UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Faculdade de Ciências e Letras
Campus de Araraquara - SP

JACKSON GOMES SOARES SOUZA

PROTEÇÃO DE DADOS PESSOAIS NA GESTÃO EDUCACIONAL: ESTUDO DE CASO SOBRE A LGPD NO CONTEXTO DO IFSP

ARARAQUARA – SP
2023

JACKSON GOMES SOARES SOUZA

PROTEÇÃO DE DADOS PESSOAIS NA GESTÃO EDUCACIONAL: ESTUDO DE CASO SOBRE A LGPD NO CONTEXTO DO IFSP

Tese de Doutorado, apresentado ao Conselho, Programa de Pós-Graduação em Educação Escolar da Faculdade de Ciências e Letras – Unesp/Araraquara, como requisito para obtenção do título de Doutor em Educação Escolar.

Linha de pesquisa: Política e Gestão Educacional

Orientador: Prof. Dr. Francisco Rolfsen Belda

Coorientador: Prof. Dr. José Luís Bizelli

ARARAQUARA – SP
2023

S729p

Souza, Jackson Gomes Soares
Proteção de dados pessoais na gestão educacional : estudo de caso sobre a LGPD no contexto do IFSP / Jackson Gomes Soares Souza. -- Araraquara, 2023
78 p. : il., tabs.

Tese (doutorado) - Universidade Estadual Paulista (Unesp), Faculdade de Ciências e Letras, Araraquara
Orientador: Francisco Rolfsen Belda
Coorientador: José Luís Bizelli

1. Proteção de dados pessoais. 2. LGPD. 3. Tratamento de dados pessoais. 4. Ambientes para ensino. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de Ciências e Letras, Araraquara. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

JACKSON GOMES SOARES SOUZA

PROTEÇÃO DE DADOS PESSOAIS NA GESTÃO EDUCACIONAL: ESTUDO DE CASO SOBRE A LGPD NO CONTEXTO DO IFSP

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Educação Escolar da Faculdade de Ciências e Letras – UNESP/Araraquara, como requisito para obtenção do título de Doutor em Educação Escolar.

Linha de pesquisa: Política e Gestão Educacional
Orientador: Prof. Dr. Francisco Rolfsen Belda
Coorientador: Prof. Dr. José Luís Bizelli

Data da defesa: 23/06/2023

MEMBROS COMPONENTES DA BANCA EXAMINADORA:

Presidente e Orientador:	Prof. Dr. Francisco Rolfsen Belda Universidade Estadual Paulista "Júlio De Mesquita Filho" – Unesp.
Membro Titular:	Prof. Dr. Silvio Henrique Fiscarelli Universidade Estadual Paulista "Júlio De Mesquita Filho" – Unesp.
Membro Titular:	Prof. Dr. Carlos Hideo Arima Centro Estadual de Educação Tecnológica Paula Souza – Ceeteps.
Membro Titular:	Prof. Dr. José Anderson Santos Cruz Programa de Educação Continuada em Economia e Gestão de Empresas (PECEGE/ESALQ/USP MBAs)
Membro Titular:	Profa. Dra. Grazielle Nayara Felício Silva Instituto Federal de Educação, Ciência e Tecnologia de São Paulo

Local: Universidade Estadual Paulista
Faculdade de Ciências e Letras
UNESP – Campus de Araraquara

Àqueles que apesar de todas as adversidades sempre acreditaram que eu seria capaz de atingir meus objetivos.

AGRADECIMENTOS

A Deus.

À ciência.

Às mães e aos pais.

Aos amigos e amigas.

A todas as pessoas que me auxiliaram na construção desta jornada, mestres, professoras, orientadores e orientadoras, coorientadores e coorientadoras de Programas de Pós-Graduação.

Às instituições públicas de ensino e pesquisa.

“Ainda que a prova te pareça invencível ou que a dor se te afigure insuperável, não te retires da posição de lidador [...]”
(XAVIER, 1956, p. 141).

RESUMO

Considerando-se a intensificação na utilização de dados pessoais em ambientes presenciais e remotos, assim como a preocupação com a proteção de dados, esta pesquisa básica aplicada tem por objetivo verificar, conforme os instrumentos normativos de proteção de dados pessoais adotados numa instituição pública de ensino tecnológico, os atuais desafios para o desenvolvimento de políticas e procedimentos a partir da vigência da Lei Geral de Proteção de Dados Pessoais (LGPD). Para tanto, procede-se ao estudo de caso, por meio da aplicação de questionários estruturados a docentes e gestores, cujas respostas foram coletadas, tabuladas e tratadas estatisticamente, de modo que os critérios analíticos de interpretação permitiram embasamento científico adequado. Os resultados obtidos pela análise dos dados apresentam a relação entre o contexto institucional e as dimensões de proteção de dados pessoais previstos pela LGPD, assim como a necessidade de adequações à cultura de privacidade da instituição, a partir da implementação de um programa de governança que promova ações educativas de conscientização e estabeleça um vínculo de comprometimento e confiança para com o titular de dados, na busca do contínuo alinhamento entre o ecossistema organizacional e sua segurança.

Palavras-chave: Proteção de dados pessoais; LGPD; Tratamento de dados pessoais; Ambientes para ensino.

ABSTRACT

Considering the intensification in the use of personal data in remote attendance environments as well as the concern with data protection, this basic applied research aims to verify, according to data protection regulatory instruments adopted by a public institution of technological education, the current challenges for the development of policies and procedures according to the General Data Protection Law (GDPR). For this purpose, a case study is conducted through the application of structured questionnaires to professors and managers, whose answers were collected, tabulated, and treated statistically, through which analytical interpretation criteria enabled adequate information analysis and scientific basis. Results obtained from the data analysis state the link between institutional context and GDPR's personal data protection dimensions, as well as the need to adjust the institution's privacy culture by implementing a governance program that promotes educational awareness actions of commitment and trust within the data subject, aiming continuous alignment between the organization ecosystem and its security.

Keywords: Personal data protection; GDPR; Personal data processing; Learning environments.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
CEPD	Comitê Europeu para a Proteção de Dados
CETIC.BR	Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação
CGI.BR	Comitê Gestor da Internet no Brasil
CONEP	Conselho Nacional de Ética em Pesquisa
DPO	*Data Protecion Officer*
EPR	Ensino Presencial Remoto
EC115	Emenda Constitucional nº 115
EDPB	*European Data Protection Board*
GDPR	*General Data Protection Regulation*
GT29	Grupo de Trabalho do Artigo 29
HTTP	*Hype Text Tranfer Protocol*
IEML	*Information Economy Meta Language*
IFSP	Instituto Federal de Educação, Ciência e Tecnologia de São Paulo
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
NIC.BR	Núcleo de Informação e Coordenação do Ponto BR
SUAP	Sistema Unificado de Administração Pública
TICs	Tecnologias de Informação e Comunicação
URL	*Uniform Resource Locator*
WP29	*Article 29 Working Party*
WWW	*World Wide Web*

SUMÁRIO

1 INTRODUÇÃO

A proteção de dados pessoais ganhou destaque mais recente, inicialmente na União Europeia, com o surgimento do Regulamento Geral de Proteção de Dados – do inglês, *General Data Protection Regulation (GDPR)* 2016/679 –, estabelecendo desde 2018 regras de implementação obrigatórias relativas à proteção das pessoas, direitos e liberdades fundamentais e, em particular, o seu direito à proteção dos dados pessoais no que diz respeito ao tratamento de dados e à livre circulação (EUROPEAN COMMISSION, 2018).

Dados são facilmente estruturados, obtidos por máquinas, frequentemente quantificados, facilmente transferíveis, simples observações sobre o estado do mundo; enquanto informação seriam dotados de relevância e propósito, requerendo unidade de análise, consenso em relação ao significado e mediação humana (DAVENPORT, 1998).

Existem diversas tecnologias ao nosso redor, logo, o uso de ferramentas digitais para ensino e aprendizagem está diretamente ligado ao tratamento de dados pessoais que as instituições armazenam e usam. Dessa forma, é necessário que elas adotem políticas de proteção conforme a legislação vigente.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº. 13.709, de 14 de agosto de 2018, regulamenta o tratamento de informações pessoais, inclusive em meios digitais, por indivíduos ou entidades de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade do indivíduo (BRASIL, 2018). Esta lei é semelhante à nova promulgação da Emenda Constitucional nº. 115 (EC115), publicada em 11 de fevereiro de 2022 na Seção 1, Edição 30, Página 2 do Diário Oficial da União, onde a Constituição Federal de 1988 contempla também os direitos e garantias fundamentais à proteção de dados, inclusive por meios digitais (BRASIL, 2022).

De acordo com Mendes e Doneda (2018), a LGPD inaugura um marco normativo importante para a sociedade da informação e para a proteção de dados pessoais, pois considera que o tratamento de dados deve apoiar-se em bases normativas que o afiancem. Todavia, a efetiva implementação da lei esbarra-se em entraves, como a necessidade de mudança de aspectos culturais e institucionais, que prospectem a compreensão sobre a seriedade de proteção jurídica para os dados pessoais.

> Quase todas as organizações tratam de dados pessoais (DP). Além disso, a quantidade e os tipos de DP tratados estão aumentando, assim como o número de situações em que uma organização precisa cooperar com outras organizações em relação ao tratamento de DP. A proteção da privacidade no

> contexto do tratamento de DP é uma necessidade da sociedade, bem como um tópico de legislação e/ou regulamentação dedicada em todo o mundo (ABNT, 2019, p. ix).

Diante disso, entende-se que é necessário analisar como são administrados os protocolos de proteção de dados pessoais em um *campus* pertencente a uma organização de ensino pública sob a legislação recente. Nesse trajeto, é possível questionar, quais adequações são necessárias para que os protocolos de proteção de dados pessoais presentes no campus da instituição atendam à Lei Geral de Proteção de Dados?

Cabe pontuar a ausência de pesquisas sobre o tema. A partir das palavras chaves deste estudo e da sigla LGPD, durante o mês de junho de 2023, foi realizado levantamento no Portal de Periódicos da CAPES para aferir a produção científica sobre o tema. No que diz respeito à sigla LGPD, foi possível identificar a quantidade de 153 artigos revisados por pares. No que tange às palavras chaves do estudo, a mensuração identifica 379 artigos para o assunto proteção de dados pessoais; 551 trabalhos para as palavras tratamento de dados pessoais e 7.289 artigos para as palavras ambientes para ensino. Esse levantamento propiciou analisar que o tema desta tese é pouco problematizado e explorado no mundo acadêmico.

Em relação à produção científica no âmbito de programas de mestrado e doutorado, observou-se, a partir do Portal Capes de teses e dissertações, um número incipiente de teses, defendidas entre 2021 e 2022. O levantamento permitiu mensurar sete teses, nas quais cinco foram defendidas na área do direito, uma na área de comunicação e informação, uma na engenharia e uma na área interdisciplinar. Destaca-se a ausência de teses que debatem o tema da LGPD e proteção de dados pessoais em contextos educacionais e defendidas no âmbito de programas relacionados à Educação, o que traz um ineditismo ao estudo realizado nesta tese, defendida no Programa de Pós-Graduação em Educação Escolar da Unesp Araraquara.

O objetivo desta pesquisa é analisar as normas de proteção de dados pessoais adotadas em uma instituição pública de ensino tecnológico e os atuais desafios para o desenvolvimento de políticas e procedimentos a partir da vigência da LGPD. A instituição em questão integra a Rede de Educação Profissional, Científica e Tecnológica (REPCT), instituída pela Lei nº. 11.892, de 29 de dezembro de 2008, formada pelos Institutos Federais de Educação, Ciência e Tecnologia presentes em todos os estados brasileiros, com estrutura *multicampi* e oferta de educação profissional e tecnológica em todos os seus níveis e modalidades, assim como em ambientes virtuais por meios digitais de comunicação (BRASIL, 2008).

Eliezer Pacheco (2011), um dos idealizados das concepções e diretrizes que norteiam o desenho dos Institutos Federais, apresenta que estes são uma revolução na Educação

Profissional e Tecnológica. A Rede Federal de Educação, Ciência e Tecnologia tem sua arquitetura embrionária datada do início datado de 1909, com a criação de dezenove Escolas de Aprendizes Artífices pelo presidente da época, Nilo Peçanha. Sua trajetória histórica perpassa por diferentes nomenclaturas e desenhos, como, por exemplo, os Centros Federais de Educação Tecnológica (CEFET), que são transformados nos Institutos Federais de Educação, Ciência e Tecnologia em quase todas as unidades federativas do país, exceto Rio de Janeiro e Minas Gerais (CAIRES e OLIVEIRA, 2018).

A Plataforma Nilo Peçanha apresenta, dentre vários elementos, os indicadores de gestão e dados gerais das instituições que compõem a Rede Federal. Com referência ao ano de 2022, é possível caracterizar em dados gerais que a REPCT hoje possui 656 unidades e 1.513.075 matrículas, números que demonstram a grandiosidade desta rede.

Os Institutos Federais estão alocados em todas as unidades federativas do país, nos quais são ofertados diversos cursos, que perpassam da Educação Básica (em cursos de ensino médio integrados ao técnico, por exemplo) à Educação Superior, em cursos de bacharelados, licenciaturas, tecnológicos e pós-graduação lato e *stricto senso.* Essa caracterização corrobora para a definição dada por Frigotto (2018, p. 7), ao afirmar que os IFs “desde sua criação [...] expressam a mais ampla e significativa política no campo da educação pública”.

Os Institutos Federais de Educação, Ciência e Tecnologia ofertam educação profissional e tecnológica em diversos níveis e modalidades, assim como o Ensino Presencial Remoto (EPR) em ambientes virtuais, por meios digitais de comunicação. Com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, a LGPD dispõe sobre a proteção de dados pessoais armazenados e utilizados pelas instituições, que, por sua vez, devem adotar políticas de proteção baseadas em legislação específica.

A pesquisa se justifica pelo aumento do uso de ambientes virtuais e pelos cuidados com os dados pessoais em uma instituição pública de ensino, a fim de verificar, em um de seus *campi*, os atuais desafios para o desenvolvimento de políticas e procedimentos a partir da vigência da LGPD. Além disso, este estudo tem relevância para contribuir no âmbito da Política Educacional, pois permite elucidar trajetos tangentes à aplicabilidade e implementação da Lei Geral de Proteção de Dados Pessoais e prevê a proposição de criação de um programa educacional de conscientização, propiciando, também, em termos de trabalhos futuros, aplicações potenciais da pesquisa em instituições de ensino. Cabe mencionar que esta pesquisa

foi autorizada pelo Comitê de ética em Pesquisa da Unesp[1] e do Instituto Federal de São Paulo (IFSP)[2], conforme os anexos A e B desta tese, tendo como participantes da pesquisa docentes e gestores.

No âmbito da instituição pesquisada observa-se o uso constante de ferramentas que denotam o acesso aos dados pessoais de estudantes e servidores, como o Sistema Unificado de Administração Pública (SUAP), que gerencia todas as ações no âmbito do ensino, pesquisa, extensão e gestão. Seu uso promove o tratamento permanente de dados pessoais, considerando, por exemplo, desde o gerenciamento de acesso e alterações de informações da comunidade acadêmica interna até a realização de inscrições para a Política de Assistência Estudantil, envio de mensagens e comunicados, gestão de servidores, processos internos, solicitações de históricos, declarações e a administração de diários de registros de notas, aulas e presenças etc. Ainda há o uso de plataformas virtuais de aprendizagem, como o *moodle*.

Este estudo está estruturado de forma a apresentar, em linhas gerais, o problema de pesquisa, a fundamentação teórica, o estudo de caso, e as conclusões gerais. A seguir, apresenta-se, em detalhes, o que a estrutura contempla. A Figura 1 representa a forma como o trabalho foi conduzido.

Figura 1 – Fluxo da Estrutura do Trabalho

Fonte: Elaboração própria.

[1] Certificado de Apresentação de Apreciação Ética (CAAE): 52015721.3.0000.5400

[2] Certificado de Apresentação de Apreciação Ética (CAAE): 52015721.3.3001.5473

Inicialmente, apresentam-se os objetivos da pesquisa, a justificativa e as contribuições do estudo, bem como esta seção referente à estrutura da tese. A fundamentação teórica identifica os principais conceitos em relação a informações, dados pessoais e à lei de proteção de dados pessoais.

Continuamente, a metodologia usada para o estudo de caso é descrita, assim como seus protocolos, a caracterização do estudo, as informações sobre a instituição, o estudo quantitativo e o estudo qualitativo são descritos, assim como a análise dos resultados.

Encontram-se, por fim, as conclusões alcançadas, limitações da presente pesquisa, sugestões para estudos futuros e as referências bibliográficas utilizadas como fundamento para a elaboração da tese, bem como os materiais complementares apresentados nos apêndices.

2 PROCEDIMENTOS METODOLÓGICOS

A ciência é o enlace de uma malha teórica com dados empíricos, uma articulação do lógico com o real, do teórico com o empírico, do ideal com o real. Toda modalidade de conhecimento realizado por nós implica uma condição prévia, um pressuposto relacionado à nossa concepção da relação sujeito e objeto, ao passo que o pesquisador aborda os fenômenos aplicando recursos técnicos, seguindo um método e apoiando-se em fundamentos epistemológicos que sustentam e justificam a própria metodologia praticada (SEVERINO, 2017).

Para se realizar uma pesquisa é preciso promover o confronto entre os dados, as evidências, as informações coletadas sobre determinado assunto e o conhecimento teórico construído a respeito dele. É o estudo de um problema, que desperta o interesse do pesquisador e limita sua atividade de pesquisa a determinada porção do saber, ao passo que a escolha do método se faz em função do tipo de problema estudado (LÜDKE; ANDRÉ, 2018).

