSINTO que os dados sejam utilizados e os resultados obtidos sejam apresentados e publicados em eventos e artigos científicos.

( ) Declaro que, após ter sido devidamente esclarecido pelo pesquisador, NÃO consinto que os dados sejam utilizados e os resultados obtidos sejam apresentados e publicados em eventos e artigos científicos.

Caso opção foi **não consentimento**, o e-mail com o link para acesso aos resultados e a reunião não serão enviados – Obrigada!

Caso opção foi **consentimento**, o e-mail com o link para acesso aos resultados e a reunião será enviado após a confirmação – Obrigada!

E-mail Explicativo

Apresento o resultado da pesquisa aplicada aos 70 profissionais de TI de SENAC, através do questionário gerado pelo Google Forms ,e, enviado no mês de janeiro de 2021 sobre a LGPD na Instituição, intuito de validar os pressupostos de pesquisas – quanto a compreensão do profissional de TI na dissertação apresentada ao curso de Mestrado Profissional em Administração do Núcleo de Pós-Graduação em Administração da Escola de Administração da Universidade Federal da Bahia, sob a orientação: Prof. Dr. Antônio Eduardo de Albuquerque Junior.

Neste momento, segunda parte da pesquisa com a aplicação da metodologia Grupo Focal, no formato de reunião *online*, na ferramenta *Microsoft Teams* no dia 22 de abril de 2021 das 17:00 as 19:00 horário de Brasília, contará com a mediação da pesquisadora do Mestrado em Administração da UFBA – Naira Maria da Silva Duarte, que apresentará o resultado da pesquisa aplicada e os participantes serão convidados a apresentar suas considerações e colaborações quanto ao resultado da 1ª pesquisa que será enviado através do link abaixo.

https://teams.microsoft.com/l/meetup-join/19%3ameeting_ZGQzMjAxZTUtZDJmMi00MTdjLWEzYmYtYWM1ZWYwZDFjYWFl%40thread.v2/0?context=%7b%22Tid%22%3a%2274c618f9-b1b7-4296-9eff-64106c1530c4%22%2c%22Oid%22%3a%22258062d4-f747-4000-93c6-515c9faa55b1%22%7d

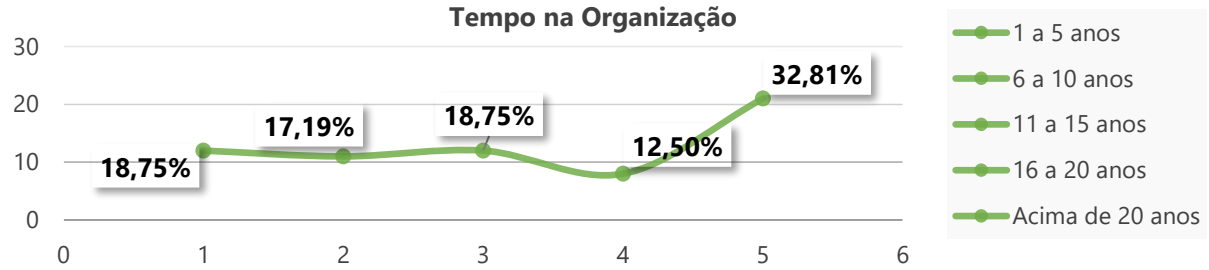
Gentileza confirmar a participação até 20/04/2021.

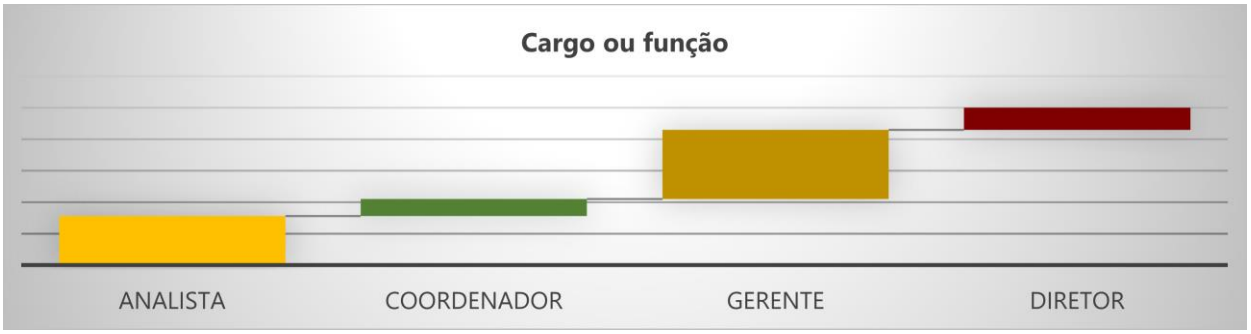
Agradeço a sua participação!

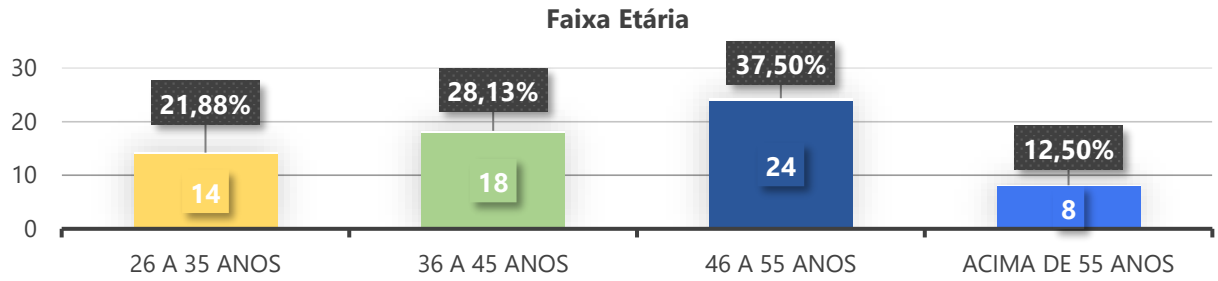
Resultados Anexados ao E-mail Explicativo

Bloco I – Perfil dos Profissionais de TI que participaram da Pesquisa.

Notou-se que o perfil dos profissionais de TI do SENAC, considerando apenas os que deram o consentimento, são na sua maioria do sexo masculino, com idade entre 46 a 55 anos, com mais de 20 anos trabalhando na instituição na função de gerente de TI na condução de ações estratégicas e inovadoras para a tecnologia da informação.

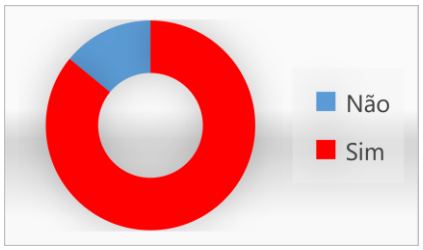






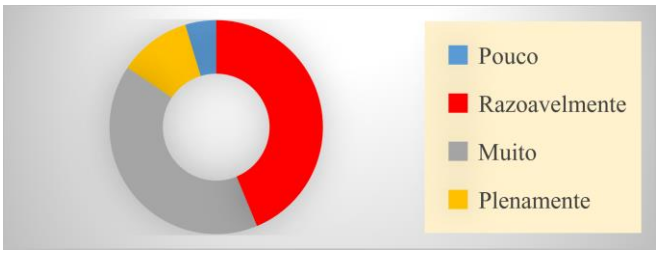
Bloco II - Gestão da Segurança da Informação:

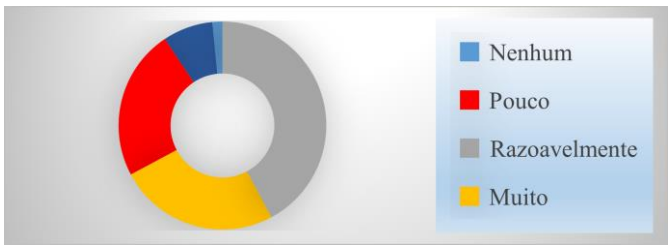
Observou-se a Gestão da Segurança da Informação sobre as dimensões **Técnicas** (adequar a gestão de TI através da implantação de novas tecnologias de segurança da informação), **Formais** (definir as responsabilidades e realizar as mudanças nas estruturas organizacionais) e **Informais** (adotar ações éticas no tratamento de dados pessoais através da conscientização organizacional).



Observamos que 86% dos regionais que participaram estão com a **gestão da Segurança da Informação** de acordo com as recomendações técnicas do Código Nacional de TI - CODETI.

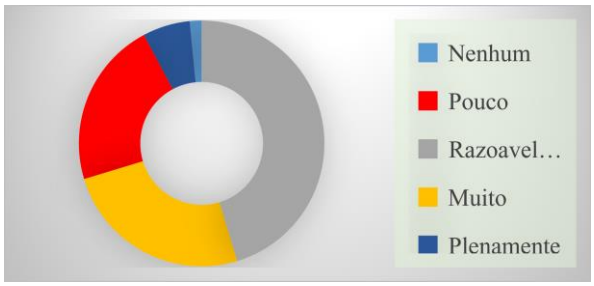
Quanto a ***Compreensão da Lei 13.709/2018 – LGPD*** na gestão da Segurança da Informação:
51% com o nível de entendimento muito bom e 49% estão em fase de construção deste conhecimento.

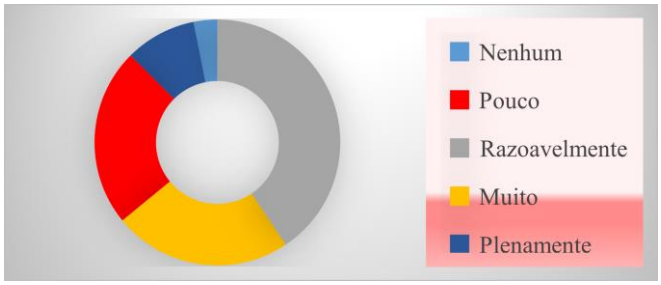




Quanto a Instituição está ***adequada e ou se adequando as necessidades tecnológicas para atender a LGPD*** na gestão da Segurança da Informação:
55% classificam que as adequações tecnológicas para a GSI estão sendo razoáveis e 33% se classificam com adequações muito boas.

Quanto as configurações ***técnicas e tecnológicas necessárias na TI para atender a Lei*** na gestão da Segurança da Informação:
67% classificam que as configurações de TI para a GSI estão em níveis razoáveis e 31% como muito bons.



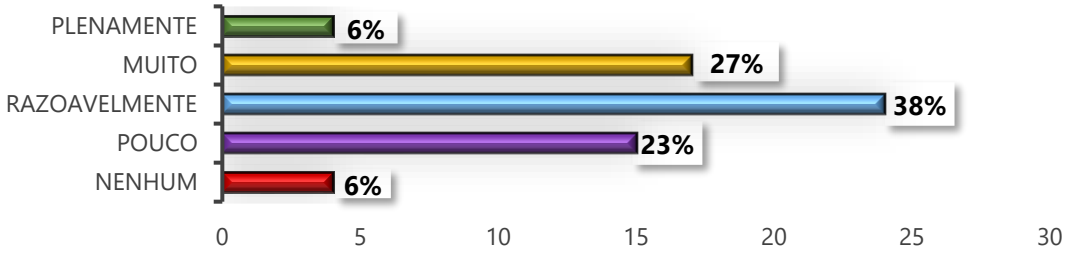


Quanto aos ***controles, normas e divulgações da gestão da Segurança da Informação – para as adequações aos requisitos da LGPD***:
65% classificam que os processos para a adequação aos estão em níveis razoáveis e 32% classificam como muito bons.