O pesquisador desenvolve a sua investigação passando por três etapas: exploração, decisão e descoberta. A primeira fase envolve a seleção e definição de problemas, escolha do local, entre outros. A segunda fase consiste na busca mais sistemática dos dados tidos como mais importantes para compreender e interpretar o fenômeno estudado. Por fim, a terceira fase consiste na explicação da realidade, na tentativa de encontrar os princípios subjacentes ao fenômeno estudado (LÜDKE; ANDRÉ, 2018). É notório que o estudo de caso em educação ainda tem um grande potencial, desde que bem delineado, claro e definido em seu percurso. Isso se deve ao seu interesse singular, uma vez que constrói uma unidade dentro de um sistema mais amplo e incide naquilo que ele tem de único, mesmo que posteriormente venham a ficar evidentes certas semelhanças com outros casos ou situações.

Conforme salienta Yin (2001), o estudo de caso é uma inquirição empírica que investiga fenômenos contemporâneos inseridos em algum contexto da vida real, permitindo a utilização de fontes de evidências, como a observação direta e entrevistas, utilizando protocolos.

A Figura 2 mostra o caminho metodológico utilizado neste trabalho.

Figura 2 – Fluxo do Percurso Metodológico

Fonte: Elaboração própria.

Dessa forma, o fluxo do percurso metodológico ancorou-se em métodos e técnicas que garantiram analisar a realidade empírica, a partir de informações coletadas no cotidiano de uma instituição educacional e que contribuíram para que os objetivos propostos pela pesquisa fossem alcançados e mensurados neste estudo.

2.1 Caracterização

Segundo a classificação de pesquisa feita pelo cientista político Donald Stokes, esta é uma pesquisa básica-aplicada, impulsionada pela curiosidade investigativa sobre fenômenos particulares, não necessariamente tendo em vista objetivos explanatórios gerais ou utilização prática à qual se destinem seus resultados (STOKES, 2005).

2.2 Protocolo

O protocolo de estudo, além de aumentar a confiabilidade da pesquisa, contém os procedimentos e as regras gerais para conduzir e realizar o estudo, além de oferecer a segurança de que o trabalho científico foi realizado com planejamento e execução. Essas preocupações garantem resultados que, de fato, possibilitaram explicações sobre a realidade investigada (MARTINS; THEÓPHILO, 2007; MARTINS, 2006; YIN, 2001).

As seguintes seções compõem o protocolo do estudo de caso:

- Visão geral do projeto do estudo de caso com a descrição da pesquisa etc.
- Procedimentos, apresentações, locais de estudo, fontes de informação etc.
- Questões do estudo de caso com questões específicas para a coleta de dados.

Os procedimentos adotados, termo de consentimento, autorização e questionários utilizados na condução deste estudo encontram-se nos APÊNDICE A e B. Os instrumentos de coleta utilizados foram questionários digitais estruturados na plataforma *Google Forms*. A visão geral do protocolo de estudo de caso encontra-se descrita nas etapas a seguir.

Segundo Yin (2001), os estudos de caso, em geral, possuem três etapas principais: definição e planejamento; preparação, coleta e análise de dados; e análise das informações e conclusão, conforme os detalhamentos:

1) Definição e planejamento

- Escolha do caso: o estudo bibliográfico realizado nesta pesquisa abrange o tratamento de dados e a aplicação da LGPD no contexto do IFSP. Para melhor compreensão deste contexto, investigam-se instrumentos normativos de proteção de dados e os atuais desafios para o desenvolvimento de políticas e procedimentos na instituição a partir da vigência da LGPD.
- Amostragem: o processo de amostragem adotado será classificado como não probabilístico e por conveniência.
- Critério de escolha dos entrevistados: a amostra desta pesquisa se restringe ao Campus Campinas do IFSP, não se aplicando aos demais *campi*. Este campus foi escolhido considerando que é *lócus* de inserção profissional deste pesquisador e há elementos do cotidiano que contribuíram para o desenvolvimento de hipóteses e objetivos desta pesquisa. A amostra consiste em 80 servidores cadastrados no Sistema Unificado de Administração Pública (SUAP) que atuam como docentes e/ou gestores e se disponibilizaram voluntariamente a participar da pesquisa.

- Elaboração do protocolo do estudo de caso: o protocolo deste estudo realiza-se por meio da aplicação de questionários estruturados fechados ou abertos, instrumentos de coleta constituídos por uma série de perguntas ordenadas.

2) Coleta e análise de dados
   - Aplicação dos questionários: tendo como base as questões elaboradas no protocolo, no critério de escolha dos entrevistados e análise ética pelo Conselho Nacional de Ética em Pesquisa (CONEP), foi aplicado questionário digital estruturado na plataforma Google Forms, com tratamento estatístico das respostas para levantamento de informações quantitativas ou qualitativas para maior profundidade de análise dos dados obtidos.
   - Elaboração do relatório preliminar: a partir das respostas obtidas no questionário, um relatório preliminar foi elaborado para análise detalhada.
   - Análise das informações: a partir do relatório preliminar elaborado, foi realizada a análise detalhada das respostas obtidas.
   - Publicação preliminar dos resultados: a partir do estudo realizado, foi publicado artigo científico na Revista Ibero Americana de Estudos em Educação, como parte do exercício de sistematização dos resultados. Além disso, a análise por pares realizada durante o processo de validação do artigo consolida os resultados obtidos na pesquisa (SOUZA; BELDA; ARIMA, 2022).
   - Elaboração das conclusões: registro das observações decorrentes da análise das informações obtidas durante a pesquisa.

2.3 A Instituição

O estudo de caso se aplica ao *campus* Campinas do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo - IFSP, tendo como instrumento de coleta de dados um questionário digital estruturado na plataforma *Google Forms* contemplando 80 docentes cadastrados no Sistema Unificado de Administração Pública (SUAP). Por tratar-se de estudo de caso único, os dados coletados e sua consequente análise não permitirão a generalização dos resultados.

O IFSP é uma parte integrante da rede de Institutos Federais de Educação, Ciência e Tecnologia, ligados diretamente ao Ministério da Educação. Essas instituições fazem parte da rede pública federal de educação profissional, científica e tecnológica, cobrindo todos os estados brasileiros, oferecendo cursos técnicos, superiores de tecnologia, licenciaturas,

mestrado e doutorado. De acordo com a Plataforma Nilo Peçanha e com base nos dados de 2022, o IFSP possui hoje 38 unidades, 763 cursos e 81.744 matrículas. Em número de *campi* configura-se como o maior do país.

Como autarquia pública federal, o IFSP está diretamente vinculado a dispositivos legais, decretos e instruções normativas que tratem da implementação e aplicação de procedimentos e diretrizes de proteção que possam causar consequências adversas previstas pela Política Nacional de Segurança da Informação (SOUZA, 2017; SOUZA; ARIMA; BELDA, 2020).

Este estudo investiga os instrumentos normativos adotados do IFSP para atender à LGPD; a pesquisa documental deste estudo contempla o Estatuto da instituição e as Portarias mais recentes que aprovam o Regimento Interno do Comitê de Governança Digital e que atualizam a Política de Segurança da Informação e Comunicação – PoSIC, assim como a Política de Proteção de Dados Pessoais.

Segundo o Estatuto, a Pró-Reitoria de Desenvolvimento Institucional faz parte de sua estrutura organizacional administrativa, responsável por planejar, definir, acompanhar e avaliar o desenvolvimento das políticas definidas pela Reitoria, levantando e analisando os resultados obtidos, buscando o aprimoramento do processo educacional e administrativo, em consonância com as diretrizes definidas pelo Ministério da Educação e disposições do Conselho Superior (BRASIL, 2009).

A Portaria nº. 2.534, de 14 de julho de 2020, institui o Comitê de Governança Digital que dispõe e aprova o Regimento Interno do Comitê de Governança Digital (CGD), de caráter estratégico e deliberativo, com as finalidades de deliberar sobre assuntos relativos à Governança Digital, assegurar que a governança de TIC seja parte integrante da governança corporativa, aconselhar sobre o direcionamento estratégico de TIC, direcionar os investimentos de TIC e, por fim, assessorar na implementação das ações de segurança da informação e comunicação no âmbito do IFSP (BRASIL, 2020a).

A Portaria nº. 4.296, de 14 de dezembro de 2020, aprova a atualização da Política de Segurança da Informação e Comunicação — PoSIC, contemplando, dentre outros pontos, o histórico, o objetivo, a estrutura normativa, as diretrizes e, por fim, as referências legais e normativas a serem seguidas. Neste rol, encontra-se a Lei nº. 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2020b).

Por sua vez, a Portaria nº. 2.755/2021 estabelece a Política de Proteção de Dados do IFSP, visando, conforme seu artigo 1º, estabelecer diretrizes e compromissos institucionais quanto ao tratamento de dados pessoais, nos meios físicos e digitais, para proteção dos direitos fundamentais de liberdade, segurança e de privacidade. A política se utiliza dos mesmos

conceitos e definições trazidos pelo artigo 5º da LGPD, e o mesmo ocorre quanto aos fundamentos e princípios elencados pelos artigos 2º e 6º da Lei (BRASIL, 2021).

A Política de Proteção de Dados Pessoais do IFSP é aplicável ao tratamento de qualquer dado pessoal, como nome, endereço, e-mail, idade, estado civil e situação patrimonial, obtido em qualquer tipo de suporte: papel, eletrônico, informático, som e imagem, bem como a identificação de seus responsáveis pelo controle, operação e tratamento.

A seguir, salienta-se a correlação entre as Políticas de Segurança do IFSP, já que, como apontado acima, a Portaria nº. 4.296, que regulamenta a PoSIC, cita diretamente a LGPD em seu texto. Além disso, a Portaria nº. 2755 estabelece em suas disposições temporárias, mais especificamente em seu artigo 34, incisos II e III, que Política de Proteção de Dados Pessoais pode ser definida e publicada em documento específico ou até mesmo incluída no texto da PoSIC já existente, assim como deve concordar com a PoSIC de forma a fornecer apoio e comprometimento do IFSP para alcançar a conformidade com os normativos de proteção de dados pessoais.

Dessa forma, nota-se que a PoSIC do IFSP tem um papel fundamental, dentro de suas atribuições, para a governança institucional. Sendo assim, inclui, dentre outros tópicos, as diretrizes jurídicas e regulatórias a serem seguidas, dentre elas, o cumprimento da LGPD.

2.4 Coleta de dados

Para a investigação dos desafios para o desenvolvimento de políticas e procedimentos, aplica-se um questionário digital como instrumento de coleta de dados, estruturado na plataforma *Google Forms*, contemplando 80 docentes cadastrados no Sistema Unificado de Administração Pública – SUAP.

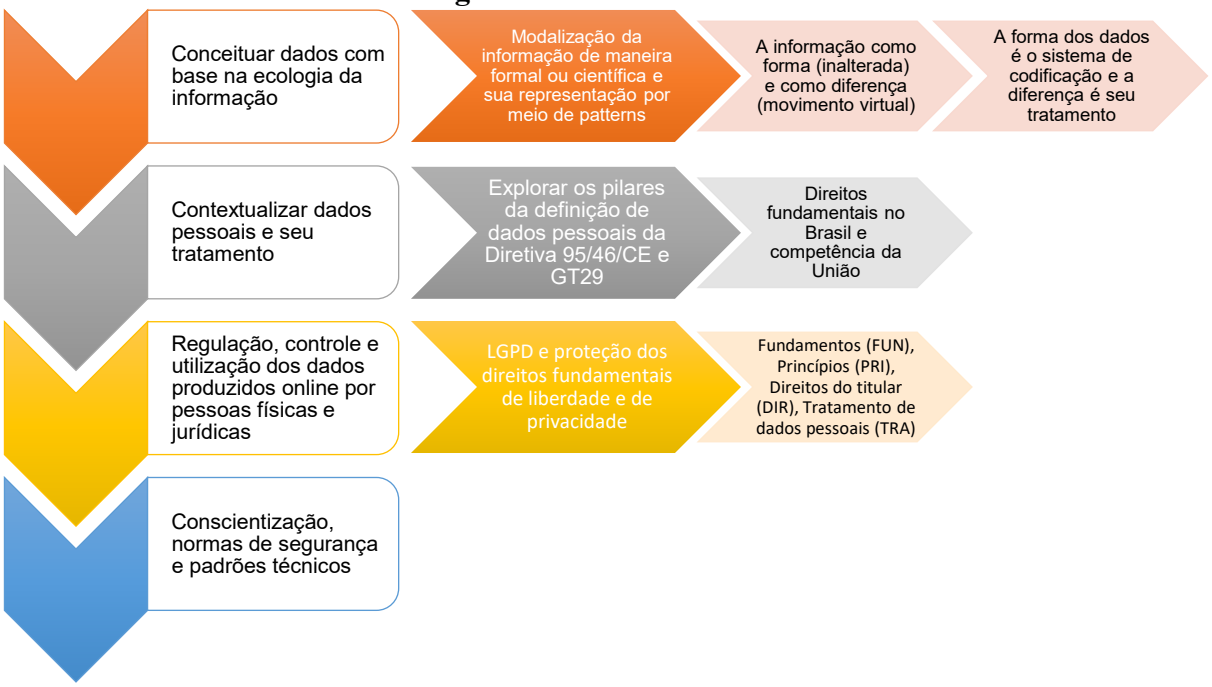
A elaboração do questionário estruturado fundamenta-se no estudo bibliográfico, a análise documental das Portarias do IFSP mencionadas neste método, bem como na Tabela 1 deste estudo, elaborada a partir da análise do disposto na LGPD. As respostas foram coletadas, tabuladas e tratadas estatisticamente, de modo que os critérios analíticos de interpretação permitirão a análise das informações numéricas.

Os resultados foram discutidos a partir dos registros e das observações que surgiram da análise das informações coletadas durante a pesquisa.

3 FUNDAMENTAÇÃO TEÓRICA

Os dados podem ser interpretados como símbolos que, ao serem modulados, geram informações. Quando processados por computador, os dados são estruturados, quantificados, associados, transferidos, tratados e, às vezes, podem até identificar pessoas. Com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e do livre desenvolvimento da personalidade da pessoa natural, a legislação prevê instrumentos de proteção relativos às operações de tratamento de dados pessoais. A Figura 3 representa os elementos que são discutidos neste tópico.

Figura 3 – Percurso Teórico



Fonte: Elaboração própria.

Assim, o debate proposto pelo percurso teórico propiciará refletir sobre o conceito de dados a partir da perspectiva da ecologia da informação, além de compreender o significado acerca do uso dos dados pessoais e do tratamento que deve ser dado a eles, considerando a produção feita em contextos relacionados às pessoas físicas e jurídicas, que devem ter como norte elementos que se referem à conscientização, normas de segurança e padrões técnicos.

3.1 Dados

Thomas H. Davenport (1998) conceitua dados com base na ecologia da informação, ou seja, na maneira como as pessoas criam, distribuem, compreendem e usam a informação, que não pode ser facilmente arquivada em computadores e não sendo constituída apenas de dados,

uma vez que a tecnologia é apenas um dos componentes do ambiente de informação, existindo, portanto, um processo evolutivo de dados para informação, e de informação para conhecimento.

Para Pierre Lévy (2014), nós não sabemos ainda como transformar sistematicamente dados em conhecimento, e ainda menos o meio digital em observatório reflexivo de nossas inteligências coletivas, trazendo a reflexão quanto a uma memória digital participativa, em vias de constituição, comum ao conjunto da humanidade em busca de solucionar este problema de interoperabilidade semântica.

Para tanto, o autor propõe um sistema de codificação das significações denominado *Information Economy Meta Language (IEML)*, ou metalinguagem da economia da informação em português, na busca de aumentar os processos cognitivos com base nos imperativos semântico, ético e técnico.

Este sistema, por tratar-se de um protocolo, supõe princípios dialéticos de direitos onde os indivíduos e as comunidades decidam sobre finalidades e objetivos de seu uso. Tem em vista colocar a serviço do desenvolvimento humano toda a infraestrutura contemporânea de memória, de comunicação e de tratamento digital, cujo ponto crítico está na gestão dos conhecimentos, partilha dos saberes e exploração colaborativa de imensas massas dados que se automatizaria, tanto quanto possível, enquanto a humanidade é uma espécie social especializada na manipulação simbólica (LÉVY, 2014).

Inúmeros símbolos são enviados e recebidos o tempo todo, armazenados nas memórias, propagados nas redes de comunicação, processados pelos computadores e sugeridos nas interfaces sensoriais-motoras de nossos momentos de pensamento. A *Web* das pessoas, *Web* dos dados, *Web* das coisas, *Web* local e ubíqua, *Web* dos saberes e dos tesouros culturais – a grande rede constituiu um só e um único meio digital, de tal forma que a inteligência humana se auto-organiza em um meio para recolher dados que ela produz e explorar os dados que ela reconhece (LÉVY, 2014).

O autor estabelece uma unidade da natureza baseada na ideia de informação, apresentando uma imagem sintética da natureza informacional e seu conceito científico, concebendo a natureza da informação em diferentes níveis: das partículas elementares aos átomos, das moléculas aos organismos, dos sistemas nervosos aos fenômenos e dos símbolos aos conceitos (LÉVY, 2014). Uma interpretação possível é de que os dados equivalem a símbolos, ainda que não modalizados, porém, não sem significado.

A principal maneira de modalizar a informação de maneira formal ou científica é representá-la por meio de *patterns* – isto é, modelos ou padrões – de símbolos ou de relações entre *patterns* simbólicos, uma vez que símbolos seriam objetos abstratos, e não coisas

concretas, precisamente porque eles pertencem a sistemas simbólicos, porém não impedindo que estes se inscrevam no mundo material, ainda que seja para perceber. A abordagem científica contemporânea em geral só considera como informação quando definida por um sistema simbólico tomado como modelo, deste modo, apenas certos traços dos fenômenos são considerados pertinentes e, assim, tomados como informação (LÉVY, 2014).

Em termos computacionais, a unidade de medida de quantidade de informação, o *bit*, permite que ela seja transmitida por uma mensagem binariamente codificada, cujos símbolos elementares podem ser 0 (zero) ou 1 (um), isto é, cada símbolo binário traz um *bit* de informação (LÉVY, 2014).

No campo informacional, forma e diferença aparecem de conceitos transdisciplinares. A informação, como forma, é aquilo que permanece inalterado de um sistema de codificação para outro, capaz de atravessar o tempo e espaço físico por meio de transmissão, indissociável de uma constelação onde ela se associa às noções de código, de transmissão, de tradução, de ruído e de redundância. A informação, enquanto diferença, pode ser comparada a um movimento virtual no universo – a transição de uma forma para outra –, que faz sentido em uma rede semântica onde os conceitos de operação, operador e transformação são os papéis principais (LÉVY, 2014).

Por ser abstrata, a forma é, a princípio, independente dos seus suportes materiais, podendo ser expressa em diferentes sistemas de codificação. Da mesma maneira que, para se atualizar, uma configuração simbólica se inscreve necessariamente ao mundo dos fenômenos, a forma se define codificando-se necessariamente a um sistema simbólico, não podendo se manifestar fora da codificação. Por exemplo, o número 12 pode ser codificado no alfabeto fonético “doze”, no sistema binário “1100”, no sistema de numeração romano “XII” etc. (LÉVY, 2014).

Diante das definições apresentadas, é possível inferir uma correlação conceitual entre os dados e a unidade de *bit*. Quando os dados estão associados a um sistema de codificação, suas configurações simbólicas representam a forma – como conceito –, e seu tratamento representa a diferença – também como conceito. Em outras palavras, a associação de dados binários cria uma configuração simbólica no sistema de codificação binário, cuja estrutura representa uma informação – uma forma, que pode ou não ser submetida a um tratamento – e uma diferença.

3.2 Dados pessoais

Em 24 de outubro de 1995, o Parlamento Europeu e o Conselho da União Europeia publicaram no Jornal Oficial nº. L 281 de 23/11/1995, páginas 31 a 50, a Diretiva 95/46/CE, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (UNIÃO EUROPEIA, 1995).

O Artigo 29 da Diretiva 95/46/CE estabeleceu a criação do grupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais. De caráter consultivo e independente, o *Article 29 Working Party (WP29)*, ou Grupo de Trabalho do Artigo 29 (GT29), teve suas atribuições descritas no artigo 30, envolvendo análises, pareceres, opiniões, aconselhamentos, soluções de divergências, relatórios e recomendações sobre quaisquer questões relativas à proteção das pessoas no que diz respeito ao tratamento de dados pessoais (UNIÃO EUROPEIA, 1995).

Ainda que tenha sido extinto em 25 de maio de 2018, dando origem ao *European Data Protection Board (EDPB)* ou Comitê Europeu para a Proteção de Dados (CEPD), o GT29 emitiu documentos relativos aos trabalhos executados durante seu período de atuação (UNIÃO EUROPEIA, 2018).

No Parecer nº. 4/2007, o GT29 traz a análise do conceito de dados pessoais, cuja expressão inclui informação que toca a esfera da vida privada e familiar da pessoa *stricto sensu*, mas inclui também informação sobre qualquer tipo de atividade realizada pela pessoa, tal como a que diz respeito às relações de trabalho ou ao seu comportamento econômico e social. Inclui, assim, informação sobre pessoas singulares, independentemente do seu estatuto ou papel, como por exemplo, de consumidor, paciente, empregado, cliente etc. (UNIÃO EUROPEIA, 2007).

Para tal, baseou-se na definição contida na Diretiva 95/46/CE, fragmentando-a em 4 (quatro) pilares ou elementos principais que podem ser distinguidos na definição de dados pessoais: “qualquer informação”, “relativa a”, “identificada ou identificável”, “pessoa singular”. Estes elementos estão ligados, apoiam-se uns nos outros, e juntos determinam se uma informação deverá ser ou não considerada dados pessoais (UNIÃO EUROPEIA, 2007).

O primeiro elemento – “qualquer informação” –, apela a uma interpretação ampla do conceito, independentemente da natureza ou do conteúdo da informação, e do formato ou meio técnico em que é apresentada. Deste modo, tanto informação objetiva como subjetiva sobre uma pessoa, seja em que capacidade for, pode ser considerada dados pessoais, independentemente do meio técnico em que está contida. O parecer debate ainda os dados

biométricos e as distinções jurídicas sobre as amostras humanas das quais estes podem ser extraídos (UNIÃO EUROPEIA, 2007).

O segundo elemento – "relativa a" –, remete ao âmbito material do conceito, especialmente em relação a objetos e novas tecnologias. O parecer apresenta três elementos: conteúdo, finalidade e resultado, para determinar se uma informação é relativa a uma pessoa. Abrange igualmente informação que possa ter um claro impacto na forma como é tratada ou avaliada uma determinada pessoa (UNIÃO EUROPEIA, 2007).

O terceiro elemento – "identificada ou identificável" –, diz respeito às condições nas quais uma pessoa deverá ser considerada identificável, sobretudo nos meios suscetíveis de serem razoavelmente utilizados pelo responsável pelo tratamento ou por outrem na identificação da pessoa em causa. Deste modo, o contexto e circunstâncias especiais de um caso específico desempenham um papel importante nesta análise. O parecer trata também dos dados anonimizados e do uso de dados codificados na investigação estatística ou farmacêutica (UNIÃO EUROPEIA, 2007).

O quarto elemento – "pessoa singular" –, trata do requisito de que dados pessoais são relativos a pessoas vivas. O parecer debate igualmente a interação com dados sobre pessoas mortas, nascituros e pessoas coletivas ou jurídicas (UNIÃO EUROPEIA, 2007).

Por fim, o parecer trata da possibilidade de dados não abrangidos pela definição de dados pessoais, de modo que nestes casos caberia à legislação específica dispor sobre o tema (UNIÃO EUROPEIA, 2007).

No Brasil, a promulgação da EC115 alterou o texto base da Constituição Federal de 1988, incluindo a proteção de dados pessoais entre os direitos e garantias fundamentais e fixando a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Entre outros direitos e garantias fundamentais, o artigo 5º estabelece que todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade. Estabelece também, em seu inciso LXXIX, sendo assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais (BRASIL, 2022).

Em seu inciso XXVI, o artigo 21 da lei fixa a competência da União para organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei. Enquanto o artigo 22 fixa em seu inciso XXX a competência privativa da União em legislar sobre proteção e tratamento de dados pessoais.

É notório que os artigos 21 e 22 apresentam divergências no uso dos termos "competência" e "competência privativa". A competência disposta no artigo 21 é exclusiva, uma vez que este não contempla a possibilidade de delegação a outrem. A competência privativa, apesar do nome, permite aos estados legislarem sobre questões específicas das matérias relacionadas, desde que Lei complementar autorize esta competência, conforme o parágrafo único do artigo 22.

3.3 Informações pessoais e controle

O uso de dados pelo Estado e pelas instituições em geral não é prática nova. Foucault (2013) já alertava sobre o crescente controle que as organizações exerceriam enquanto dispusessem de mais informações sobre os usuários/clientes/cidadãos. Na cena contemporânea, as relações sociais também se materializam em ambientes digitais como a internet, o que denota a importância de se atentar a elementos relacionados à disciplina, vigilância e controle, sobretudo no âmbito da sociedade da informação. As tentativas recentes de vários países e entidades supranacionais (como a União Europeia) em regular a utilização dos dados produzidos *online* por pessoas físicas e jurídicas materializam a preocupação que paira sobre a segurança individual em relação aos "rastros digitais" que todos deixamos ao navegar nas redes.

Concorda-se com Ferreira na seguinte afirmação:

> Conforme Michel Foucault (2013, p. 181), se entre os séculos XVIII e XX um "poder de escrita" próprio do campo documentário já se aplicava à disciplina, registrando tudo o que alcançava os olhos de observadores especializados, convertendo-se em uma espécie de saber sobre os indivíduos, tal como se dava nos domínios de ciências como Medicina, Educação, Psicologia e Psiquiatria, ***no século XXI o que se verifica é um novo regime de vigilância, cujas regras de funcionamento se descolam da coleta de volumes de informações em suportes analógicos para a acumulação de grandes quantidades de dados digitais e/ou digitalizáveis***; do registro que estava a cargo do observador para uma documentação agora produzida pelo próprio observado, notadamente a partir do que ele próprio escreve, fala, filma, fotografa, acessa e/ou compartilha nas redes digitais (FERREIRA, 2014, p. 116, grifos nossos).

Para Althusser (1985), as instituições educacionais, enquanto aparelhos ideológicos do Estado, também teriam interesse em saber mais sobre seus alunos e utilizar esses saberes para aprimorar o controle exercido no interior das escolas. Este trabalho está focado, dessa forma, na percepção dos docentes de determinada IES, procurando entender como eles percebem a Política de Segurança da Informação e Comunicação aplicada na organização em que estão inseridos.

Como já referenciado anteriormente, Davenport (1998) apresenta o conceito de dados, informação e conhecimento. Portanto, a guisa de elucidação e complementação, e entendendo que o "conhecimento é poder"[3], investiga-se o quanto os professores **sabem** e **concordam** com a gestão dos seus próprios dados no local de trabalho. Dessa forma, pode-se analisar a importância que a organização, de fato, atribui ao compartilhamento de informações com seu corpo docente. Apesar de não ser possível generalizar os resultados, tem-se uma amostra de como uma instituição de ensino lida com a questão da informação e do controle, atualmente.

3.4 Lei Geral de Proteção de Dados Pessoais (LGPD)

As políticas de privacidade de dados pessoais permitem aos usuários terem conhecimento das formas pelas quais seus dados serão usados, o que possibilita evitar ou reduzir a coleta e o uso informações por terceiros.

A Lei nº. 13.709, de 14 de agosto de 2018, tem como objetivo proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural, inclusive nos meios digitais, sejam elas pessoas naturais ou jurídicas de direito público ou privado (BRASIL, 2018).

A LGPD regulamenta em seus 10 (dez) capítulos disposições gerais; tratamento de dados pessoais; direitos do titular; tratamento de dados pessoais pelo poder público; transferência internacional de dados; agentes de tratamento de dados pessoais; segurança e boas práticas; fiscalização; Autoridade Nacional de Proteção de Dados (ANPD) e Conselho Nacional de Proteção de Dados Pessoais e da Privacidade e, por fim, disposições finais e transitórias.

No capítulo em questão, contendo suas disposições gerais, o único parágrafo do artigo 1º demostra que as normas ali presentes são de importância nacional, devendo ser observadas pela União, Estados, Distrito Federal e Municípios, estabelecendo assim a obrigatoriedade por parte de todos os entes federativos em seguirem a norma e protegerem os dados pessoais com base em fundamentos apresentados no artigo 2º.

Se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de

---

[3] Não é objetivo desta tese adentrar no debate sobre conhecimento como forma de poder. Todavia, cabe apontar que a expressão é de autoria do pensador e filósofo inglês Francis Bacon. A interpretação da frase reflete a importância dada à acumulação de conhecimento a partir da Educação, compreendendo que a Educação é parte constitutiva dos sujeitos sociais e tem relevância para a construção de valores e visões de mundo. Para compreender melhor sobre a Educação como parte ontológica dos sujeitos, ver Saviani (2007).

bens ou serviços, ou o tratamento de dados de indivíduos localizados no território nacional; ou que os dados pessoais objeto do tratamento tenham sido coletados no território nacional, conforme estabelece o artigo 3º.

As exceções à sua aplicação no tratamento de dados estão previstas no artigo 4º, tais como quando é realizada por uma pessoa natural para fins exclusivamente pessoais e não econômicos, assim como o tratamento para fins acadêmicos, desde que atendidas as condições necessárias. Apesar de também excetuar quando do tratamento para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais ou provenientes de fora do território nacional, a Lei aqui estabelece critérios a serem atendidos dos parágrafos §1º ao §4º.

O artigo 5º apresenta termos e definições que abordam conceitos de dado pessoal, dado pessoal sensível, dado anonimizado, titular dos dados, agentes de tratamento, controlador, operador, encarregado, tratamento de dados, anonimidade, consentimento, bloqueio, eliminação, transferência internacional, uso compartilhado, relatório de impacto à proteção de dados pessoais, órgão de pesquisa e autoridade nacional. Tal arcabouço conceitual será utilizado como base por estar diretamente relacionado aos termos e definições apresentados anteriormente, especialmente ao tratar elementos como fundamentos, princípios e preocupações quanto ao tratamento de dados pessoais e os direitos do titular.

Por sua vez, o artigo 6º estabelece que as atividades de tratamento de dados, isto é, toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, deverão observar a boa-fé e os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Visando aplicar os conceitos, sintetizaram-se tais elementos em dimensões, conforme apresentados na Tabela 1.

Tabela 1 – Dimensões de proteção de dados pessoais

1. **Fundamentos (FUN)**: Preocupação com a "proteção de dados pessoais quando do seu tratamento, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018, n.p.).

2. **Princípios (PRI)**: Atendimento aos princípios da "finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas" (BRASIL, 2018, n.p.).
3. **Tratamento de dados pessoais (TRA)**: "Toda operação realizada com dados pessoais", sendo indispensável o consentimento do titular "por escrito ou por outro meio que demonstre a manifestação de vontade" "livre e inequívoca" (BRASIL, 2018, n.p.).
4. **Direitos do titular (DIR)**: O direito de "revogação do consentimento", "atualização", "anonimização", "bloqueio" ou "eliminação" dos dados pessoais ao titular dos dados (BRASIL, 2018, n.p.).

Fonte: Adaptado com base na LGPD (BRASIL, 2018).

O capítulo 4 regulamenta o tratamento pelo poder público, inclusive fazendo referência direta no caput do artigo 23 à Lei nº. 12.527, de 18 de novembro de 2011, também conhecida como Lei de Acesso à Informação (LAI), devendo ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, visando executar as competências legais ou cumprir as atribuições legais do serviço público.

O uso compartilhado de dados pessoais pelo poder público também deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios do artigo 6º. A LGPD veda o poder público de transferir para entidades privadas dados pessoais constantes de bases de dados a que tenham acesso, não obstante, há algumas exceções, como a execução descentralizada de atividade pública, dados que sejam acessíveis publicamente, quando há previsão legal ou instrumentos de celebração contratual e congêneres, assim como para prevenção de fraudes, irregularidades e proteção ou segurança do titular dos dados.

Ademais, as pessoas jurídicas de direito público devem indicar um encarregado – ou *Data Protecion Officer (DPO)* –, para atuar como canal de comunicação quando forem realizadas operações de tratamento de dados pessoais, informando também as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

O capítulo 6 regulamenta as atribuições dos agentes de tratamentos de dados, isto é, controlador, operador e encarregado. Controlador é pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. Operador é pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Por sua vez, o encarregado atua como canal de

comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

É obrigação do controlador ou operador reparar o dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais que causarem em razão do exercício de atividade de tratamento.

O capítulo 7 complementa as responsabilidades por parte dos agentes de tratamento ao estabelecer que devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado, ou ilícito. O artigo 50 traz, nos três parágrafos, referências diretas a princípios apresentados no artigo 6º, tais como da finalidade, qualidade, segurança, prevenção e prestação de contas.

Desde que seja no âmbito de suas competências, ainda que individualmente ou por meio de associações, a Lei orienta que, pelo tratamento de dados pessoais, controladores e operadores poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento dos dados.

Diante do exposto, entende-se que a LGPD altera a maneira como as instituições devem lidar com o tratamento de dados pessoais. Ela tem influência em legislações anteriores, como o Marco Civil da Internet (MENDES; DONEDA, 2018), e significa um avanço na proteção de dados pessoais, implicando a necessidade de as instituições proverem políticas de segurança da informação.

3.5 Proteção de dados pessoais, segurança da informação e conscientização

O Artigo 50 da LGPD prevê a adoção de normas de segurança e padrões técnicos, assim como de ações educativas. A possibilidade de utilização de normas técnicas permite a aplicação de práticas de segurança da informação e proteção de dados com base em um sistema de gestão, como da família ISO/IEC 27000.

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, **poderão formular regras de boas práticas e de governança** que estabeleçam as **condições de organização, o regime de funcionamento, os procedimentos**, incluindo reclamações e petições de titulares, as **normas de segurança, os padrões técnicos, as obrigações específicas para os diversos**

> **envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos** e outros aspectos relacionados ao tratamento de dados pessoais [...] (BRASIL, 2018, *online*, grifos nossos*)*

O Sistema de Gestão de Segurança da Informação (SGSI) é especificado pela ISO/IEC 27001 e tem por objetivo auxiliar as instituições a definirem as competências das pessoas nos processos organizacionais; as melhorias por meio de aferições e modificações; o envolvimento da alta direção e das partes interessadas nas ações institucionais; as análises críticas, auditorias e ações corretivas; as documentações; as políticas a serem seguidas e os requisitos de segurança. Já a ISO/IEC 27002 oferece orientações que podem ser utilizadas como referência na seleção de controles no processo de implementação de um SGSI por meio de um código de prática para controles de segurança da informação.