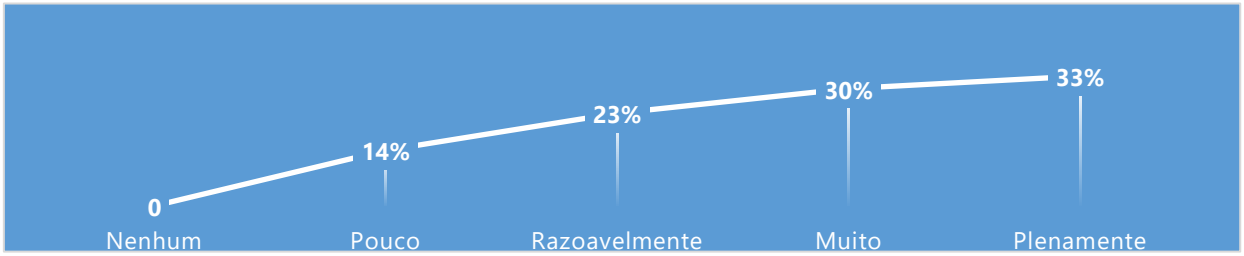
Bloco III – Controle da Informação "Politica de Segurança da Informação"

Buscou avaliar se os processos técnicos, formais e informais quanto aos controles da informação – PSI estão adequados as diretrizes e obrigações da LGPD estipula, e o quanto os profissionais de TI as compreendem.

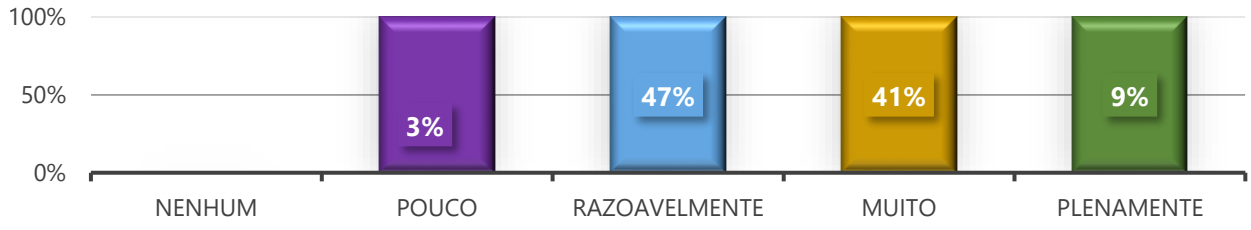
Como os profissionais de TI validam os ajustes a serem adodos nos Planos, Regulamentos e das Politicas organizacionais para estar em conformidade com a LGPD?



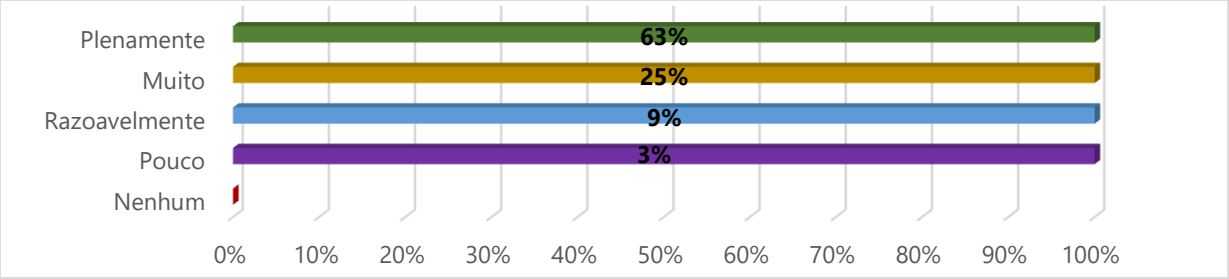
Quanto aos impactos que a LGPD pode e ou poderá insidir na Politica de Segurança da Informação – PSI como eles avaliaram?



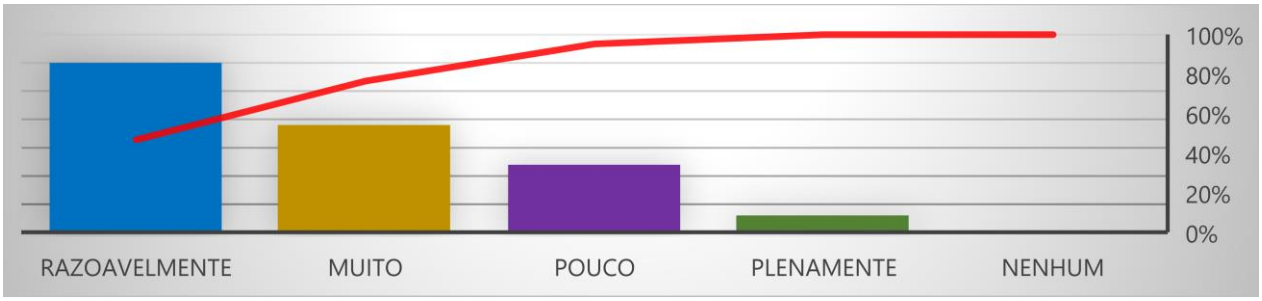
Quanto aos controles adotados na PSI serem eficientes e atenderem a LGPD, como eles consideraram?



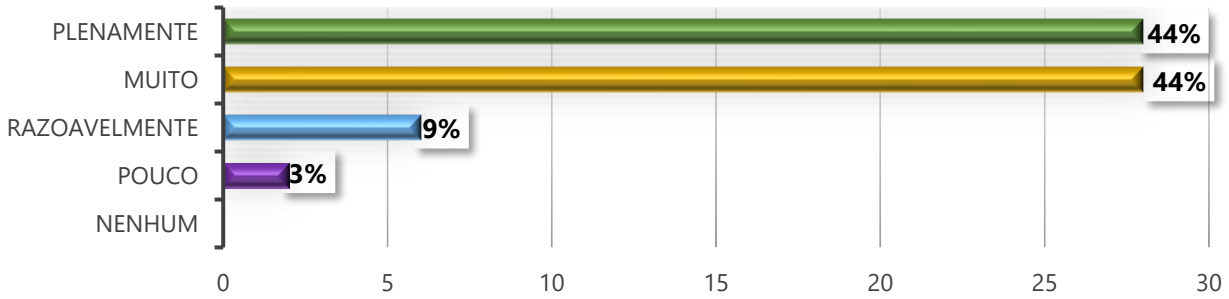
Quanto aos impactos que os Usuários de TI poderão influenciar na PSI, considerando a não aplicação dos controles de proteção aos dados pessoais, como esses profissionais avaliaram?



Quanto a aplicação de medidas de controles dos dados pessoais, como eles avaliaram a situação atual em relação aos requisitos da LGPD?

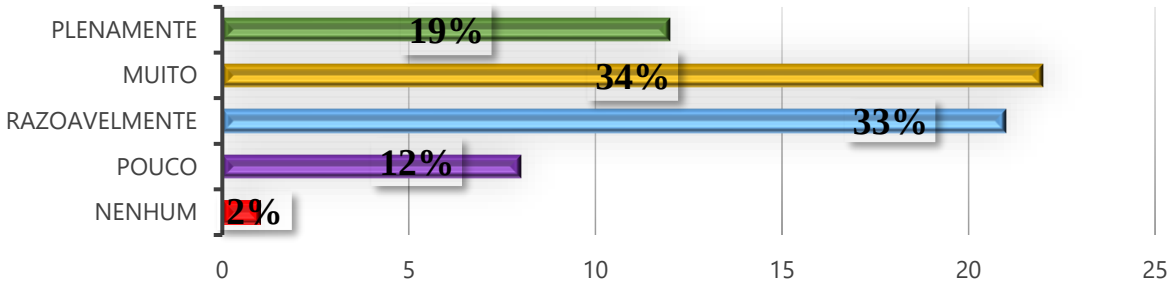


Como avaliam às responsabilidades no tratamento dos dados pessoais, segundo às diretrizes da LGPD?



Quanto às adequações para as estrutura de TI, como consideram as medidas adotadas na PSI para atender as diretrizes para os controles dos dados pessoais?

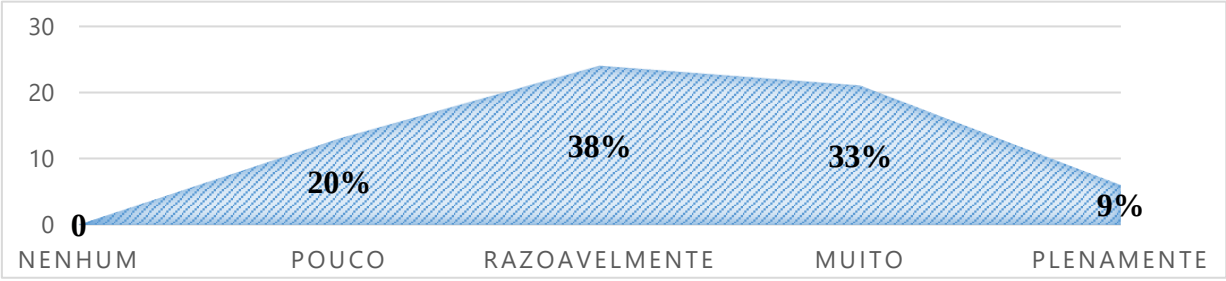
Como os profissionais de TI validaram as ações de comunicação e dulgação da PSI em relação aos controles os dados pessoais a serem adotados?



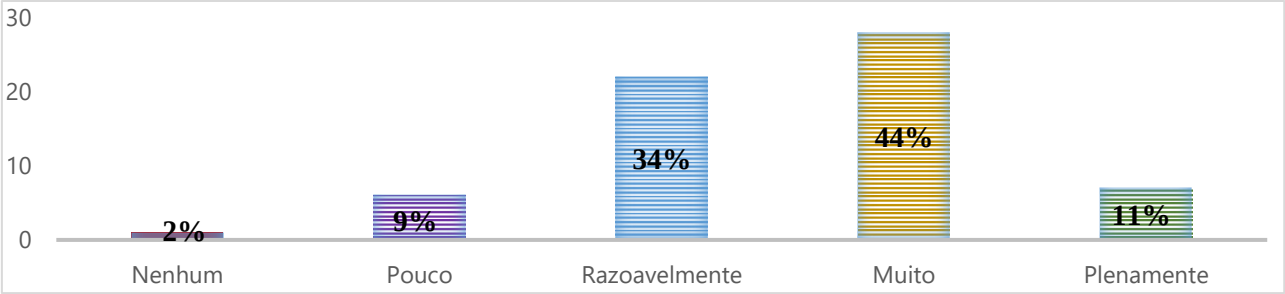
Bloco IV – Controle das Informações quanto a Responsabilidades e Penalidades:

Procurou-se verificar o nível de responsabilidade dos profissionais de TI quanto ao controle dos dados pessoais nas bases sistêmicas, e, os critérios adotados no SENAC quanto a aplicação de penalidades nos casos de perdas das informações. Como também a comprensão das sanções que a lei 13.709/2018 atribui aos profissionais de TI.