> Esta Norma é projetada para as organizações usarem como uma referência na seleção de controles dentro do processo de implementação de um sistema de gestão da segurança da informação (SGSI), [...] ou como um documento de orientação para as organizações implementarem controles de segurança da informação comumente aceitos. Esta Norma é também usada no desenvolvimento de organizações e indústrias específicas de gerenciamento de segurança da informação, levando em consideração os seus ambientes de risco de segurança da informação específicos (ABNT, 2022, p. x).

A ISO/IEC 27701 – extensão da 27001 e 27002 –, aponta que as organizações lidam com diferentes quantidades e tipos de dados pessoais, necessitando, assim, proteger a privacidade – como indicado no artigo 1º da LGPD, que estabelece a proteção de dados pessoais como um fundamento. Em termos de contexto, é indispensável à proteção de dados pessoais, uma vez que é assegurada a toda pessoa natural a titularidade de seus dados.

O documento fornece também diretrizes e específica os requisitos de um Sistema de Gestão de Privacidade da Informação (SGPI) – uma extensão do SGSI –, visando aprimorar a gestão da privacidade no contexto organizacional. Dentre os requisitos, o de apoio engloba a questão da conscientização, educação e treinamento em segurança da informação.

> Este documento especifica os **requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação** (SGPI) [...] para a gestão da privacidade dentro do contexto da organização. [...] fornece as **diretrizes** para os controladores de DP e operadores de DP que têm responsabilidade e responsabilização com o tratamento de DP. [...] é **aplicável a todos os tipos e tamanhos de organizações**, incluindo as companhias públicas e privadas, entidades governamentais e organizações sem fins lucrativos, que são controladoras de DP e/ou que são operadoras de DP (ABNT, 2019, p. 1, grifos nossos).

Por meio de um mapeamento, é possível estabelecermos diferentes relações de vínculo entre a ISO/IEC 27701 e a LGPD, como a demonstrada pelo Quadro 1.

Quadro 1 – Vínculo entre ISO/IEC 27701 e LGPD

ISO/IEC 27701	LGPD
5.2 - Contexto da organização	Artigo 50
6.2 - Políticas de segurança da informação	Artigo 38
6.4.2.2 - Conscientização, educação e treinamento	Artigo 50

Fonte: Resultados da pesquisa.

Tal vínculo e as ações educativas previstas pelo Artigo 50 da LGPD nos permite invocar, também, a Lei de Diretrizes e Bases da Educação Nacional (LDB) – Lei nº. 9.394, de 20 de dezembro de 1996 –, ao estabelecer em seu Artigo 1º que educação abrange os processos formativos que se desenvolvem [...] na convivência humana, no trabalho, nas instituições de ensino e pesquisa [...]. Note-se aqui que as tais ações educativas e os requisitos estabelecidos pelas normas dialogam entre si, em favor de um processo de conscientização (BRASIL, 1996).

Processo que demandará a aplicações de medidas – como treinamentos periódicos –, visando que pessoas tenham ciência das possíveis consequências de violações de privacidade quando do tratamento de dados pessoais. Haveria, por exemplo, consequências jurídicas ou de imagem para as instituições; consequências disciplinares para os seus membros; e consequências materiais, emocionais ou de outra natureza para os titulares dos dados.

A Lei nº. 14.533, de 11 de janeiro de 2023, que institui a Política Nacional de Educação Digital, estabelece no § 2º do Artigo 1º o eixo estruturante de Educação Digital Escolar. Conforme Artigo 3º, o eixo tem em vista garantir a inserção da educação digital nos ambientes escolares, em todos os níveis e modalidades, a partir do estímulo ao letramento digital e informacional [...], englobando no Inciso IV direitos digitais que envolvem a conscientização a respeito dos direitos sobre o uso e o tratamento de dados pessoais, nos termos da LGPD, a promoção da conectividade segura e a proteção dos dados da população mais vulnerável, em especial, crianças e adolescentes (BRASIL, 2023).

As instituições educacionais, de uma maneira geral, podem proporcionar cursos elaborados sobre gestão e proteção de dados, através de seminários, oficinas, workshops etc, além das disciplinas já existentes nos cursos técnicos e de graduação da área de ciências da informação. A educação para as mídias é assunto cada vez mais tratado pelos acadêmicos que não se furtam ao debate sobre o impacto que as ferramentas de comunicação e informação

trouxeram para a vida em sociedade, em geral, e para a educação, em particular (a esse respeito, cf. KENSKI, 2005; RECUERO, 2012; SANTAELLA, 2013).

Acredita-se ser fundamental aproveitar o momento atual, de aplicação de leis como a LGPD, para aprimorar as discussões ocorridas nas escolas (de ensino básico e superior), qualificando não só como os dados e informações produzidos virtualmente serão tratados, mas principalmente as bases éticas que balizarão esse tratamento. Trabalhos como o de Spanceski (2004), por exemplo, auxiliam com diretrizes que podem ser generalizáveis a variadas realidades educativas, oportunizando a aprendizagem da ciência de dados a toda a comunidade escolar.

Como destacado anteriormente, a ISSO/IEC 27701 prevê que as instituições desenvolvam, implementam, mantenham e monitorem um programa relacionado à privacidade e à governança da instituição, de forma a garantir que sejam aplicadas e cumpridas todas as normativas relacionadas ao tratamento de dados pessoais (ABNT, 2019). É nesta direção que um dos produtos produzidos por esta tese se relaciona com a criação de um programa educacional de conscientização em proteção de dados pessoais, como será exposto mais adiante.

Este programa propõe nove etapas, sendo elas: a conscientização relacionada aos objetivos da LGPD, aos fundamentos e princípios básicos da lei, a necessidade de adequação e sustentação, a matriz de responsabilidades, os processos e procedimentos internos, além do alinhamento entre os sistemas, a PoSIC, demais políticas e a LGPD, a *Privacy by Design e* a comunicação. Além disso, o programa direciona uma etapa relacionada à avaliação e monitoramento, entendendo a necessidade de analisar o grau de maturidade da comunidade acerca da conscientização.

Todas as etapas propostas visam contribuir para a compreensão da necessidade de proteção aos direitos fundamentais e das implicações para as instituições, de forma a alinhar a missão, visão e valores institucionais. Ademais, o produto proposto tem como um dos resultados esperados o direcionamento das responsabilidades das partes envolvidas no processo de tratamento de DP, contribuindo para que os processos e procedimentos internos sejam mais bem especificados e detalhados, garantindo uma abordagem que relacione os sistemas de segurança da informação e a privacidade de dados pessoais e estejam alinhados com as políticas institucionais.

4 ANÁLISE DE DADOS

A construção da análise se dá a partir da coleta de dados quanto à percepção dos docentes do Instituto Federal de São Paulo, *campus* Campinas, sobre como são tratados protocolos de proteção de dados no *campus*, e auxiliará na verificação dos desafios para o desenvolvimento de políticas e procedimentos e possíveis adequações que atendam à LGPD.

4.1 Metodologia

4.1.1 Escala Likert

Segundo Likert (1932), pesquisas que incluem opiniões e atitudes são consideradas um método indireto para medir disposições que são mais facilmente significadas e expressas na forma verbal, e podem, consequentemente, ser agrupadas em padrões. São apresentados métodos para verificar objetivamente as afirmações de uma escala, a fim de ajudar o experimentador na elaboração de escalas de atitude.

A escala Likert será usada para que se possa conhecer a forma como os dados foram coletados e, assim, obter uma modelagem estatística que melhor se adequa aos dados. Isso porque as respostas emitidas nessa escala indicam o grau de concordância dos participantes com a frase.

Elas são construídas de forma linear e gradativa, de modo que os níveis de 1 a 5 da escala estão classificados respectivamente como: “Discordo totalmente”, “Discordo”, “Neutro”, “Concordo” e “Concordo totalmente”.

Um cuidado importante durante a pesquisa, tanto na formulação dos questionamentos quanto na análise deles, é a neutralidade. Permitiu-se aos respondentes a liberdade de posicionarem de forma neutra em relação ao conteúdo abordado. Deste modo, a análise considerará a neutralidade como a necessidade da adoção de ações de conscientização e educativas que concordem com boas práticas e da governança de aspectos relacionados ao tratamento de dados pessoais, tendo que em vista que, se os respondentes não se sentem confiantes a ponto de responderem afirmativamente, precisam, no mínimo, serem mais bem informados sobre as ações da instituição no que se refere ao assunto.

4.1.2 Análise Descritiva

Por meio da análise descritiva das respostas pode-se explorar o comportamento das variáveis por meio de porcentagens, medidas de associação e medidas sumárias. Ademais,

ferramentas como gráficos e tabelas auxiliam uma melhor visualização e entendimento dos resultados obtidos (REIS; REIS, 2002).

O primeiro passo nessa análise é a construção de um conjunto de categorias descritivas. O referencial teórico do estudo fornece a base inicial de conceitos a partir dos quais é efetuada a primeira classificação dos dados. Em alguns casos, pode ser que essas categorias iniciais sejam suficientes, pois sua amplitude e flexibilidade permitem abranger a maioria dos dados. Em outros casos, as características específicas da situação podem exigir a criação de novas categorias conceituais (LÜDKE; ANDRÉ, 2018).

A análise dos resultados se dará inicialmente a partir da seguinte estrutura:

- PDP – Perfil dos participantes
- CDI – Contexto da instituição

Em seguida, serão analisadas as dimensões de proteção de dados pessoais:

- FUN – Fundamentos da proteção de dados pessoais
- PRI – Princípios da proteção de dados pessoais
- TRA – Tratamento de dados pessoais
- DIR – Direitos do titular de dados pessoais

4.2 Perfil dos participantes

A fim de analisar o perfil dos entrevistados, é importante notar que a amostra usada nesta pesquisa é composta por 80 professores do *campus* Campinas do IFSP. A amostra se caracteriza como probabilística e aleatória, uma vez que a participação da população se deu de forma anônima e voluntária. Ao total, foram coletadas 15 respostas.

A amostra caracteriza-se conforme faixa etária, escolaridade, tempo na instituição e se a pessoa participante ocupa cargo de gestão atualmente, conforme Tabela 2.

Tabela 2 – Perfil dos participantes

Docentes	Faixa etária	Escolaridade	Tempo instituição	Gestor
D1	30 a 39 anos	Mestrado	entre 4 e 10 anos	Não
D2	50 a 59 anos	Doutorado	entre 4 e 10 anos	Não
D3	30 a 39 anos	Mestrado	entre 4 e 10 anos	Não
D4	30 a 39 anos	Mestrado	entre 10 e 20 anos	Não
D5	50 a 59 anos	Doutorado	Mais de 20 anos	Sim
D6	40 a 49 anos	Doutorado	entre 4 e 10 anos	Sim
D7	60 a 69 anos	Doutorado	entre 4 e 10 anos	Não
D8	50 a 59 anos	Mestrado	entre 4 e 10 anos	Não

D9	30 a 39 anos	Doutorado	entre 4 e 10 anos	Sim
D10	40 a 49 anos	Doutorado	entre 4 e 10 anos	Sim
D11	50 a 59 anos	Doutorado	entre 4 e 10 anos	Não
D12	50 a 59 anos	Doutorado	entre 4 e 10 anos	Não
D13	40 a 49 anos	Mestrado	entre 4 e 10 anos	Não
D14	30 a 39 anos	Mestrado	entre 4 e 10 anos	Não
D15	18 a 29 anos	Mestrado	entre 4 e 10 anos	Não

Fonte: Resultados da pesquisa.

Para uma melhor compreensão do perfil dos entrevistados, as análises entre as escolaridades de Mestrado e Doutorado estarão divididas de acordo com a Tabela 3. Como as frequências possuem uma pequena variação, nota-se que a proporção entre os níveis de escolaridade dos participantes possui diferença mínima.

Tabela 3 – Escolaridade

Escolaridade	Freq. Absoluta	Freq Relativa	Porcentagem
Mestrado	7	0.47	47%
Doutorado	8	0.53	53%
Total	15	1	100%

Fonte: Resultados da pesquisa.

O perfil do participante vária de acordo com o nível de escolaridade. A Tabela 4 demonstra a comparação entre a frequência absoluta e relativa de cada nível de instituição em relação ao número total de entrevistados.

Tabela 4 – Comparação entre os níveis de escolaridade por faixa etária

	Freq. absoluta		Freq. relativa	
Faixa etária	**Mestrado**	**Doutorado**	**Mestrado**	**Doutorado**
18 a 29 anos	1	0	0.06	0.00
30 a 39 anos	4	1	0.26	0.06
40 a 49 anos	1	2	0.06	0.13
50 a 59 anos	1	4	0.06	0.26
60 a 69 anos	0	1	0.00	0.06

Fonte: Resultados da pesquisa.

Assim, observa-se que apenas duas faixas etárias englobam 64% dos docentes, sendo essas de 30 a 39 anos e 50 a 59 anos, enquanto na primeira faixa a maior concentração é de mestrado, e na segunda, doutorado.

4.3 Contexto da instituição

A análise do contexto da instituição (CDI) e os questionamentos feitos aos respondentes tiveram como base a norma ABNT NBR ISO/IEC 27701/2019 e o artigo 50 da LGPD, abrangendo a investigação dos seguintes elementos:

- CDI1 – Adoção de uma Política de Segurança da Informação e Comunicações (PoSIC) suficientemente esclarecedora por parte da instituição;
- CDI2 – Controles técnicos de proteção de dados pessoais armazenados;
- CDI3 – Transparência e livre acesso às informações e dados pessoais armazenados;
- CDI4 – Treinamentos ou eventos que tratem da privacidade e proteção de dados pessoais e operacionais;
- CDI5 – Adoção de diferentes métodos de autenticação;
- CDI6 – Comunicação, por meio de avisos, de questões relacionadas à privacidade e proteção de dados pessoais;
- CDI7 – Conscientização sobre segurança da informação;
- CDI8 – Conscientização sobre proteção de informações confidenciais em formato eletrônico;

Inicialmente, a ciência dos resultados quanto à adoção de uma Política de Segurança da Informação e Comunicações (PoSIC) suficientemente esclarecedora por parte da instituição, abordada pelo elemento CDI1, nos trará evidências de possíveis respostas neutras nas afirmações sobre o contexto da instituição. Para isso, analisou-se as seguintes afirmações apresentadas na Tabela 5, com seus respectivos resultados:

Tabela 5 – Representação em porcentagem das respostas de CDI1

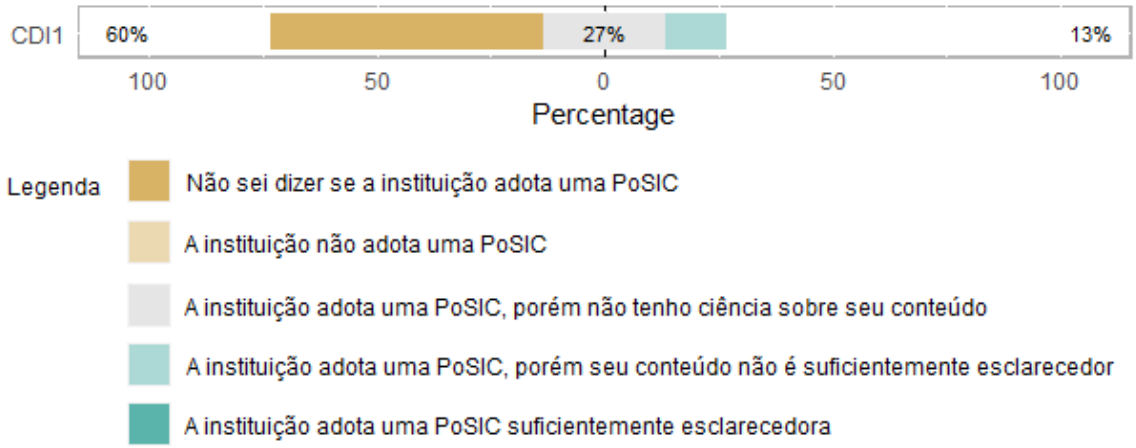
CDI1	Porcentagem
Não sei dizer se a instituição adota uma PoSIC	60.00%
A instituição não adota uma PoSIC	0.00%
A instituição adota uma PoSIC, porém não tenho ciência sobre seu conteúdo	26.67%
A instituição adota uma PoSIC, porém seu conteúdo não é suficientemente esclarecedor	13.33%
A instituição adota uma PoSIC suficientemente esclarecedora	0.00%

Fonte: Resultados da pesquisa

Conforme também pode ser visualizado pelo Gráfico 1, 40% dos participantes concordam que a instituição adota uma PoSIC, entretanto, 26,67% afirmam não terem ciência sobre seu conteúdo e, 13,33%, que seu conteúdo não é suficientemente esclarecedor.

Apesar de 60% dos participantes não serem capazes de dizer se a instituição tem uma PoSIC, uma conclusão prematura desse fenômeno poderia questionar o quanto eles estão familiarizados com o assunto. Entretanto, os participantes complementam em suas respostas que “na instituição os servidores pouco conhecem sobre a LGPD, e não há medidas institucionais adotada para proteção de dados, ficando a cargo do bom senso do servidor a proteção dos dados”, e ainda “não ter conhecimento algum sobre proteção de dados em nossa instituição”.

Gráfico 1 – Representação gráfica das respostas de CDI1



Fonte: Resultados da pesquisa

Para uma análise mais aprofundada, os fatores relacionados a este ponto serão examinados com maior profundidade nos próximos elementos de CDI e nas análises das dimensões de proteção de dados pessoais.

Os elementos investigados dizem respeito tanto à privacidade em geral quanto àqueles listados na Lei Geral de Proteção de dados (LGPD), como disposto no artigo 50, que trata das boas práticas e da governança. A Lei prevê diversos aspectos que devem ser levados em consideração para a implantação de um programa de governança em privacidade que, pelo menos, demonstre o comprometimento do controlador em adotar processos e políticas internas que garantam o cumprimento integral de normal e boas práticas relativas à proteção de dados pessoais.

Conforme a Tabela 6, observa-se que as porcentagens de neutros são em sua maioria constantes e possuem pouca variabilidade. Adicionalmente, em quase todas as afirmações, o neutro é inferior ao nível mais escolhido que expressa alguma opinião, sendo ela de concordância ou discordância, com exceção de CDI3.

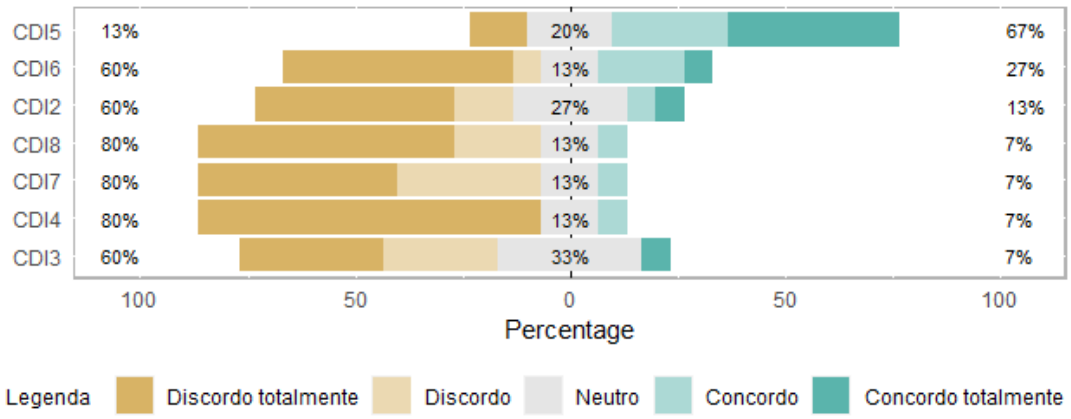
Tabela 6 – Representação em porcentagem das respostas de CDI2 a CDI8

	Disc. total.	Discordo	Neutro	Concordo	Conc. total.
CDI2	46,67%	13,33%	26,67%	6,67%	6,67%
CDI3	33,33%	26,67%	33,33%	0%	6,67%
CDI4	80,00%	0%	13,33%	6,67%	0%
CDI5	13,33%	0%	20,00%	26,67%	40,00%
CDI6	53,33%	6,67%	13,33%	20,00%	6,67%
CDI7	46,67%	33,33%	13,33%	6,67%	0%
CDI8	60,00%	20,00%	13,33%	6,67%	0%

Fonte: Resultados da pesquisa

Inicialmente, observa-se pelo Gráfico 2 que o único aspecto que apresentou alto grau de concordância (67%) foi CDI5, que se refere ao fato de a instituição adotar, para o acesso dos usuários aos sistemas, diferentes métodos de autenticação, como, por exemplo, usuário e senha, biometria, tokens por aplicativos.

Gráfico 2 – Representação gráfica das respostas de CDI2 a CDI8



Fonte: Resultados da pesquisa

As demais respostas apresentam um alto grau de discordância, podendo ser divididas em dois grupos, um com 80% de discordância e outro com 60% de discordância. Com 80%, estão CDI4, CDI7 e CDI8, ao abordarem aspectos referentes à condução de treinamentos ou eventos que lidem com a privacidade e proteção de dados pessoais; à ciência do contexto da segurança da informação; e de como proteger informações confidenciais em formato eletrônico.

Em seguida, com 60% de discordância, tem-se CDI2, CDI3 e CDI6, ao tratarem de aspectos institucionais no tocante à implementação de controles técnicos para proteger dados pessoais armazenados em seus sistemas; se oferece aos titulares de dados transparência e livre acesso às informações e dados pessoais armazenados em seus sistemas; e a comunicação de questões relacionadas à privacidade e proteção de dados.

Destaca-se também o fato de CDI2, CDI3 e CDI5 apresentarem um certo grau de neutralidade em relação aos demais aspectos analisados, com destaque a 33% de CDI3 ao tratar da transparência e livre acesso às informações, indicando uma possível relação dos índices aqui analisados com o fenômeno observado em CDI1.

A segurança da informação e a proteção de dados pessoais devem ser avaliadas de acordo com o contexto institucional. Ele inclui a investigação de vários fatores, como a adoção de uma PoSIC esclarecedora, controles técnicos de proteção de dados pessoais, transparência e acesso às informações e dados pessoais, treinamentos e eventos sobre privacidade e proteção de dados, métodos de autenticação, comunicação de questões relacionadas à privacidade e proteção de dados, conscientização sobre segurança da informação e proteção de informações confidenciais em formato eletrônico.

Os resultados de CDI indicam haver controles técnicos de proteção de dados pessoais armazenados, mas há uma falta de transparência e acesso às informações. Além disso, há poucos treinamentos ou eventos que tratem da privacidade e proteção de dados pessoais e operacionais, e a instituição não utiliza diferentes métodos de autenticação. A transmissão de problemas ligados à privacidade e à proteção de dados também é insuficiente, assim como a conscientização sobre segurança da informação e proteção de informações confidenciais em formato eletrônico.

4.4 Dimensões

A análise a seguir contemplará as dimensões de proteção de dados pessoais quanto aos seus Fundamentos (FUN), Princípios (PRI), Tratamento (TRA) e Direitos do Titular (DIR).

4.4.1 Fundamentos de proteção de dados pessoais

A análise dos fundamentos de proteção de dados pessoais (FUN) e os questionamentos feitos aos respondentes tiveram como base o artigo 1 da LGPD e abrangem a investigação do seguinte elemento:

- FUN1 – A instituição, em suas diversas atividades, preocupa-se com a proteção de dados pessoais quando do seu tratamento, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Os resultados da coleta são apresentados na Tabela 7.

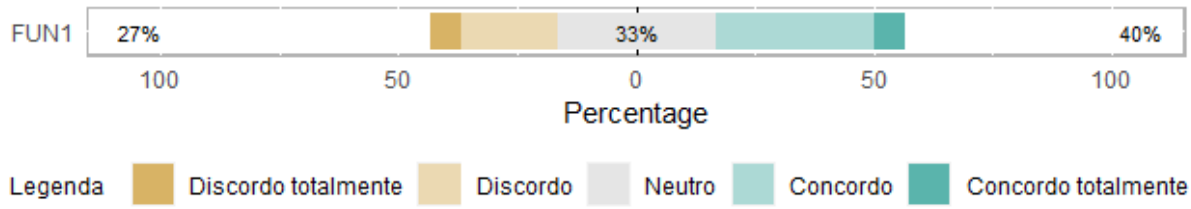
Tabela 7 – Representação em porcentagem das respostas de FUN

	Disc. total.	Discordo	Neutro	Concordo	Conc. total.	Total
FUN1	6,67%	20,00%	33,33%	33,33%	6,67%	100,00%

Fonte: Resultados da pesquisa.

No que diz respeito aos fundamentos de proteção de dados pessoais, tem-se como pilar o disposto no caput do artigo 1º da LGPD, ao estabelecer que a instituição, em suas diversas atividades, deve preocupar-se com a proteção de dados pessoais quando do seu tratamento, inclusive nos meios digitais, visando proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Gráfico 3 – Representação gráfica das respostas de FUN1



Fonte: Resultados da pesquisa

Como é possível observar no Gráfico 3, embora 40% dos entrevistados concordem, há um alto nível (de 33%) de neutralidade em relação ao total, e também cerca de 27% de discordância, o que resulta em dados divergentes e inconclusivos.

Sem mais considerações dos presentes, aqui se apresentam pontos que devem ser observados pela instituição, pois dizem respeito diretamente a direitos fundamentais, tais como liberdade, privacidade e autonomia pessoal. Com o advento da EC115, tais aspectos estão, inclusive, em consonância com o artigo 5º da Constituição Federal sobre direitos e garantias fundamentais, especificando, no inciso LXXIX, o dever de ser assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

4.4.2 Princípios de proteção de dados pessoais

A análise dos princípios de proteção de dados pessoais (PRI) e os questionamentos feitos aos respondentes tiveram como base o artigo 6 da LGPD e abrangem a investigação de se,

durante o processo de coleta e tratamento de dados pessoais, a instituição informa a seus titulares:

- PRI1 – A(s) finalidade(s) específica(s) do uso desses dados;
- PRI2 – O nível de comprometimento em atender à(s) finalidade(s) informada(s);
- PRI3 – Se permite consulta gratuita e facilitada sobre a forma e duração do tratamento, bem como a integralidade de seus dados pessoais;
- PRI4 – Se permite a atualização de seus dados;
- PRI5 – Se fornece acessibilidade e clareza de informações sobre a realização de tratamento;
- PRI6 – Se utiliza de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração e comunicação;
- PRI7 – Se utilizam de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (Exemplos: restrições de acessos e autenticações, adoção de criptografias);
- PRI8 – Se impossibilitará a realização de tratamento para fins discriminatórios, ilícitos ou abusivos (desde a coleta à sua utilização, modificação, difusão e eliminação dos dados);
- PRI9 – Se adotará medidas de observância ao cumprimento das normas de proteção de dados pessoais, se responsabilizando pela eficácia dessas medidas.

Os resultados da coleta são apresentados na Tabela 8:

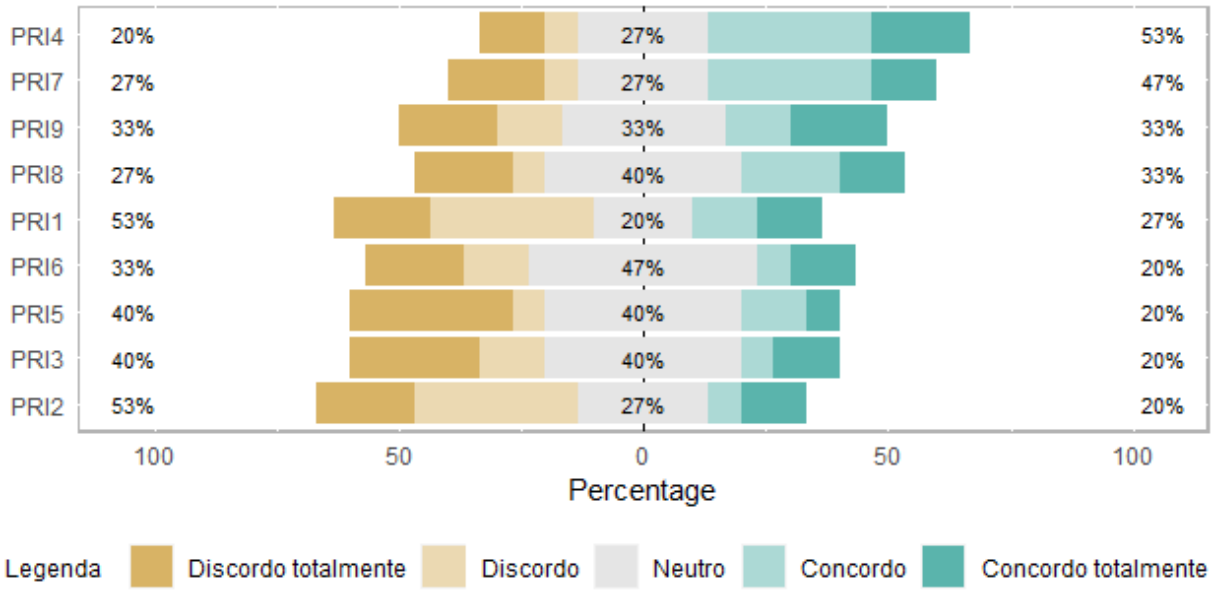
Tabela 8 – Representação em porcentagem das respostas de PRI

	Disc. total.	**Discordo**	**Neutro**	**Concordo**	**Conc. total.**
PRI1	20,00%	33,33%	20,00%	13,33%	13,33%
PRI2	20,00%	33,33%	26,67%	6,67%	13,33%
PRI3	26,67%	13,33%	40,00%	6,67%	13,33%
PRI4	13,33%	6,67%	26,67%	33,33%	20,00%
PRI5	33,33%	6,67%	40,00%	13,33%	6,67%
PRI6	20,00%	13,33%	46,67%	6,67%	13,33%
PRI7	20,00%	6,67%	26,67%	33,33%	13,33%
PRI8	20,00%	6,67%	40,00%	20,00%	13,33%
PRI9	20,00%	13,33%	33,33%	13,33%	20,00%

Fonte: Resultados da pesquisa.

Como se pode observar pelo Gráfico 4, as respostas variaram entre 20% e 46,67% de neutralidade, o que pode indicar a necessidade de mais cuidado com os princípios elencados pela LGPD, em especial ao PRI6 — princípio da segurança descrito no artigo 6º, inciso VII, que trata da utilização, por parte da instituição, de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Gráfico 4 – Representação gráfica das respostas de PRI



Fonte: Resultados da pesquisa.

Ainda analisando as respostas com alto índice de neutralidade quando comparadas aos índices de concordância e discordância, PRI8 — princípio da não discriminação previsto pelo artigo 6º, inciso IX, apesar dos 33,33% de concordância, apresenta um grau ainda maior, de 40%, de neutralidade, fato que preocupa se associado aos 26,67% de discordância, ao tratar da adoção de medidas por parte da instituição que impossibilitem a realização de tratamento para fins discriminatórios, ilícitos ou abusivos desde a coleta à sua utilização, modificação, difusão e eliminação dos dados.

Neste mesmo intervalo de 40% de neutralidade, PRI5 — princípio da transparência previsto pelo artigo 6º, inciso VI, apresenta ainda 40% de discordância e atenta para possíveis adequações por parte da instituição quanto à garantia, aos titulares, de acessibilidade e clareza de informações sobre a realização de tratamento e respectivos agentes responsáveis pelo tratamento de dados. Situação análoga ocorre com PRI3 — princípio do livre acesso previsto pelo artigo 6º, inciso IV, que prevê que a instituição garanta aos titulares consulta gratuita e

facilitada sobre a forma e duração do tratamento, bem como a integralidade de seus dados pessoais.

Com índices iguais de 33,33% para discordância, neutralidade e concordância, PRI9 — princípio da responsabilização e prestação de contas previsto pelo artigo 6º, inciso X, ao abordar a adoção de medidas de observância e cumprimento das normas de proteção de dados pessoais, se responsabilizando pela eficácia dessas medidas.

O maior grau de discordância encontra-se em PRI1 e PRI2, com o índice de 53,33%. PRI1 — princípio da finalidade previsto pelo artigo 6º, inciso I, prevê que a realização do tratamento seja para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. No mesmo contexto, PRI2 — princípios da adequação e necessidade previstos pelo artigo 6º, incisos II e III, trata do nível de comprometimento em atender às finalidades do tratamento de dados informadas ao titular, limitando o tratamento ao mínimo necessário.

PRI4 e PRI7 foram os únicos elementos que apresentaram grau de concordância superior aos demais. Com 53,33% de concordância, PRI4 — princípio da qualidade previsto pelo artigo 6º, inciso V, prevê que seja garantida ao titular a possibilidade de atualização, exatidão, clareza e relevância de seus dados, conforme a necessidade e para o comprimento da finalidade de seu tratamento. Enquanto com 46,66% de concordância, PRI7 — princípio da prevenção previsto pelo artigo 6º, inciso VIII, trata da adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, como, por exemplo, restrições de acessos e autenticações e adoção de criptografias.

Em relação aos comentários adicionais, um dos participantes afirma “desconhecer completamente o processo de coleta e tratamento de dados pessoais”. Outro participante acrescenta que “o sistema SUAP é uma plataforma que contém mecanismos de controle e autenticação. No entanto, outras formas de coleta de dados como inscrições em processos seletivos matrículas, não possuem um mecanismo institucional de controle ou de segurança dos dados, dependendo apenas da boa vontade do servidor envolvido na atividade”. Esses comentários corroboram as análises dos resultados encontrados, de forma que os princípios elencados pelo artigo 6º devem ser observados e a instituição deve adotar mecanismos de controle e proteção quanto ao tratamento de dados.

4.4.3 Tratamento de dados pessoais

A análise do tratamento de dados pessoais (TRA) e os questionamentos feitos aos respondentes tiveram como base o artigo 5 da LGPD e abrangem a investigação do seguinte elemento:

- TRA 1 – A instituição solicita aos titulares ou responsáveis legais seu consentimento por escrito, ou por algum outro meio que demonstre manifestação de vontade, caso haja interesse no tratamento de dados.

Os resultados da coleta são apresentados na Tabela 9:

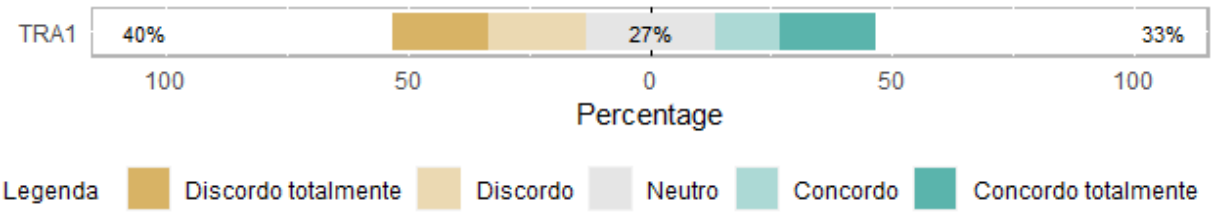
Tabela 9 – Representação em porcentagem das respostas de TRA

	Disc. total.	Discordo	Neutro	Concordo	Conc. total.
TRA1	20,00%	20,00%	26,67%	13,33%	20,00%

Fonte: Resultados da pesquisa.