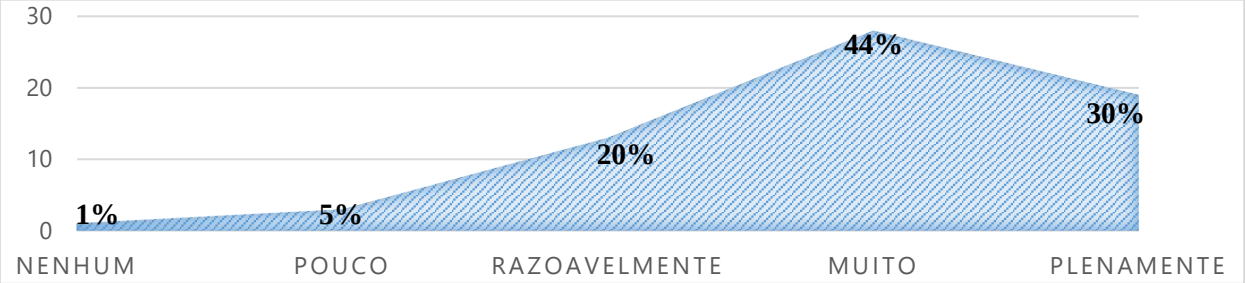
Quanto aos dados sensíveis existentes na instituição, como classificam o controle?



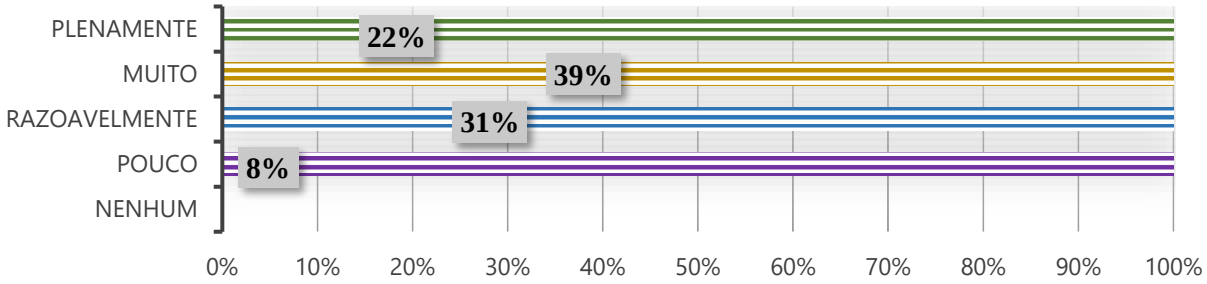
Quanto ao controle das informações, considerando os possiveis vazamentos e ataques cibernéticos?



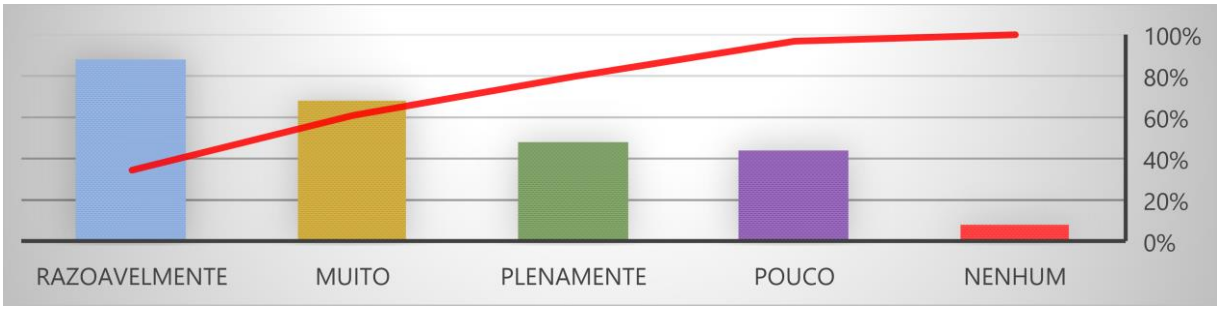
Em caso de vulnerabilidade e ou vazamento da informação, qual o nivel de responsabilidade do profissional de TI?



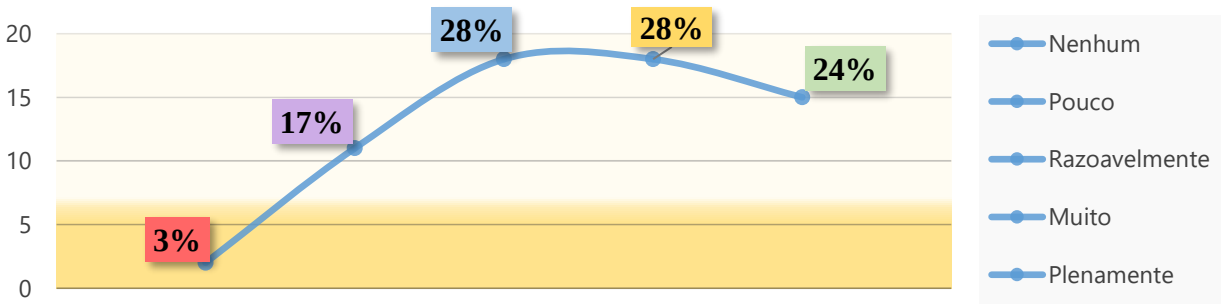
Quanto à percepção do controle da informação, garantias da privacidade, está sendo atribuida a responsabilidade e a penanlidade quanto a LGPD?



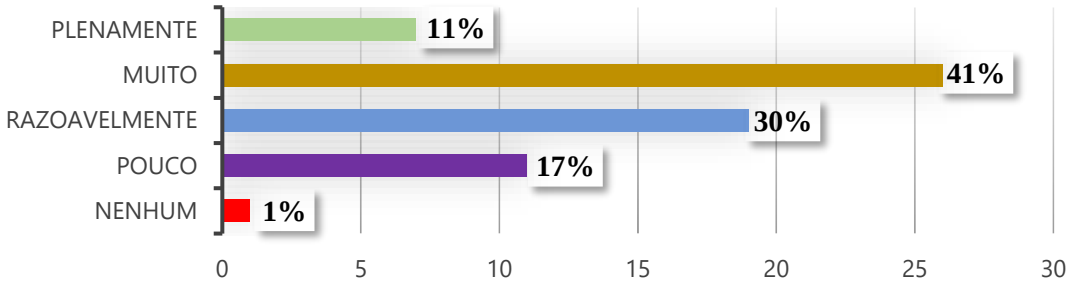
Como está sendo considerado às divulgações na Instituição quanto às sanções e penalidades quanto ao descumprimento da Lei?



As medidas adotadas pela Instituição para a disseminação dos conhecimentos quanto as mudanças organizacionais quanto a LGPD estão sendo consideradas eficientes?



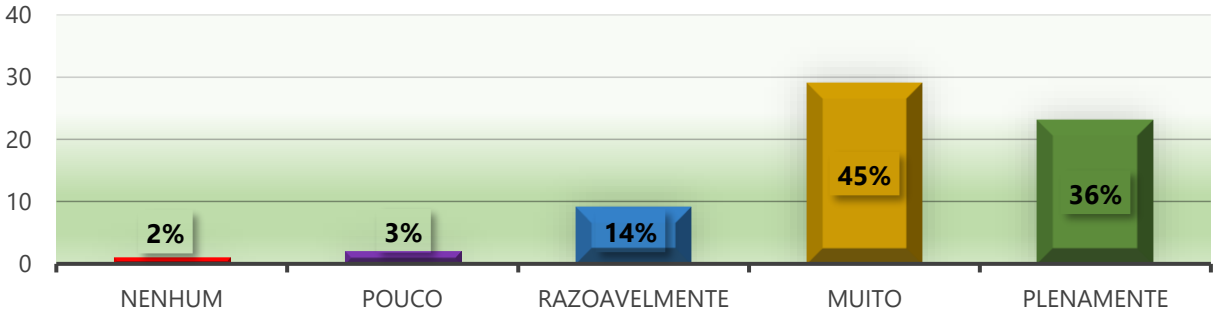
Como os profissionais de TI do SENAC estão percebendo às capacitações aplicadas para o entendimento da LGPD?



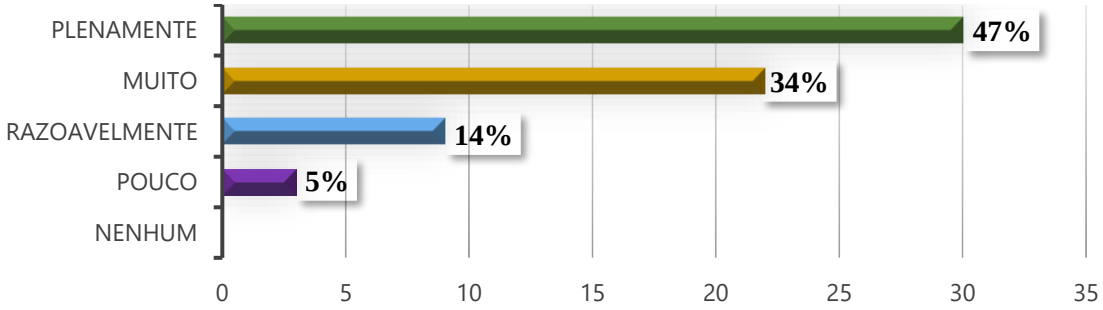
Bloco V - Governança de TI- Impactos e Oportunidades oriundas LGPD:

No bloco final da pesquisa, procurou verificar se os profissionais de TI conseguem compreender as oportunidades e os impactos que a adequação da Lei LGPD poderá incidir no seu contexto.

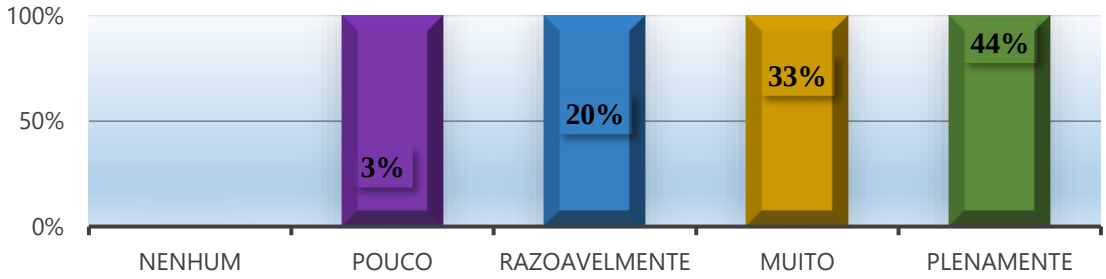
Como às mudanças operacionais estão sendo percebidas pelos profissionais de TI em consequencia da adequação da LGPD no SENAC?



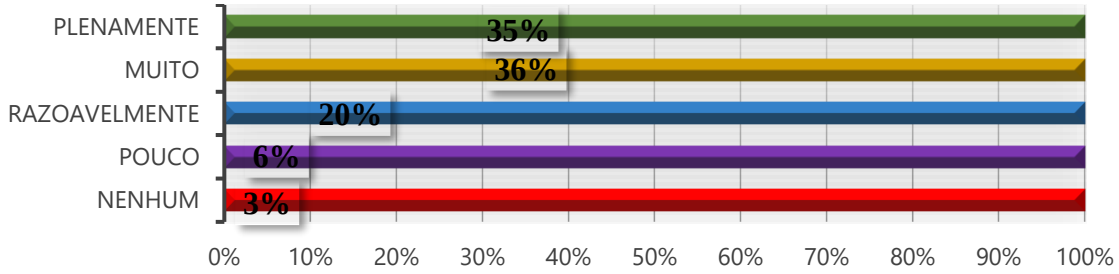
Como os profissionais e TI percebem os impactos que a implantação da LGPD trará para a gestão de TI?



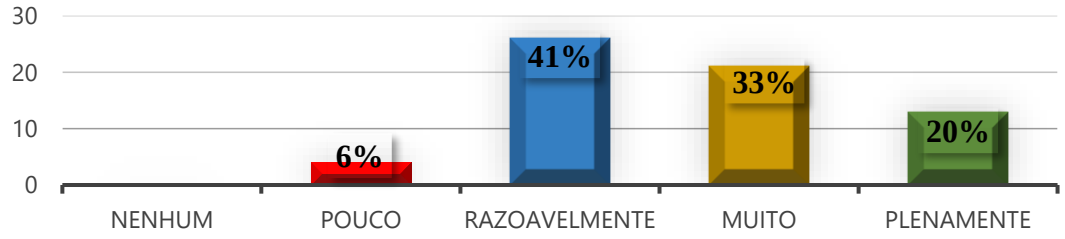
Como esses profissionais percebem o nível de impacto que a LGPD incidirá na Instituição?



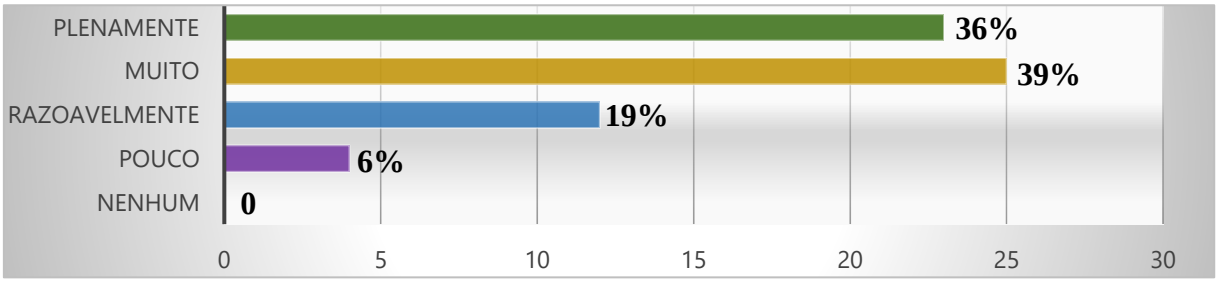
Quanto as definições de para o DPO – Encarregado dos Dados e os Operador, podem impactar a gestão de TI, considerando as diretrizes atuais da área?



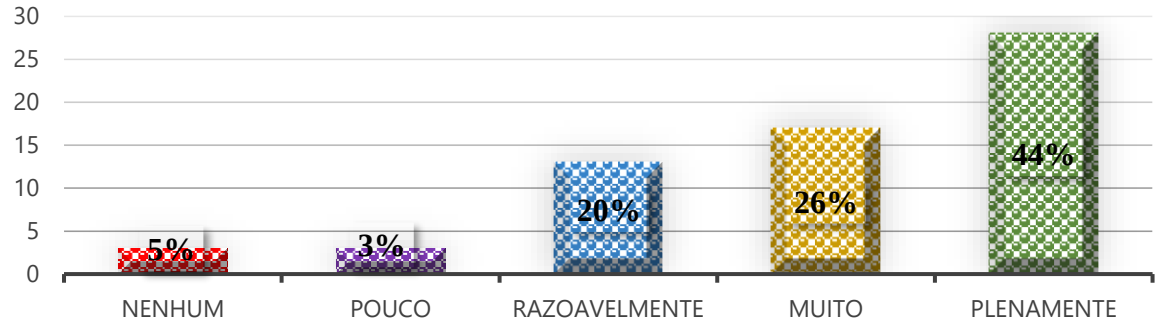
Como prpfisionais se consideram, quanto a competência existente para a gestão da sobre a Segurança da Informação?



Como os profissionais de TI se identificaram quanto ao “desemepnho” tecnico e tecnologico para atuarem na adequação da Lei 13.709/2018?



Como os profissional de TI, visualizaram as oportunidades oriundas da LGPD?



Roteiro do Grupo Focal – 2ª etapa
Roteiro da Reunião

<u>Mediado – Inicio do Grupo Focal</u>

Mediado – Abertura da sala no Teams para iniciar a Reunião.

(Inicia a gravação) - Boa tarde, sejam todos bem vindos!

Hoje dia 22 de abri de 2021 as 17:05, estaremos concluindo a 2ª etapa da pesquisa aplicada para a construção da dissertação de mestrado cujo título é A Compreensão dos Profissionais de TI quanto A Lei Geral de Proteção de Dados Pessoais e suas Implicações nas Organizações, tendo como objetivo geral identificar como os profissionais de TI percebe, a adequação dos controles de segurança da informação nas organizações quanto às exigências da LGPD.

Estarei mediando a reunião, denominada “Mesa Redonda – Resultado da Pesquisa aplica aos 70 profissionais de TI do SENAC, quanto a Compreensão dos Profissionais de TI sobre a lei 13.709/2018”, os quais, foi enviado atraves do e-mail corporativo do SENAC os dados estatisticos obtidos atraves do questionario aplicado pelo *Google Forms* em janeiro deste mesmo anos.

Estamos contando com a participação dos Gestores A, B, C, D, E, F, e G que comporam a mesa, os demais Gestores presentes estaram participando atraves do chat com perguntas e considerações.

Saleinto que as abordagens deverão transcorrer no maximo de 2 (duas) horas, sobre a observação da Mediadora e um Secretario X que estará registrando a reunião. Os resultados da pesquisa ficarão a disposição dos participantes.

Lembramos que todos os dados obtidos serão sigilosos e quando transcritos para o trabalho academico serão anonimizados.

O roteiro da reunião seguira a composição da pesquisa survey aplicada no questionario, composta pelos blocos: Bloco I – Informações gerais das participantes, Bloco II – Gestão da Segurança, Bloco III – Controle das Informações, Bloco IV – Controle das Informações quanto à Responsabilidade e a Penalidade e Bloco V – Impactos e Oportunidades para os Profissionais de TI. Contudo, o objetivo é que cada um dos convidados realizem suas ponderações sobre o tema sinalizando se possiveis os “aspectos Positivos”, “os entraves” e as “recomendações especificas”. Com a palavra:

1º Convidado: Gestor A.

Iniciou fazendo uma reflexão sobre a lei no Brasil, as reverberações da GPDR com a LGPD e os principais pilares e fundamentos da lei brasileira. Em seguida lembrou que o SENAC a nivel nacional vem contribuindo com todos sobre o tema. Considerou a pesquisa interessante, e quanto os resultados apresentados são reflexos da independência e autonomia que cada Regional tem para a GSI. Considerou que os melhores resultados estão para aqueles que fazem parte do Comitê técnico que delibera e trata todos as questões técnicas e tecnológicas, e para o tema LGPD vem atuando de forma colaborativa, assim como; os demais temas da TI. Além disso, socializa os processos e procedimentos que estão sendo adotados para adequação da lei como: a construção da Cartilha Nacional sobre a LGPD; Termo de Referência para a contratação de uma Consultoria para realizar o “assessment” analisando todas as áreas e todos os processos. Considerou sobre a importância de “informação”, onde vem atuando em Workshops com todas as áreas onde atua para que a fique explicito a abrangência da lei em seus processos e porque é necessário um controle diferente. Explicou que o DPO não deve ser uma CPF e ou CNPJ, e sim um Comitê Multidisciplinar com integridade e decisões em conjunto. Observou a necessidade de identificar quais processos tratam de dados pessoais e criação de ranking por ordem de criticidade/prioridade/riscos. Considerou a importância de um inventário das informações pessoais (quais são e como estão sendo armazenados em meios físicos e digitais), como também, o inventário das bases legais para obtenção e armazenamento dessas

informações. Apontou a indispensabilidade do mapeamento das vulnerabilidades dos processos quanto ao uso dos dados pela Instituição, através da “Roadmap” e o acompanhamento por meio do relatório de impacto da LGPD na instituição (DPIA). Alertou para o fato que nem tudo precisa ser criptografado, em função dos altos custos do processo, mas que é imprescindível a criptografia dos pedaços das bases que possuem dados pessoais, além da incorporação da criptografia nos dispositivos móveis e em toda comunicação de ponta a ponta entre a rede e a nuvem. Cita que o conhecimento dos profissionais de TI sobre a Lei é fundamental, mas que, as adequações e implantações da LGPD não devem ser atribuídas apenas para os profissionais de TI, pois a lei tem muitos pormenores que estão além da tecnologia. Diz: “.... Se os problemas na implantação da LGPD, fosse tecnologia, tudo estaria solucionado...”.

2º Convidado: Gestor B.

Parabenizando o trabalho e agradecendo o convite, reintera que a pesquisa reflete o perfil dos profissionais de TI que atuam e os pontos maior reflexão são os são evidenciados diariamente. Salienta que os tratamentos dos dados pessoais e sensíveis processados na Instituição SENAC Nacionalmente estão amparados em leis que embasam a utilização dessas informações para a atividade desempenhada pela organização, entretanto, traz a reflexão que não estamos isentos da responsabilidade em caso de vazamento, e elucida que um usuário com todos os bloqueios e controles de acesso, desde que ele tenham acesso aos dados, o mesmo poderá fazer um print pelo celular, o que colocaria em cheque todos os bloqueios e as criptografias definidas pela segurança da informação, provando que o pilar “pessoas” talvez seja o mais difícil de se acomodar aos padrões, exigindo um forte trabalho de conscientização de toda a equipe. Questionei ao grupo quanto a responsabilidade do “Controlador da LGPD” em casos como este, pois, julgando que todos os critérios de segurança possíveis são implementados nos ERP´s, mesmo assim, o “controlador” não tem como garantir o controle de acesso dos usuários que usam os sistemas, e, como de fato eles estão assegurando o acesso aos dados e ou evitando, como por exemplo quanto ao uso de celular para captura informações, que simplesmente, comprometer todas as medidas adotadas, o que acende um alerta quanto ao rigor no controle dos dispositivos que fragilizam a Segurança da Informação. Salientou que este compartilhamento de dados e a segurança da informação é o ponto de atenção que mais o preocupa na Gestão do Sistema da Informação. Destacou que este está sendo seu principal desafio na adequação da LGPD no seu Regional, e como segregar os dados sobre sua responsabilidade na adequação da lei quanto a proteção dos dados pessoas e sensíveis.

3º Convidado: Gestor C.