Inicialmente, observa-se que as respostas apresentam certo grau de neutralidade, de 26,67%, quando comparado aos demais índices. Conforme também pode ser visualizado na Gráfico 5, o índice total de discordância é de 40%, enquanto o total de concordância é de 33,33%.

Gráfico 5 – Representação gráfica das respostas de TRA



Fonte: Resultados da pesquisa.

No que diz respeito aos 40% de discordância, observa-se a necessidade por parte da instituição em solicitar aos titulares ou responsáveis legais seu consentimento caso haja interesse no tratamento de dados, conforme o artigo 7º da LGPD, inciso I. Além deste, há outros nove incisos contendo as hipóteses que devem ser atendidas para poder ser realizado o tratamento de dados pessoais.

Destaca-se aqui o inciso III do mesmo artigo, ao prever a possibilidade, por parte da administração pública, de realizar o tratamento e uso compartilhado de dados necessários à execução de políticas públicas, desde que seja exclusivamente para o atendimento de sua

finalidade pública, na persecução do interesse público, visando executar as competências legais ou cumprir as atribuições legais do serviço público.

Além disso, sempre que for necessário tratar dados pessoais, deve haver um responsável, fornecendo aos titulares desses dados informações legais, objetivas e atualizadas sobre a finalidade, os procedimentos e as práticas que serão usadas para esta atividade.

4.4.4 Direitos do titular de dados

A análise dos direitos do titular de dados (DIR) e os questionamentos feitos aos respondentes tiveram como base o artigo 17 da LGPD e abrangem a investigação de se, quanto do término da finalidade específica do tratamento, a instituição garante aos titulares dos dados o direito de:

- DIR1 – Revogação do consentimento;
- DIR2 – Anonimização dos dados pessoais;
- DIR3 – Bloqueio dos dados pessoais;
- DIR4 – Eliminação dos dados pessoais.

Os resultados da coleta são apresentados na Tabela 10:

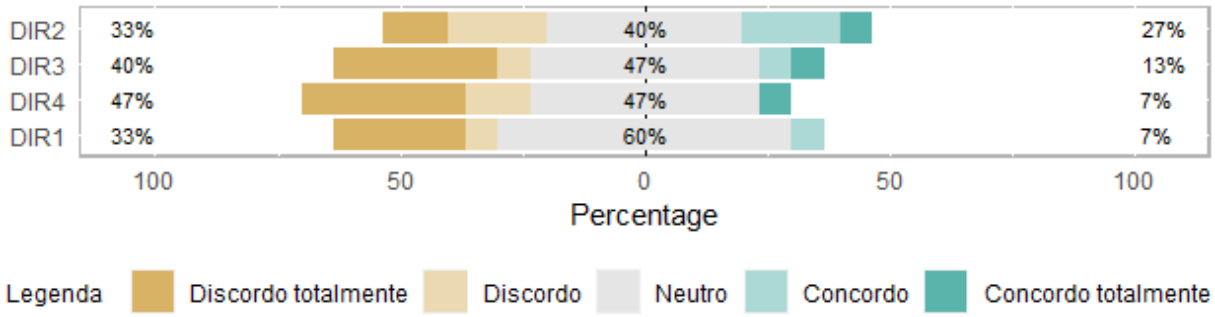
Tabela 10 – Representação em porcentagem das respostas de DIR

	Disc. total.	Discordo	Neutro	Concordo	Conc. total.
DIR1	26,67%	6,67%	60,00%	6,67%	0,00%
DIR2	13,33%	20,00%	40,00%	20,00%	6,67%
DIR3	33,33%	6,67%	46,67%	6,67%	6,67%
DIR4	33,33%	13,33%	46,67%	0,00%	6,67%

Fonte: Resultados da pesquisa.

Como é possível perceber pelo Gráfico 6, as respostas se concentraram em uma faixa entre 40% e 60,00% de neutralidade, podendo indicar a necessidade de atenção aos direitos do titular de dados elencados pela LGPD, em especial ao DIR1 — direito do titular de revogar seu consentimento, previsto pelo artigo 18, inciso IX.

Gráfico 6 – Representação gráfica das respostas de DIR



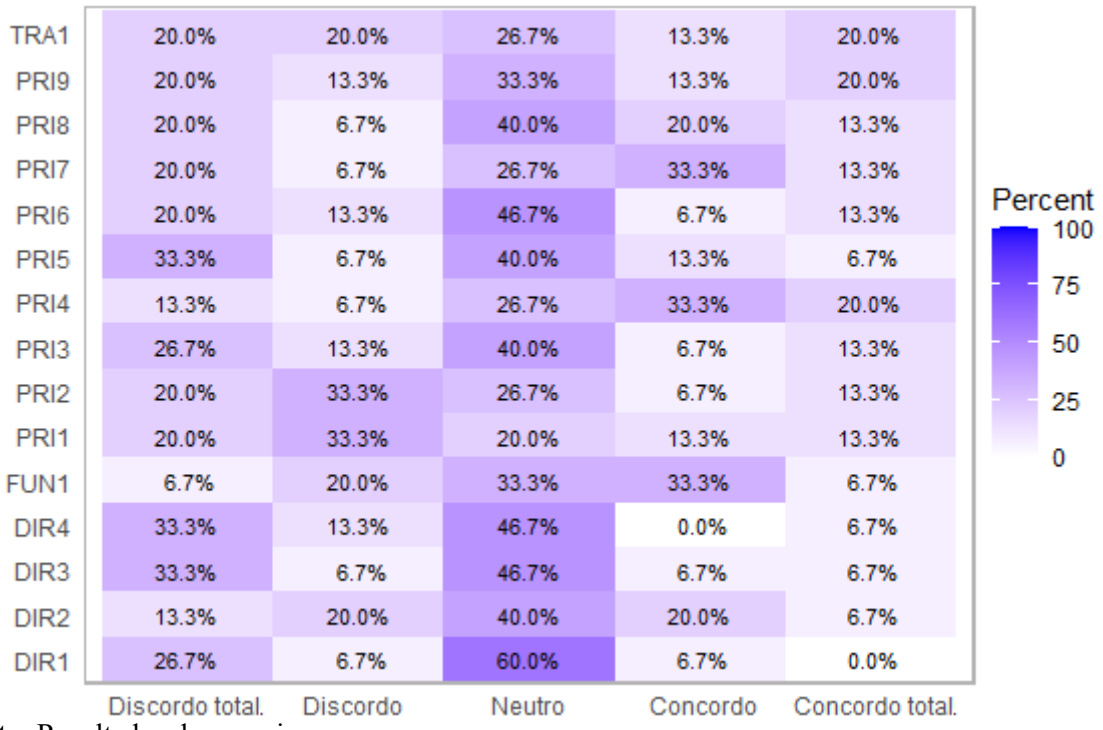
Fonte: Resultados da pesquisa.

O DIR4 - direito do titular de solicitar a eliminação de seus dados pessoais, conforme o artigo 18, inciso VI, apresenta uma porcentagem de 46,67% de neutralidade e de discordância. DIR3 - direito do titular de solicitar o bloqueio de seus dados pessoais previsto pelo artigo 18, inciso IV, apresenta, além dos 46,67% de neutralidade, 40% de discordância. Por fim, DIR2 - direito do titular de solicitar a anonimização de seus dados pessoais previsto pelo artigo 18, inciso IV, apresenta 40% de neutralidade, 33,33% de discordância e 26,67% de concordância.

Os resultados encontrados apresentam-se congruentes com os comentários adicionais dos participantes ao afirmarem que “o usuário não é informado de como seus dados serão tratados, e não é indicado uma manifestação ou autorização do usuário em relação ao uso de seus dados; não há processo institucional de eliminação dos dados; quanto à anonimidade dos dados, não há clareza entre divulgação e publicação dos dados, tendo confusão entre esses dois conceitos”. Adicionalmente, um dos participantes afirma “nunca ter tido informações a respeito das questões acima, crendo que falta mais ênfase na divulgação deste trabalho, caso exista”.

Por sua vez, a análise das dimensões apresenta certo grau de neutralidade quando comparado aos de discordância e concordância, conforme pode ser visualizado no mapa de calor ilustrado pelo Gráfico 7.

Gráfico 7 – Mapa de calor das respostas das dimensões de proteção de dados pessoais



Fonte: Resultados da pesquisa.

Adicionalmente, quando do tratamento de seus dados pessoais, o consentimento do titular deve evidenciar sua manifestação de vontade expressa e inequívoca, assim como os direitos de revogação do consentimento, alteração, anonimidade, bloqueio ou eliminação dos dados pessoais. Deve-se, ainda, assegurar que cada ‘finalidade’ seja exclusiva, legítima, detalhada, clara e adequada ao contexto de cada finalidade informada, de modo que a operação se limite ao mínimo indispensável e permita o seu acesso total, gratuito e simplificado, garantindo a ‘qualidade dos dados’ pela sua precisão, relevância, atualização e ‘transparência’, sem abrir mão da adoção de medidas que comprovem a ‘segurança’, ‘prevenção’, ‘não discriminação’, ‘responsabilização e prestação de contas’ por parte do agente de tratamento.

O Gráfico 8 representa os elementos aqui discutidos e analisados, ilustrando o fluxo de proteção de dados pessoais dentro da instituição.

Gráfico 8 – Fluxo de proteção de dados pessoais

Fonte: Resultados da pesquisa.

Apesar de a instituição adotar uma PoSIC, observa-se pela Tabela 6 que grande parte dos participantes afirmam não saberem dizer que isto ocorre. A afirmação concorda com o alto nível de discordância demonstrada pelo Gráfico 2, quanto à adoção de controles técnicos, transparência e livre acesso, treinamentos ou eventos que tratem da privacidade, comunicação e conscientização sobre segurança da informação. A única exceção é o uso de diferentes métodos de autenticação pela instituição, o que aumenta significativamente a segurança em relação aos controles de acesso.

As adequações para o *campus* são necessárias no que diz respeito ao relacionamento do contexto institucional com as dimensões de proteção de dados pessoais previstas pela LGPD, evidenciando a necessidade de implementação de um programa de governança em privacidade

que esteja conforme a PoSIC institucional, de forma transparente, com controles técnicos, treinamentos, comunicações e conscientizações.

Essas medidas estabelecem um vínculo de comprometimento e promovem uma relação de confiança entre o titular de dados e a instituição por serem efetivas, aplicáveis e adaptáveis.

Portanto, mesmo sendo limitada a um estudo de caso único, a análise dos dados permitiu que a pesquisa atinja seu objetivo de verificar, conforme os instrumentos normativos de proteção de dados adotados pela instituição, os atuais desafios para o desenvolvimento de políticas e procedimentos e verificar como são tratados e divulgados internamente os protocolos de proteção de dados em um de seus *campi*.

A segurança da informação e a proteção de dados pessoais devem ser consideradas de acordo com o contexto institucional. Ele inclui a investigação de vários fatores, como a adoção de uma PoSIC esclarecedora, controles técnicos, transparência e acesso às informações, treinamentos e eventos sobre privacidade, métodos de autenticação, comunicação e conscientização sobre proteção de informações confidenciais em formato eletrônico.

Apesar dos resultados indicarem a presença de controles técnicos de proteção de dados pessoais armazenados, sugere-se ampliar a transparência e o acesso às informações, além disso, há poucos treinamentos ou eventos que tratem da privacidade e operações que envolvam dados pessoais. A conscientização e a comunicação de questões relacionadas à segurança, privacidade e proteção de dados confidenciais em formato eletrônico também são insuficientes.

Sugerimos, para além de uma maior divulgação organizacional da Política de Segurança da Informação e Comunicação da instituição, a inclusão em seu texto de um Programa de Capacitação de Segurança da Informação que abranja em seus módulos a importância e as diversas maneiras de se aperfeiçoar as práticas de proteção de dados pessoais.

O direito à privacidade tornou-se relevante na atualidade, como discutimos em tópicos anteriores, e está tingido de matizes éticas ainda bastante sutis: todos sabemos que estamos expostos na rede, mas poucos temos plena consciência de quanto ou do que pode ser feito com nossas informações.

É notável que, em uma Instituição de Ensino Tecnológico, que oferta cursos na área de TICs, mais da metade de seu corpo docente ainda não tenha clareza de quais são as diretrizes da política institucional que trata do manejo dos dados pessoais produzidos por eles próprios no exercício das suas funções, uma vez que essa também poderá ser a realidade de vários outros *campi* e outras instituições de ensino.

Cabe, portanto, integradamente às boas práticas institucionais, o desenvolvimento e aplicação de um programa de gestão educacional conscientização com oferta contínua de ações

educativas de métodos diversos como, por exemplo, materiais digitais, treinamentos, *workshops*, seminários, cursos, entre outros, na busca de estabelecer um ecossistema integrado e consciente quanto aos direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural quando do tratamento de dados pessoais.

E compete à sociedade, como um todo, fomentar e aprimorar a discussão sobre um tema tão sensível. A falta de envolvimento das instituições de educação, seus profissionais e estudantes, torna impossível a realização deste objetivo, portanto, é necessário que sejam feitas mais pesquisas a respeito.

5 CONSIDERAÇÕES FINAIS

O processo de conclusão desta pesquisa materializa um longo e profícuo processo de doutoramento, realizado no Programa de Pós-Graduação em Educação Escolar da Unesp Araraquara, e esteve permeado de desafios relacionados a compreender o debate sobre a Lei Geral de Proteção de Dados no âmbito da Política Educacional. Como demonstrado na introdução, vale ratificar a informação sobre a ausência de pesquisas relacionadas ao tema e materializadas em outras teses, o que fez com que o ineditismo do debate estimulasse a sistematização da produção de conhecimento, todavia suscitou lacunas nas quais esta tese visou preencher, entendendo os limites que aqui são postos.

Enquanto pesquisador tem-se a concepção da produção de conhecimento como algo em movimento. A realidade social aguça novos elementos e o tema provoca muitos outros debates, que poderão e deverão ser incorporados no âmbito da pesquisa e ciência. Entretanto, inicialmente, cabe apontar que o objetivo desta pesquisa foi examinar, de acordo com os regulamentos de proteção de dados adotados numa instituição pública de ensino tecnológico, os desafios atuais para o desenvolvimento de políticas e procedimentos a partir da vigência da LGPD.

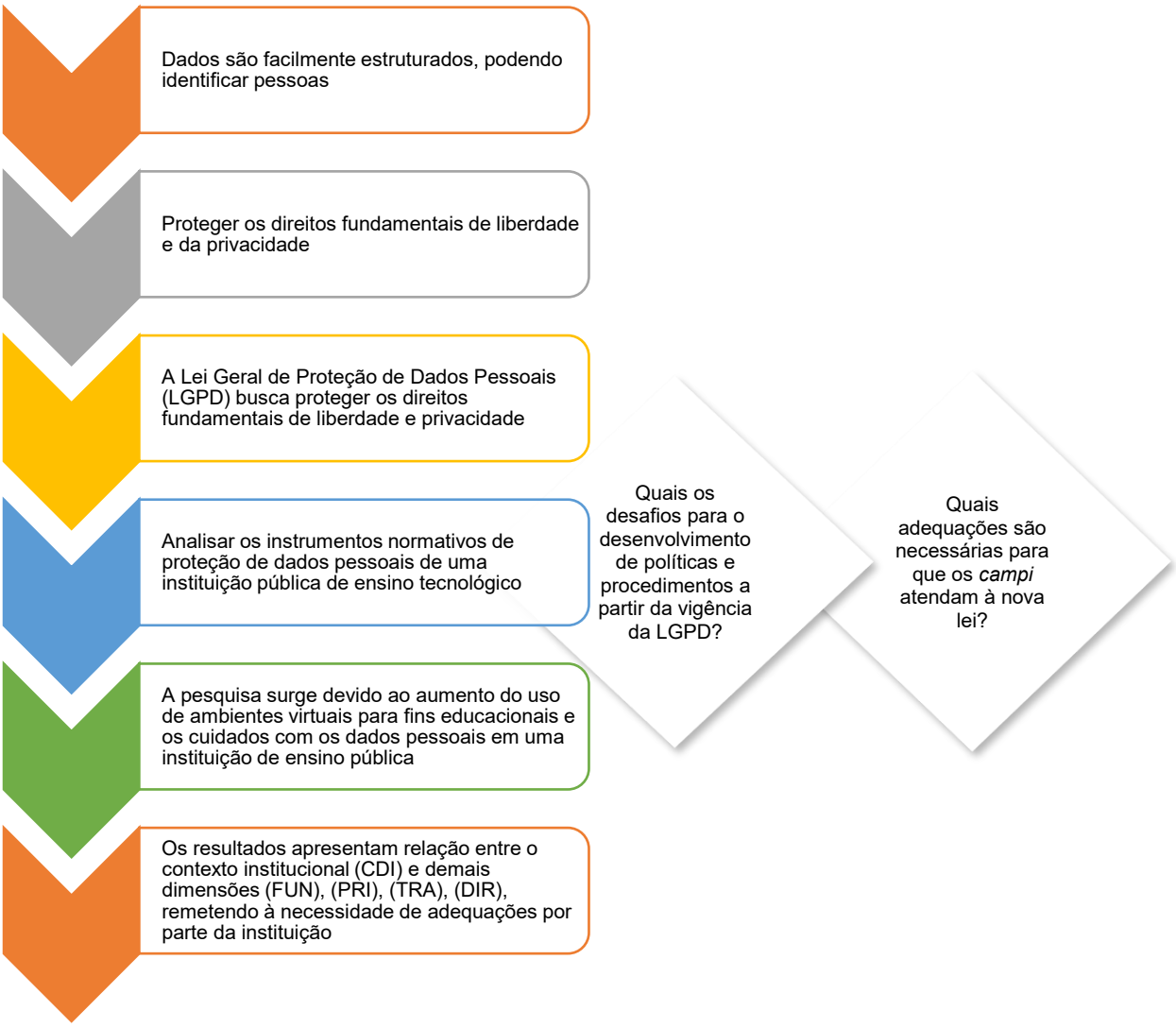
Entende-se que o trabalho é relevante tanto do ponto de vista prático quanto teórico, pois analisou como os protocolos de proteção de dados são tratados em um *campus* de uma instituição pública de ensino tecnológico, à luz da Lei Geral de Proteção de Dados (LGPD), considerando o seu contexto e as suas dimensões. Porém, cabe pontuar que uma vez que se trata de um estudo de caso único, os resultados não permitem uma generalização, que, para tal, requereria a abordagem em diferentes *campi* e instituições, embora avalie-se que há similitudes e divergências que novos estudos poderão demonstrar.