Expôs que os danos, nos casos de aplicações de penalidades por parte da ANPD, podem extrapolar o valor financeiro, considerando que uma sanção aplicada poderia comprometer a utilização da base de uma organização ou até suspender o direito de utilizar o banco de dados, o que pode trazer um impacto muito mais severo do que a aplicação de uma multa, colocando em risco, inclusive, as atividades que a Instituição desempenha. Exemplificando, considerou que o SENAC por ter uma base única nos ERP Financeiro e Educacional, se tiver uma ocorrência junto a ANPD, por ser base única, a sanção de bloqueio a base de dados, estará mobilizando o SENAC a nível Nacional, que resultará uma paralização da Instituição e a sanção trará prejuízos em escala. Destacou um ponto frágil da LGPD que é o Termo de Consentimento fornecido pelo titular do dado, que por lei, ele tem o direito de remover o consentimento que havia sido dado anteriormente em qualquer momento, exigindo um controle maior sobre até quando e como os dados serão armazenados dentro das bases sistêmicas e físicas dentro da organização em caso de remoção do "aceite" do titular. Elucidou a necessidade de cláusulas claras nos contratos quanto ao tratamento dos dados com os Fornecedores referentes à LGPD e quais são os deveres e responsabilidade de todos que participam da contratação. Enfatizou que os critérios e os procedimentos adotados quanto ao tratamento dos dados nos casos de incidentes e vazamentos devem ser rigorosamente registrado, mitigados e reportados a ANPD. Salientou a importância do conhecimento dos profissionais de TI quanto a lei, e ele foi um dos que aproveitou as oportunidades que a LGPD poderá oportunizar para aqueles que busquem conhecimentos. Finaliza agradecendo o convite e parabenizou pelo trabalho. Colocou-se à disposição de auxiliar na construção do entendimento da LGPD junto aos Regionais da Instituição.

4º Convidado: Gestor D.

Parabenizou a pesquisa, onde o mesmo participou e comprova que os resultados refletem o cenário atual quanto os conhecimentos da LGPD para os profissionais de TI, e, corrobora com a opinião dos demais Gestores que o maior desafio da lei não está com a TI e sim com o processo de conscientização organizacional quanto a "privacidade". Destaca que está na fase de contratação de uma empresa de consultoria para realizar o "assessment" analisando todas as áreas e todos os processos e assim iniciar as implantações segundo a lei. Afirma dizem: "...é muito importante termos momentos como este que solidificam e ampliam os conhecimentos..."

5º Convidado: Gestor E.

Relata que os pontos apresentados na pesquisa reflete o momento de inovação e adequação que os regionais estão vivenciando, e que a LGPD só reforça a necessidade de ampliamos as tratativa de melhoria continua da governaça de TI.

Corrobora com as preoculpações do Gestor C quanto a exposição dos dados pessoais e os danos que podem ser gerados pela não adequação a Lei. Pois a pesquisa evidencia a fragilidade na percepção dos profissionais quanto ao tema.

Considera que o **fato capacitação e divulgação** são essenciais para o processo de adequação e transformação que a Lei trara para todos os profissionais que estiverem envolvidos, como também, lembra que não é só TI.

Destaca que a pesquisa deveria ser compartilhada e o Comitê Nacional deveria promover um trabalho com todos, considerando os pontos de reflexão observados na pesquisa. Onde parabeniza os gráficos apresentdaos.

6º Convidado: Gestor F.

Argumenta sobre a importância e os cuidados quanto a Segurança Administrativa e Segurança Jurídica que a lei inclui no contexto das organizações. Concordou com todas as colocações discutidas no grupo, onde também adotaram o Comitê multidisciplinar de Segurança da Informação que é presidida pelo DPO (o DPO é da área de Compliance é formado em direito, com conhecimento profundos de processos e normativos além de conhecer muito sobre a gestão dos sistemas de informações), onde foi criado um regimento para o Comitê e o mesmo aprovado via Portaria na reunião do conselho Regional. Destacou que montaram 8 grupos de trabalhos para tratar da LGPD, indo desde o mapeamento de processos, gestão de riscos, gestão de acessos, políticas de privacidade, gestão de contratos, normativos e procedimentos, códigos de éticas colaboradores / alunos / fornecedores entre outros, onde mensalmente os coordenadores destes grupos fazem uma reunião de repórter status para as diretorias. Também foi criado uma Comissão Especial formada por Conselheiros que acompanham os trabalhos e apresentam mensalmente na reunião do conselho. No mais, afirma a importância do conhecimento de todos, e, não somente dos profissionais de TI, pois a lei está respaldada em três pilares: Tecnologia, Pessoas e Compliance. Finaliza agradecendo e parabenizando a todos.

7º Convidado: Gestor G.

Lamenta não ter participado da 1ª pesquisa, mas se sentiu representado diante dos resultados apresentados, e que com certeza sua participação não mudaria o resultado apresentado. Considera que como ponto positivos a evidencia que o corpo tecnico de TI precisa ser mais prepado numa visão mais generalista, pois quanto de fala em "conhecimento" o time só pensa nas questões tecnicistas. Contudo, a LGPD traz um novo olhar para aquestão da Gestão de Segurança da Informação, pois como vimos em todos os depoimentos... "as medidas técnicas para serem eficientes e eficazes vão precisar da concientização do processo sistemico...". Então, os profissionais de TI devem compreender as nuances que a Lei traz para além do "tecnes" e considerar que a compreensão de como os efeitos legais podem impactar nas atividades da TI, e, como isso pode impactar negativamente sobre sanções que compromente a responsabilidade pela gestão da informação. Na qual, é cada vezes mais sob a responsabilida de da TI sua gestão. Considara que todos os entraves poderão ocorrer na adequação da LGPD em consequencia do não cumprimento da diretrizes bem clara da Lei e a falta de investimento nas "mudanças" necessarias: sejam elas na aquisição de equipamentos e soluções tecnologica, na contratação de especialistas em normatização de processos e documentos e na aplição de ações de divulgação e treinamento para todos do SENAC. Sem mais, corrobora todos, sob a importância do conhecimento não da TI, mais de todas as áreas que compoem a Instituição, pois a lei esta ai não vei para "pegar" veio para ser cumprida. Finaliza agradecendo e parabenizando a todos!.

Demais participantes:

Gestores H, I, L e K, o Diretor W e os Coordenadores P e Q.

Todos sinalizam suas dúvidas, considerações e contribuições no chat durante a reunião, as quais foram tratadas e respondidas. Todos participantes destacaram a importancia de se alinhar os conhecimentos e que a pesquisa reflete o momento de investimento e inovação que o SENAC vem adotando. Mas, o perfil do profissional de TI ainda é muito técnico e uma lei multidisciplar está provocando uma mudança para aqueles que percebem que as atividades de TI cada vezes será transversal. Destacaram a importancia do tema e como ainda existem muitos pontos de divergencia de entendimentos dos profissionais da TI dos Regionais sobre o tema abordado. Muitos contraporão considerado que diante de um grupo teoricamente equivalente a riqueza das contribuições foram absurdas... imaginem para os demais profissionais de TI dos Regionais?..., confirmaram que a pesquisa refletir o profissional da Instituição, salientaram a importância do encontro e agradeceram o convite.

Mediadora – Final do Grupo Focal

Em seguida, a mediadora Naira Duarte SENAC Bahia, agradeceu a participação e a contribuições de todos os convidados, e, assim encerrar a reunião, denominada “Mesa Redonda – Resultado da Pesquisa do SENAC quanto a Compreensão dos Profissionais de TI sobre a lei 13.709/2018”, as 19:08.

Agradeço a todos os colegas “gestores de TI” que participaram das pesquisas e que colaboraram com seu tempo respondendo ao formulário aplicado e na participação da “reunião” como convidados e participantes do bate papo sobre a percepção do profissional de TI quanto à adequação da LGPD nas suas organizações.

Gratidão pela colaboração na construção diária do “conhecimento” e nas “ações práticas” que todos da Instituição chamada SENAC fazem quando são solicitados.

APÊNDICE C – e-Book

SENAC - Serviço Nacional de Aprendizagem Comercial

ADMINISTRAÇÃO REGIONAL DA BAHIA

Presidente do Conselho Regional
Carlos de Souza Andrade

Diretora Regional do Senac Bahia - Marina Vianna Alves de Almeida

Dados Internacionais de Catalogação na Publicação (CIP)

G943 Guia da lei geral de proteção de dados (LGPD) [recurso eletrôni-co] / Organizado por Naira Duarte. – Salvador, 2021.

40 p.: il.
Acesso em: https://intranet.ba.senac.br/Login.pdf

1. Direito á privacidade. 2.Guia. 3. Proteção de dados. 4. Segurança da Informação.I. SENAC. II. Duarte, Naira. III.Titulo .

CDD 342.810858
Elaborada pela Bibliotecária Verônica Oliveira CRB-5/1864
Serviço Nacional de Aprendizagem Comercial
SENAC

Sumário

A Lei Geral de Proteção de Dados Pessoais (LGPD)

A **Lei Geral de Proteção de Dados Pessoais (LGPD)** representa um importante avanço para o Brasil pois estabelece diretrizes importantes e obrigatórias de como devem ser tratados os dados dos brasileiros no processo de coletas, armazenamentos, alterações, descartes e proteção, prevendo punições para descumprimento em casos de vazamentos ou outras irregularidades.

A LGPD foi inspirada na **General Data Protection Regulation (GDPR)**, que entrou em vigência em 2018 na União Europeia, fortalecendo a necessidade de leis equivalentes que protegessem dados pessoais no Brasil.

Em 14 de agosto de 2018, a **Lei Geral de Proteção de Dados do Brasil (LGPD)** - Lei 13.709/2018 - foi sancionada, mas entrou em vigor em setembro de 2020, traçada em princípios éticos como a transparência, a prestação de contas e a boa-fé. A Lei visa preservar o direito constitucional à liberdade e à privacidade que todos os indivíduos brasileiros têm, assim como protegê-los de danos causados por rupturas desses direitos.

O **SENAC BAHIA** vem adotando medidas para se adequar à lei, visando garantir a privacidade de dados dos indivíduos e mitigando os riscos do uso indevido de informações pessoais contidas em suas bases digitais ou físicas.

Este e-book tem como objetivo orientar o planejamento das ações de adequação no Senac para além do cumprimento da lei, conscientizando os colaboradores em relação aos cuidados com informações que circulam na Instituição.

DÚVIDAS SOBRE A LEI?

Site: www.senac.ba.br
(Aba – Compliance)

ONDE REGISTRAR?

- lgpd.ti@ba.senac.br (público interno)
- dpo@ba.senac.br (público externo)
- comitelgpd@ba.senac.br

COMO ACESSAR MINHAS INFORMAÇÕES?

No site do Senac, por meio do CPF e ou CNPJ.

O que é a LGPD?

LGPD segundo definição da lei

"Tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."

Dados Pessoais

Artigo 5º

Dado pessoal

Qualquer informação que possa levar à identificação de uma pessoa física (nome completo, número de CPF, endereço, filiação...).

Dado pessoal sensível

Assim considerado por haver a real possibilidade de mau uso para fins discriminatórios e prejudiciais ao indivíduo, como informações relativas à raça/etnia, religião, opinião política, sexualidade e dados genéticos ou biométricos (como a biometria facial ou o DNA de um indivíduo).

Dado anonimizado

Um dado pessoal ou dado pessoal sensível passa a ser um dado anonimizado quando deixa de ser diretamente relacionado a uma pessoa. Isso acontece, por exemplo, quando um conjunto de dados sensíveis (como a autodeclaração de raça dos colaboradores de uma empresa) torna-se estatística (a porcentagem de colaboradores que se identificam com cada raça).