Os limites aqui postos apontam limitações de recursos financeiros e possível indisponibilidade de aplicar a pesquisa em diferentes locais, uma vez que, ao respeitarem normas internas e serem observadas as disposições contidas na própria LGPD, não seria adequado o fornecimento de informações a pesquisadores externos sem a participação de docentes internos que detêm autorização institucional para projetos de natureza *intercampi* ou interinstitucionais. Entretanto, é fundamental que o estudo não se finde na conclusão desta tese e avance com elementos futuros no âmbito da produção de conhecimento e ciência no país.

Nesta direção, a Figura 4 apresenta os elementos principais considerados para a execução desta pesquisa, demonstrando que, com o crescimento de ambientes virtuais, tornou-se indispensável um maior cuidado com os dados pessoais e quais as normas de proteção desses

dados foram adotadas em um *campus* de ensino tecnológico a partir da vigência da Lei Geral de Proteção de Dados Pessoais (LGPD). Portanto, é necessário entender que há relação entre o fluxo dos elementos principais que se articulam nesta pesquisa.

Figura 4 – Fluxo dos Elementos Principais



Fonte: Elaboração própria.

Considera-se que os resultados e as análises dos dados apresentam a relação entre o contexto institucional (CDI) e as dimensões de proteção de dados pessoais que tangem fundamentos (FUN), princípios (PRI), tratamento de dados pessoais (TRA) e direitos do titular de dados (DIR), remetendo à necessidade de adequações por meio de um programa de conscientização em proteção de dados pessoais, que tenha por objetivo auxiliar o estabelecimento de uma cultura de privacidade institucional, ao promover ações educativas diversificadas, que visam uma compreensão satisfatória das principais diretrizes de proteção de

dados pessoais, na busca do contínuo alinhamento entre o ecossistema institucional e sua segurança.

A partir das ações educativas, poder-se-á estabelecer um indicador do índice de conscientização em segurança, como por exemplo, pela mensuração da quantidade de treinamentos realizados ou previstos, podendo também integrar-se ao programa de governança em privacidade, previsto no inciso I do Artigo 50 da LGPD, na busca de eficiência operacional no controle e categorização dos dados.

O conteúdo educativo é de livre construção, podendo incluir apresentações, vídeos, eventos de treinamento, sessões interativas com debates, ferramentas e recursos diversos, que auxiliem na compreensão da relevância da proteção de dados pessoais, como protegê-los e como implementar práticas cotidianas.

Avalia-se que a proposição de um programa educacional, como parte de produto desta tese, tem contribuição de intervenção na realidade estudada. Por isso, recomenda-se o mapeamento da comunidade pela aplicação de questionamentos sobre conhecimentos básicos e gerais sobre privacidade e proteção de dados pessoais, buscando assim identificar prioridades de implementação de ações de conscientização que podem ser estruturadas conforme o modelo proposto pela Tabela 11. Este programa engloba diferentes etapas, visando a conscientização a partir de eixos estruturantes, que contribuirão com resultados esperados e dialogarão com a garantia de cumprimento da legislação referente à proteção de dados pessoais.

Tabela 11 - Programa educacional de conscientização em proteção de dados pessoais

Etapa	Conscientização	Resultado esperado
1	Objetivos da LGPD	Compreensão da necessidade de proteção aos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural
2	Fundamentos, princípios básicos da LGPD	Compreensão dos fundamentos e princípios básicos de proteção de dados pessoais, assim como suas implicações para a instituição
3	Adequação e sustentação à LGPD	Alinhamento e direcionamento entre missão, visão e valores institucionais para com os requisitos legais de proteção de dados pessoais
4	Matriz de responsabilidades	Direcionamento das responsabilidades das partes envolvidas na Governança, como por exemplo do Comitê de Privacidade, do Encarregado de Proteção de Dados, dos Servidores, dos Colaboradores, entre outros

5	Processos e procedimentos internos	Compreensão mais específica, detalhada e aprofundada dos processos e procedimentos institucionais buscando o constante alinhamento aos fundamentos e princípios de proteção de dados pessoais
6	Alinhamento entre Sistemas e LGPD	Abordagem sobre a relação entre os sistemas de segurança da informação e a privacidade de dados pessoais
7	Alinhamento entre PoSIC, demais políticas e LGPD	Abordagem sobre as políticas institucionais e de privacidade, procedimentos, normas, medidas técnicas e documentos institucionais em conformidade à LGPD
8	*Privacy by Design*	Esclarecimentos sobre a inserção de medidas de privacidade desde a concepção dos projetos, na busca de: Proatividade e prevenção; privacidade por padrão desde a concepção de projetos, arquiteturas de sistemas e processos; privacidade incorporada à arquitetura ou desenho de sistemas, produtos ou serviços; funcionalidade total; segurança de ponta a ponta do ciclo de vida do tratamento de dados pessoais; visibilidade e transparência; respeito à privacidade do usuário
9	Comunicação	Promoção e acompanhamento do programa de conscientização; esclarecimentos e direcionamentos sobre os canais internos e externos de comunicação envolvidos na proteção de dados pessoais: ANPD, canais de alerta de incidentes de segurança, vazamento de dados pessoais e demais dúvidas relacionadas
10	Avaliação e monitoramento	Monitoramento do ambiente organizacional com objetivo de analisar o grau ou maturidade de conscientização.

Cabe pontuar que a criação de um programa educacional de conscientização em proteção de dados pessoais dialoga com os resultados da pesquisa, que demonstram ausências e fragilidades no âmbito da aplicação da LGPD na Política Educacional. Considera-se que as produções acadêmicas devem ter impactos teóricos e empíricos na realidade social que é investigada e, por isso, essa proposição partiu de eixos e lacunas observadas ao longo da realização da pesquisa.

Diante do exposto, sugere-se que além da implantação do programa aqui proposto, tenha-se como norte a necessidade deste estudo ser ampliado em projetos futuros, contemplando a coleta de diferentes amostras, bem como o uso de outras técnicas que levem em consideração este contexto em futuras pesquisas ou projetos de ensino e extensão.

REFERÊNCIAS

ABNT. **NBR ISO/IEC 27701: Técnicas de segurança - Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação - Requisitos e diretrizes.** Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2019.

ABNT. **NBR ISO/IEC 27001: Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos.** Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2022.

ABNT. **NBR ISO/IEC 27002: Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação.** Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2022.

BRASIL. **Lei n. 9.394, de 20 de dezembro de 1996**. Estabelece as diretrizes e bases da educação nacional. Brasília, DF: Presidência da República, 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9394.htm. Acesso em: 30 ago. 2020.

BRASIL. **Instituto Federal de Educação, Ciência e Tecnologia de São Paulo.** Brasília, DF: MEC, 2008. Disponível em: https://www.ifsp.edu.br/. Acesso em: 13 dez. 2020.

BRASIL. **Resolução IFSP n.º 1, de 31 de agosto de 2009**. Estatuto do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo. Brasília, DF: MEC, 2009. Disponível em: https://ifsp.edu.br/o-que-e-rss/9-assuntos/reitoria/78-documentos-institucionais. Acesso em: 05 fev. 2021.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 30 ago. 2020.

BRASIL. **Portaria IFSP n. 2.534, de 14 de julho de 2020**. Institui o Comitê de Governança Digital (CGD) e dispõe e aprova o Regimento Interno do Comitê de Governança Digital no âmbito do IFSP. Brasília, DF: MEC, 2020a. Disponível em: https://www.ifsp.edu.br/component/content/article?layout=edit&id=2679. Acesso em: 14 jul. 2020.

BRASIL. **Portaria IFSP n. 4296, de 14 de dezembro de 2020**. Aprova a atualização da Política de Segurança da Informação e Comunicação - PoSIC no âmbito do Instituto Federal de Educação, Ciência e Educação de São Pauto - IFSP. Brasília, DF: MEC, 2020b. Disponível em: https://www.ifsp.edu.br/component/content/article?layout=edit&id=2679. Acesso em: 14 dez. 2020.

BRASIL. **Portaria IFSP n. 2.755, de 22 de abril de 2021**. Implementa a Política de Proteção de Dados Pessoais do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo. Brasília, DF: MEC, 2021. Disponível em: https://www.ifsp.edu.br/component/content/article?layout=edit&id=2679. Acesso em: 22 abr. 2021.

BRASIL. **Emenda Constitucional n. 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 11 fev. 2022.

BRASIL. **Lei n. 14.533, de 11 de janeiro de 2023**. Institui a Política Nacional de Educação Digital. Brasília, DF: Presidência da República, 2023. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Lei/L14533.htm. Acesso em: 12 jan. 2023.

CAIRES, V. G.; OLIVEIRA, M. A. M. **Educação Profissional Brasileira:** da colônia ao PNE 2014-2024. Petrópolis/RJ: Vozes, 2018.

DAVENPORT, T. H. **Ecologia da informação:** Porque só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998.

EUROPEAN COMMISSION. **General Data Protection Regulation:** GDPR. 2018. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection_en. Acesso em: 30 ago. 2020.

FERREIRA, R. da S. A Sociedade da Informação como sociedade de disciplina, vigilância e controle. **Inf. cult. soc**., Ciudad Autónoma de Buenos Aires, n. 31, p. 109-120, dic. 2014. Disponible em: http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S1851-17402014000200007&lng=es&nrm=iso. Acesso em: 08 jul. 2023.

FOUCAULT, M. **Vigiar e Punir:** nascimento da prisão. Petrópolis: Vozes, 2013.

FRIGOTTO, G. Apresentação. *In*: FRIGOTTO, G (Org.). **Institutos Federais de Educação, Ciência e Tecnologia:** relação com o ensino médio integrado e o projeto societário de desenvolvimento**.** Rio de Janeiro: UERJ, LPP, 2018. p. 7-14.

KENSKI, V. M. Democratização das mídias e a gestão em educação a distância. *In*: OLIVEIRA, M. A. M. (org.). **Gestão Educacional**: Novos Olhares, Novas Abordagens. Petrópolis, RJ: Vozes, 2005.

LÉVY, P. **A esfera semântica.** Tomo 1: Computação, cognição e economia da informação. São Paulo: Annablume, 2014.

LIKERT, R. A technique for the measurement of attitudes. **Archives of Psychology**, v. 22, n. 140, p. 55, 1932. Disponível em: https://psycnet.apa.org/record/1933-01885-001. Acesso em: 19 fev. 2021.

LÜDKE, M.; ANDRÉ, M. E. D. A. **Pesquisa em educação:** Abordagens qualitativas. 2. ed. Rio de Janeiro: E.P.U., 2018.

MARTINS, G. A. **Estudo de caso:** Uma estratégia de pesquisa. São Paulo: Atlas, 2006.

MARTINS, G. A.; THEÓPHILO, C. R. **Metodologia da investigação científica para ciências sociais aplicadas.** São Paulo: Atlas, 2007.

MENDES, L.; DONEDA, D. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *In*: **Revista de Direito do Consumidor.** São Paulo: Ed. RT, vol. 120. ano 27, nov.-dez. 2018, p. 469-483.

PACHECO. E. **Os Institutos Federais:** uma revolução na educação profissional e tecnológica. Brasília/ São Paulo: Santilhana/Moderna, 2011.

RECUERO, R. **Conversação em rede:** Comunicação mediada pelo computador e redes sociais na internet. Porto Alegre: Sulina, 2012.

REIS, E. A.; REIS, I. A. Análise Descritiva de Dados. **Relatório Técnico do Departamento de Estatística da UFMG**. 2002. Disponível em: http://www.est.ufmg.br. Acesso em: 26 abr. 2022.

SANTAELLA, L. **Comunicação ubíqua**: Repercussões na cultura e na educação. São Paulo: Paulus, 2013.

SAVIANI, D. Trabalho e Educação, Fundamentos ontológicos e históricos. **Revista Brasileira de Educação**, v.12, n. 34, p. 152-180, jan./abr., 2007.

SEVERINO, A. J. **Metodologia do Trabalho Científico**: Antônio Joaquim Severino. 2. ed. São Paulo: Cortez, 2017.

SOUZA, J. G. S. **Análise de tratamento da segurança da informação na gestão de riscos da governança de tecnologia da informação de uma instituição de ensino público federal.** 2017. Dissertação (Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos) – Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2017. Disponível em: http://www.pos.cps.sp.gov.br/files/dissertacoes/file/73/b55e568c03373ffe558008fa6e0ad2fa.pdf. Acesso em: 17 jan. 2021.

SOUZA, J. G. S.; ARIMA, C. H.; BELDA, F. R. Análise de tratamento da segurança da informação na gestão de riscos da governança de tecnologia da informação de uma instituição de ensino público federal. **Revista Ibero-Americana de Estudos em Educação,** Araraquara, v. 15, n.3, p. 1309-1321, jul./set.2020. e-ISSN: 1982-5587. DOI: https://doi.org/10.21723/riaee.v15i3.13584

SOUZA, J. G. S; BELDA, F. R.; ARIMA, C. H. Análise de aplicação da LGPD numa instituição pública de ensino: Um estudo de caso. **Revista Ibero-Americana de Estudos em Educação**, Araraquara, v. 17, n. 3, p. 1856-1872, jul./set. 2022. e-ISSN: 1982-5587. DOI: https://doi.org/10.21723/riaee.v17i3.16789. Acesso em: 25 jun. 2023.

SPANCESKI, F. R. **Política de segurança da informação:** Desenvolvimento de um modelo voltado para instituições de ensino. 2004. Trabalho de Conclusão de Curso (Bacharel em Sistema de Informação) – Instituto Superior Tupy, Joinville, 2004. Disponível em: http://www.mlaureano.org/aulas_material/orientacoes2/ist_2004_francini_politicas.pdf. Acesso em: 11 fev. 2021.

STOKES, D. E. **O quadrante de Pasteur:** A ciência básica e a inovação tecnológica**.** Campinas, SP: Editora da Unicamp, 2005.

UNIÃO EUROPEIA. **Diretiva n. 95/46/CE, de 24 de outubro de 1995**. 31995L0046. Parlamento Europeu. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=EL. Acesso em: 03 mar. 2021.

UNIÃO EUROPEIA. **European Commission.** 2007. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. Acesso em: 03 mar. 2021.

UNIÃO EUROPEIA. **European Data Protection Board (EDPB)**. 2018. Disponível em: https://edpb.europa.eu/. Acesso em: 03 mar. 2021.

XAVIER, F. C. **Fonte viva**. Rio de Janeiro: FEB, 1956.

YIN, R. K. **Estudo de caso:** Planejamento e métodos**.** 2. ed. Porto Alegre: Bookman, 2001.

APÊNDICES

APÊNDICE A – Termo de consentimento livre e esclarecido

1. Você está sendo convidado(a) a participar voluntariamente da pesquisa “Proteção de dados pessoais na gestão educacional: um estudo de caso com a LGPD no contexto das ações propostas por uma instituição pública de ensino”.

2. Com a intensificação na utilização de ambientes presenciais remotos e entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709, de 14 de agosto de 2018, esta pesquisa tem por objetivo verificar, conforme os instrumentos normativos de proteção de dados pessoais adotados pela Instituição Pública de Ensino Tecnológico, os desafios para o desenvolvimento de políticas e procedimentos. Trata-se de um estudo aplicado ao campus Campinas do Instituto Federal de Educação, Ciência e Tecnologia - IFSP, com método quantitativo e qualitativo, tendo como ferramenta de coleta questionários estruturados e o tratamento estatístico dos dados. A partir do objetivo aqui apresentado, tem-se como resultados esperados da pesquisa a melhor compreensão da aderência e aplicação da LGPD no contexto do campus e possíveis melhorias no desenvolvimento de políticas e procedimentos a partir de sua vigência. Você foi selecionado(a) por ser docente ou gestor(a) vinculado ao campus Campinas, e sua participação não é obrigatória. Sua participação nesta pesquisa consistirá em responder questionários fechados e/ou abertos divididos em 5 seções e tempo de preenchimento de 35 minutos, aproximadamente.

3. Os riscos de sua participação nesta pesquisa poderão envolver desconforto ou cansaço. Portanto, recomenda-se um ambiente aconchegante e adoção de pausas ou intervalos durante o processo de leitura e preenchimento do formulário.