Banco de dados

Seja digital, seja físico, um banco de dados é qualquer conjunto de dados pessoais.

Papéis Envolvidos

Artigo 5º

Titular

Indivíduo a quem os dados pessoais sendo tratados se referem. É o soberano de qualquer assunto relacionado ao tratamento dessas informações e tem capacidade de consentir, ou não, com o tratamento.

Controlador

Responsável pelas decisões relacionadas ao tratamento dos dados pessoais. Entre outros pontos, é o controlador quem decide que dados serão tratados, de que forma e com que fim. Ele também é o principal responsável em caso de quaisquer incidentes que envolvam dados pessoais.

Operador

Quem trata os dados em nome de outra entidade, ou seja, em nome do controlador. O operador deve sempre seguir estritamente as ordens do controlador em relação ao tratamento dos dados.

Encarregado

A LGPD prevê que operadores e controladores tenham um encarregado, pessoa responsável por intermediar a comunicação entre os titulares, o controlador e a Autoridade Nacional de Proteção de Dados.

Tratamento

Artigo 5º

Tratamento

Toda e qualquer ação realizada com os dados pessoais de um titular, desde a coleta e armazenamento até o compartilhamento e uso. O ciclo completo de um dado pessoal, portanto, começa na coleta e termina na exclusão ou anonimização.

Agentes de tratamento

Tanto o operador quanto o controlador são agentes de tratamento; a responsabilidade final é sempre do controlador, mas o operador também tem obrigações a cumprir e pode ser responsabilizado em alguns casos, como quando não seguir as instruções do controlador.

Bloqueio

Suspensão do tratamento de dados, que não isenta o operador e o controlador de precisarem proteger os dados pessoais e o banco de dados em que se encontram.

Órgão de pesquisa

Especificados no texto da LGPD porque tais órgãos têm regras diferenciadas para o tratamento de dados e pedido de consentimento.

Eliminação

Exclusão de dados pessoais.

Transferência internacional de dados

Quando os dados pessoais são transferidos para fora do Brasil. É preciso assegurar que os dados terão proteção de nível equivalente ao proporcionado pela LGPD.

Uso compartilhado de dados

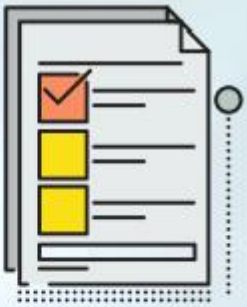
Quando os dados pessoais não ficam limitados a um único ente (privado ou público). Órgãos públicos podem compartilhar dados na prática de suas obrigações legais, enquanto entes privados podem fazê-lo mediante devido consentimento do titular.

Relatório de impacto à proteção de dados pessoais

Se houver qualquer risco de que determinado tratamento de dados possa vir a causar danos ao titular, é dever do controlador manter esse relatório. Dessa forma, em caso de incidentes, é possível entender os perigos da situação e trabalhar para mitigá-los mais rapidamente. A manutenção do relatório também visa comprovar que o tratamento que gera esses riscos recebe os devidos cuidados para evitá-los.

Consentimento

Artigo 5º



O QUE É

De acordo com o Art. 5º, Inciso XII, da LGPD, **consentimento** é a "manifestação **livre, informada** e **inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". É a permissão dada pelo titular para que determinado dado ou dados pessoais sejam tratados. Deve ser pedido de forma explícita, clara e transparente pelo operador ou controlador, e se referir a uso específico e limitado.

Livre

O titular não pode ser obrigado a dar o seu consentimento e este também não pode ser obtido de forma automática, como em caixas de textos já pré-selecionadas ou em casos em que a própria navegação na plataforma já pressupõe o aceite de todas as condições.

Informada

O titular deve compreender exatamente o que ele está consentindo, conhecer motivo e finalidade do termo antes de tomar qualquer decisão. Além disso, a informação deve ser passada de forma completa, transparente e simples.

Inequívoca

Não pode haver dúvidas sobre a verdadeira aceitação daquelas condições pelo titular e o "atendimento" deve se esforçar ao máximo para garantir a compreensão.

O ônus da prova de que o consentimento foi obtido em conformidade com a Lei é da Instituição e não do Titular.

O termo de consentimento para o uso dos dados pessoais nas bases sistêmicas da Instituição, assim como a sua solicitação, atenderá aos princípios de transparência, de forma clara e acessível, seguindo as diretrizes:

- **A finalidade –** para que a coleta dos dados será solicitada?
- **A utilização** – como serão manipulados os dados solicitados?
- **O tratamento –** como serão armazenados e descartados os dados coletados?

Com os esclarecimentos sobre o uso das informações pessoais, o **Titular** estará apto a aceitar o termo de consentimento e fornecer seus dados. Concederá permissão para que seus **DADOS (informações)** sejam utilizados pelo requisitante, autorizando seu uso para os fins especificados.

AGENTES ENVOLVIDOS NO CONSENTIMENTO

Titular

É a pessoa natural a quem se referem os dados que serão tratados (Art. 5º, Inciso V);

Controlador: é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (Art. 5º, Inciso VI);

Operador

É a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (Art. 5º, Inciso VII);

Atendente

É a "pessoa natural ou jurídica, de direito público ou privado, que realiza a coleta de dados pessoais em nome do controlador" (Art. 5º, Inciso VIII);

COMPREENSÃO QUANTO O USO DOS DADOS PESSOAIS SEGUNDO A LEI 13.709/2018.

Com a adequação à LGPD a Instituição terá que compreender a importância e o significado de consentimento e como ele pode impactar no fluxo dos procedimentos e processos que manipulam os dados pessoais de

Clientes, Alunos, Docentes, Colaboradores, Pais, Responsáveis e Fornecedores. As informações no termo de consentimento devem ser claras e apresentar os responsáveis por fornecê-las.

Para que os dados de uma pessoa possam ser tratados pela Instituição, é necessária a solicitação de consentimento para o Titular, observando o Art. 7º da LGPD - (Lei Geral de Proteção de Dados).

CONSENTIMENTO EM CASOS ESPECIAIS

A Lei Geral de Proteção de Dados (LGPD) exige que o consentimento seja obtido de forma específica e destacada. São eles:

- Dados pessoais sensíveis: o consentimento, o tratamento de dados pessoais sensíveis somente poderá ocorrer quando o titular ou seu responsável legal autorizar, de forma específica e destacada, para finalidades determinadas.
- Dados pessoais de crianças e de adolescentes: o consentimento deve ser específico e em destaque, fornecido por pelo menos um dos pais ou pelo responsável legal.
- Transferência internacional de dados pessoais: o consentimento, este deve ser específico e em destaque, com informação prévia sobre o caráter internacional da operação, distinguindo claramente de outras finalidades.

TERMO DE USO - CONSENTIMENTO E POLÍTICA DE PRIVACIDADE.

É o documento que descreve como serão usadas as informações inseridas por usuários, como dados de cadastro, itens postados e mensagens armazenadas. Deve alertar, ainda, se as informações serão compartilhadas com outras Organizações parceiras ou utilizadas em pesquisas.

Os contratos devem estar escritos em linguagem clara, precisa e, facilitar a compreensão do Cliente. As regras devem ser facilmente acessíveis.

As cláusulas que limitem direitos dos consumidores deverão ser esclarecidas e estarem acessíveis.

O importante é que o Titular tenha as opções de aceite ou recusa para dar prosseguimento à formalização do "atendimento". Em caso de quaisquer mudanças de conteúdo, os Titulares devem ser avisados para que, novamente, se manifestem sobre as novas regras.

QUANDO NÃO É PRECISO SOLICITAR O CONSENTIMENTO?

Segundo o Art. 8º da LGPD:

- Cumprimento de obrigação legal ou regulatória por parte do controlador;
- Tratamento e uso compartilhado de dados necessários para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, por parte da administração pública;
- Realização de estudos por órgão de pesquisa, garantida a anonimização dos dados pessoais, sempre que possível;
- Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual o titular seja parte, a pedido do titular dos dados;
- Exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Proteção da vida ou da integridade física do titular ou de terceiros;
- Tutela de saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- Atendimento aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
- Proteção do crédito, inclusive quanto ao disposto na legislação pertinente;
- Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

ARTIGO 6

Assim como a maior parte das leis, a LGPD prevê a boa-fé daqueles atingidos por ela. Isso é fundamental porque, quando falamos de certas regras da Lei — como a possibilidade de o titular solicitar a exclusão de seus dados ou um relatório completo

De acordo com o Art. 8º, "O consentimento poderá ser registrado pela Instituição por preenchimento de formulários, por e-mail, via sistema, entre outros."

de tratamentos —, nem sempre será possível fornecer provas absolutamente incontestáveis de que a Lei foi obedecida.

Isso também vale para o detalhamento quanto ao tratamento a ser feito, presente na solicitação do consentimento ao titular. Até que surjam evidências do contrário, o titular deve presumir que o controlador realmente está utilizando seus dados pessoais somente para os fins acordados. Caso apareçam evidências do contrário, aí sim, caberá à Autoridade Nacional de Proteção de Dados tomar as devidas providências punitivas.

"Antes de COLETAR os dados, o titular precisa ser informado de maneira clara, objetiva e transparente sobre a razão da coleta das informações.

REVOGAÇÃO DO CONSENTIMENTO E PORTABILIDADE DE DADOS

No parágrafo 5º do Art. 8º determina que o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação.

O titular também tem direito à portabilidade dos dados, ou seja, pode transferir a outro fornecedor de serviço ou produto, mediante requisição expressa a qualquer momento.

A Instituição deverá disponibilizar um canal de atendimento que permitirá ao titular dos dados revogar o consentimento de maneira simples e gratuita, e solicitar os dados que forneceu. Como também, o acesso às informações que estão sob o controle dos seus dados.

Princípios da LGPD

PARA O TRATAMENTO DE DADOS, O SENAC DEVERÁ SEMPRE OBSERVAR OS PRINCÍPIOS DA LEI:

1. DA FINALIDADE:

O Titular autoriza e concorda com o tratamento dos dados pelo Senac Bahia com a finalidade específica de armazenamento dos dados pessoais para oferta de serviços do seu portfólio.

2. DA ADEQUAÇÃO:

O Titular tem ciência de que o tratamento dos dados pessoais atende à finalidade exposta pelo provedor de serviços do Senac Bahia.

3. DA NECESSIDADE:

O Titular autoriza o tratamento dos dados pessoais com o objetivo de permitir comunicação referente aos serviços do Senac Bahia.

4. DO CADASTRO E DO LIVRE ACESSO:

Titular é de uso estritamente pessoal e não deverá ser utilizado por terceiros, sendo que a guarda e sigilo das informações contidas no formulário serão utilizadas de forma diligente, de modo a não os colocar à disposição de terceiros. O Titular tem ciência de que poderá consultar, atualizar ou excluir os dados pessoais cadastrados a qualquer tempo.

5. DA QUALIDADE E VERACIDADE DOS DADOS:

O Titular concorda em fornecer informações verdadeiras, exatas, e completas, responsabilizando-se pelo cadastro das informações que serão utilizadas pelo Senac

Bahia, bem como por informar qualquer modificação destas informações, mantendo as informações sempre atualizadas. Caso o Titular se utilize de informações falsas ou desatualizadas, o Senac Bahia se resguarda ao direito de cancelar e encerrar o acesso do usuário aos seus serviços.

6. DA TRANSPARÊNCIA:

Toda informação tratada pela empresa precisa ser de forma clara, precisa e verdadeira, além de facilmente acessível ao titular.

7. DA SEGURANÇA:

O Senac Bahia realizará o tratamento dos dados pessoais do Titular para a finalidade acima exposta, ficando esta responsável em adotar as medidas técnicas e administrativas aptas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

8. DA PREVENÇÃO:

O Senac Bahia adotará as medidas preventivas para a manutenção da proteção e segurança dos dados pessoais do Titular.

9. DA NÃO-DISCRIMINAÇÃO:

Os dados pessoais disponibilizados pelo Titular ao Senac Bahia, em hipótese alguma, serão utilizados para fins discriminatórios, ilícitos ou abusivos.

10. DA RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS:

O Titular poderá requisitar informações relacionadas ao nível de governança da TI pelo e-mail da Controladoria da Instituição dpo@ba.senac.br ou lgpd.ti@ba.senac.br.

Modelo de Termo de Consentimento

Termo de Consentimento Senac Bahi

Prezado (a) *titular de dados pessoais*,

O presente Termo de Ciência e Consentimento ("Termo") tem como finalidade o registro da manifestação inequívoca, por meio do qual o *titular dos direitos pessoais ("Titular")* concorda com o tratamento de seus dados pelo Senac Bahia.

Assim, aceitando o presente Termo, o *Titular* consente e concorda que o Senac Bahia adote as melhores decisões para o tratamento das informações pessoais. Caso o Termo de Ciência não seja aceito, o titular não poderá prosseguir com a realização do Questionário de Assessment LGPD.

Ainda, *o Titular* declara neste ato que possui capacidade legal e detém as autorizações e permissões necessárias para realizar o presente cadastro e utilizar os serviços disponibilizados pelo Senac Bahia.

Quando é aplicável?

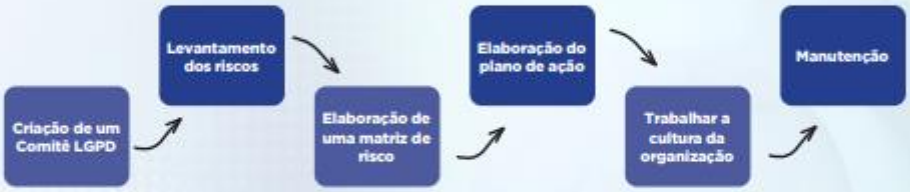
APLICÁVEL

A Lei se aplica às pessoas **físicas e jurídicas de direito público e privado** que venham realizar qualquer tipo de tratamento de dados, bem como às pessoas físicas que tenham seus dados coletados por meio físico ou digital.

NÃO APLICÁVEL

A Lei não se aplica ao tratamento de dados realizado para fins **exclusivamente particulares e não econômicos,** para fins exclusivamente jornalísticos, artísticos, acadêmicos, de segurança pública, de defesa nacional, de segurança do Estado ou de atividade de investigação ou repressão de infrações penais, entre outras, conforme expressamente disposto no artigo 4º da lei 13.709/2018.

Fases para adequação



EQUIPES ENVOLVIDAS:

- Encarregado (DPO): Responsável pela mediação entre empresa, titulares e ANPD
- Comitê da LGPD: Órgão de deliberações.
- Equipe da TI: Responsáveis pela Segurança da Informação da Instituição.

Adequação à LGPD

A Lei Geral de Proteção de Dados não foi sancionada para penalizar e sim para assegurar ao indivíduo o controle sobre seus dados e o direito à privacidade!

1. CRIAÇÃO DE UM COMITÊ LGPD AO COMPLIANCE ORGANIZACIONAL.

O termo "compliance" diz respeito a "estar em conformidade com". No âmbito organizacional é usado para garantir que os processos e procedimentos da organização estejam sempre de acordo com leis e obrigações. O comitê LGPD vai garantir que toda a organização - colaboradores, diretoria e parceiros - esteja de acordo com a lei 13.709/2018.

O compliance para a LGPD não deve ser um assunto somente de TI ou do Jurídico. A LGPD, diz respeito aos dados sensíveis de pessoas físicas e, na Instituição Senac muitas áreas lidam com esses dados. Por isso, é importante envolver todas as áreas, para entender em cada uma delas, como estão sendo tratados esses dados sensíveis, quem tem acesso a eles, como são armazenados, entre outros. O primeiro passo do guia de implementação da lei, é a criação de um comitê multidisciplinar, assim terá maiores condições de entender quais são os riscos reais que a Instituição pode estar exposta e como resolvê-los. Será este comitê responsável por levantar:

1. As questões legais;
2. Os requisitos técnicos;
3. As medidas e protocolos de segurança;
4. Investimentos em Hardware e Software;
5. Reformulação dos pedidos de cadastros;
6. Adoção de boas práticas
7. Contratação de serviços e profissionais de TI;
8. Conscientização da equipe interna.

Nomear um Responsável Geral pelo comitê de LGPD.

O membro responsável deverá acompanhar o andamento de todo o processo, desde o levantamento das informações, priorização e execução do plano de ação. Indica-se também a nomeação de um Responsável pela Execução, que irá acompanhar a execução do plano de ação elaborado. Além disso, pode convidar um representante de cada área, para acompanhar o processo e ser responsável por repassar as informações à sua área e, além disso irá contribuir com o processo de levantamento dos riscos e a manutenção da gestão.

2. LEVANTAMENTO DOS RISCOS.

Identificar os principais GAP's da Instituição e os Riscos identificados em cada processo, são essenciais para priorizar as ações de adequação à lei. A partir dessa ação será possível entender onde estão os principais pontos de atenção em relação à LGPD. O levantamento de riscos, deverá repassar por todos os setores da Instalação elencando detalhes sobre todos os dados sensíveis usados em cada atividade. Deve envolver um responsável por cada setor, onde ele deverá repassar por todas as atividades da sua área, levantando se são usados dados sensíveis e quais são, como são usados, armazenados e diversas outras informações.

Na etapa de levantamento de riscos, também será possível entender sobre terceiros, fornecedores, processos e contratos que podem estar sujeitos a riscos perante a LGPD.

"Avaliar e ajustar todos os contratos com fornecedores, parceiros, clientes e colaboradores. Incluir nas cláusulas protetivas em relação a LGPD, sobre posse e tratativa dos dados sensíveis compartilhados. "

2.1. Fornecedores

Avaliar com quais fornecedores estão sendo compartilhados dados pessoais e se eles também estão se adequando a lei. Além disso, quais as medidas estão sendo adotadas para proteção desses dados.

2.2. Infraestrutura

Avaliar as medidas de segurança e proteção dos dados que estão sendo usadas na Instituição e seu nível de eficiência. Entender onde os dados são armazenados e as práticas de segurança que estão sendo usadas, nas políticas e regramentos de senhas, firewall, antivírus, entre outros.

2.3. Revisão de processos

Reavaliar todos os processos em que existam dados pessoais. Nessa análise entenda o fluxo dos dados, desde o momento em que a Instituição passa a ter a posse dele até o momento de sua eliminação. Isso envolve atualização, compartilhamento, necessidade de uso, quem tem acesso, entre outras.

Recomenda elaborar um modelo de planilha onde vai encontrar um passo-a-passo descritivo para realizar o levantamento dos dados sensíveis na Instituição apenas para preenchimento, este guiará no levantamento de riscos em cada área.

3. ELABORAÇÃO DE UMA MATRIZ DE RISCO.

Após levantar os riscos, o próximo passo é fazer uma priorização quanto aos maiores impactos diagnosticados na Instituição e por isso deve ter preferência no Plano de Ação.

Os riscos identificados no passo anterior devem ser inseridos em uma matriz que vai estimar a probabilidade daquele risco acontecer e o impacto para o negócio. Para realizar essa priorização, deverá atribuir notas de 1 a 5 com associação ao nível de risco classificados como Extremo, Elevado, Moderado, Leve ou Baixo. Assim, conseguirá começar o plano de ação pelos riscos que mais irão afetar.

Além disso, é necessário criar também uma Planilha de Matriz de Riscos que irá ajudar nessa priorização.

4. ELABORAR PLANO DE AÇÃO.

Montar o Plano de Ação, observando os Riscos Extremos e de níveis Elevados que foram identificados na Matriz de Riscos. Deve-se fazer uma análise bem detalhada, pois caso algum risco não seja classificado como Extremo ou Elevado, mas tenha impacto grave sobre a Instituição, ele também deverá ser considerado no Plano de Ação. Nesse momento, o Responsável pela Execução do plano deverá entrar com as ações para acompanhar o processo que devem mitigar os riscos.

Além dos riscos priorizados, existem alguns "entregáveis" exigidos pela lei, portanto é importante que estejam no plano. Esses documentos são importantes tanto para guiar as ações internas da Instituição, quanto para prestação de contas junto à ANPD (Autoridade Nacional de Proteção de Dados), caso solicitado.

4.1. Mapa de dados Organizacional

Criar o Mapa de Dados que se trata de um documento sigiloso, apenas para uso interno. Ele deverá explicar quais são os dados utilizados pela Instituição, qual a finalidade e como são usados.

"Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei."

4.2. Política de privacidade

Elaborar uma Política de Privacidade institucional sobre como os dados são coletados, armazenados e tratados.

Na Política de Privacidade deve conter informações essenciais, como:

- informações sobre a Instituição responsável pelo tratamento dos dados pessoais e com as respectivas finalidades do tratamento;
- esclarecimento das bases jurídicas quanto ao tratamento;
- divulgação dos prazos de retenção dos dados pessoais;
- informações do contato do Data Protection Officer (DPO) ou encarregado de proteção de dados da organização.

4.3. DPO

Nomear um DPO, que será o guardião da compliance em relação à LGPD na Instituição. O DPO será o responsável por disseminar a cultura de proteção de dados na organização, além de criar normas e procedimentos adequados à lei. Algumas atividades relacionadas ao DPO:

Receber solicitações sobre o assunto;

Interagir com a autoridade nacional do assunto caso necessário;

Realizar treinamento sobre a LGPD internamente.

"**A legislação se fundamenta nos valores como:**

- O respeito à Privacidade;
- Autodeterminação Informativa;
- A liberdade de expressão, informação, comunicação e de opinião;
- A inviolabilidade da intimidade, da honra e da imagem;
- Ao desenvolvimento econômico, tecnológico e a inovação. "

4.4. Portal do Consentimento

Criar um "Portal de Consentimento". No Portal, o público da Instituição poderá ter acesso aos seus dados, pedir revisões, exclusões, entre outros. Isso será necessário, visto que a palavra que resume a LGPD é "consentimento". A Instituição pode reter qualquer dado sensível desde que tenha o consentimento ou alguma base legal que valide essa posse. Após o consentimento, o titular desses dados deve ter transparência indicando os dados retidos pela organização, se está atualizado e, também, deve ter direito de retirar esse consentimento.

5. TRABALHAR A CULTURA DA ORGANIZAÇÃO

A Privacidade deve-se tornar um assunto comum dentro da Instituição. Para isso, é importante que a conscientização dos Colaboradores sobre como a organização está lidando com o tema e como também compartilha as práticas que garantem a integridade dos dados.