4. Cabe esclarecer que esta pesquisa não tem finalidade de realizar diagnóstico individual, mas sim um levantamento coletivo. Seu nome ou informações que possam lhe identificar não serão coletados e os dados serão mantidos em sigilo, assegurando, assim, sua privacidade.

5. Os participantes terão assegurados o direito de acompanhamento e assistência em qualquer etapa da pesquisa com apoio da Unidade Auxiliar do Centro de Pesquisas da Infância e da Adolescência "Dante Moreira Leite" (CENPE), da Faculdade de Ciências e Letras de Araraquara pelo endereço de e-mail cenpe.fclar@unesp.br ou telefone (16) 3334-6225.

6. Qualquer acompanhamento, dúvida ou solicitação de esclarecimentos adicionais, poderão também ser esclarecidos em contato com o Comitê de Ética em Pesquisa (CEP) da Faculdade de Ciências e Letras - Câmpus de Araraquara (FCLAr) da UNESP, Rod. Araraquara-Jaú Km 1 - Machados - Araraquara/SP - CEP 14800-901. por meio do endereço de e-mail comitedeetica.fclar@unesp.br e telefone de contato (16) 3334-6224 ou equipe científica do projeto pelo endereço de e-mail jgs.souza@unesp.br e telefone de contato (016) 98132-7580.

7. A qualquer momento você poderá desistir de participar e retirar seu consentimento. Sua recusa não trará nenhum prejuízo em sua relação com o pesquisador ou com a instituição.

8. As informações coletadas serão confidenciais e estão assegurados o sigilo sobre sua participação, assim como os dados não serão divulgados de forma a possibilitar sua identificação.

9. Por tratar-se de formulário disponibilizado em plataforma online e de forma gratuita, sua participação nesta pesquisa não acarretará despesas ou custos, não havendo, portanto, necessidade de quaisquer ressarcimentos. Deste modo, sua participação voluntária estará condicionada ao aceite do convite assinalando a opção “Li e concordo”.

10. Você poderá solicitar uma via deste termo onde consta o endereço de e-mail e telefone de contato do CEP e do pesquisador principal, podendo tirar suas dúvidas sobre o projeto e sua participação, agora ou a qualquer momento.

CAAEs: 52015721.3.0000.5400 / 52015721.3.3001.5473

Declaro que entendi os objetivos, riscos e benefícios de minha participação na pesquisa e concordo em participar. O pesquisador me informou que o projeto foi aprovado pelo Comitê de Ética em Pesquisa em Seres Humanos da Faculdade de Ciências e Letras do Campus de Araraquara- UNESP, localizada à Rodovia Araraquara-Jaú, Km 1 – Caixa Postal 174 – CEP: 14800-901 – Araraquara – SP – Fone: (16) 3334-6264 – endereço eletrônico: comitedeetica@fclar.unesp.br.

Assinatura do pesquisador e consentimento eletrônico do participante da pesquisa.

APÊNDICE B – Questionário estruturado de coleta de dados

INSTRUMENTO DE PESQUISA

Saudações,

Sou Jackson Gomes Soares Souza (http://lattes.cnpq.br/0153557477666204), aluno de Doutorado Acadêmico do Programa de Pós-Graduação em Educação Escolar da Faculdade de Ciências e Letras - Câmpus de Araraquara da Universidade Estadual Paulista "Júlio de Mesquita Filho" - UNESP. Estou desenvolvendo sob a orientação do Professor Doutor Francisco Rolfsen Belda (http://lattes.cnpq.br/9910965797411044), pesquisa com o título de "Proteção de dados pessoais na gestão educacional: um estudo de caso com a LGPD no contexto das ações propostas por uma instituição pública de ensino" e, para tanto, necessito coletar dados junto a docentes e gestores do Campus Campinas do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo.

Trata-se, portanto, de um convite para participação voluntária em responder ao formulário de pesquisa.

Ressalto que os dados coletados individualmente não permitirão a identificação dos participantes, serão mantidos em sigilo, e o relatório de pesquisa poderá ser publicado cientificamente. Informo também que se trata de trabalho de cunho científico e acadêmico, vinculado à linha de pesquisa em Política e Gestão Educacional, e os resultados permitirão uma melhor compreensão da aderência e aplicação da Lei Geral de Proteção de dados pessoais - LGPD -, no contexto do campus, assim como possíveis melhorias no desenvolvimento de políticas e procedimentos a partir de sua vigência.

Por fim, qualquer dúvida sobre a pesquisa poderá ser esclarecida diretamente com pesquisador por meio do e-mail: jgs.souza@unesp.br.

INFORMAÇÕES PRELIMINARES

Os questionamentos a seguir foram elaboradas com base na Lei Geral de Proteção de Dados (LGPD) - Lei nº. 13.709, de 14 de agosto de 2018, e auxiliarão a compreender e verificar, a partir de sua vigência, o contexto do Campus Campinas em relação às normas de segurança da informação adotadas pelo IFSP, assim como os desafios para o desenvolvimento de políticas e procedimentos, considerando-se os instrumentos normativos de proteção de dados adotados pela Instituição Pública de Ensino Tecnológico.

Sugere-se a abertura do link abaixo em uma segunda aba no navegador para consultas necessárias e caso surjam dúvidas quanto aos termos utilizados.

Lei 13.709/2018 (LGPD):
http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm

Terminologia (Artigo 5º da LGPD):
Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
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;
Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
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;
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;
Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

QUESTÕES DE PESQUISA

PERFIL DO PARTICIPANTE (PDP)

PDP1) Faixa etária
18 a 29 anos; 30 a 39 anos; 40 a 49 anos; 50 a 59 anos; 60 a 69 anos.
PDP2) Escolaridade
Graduação; Especialização; Mestrado; Doutorado; Pós-Doutorado.
PDP3) Tempo na instituição (em anos)
até 1 ano; entre 1 e 3 anos; entre 4 e 10 anos; entre 10 e 20 anos; Mais de 20 anos.
PDP4) Ocupa cargo de gestão atualmente?
Sim; Não.

CONTEXTO DA INSTITUIÇÃO (CDI)

CDI1) A instituição adota uma Política de Segurança da Informação e Comunicações (PoSIC) suficientemente esclarecedora sobre o que deve ser feito para aprimorar a proteção dos dados e informações das pessoas?
A instituição não adota uma PoSIC; A instituição adota uma PoSIC, porém não tenho ciência sobre seu conteúdo; Não sei dizer se a instituição adota uma PoSIC; A instituição adota uma PoSIC, porém seu conteúdo não é suficientemente esclarecedor; A instituição adota uma PoSIC suficientemente esclarecedora

Obs.: Todos os próximos questionamentos adotarão como possíveis respostas a escala Likert de discordo totalmente (1) a concordo totalmente (5), com exceção ao último campo de cada seção que permitirá ao respondente complementar ou detalhar de forma descritiva suas respostas.

CDI2) Tenho conhecimento de que a instituição implementa controles técnicos para proteger dados pessoais armazenados em seus sistemas de TI
CDI3) A instituição oferece, aos seus titulares, transparência e livre acesso às informações e dados pessoais armazenados em seus sistemas de TI
CDI4) A instituição conduz treinamentos ou eventos que tratem da privacidade e proteção de dados pessoais e operacionais/institucionais

CDI5) A instituição adota, para o acesso dos usuários aos sistemas, diferentes métodos de autenticação, como por exemplo usuário e senha, biometria, tokens por aplicativos
CDI6) A instituição comunica, por meio de avisos, questões relacionadas à privacidade e proteção de dados
CDI7) Eu acredito que todos na instituição estejam cientes do contexto da segurança da informação
CDI8) Eu acredito que todos na instituição estejam cientes de como proteger informações confidenciais em formato eletrônico
CDI-D) Gostaria de detalhar ou complementar alguma resposta desta seção?

FUNDAMENTOS E PRINCÍPIOS (FUN)

FUN1) A instituição preocupa-se com a proteção de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural
PRI) Durante o processo de coleta e tratamento de dados pessoais, a instituição INFORMA a seus titulares:
PRI1) A(s) finalidade(s) específica(s) do uso desses dados
PRI2) Seu nível de comprometimento em atender à(s) finalidade(s) informada(s)
PRI3) Se permite consulta gratuita e facilitada sobre a forma e duração do tratamento, bem como a integralidade de seus dados pessoais
PRI4) Se permite a atualização de seus dados
PRI5) Se fornece acessibilidade e clareza de informações sobre a realização de tratamento
PRI6) Se utilizam de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração e comunicação
PRI7) Se utilizam de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (Exemplos: restrições de acessos e autenticações, adoção de criptografias)
PRI8) Se impossibilita a realização de tratamento para fins discriminatórios, ilícitos ou abusivos? (desde a coleta à sua utilização, modificação, difusão e eliminação dos dados)
PRI9) Se adotará medidas de observância o cumprimento das normas de proteção de dados pessoais, se responsabilizando pela eficácia dessas medidas
PRI-D) Gostaria de detalhar ou complementar alguma resposta desta seção?

DIREITOS DO TITULAR E TRATAMENTO (TRA)

TRA1) A instituição solicita aos titulares ou responsáveis legais seu consentimento por escrito ou por algum outro meio que demonstre manifestação de vontade, caso haja interesse no tratamento de dados

DIR) Ao término da finalidade específica do tratamento, a instituição garante aos titulares dos dados o direito de:

DIR1) Revogação do consentimento

DIR2) Anonimização dos dados pessoais

DIR3) Bloqueio dos dados pessoais

DIR4) Eliminação dos dados pessoais

DIR-D) Gostaria de detalhar ou complementar alguma resposta desta seção?

Muito obrigado pela sua participação!

ANEXOS

ANEXO A – Pareceres consubstanciados de aprovação do comitê de ética em pesquisa

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SÃO PAULO - IFSP

PARECER CONSUBSTANCIADO DO CEP

Elaborado pela Instituição Coparticipante

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: Proteção de dados na gestão educacional: um estudo de caso com a LGPD no contexto das ações propostas por uma instituição pública de ensino.
Pesquisador: JACKSON GOMES SOARES SOUZA
Área Temática:
Versão: 1
CAAE: 52015721.3.3001.5473
Instituição Proponente: INSTITUTO FEDERAL DE EDUCACAO, CIENCIA E TECNOLOGIA DE SAO
Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 5.152.130

Apresentação do Projeto:

As informações elencadas nos campos "Apresentação do Projeto", "Objetivo da Pesquisa" e "Avaliação de Riscos e Benefícios" foram retiradas do arquivo PB_INFORMAÇÕES_BASICAS_DO_PROJETO_1854364, de 12/11/2021 e/ou do Projeto Detalhado ("JACKSON_SOUZA_UNESP_DOUTORADO_PROJETO.PDF", de 20/10/2021):

Título da pesquisa: Proteção de dados na gestão educacional: um estudo de caso com a LGPD no contexto das ações propostas por uma instituição pública de ensino.

De acordo com os autores, pretende-se "estudar os instrumentos normativos de proteção de dados em uma instituição pública de ensino tecnológico e os atuais desafios para o desenvolvimento de políticas e procedimentos a partir da vigência da LGPD" (projeto detalhado, p. 7).

"Propõe-se um "estudo de caso, por meio da aplicação de questionários estruturados [Google Forms] a docentes e gestores" (p.1)

"a amostra desta pesquisa se restringe ao campus Campinas do IFSP [...]. Consiste de 80 servidores cadastrados no Sistema Unificado de Administração Pública – SUAP que atuem como

Endereço: Rua Pedro Vicente, 625
Bairro: Canindé **CEP:** 01.109-010
UF: SP **Município:** SAO PAULO
Telefone: (11)3775-4665 **E-mail:** cep_ifsp@ifsp.edu.br

docentes e/ou gestores e se disponibilizarem voluntariamente a participar da pesquisa." (p.10)

Objetivo da Pesquisa:

"Verificar, conforme os instrumentos normativos de proteção de dados adotados numa instituição pública de ensino tecnológico, os atuais desafios para o desenvolvimento de políticas e procedimentos a partir da vigência da Lei Geral de Proteção de Dados." (projeto detalhado, p.2)

Avaliação dos Riscos e Benefícios:

Segundo o arquivo PB_INFORMAÇÕES_BASICAS_DO_PROJETO_1854364, de 12/11/2021, "Os riscos da participação poderão envolver desconforto ou cansaço. Portanto, recomenda-se um ambiente aconchegante e adoção de pausas ou intervalos durante o processo de leitura e preenchimento do formulário."

Comentários e Considerações sobre a Pesquisa:

Pesquisa de doutorado em Educação Escolar, linha de Pesquisa: Política e Gestão Educacional. O Cronograma de Execução incluído no arquivo PB_INFORMAÇÕES_BASICAS_DO_PROJETO_1854364, de 12/11/2021, prevê a coleta de dados a partir do dia 01/01/2022. Já o projeto detalhado (arquivo de 20/10/2021) apresenta um cronograma que previa essa coleta de dados ao longo do ano de 2021.

Nos termos do Art. 28 da Res. 510/2016 e do item XI.2 da Res. 466/2012-CNS, salientamos que cabe aos pesquisadores aguardar a aprovação dos protocolos de pesquisa por parte do Comitê de Ética antes de iniciar a coleta de dados com seres humanos.

Considerações sobre os Termos de apresentação obrigatória:

Vide o campo "Conclusões ou Pendências e Lista de Inadequações".

Recomendações:

Vide o campo "Conclusões ou Pendências e Lista de Inadequações".

Conclusões ou Pendências e Lista de Inadequações:

Os documentos apresentados pelos pesquisadores (Projeto, TCLE e Questionário) atendem aos parâmetros éticos avaliados por este CEP, justificando a aprovação do projeto.

Considerações Finais a critério do CEP:

Prezado pesquisador, de acordo com a legislação vigente (Resoluções 466/2012 e 510/2016 do

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SÃO PAULO - IFSP

Continuação do Parecer: 5.152.130

CNS), futuramente deverão ser entregues os relatórios parcial e final, por meio do recurso de notificação disponível na Plataforma Brasil.

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_1854364.pdf	12/11/2021 12:12:41		Aceito
Outros	JACKSON_SOUZA_UNESP_DOUTORADO_QUESTIONARIO_12_11_2021.pdf	12/11/2021 12:03:37	JACKSON GOMES SOARES SOUZA	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	JACKSON_SOUZA_UNESP_DOUTORADO_TCLE.pdf	20/10/2021 07:11:17	JACKSON GOMES SOARES SOUZA	Aceito
Projeto Detalhado / Brochura Investigador	JACKSON_SOUZA_UNESP_DOUTORADO_PROJETO.pdf	20/10/2021 07:11:07	JACKSON GOMES SOARES SOUZA	Aceito
Outros	JACKSON_SOUZA_UNESP_DOUTORADO_QUESTIONARIO.pdf	15/09/2021 19:01:56	JACKSON GOMES SOARES SOUZA	Aceito

Situação do Parecer:
Aprovado

Necessita Apreciação da CONEP:
Não

SAO PAULO, 07 de Dezembro de 2021

Assinado por:
diogo henrique constantino coledam
(Coordenador(a))

Endereço: Rua Pedro Vicente, 625
Bairro: Canindé **CEP:** 01.109-010
UF: SP **Município:** SAO PAULO
Telefone: (11)3775-4665 **E-mail:** cep_ifsp@ifsp.edu.br

UNESP - FACULDADE DE CIÊNCIAS E LETRAS - CAMPUS ARARAQUARA

PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: Proteção de dados na gestão educacional: um estudo de caso com a LGPD no contexto das ações propostas por uma instituição pública de ensino.

Pesquisador: JACKSON GOMES SOARES SOUZA

Área Temática:

Versão: 2

CAAE: 52015721.3.0000.5400

Instituição Proponente: Faculdade de Ciências e Letras - UNESP - Campus Araraquara

Patrocinador Principal: Financiamento Próprio

DADOS DA NOTIFICAÇÃO

Tipo de Notificação: Envio de Relatório Final

Detalhe:

Justificativa: Relatório final de pesquisa

Data do Envio: 17/01/2023

Situação da Notificação: Parecer Consubstanciado Emitido

DADOS DO PARECER

Número do Parecer: 6.053.712

Apresentação da Notificação:

Envio de Relatório Final

Objetivo da Notificação:

Finalização do protocolo.

Avaliação dos Riscos e Benefícios:

não houve mudanças

Comentários e Considerações sobre a Notificação:

não houve mudanças

Considerações sobre os Termos de apresentação obrigatória:

não houve mudanças

Endereço: Rodovia Araraquara- Jaú Km1 - sala 105
Bairro: CENTRO **CEP:** 14.800-901
UF: SP **Município:** ARARAQUARA
Telefone: (16)3334-6467 **E-mail:** comitedeetica.fclar@unesp.br

Recomendações:

não há

Conclusões ou Pendências e Lista de Inadequações:

Relatório final aprovado.

Considerações Finais a critério do CEP:

O Comitê de Ética em Pesquisa da FCLAr/Unesp, reunido em 11/05/2023, manifesta-se pela aprovação do relatório final da pesquisa.

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Envio de Relatório Final	JACKSON_SOUZA_UNESP_DOUTORADO_RELATORIO_FINAL.pdf	17/01/2023 14:54:01	JACKSON GOMES SOARES SOUZA	Postado

Situação do Parecer:

Aprovado

Necessita Apreciação da CONEP:

Não

ARARAQUARA, 11 de Maio de 2023

Assinado por:
Tatiana Noronha de Souza
(Coordenador(a))