Sugestões:

a. Incluir o assunto no onboarding dos novos Colaboradores, ou seja, no treinamento e/ou integração dos funcionários recém-contratados;

b. Criar um manual de boas práticas para segurança de dados ou incluir o assunto no código de conduta da Instituição, mas a ideia é disseminar quais são essas práticas, então use dos meios de comunicação direta com os colaboradores e garanta que eles irão acompanhar;

ATENÇÃO COM AS PUNIÇÕES

- Processos, sanções administrativas e advertências;
- Multas de até 2% do seu faturamento;
- Apreensão de dados;

c. Realizar treinamentos com a equipe sobre a LGPD e a política de privacidade da Instituição. Muitos colaboradores podem não saber do que se trata essa nova lei, então é importante que todos estejam cientes sobre a atuação e o seu papel para a adequação à lei;

d. Fazer campanhas de comunicação interna destacando os principais pontos da LGPD e da política da Instituição.

6. MANUTENÇÃO

Após a implementação da LGPD, é essencial garantir a manutenção das boas práticas adotadas na organização. Para tal, o DPO será o elo forte na manutenção das políticas implantadas.

"Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição. "

DIREITO DOS TITULARES DOS DADOS

- Conhecimento do processo de tratamento de dados pessoais;
- Acesso total aos seus dados sob custódia da empresa;
- Anonimização;
- Possibilidade de solicitação de portabilidade dos dados para outras empresas;
- Exclusão dos dados a qualquer tempo;
- Informação sobre compartilhamento de dados;
- Revogação do consentimento.

Bases Legais

BASES LEGAIS PARA TRATAMENTO DE DADOS PESSOAIS NA LGPD

O propósito da base legal é determinar as situações e condições para tratamento de dados pessoais e evitar a sua coleta e seu uso indiscriminado. As bases legais serão atribuídas a cada uma das atividades de tratamento de dados pessoais nas organizações. Por exemplo, na venda de um produto, a instituição coleta os dados pessoais para fazer atividades relacionadas à venda e entrega, como nome, endereço, contatos e cartão de crédito.

Tratamento de dados realizado no Brasil.

Tratamento de dados que tenha por objetivo a oferta ou fornecimento de bens e/ou serviços no Brasil.

Dados que tenham sido coletados no território nacional.

Dados pessoais são informações relativas a uma pessoa viva e compreendem dados pessoais (indivíduos identificados ou identificáveis)

Também constituem dados pessoais o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa.

Todo dado pessoal só pode ser tratado se seguir um ou mais critérios definidos pela

LGPD, mas, dentro do conjunto de dados pessoais, há ainda aqueles que exigem um pouco mais de atenção: são aqueles "sobre crianças e adolescentes"; e aqueles "sensíveis", dados sobre origem racial ou étnica, saúde, dados genéticos ou biométricos, convicção religiosa, orientação sexual e filiação a sindicatos ou organização filosófica ou política;

Os 12 principais Direitos Garantidos pela LGPD aos Titulares dos Dados Pessoais.

1. Acesso aos dados
2. Informação de dados pessoais compartilhados
3. Objeção ao Tratamento dos dados
4. Não Consentimento
5. Restrição do tratamento dos dados
6. Revogação do Consentimento
7. Revisão de decisão automatizada
8. Retificação
9. Portabilidade
10. Eliminação
11. Peticionar contra o Responsável
12. Inversão de ônus da prova

Quem fiscaliza

A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), CRIADA PELA LEI Nº 13.853/2019, ATUARÁ COMO UMA AGÊNCIA REGULADORA.

Criada em 2018 e sancionada em 2019, a ANPD (Autoridade Nacional de Proteção de Dados) é o órgão federal responsável por fiscalizar e aplicar a LGPD, a Lei Geral da Proteção de Dados. A criação de uma autoridade independente é necessária para que empresas que têm acesso às informações pessoais cumpram a legislação e possam ser auditadas nos casos em que não observarem o devido tratamento destes dados, além disso, uma autoridade nacional poderá deliberar sobre questões que não ficaram tão claras ou que possam gerar algum tipo de questionamento quanto à sua interpretação.

Autoridade nacional: a Autoridade Nacional de Proteção de Dados (ANPD) será o órgão responsável por implementar e gerenciar as regras da LGPD, garantindo que a Lei seja cumprida. A ANPD também é responsável por realizar auditorias, assim como aplicar as devidas sanções em casos comprovados de descumprimento da Lei.

Sanções

Artigo 52º

1	2	3	4	5
ADVERTÊNCIA	**DIVULGAÇÃO**	**MULTA**	**BLOQUEIO/ ELIMINAÇÃO**	**SUSPENSÃO PARCIAL OU TOTAL**
Empresas poderão ser advertidas caso desobedeçam à Lei. As advertências exigirão planos de ação com prazo definido para adoção de medidas corretivas.	As empresas serão obrigadas a divulgar publicamente casos de vazamento de dados pessoais, para que os titulares e a sociedade saibam que os dados foram comprometidos.	Em casos graves dedescumprimento da Lei, serão aplicadas multas de até 2% do faturamento, limitadas a 50 milhões de reais por infração.	Em casos de solicitação por parte da ANPD devido a alguma infração, haverá a suspensão temporária do tratamento ou a eliminação de dados pessoais de determinado titular.	Poderá haver a suspenção do Banco de Dados ou o exercício do tratamento de dados até que se desenvolva mecanismos de segurança eficientes.

O operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador. A Autoridade Nacional de Proteção de Dados (ANPD), criada pela Lei nº 13.853/2019, atuará como uma agência reguladora.

Capítulos da lei

1 – Disposições Preliminares

2 – Do Tratamento dos Dados Pessoais

3 – Dos Direitos dos Titulares

4 – Do Tratamento de Dados Pessoais Pelo Poder Público

5 – Da Transferência Internacional de Dados

6 – Dos Agentes de Tratamento de Dados Pessoais

7 – Da Segurança e das Boas Práticas

8 – Da Fiscalização

9 – Da Autoridade Nacional de Proteção de Dados (ANPD e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade).

10 – Disposições Finais e Transitórios.

01	02	03	04	05	06	07	08
09	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	37	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64
65							

Artigos sem necessidade de ação, apenas processo de informação na fiscalização.

Artigos focados em segmentos específicos (transferência internacional, governos, crianças e adolescentes.

Artigos de caráter opcional ou sem obrigatoriedade.

Artigos Obrigatórios

Considerações finais

Neste material, você pode compreender melhor o que é a **Lei Geral de Proteção de Dados Pessoais**. A fim de prevenir a violação e o uso abusivo de dados, as novas regras exigem adequações operacionais e, para o **Senac**, é importante a sua aplicação, de forma clara e direta, de modo que as informações sejam aceitas e compreendidas pelos envolvidos.

A adequação à **LGPD** é uma preocupação de todas as áreas da Instituição e esse processo deve ser feito em três fases: levantamento, execução e monitoramento.

Esperamos que o conhecimento gerado neste e-book contribua para o desempenho de suas atividades.

Bom trabalho!

Referências

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 22 abr. 2021.

Escape das "armadilhas" da LGPD. Disponível em: https://www.serpro.gov.br/lgpd/noticias/escape-armadilhas-lgpd-lei-geral-de-protecao-de-dados-pessoais. Acesso em 15 mai.2021.

Lei Geral de Proteção de Dados Pessoais – LGPD. LEI Nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em 03 mar.2021.

O que muda com a LGPD. Disponível em: <https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd>. Acesso em 14 mai.2021.

Termo de consentimento do uso de dados da LGPD. Disponível em: <https://documentacao.senior.com.br/lgpd/manual-do-usuario/termo-de-consentimento.htm>. Acesso em 16 mai.2021.

Senac Fecomércio Sesc

APÊNDICE D – Resumo - Lei de Proteção de Dados e de Privacidade - visão histórica.

Lei/ Decreto/ Conselho/ Conversão e Ato	Países	Ano
Ato de Justiça da Paz de proteção contra peeping Toms e bisbilhoteiros.	Inglaterra	1361
Lei de Acesso aos Registros Públicos.	Suiça	1776
Declaração dos Direitos do Homem e do Cidadão.	França	1792
Decreto de proibiu a publicação de fatos particulares sobre indivíduos.	França	1858
1º artigo - Direito à privacidade foi o resultado direto de tecnologia e estilo de vida – de Samuel Warren e Louis Brandeis.	Estados Unidos	1890
Declaração Universal do Homem Direitos forneceram uma referência de privacidade moderna.	ONU	1948
1º órgão supervisor – Comissão Europeia de Direitos Humanos e o Tribunal Europeu dos Direitos Humanos	União Europeia	1950
Declaração Americana dos Direitos e Deveres do homem.	Estados Unidos	1965
1ª Lei de Proteção de Dados – Alemanha.	Alemanha	1970
1ª Lei Nacional de Proteção de Dados – Ato de Hesse.	Suécia	1973
Ato de Privacidade.	Estados Unidos	1974
Ato Federal de Proteção de Dados.	Alemanha	1977
Ato de Registros Privados.	Dinamarca	1977
Lei Francesa de Processamento de Dados.	França	1978
Lei Datenschutzgesetz (DSG).	Áustria	1978
1ª Conselho Internacional – Conselho da Europa (COE).	União Europeia	1980
1ª Convenção Proteção de Pessoas - relação ao processamento automático de Dados Pessoais e a Organização para Cooperação Econômica e Diretrizes de Desenvolvimento (OCDE) Proteção de privacidade e fluxos de transferência de dados pessoais.	União Europeia	1980
Lei de Proteção à Privacidade	Estados Unidos	1980
Lei Austrália – Apps – Australian Privacy Principles	Austrália	1988
Diretiva na Proteção de Dados – estabelece Normas e Processamento específicos para a utilização de dados pessoais.	União Europeia	1995
1ª Diretiva de Telecomunicações.	União Europeia	1997
Lei Gramm-Leach-Bliley .	Estados Unidos	1999
Lei PIPEDA – Personal Information Protection And Electronic Documents Act	Canada	2000
Lei 21 Tecnologia da Informação – Genérica	Índia	2000
Lei de Privacidade Eletrônica 3.471	Grécia	2006
Lei 709	Malásia	2010
Lei de Acesso a Informação – LAI 12.527/2011	Brasil	2011
Lei de Retenção de Dados 3.917	Grécia	2011
Lei 1.581/12	Colômbia	2012
Lei Nacional nº 10.173	Filipinas	2012
Marco Civil da Internet – Lei 12.965/2014.	Brasil	2014
Lei Federal de Proteção de Dados Pessoais	México	2014
Lei 2 de Proteção de Dados (2016-1321)	França	2016
Lei Federal de Proteção de Dados – BDSG	Alemanha	2017

Lei GB/T 35273-2017 – Lei Tecnologia Da Informação	China	2017
Emenda APPI de 2017 - Lei 57 de 2003	Japão	2017
Lei Dinamarquesa de Proteção de Dados.	Dinamarca	2018
Lei HE 9/2018 VP	Filandia	2018
Lei 11 –Proteção de dados e Transações Eletrônicas	Indonesia	2018
Lei 90	Islândia	2018
Lei de Privacidade de 2018	Nova Zelândia	2018
Lei 25.326 - Lei De Proteção De Dados	Argentina	2020