ReGeo ISSN: 2177-3246

IDENTIFICAÇÃO DE PONTOS CRÍTICOS NO PROCESSO DE ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS EM INSTITUIÇÃO DE ENSINO INFANTIL E MÉDIO

IDENTIFICATION OF CRITICAL POINTS IN THE PROCESS OF GENERAL DATA PROTECTION LAW COMPLIANCE IN AN EARLY CHILDHOOD AND SECONDARY EDUCATION INSTITUTION

IDENTIFICACIÓN DE PUNTOS CRÍTICOS EN EL PROCESO DE CUMPLIMIENTO DE LA LEY GENERAL DE PROTECCIÓN DE DATOS EN UNA INSTITUCIÓN DE EDUCACIÓN INFANTIL Y SECUNDARIA

10.56238/revgeov17n2-144

Dacyr Dante de Oliveira Gatto
Doutor em Informática e Gestão do Conhecimento
Instituição: Universidade Nove de Julho (UNINOVE)
E-mail: dacyr.gatto@uni9.pro.br
Orcid: https://orcid.org/0000-0003-2146-4819
Lattes: https://lattes.cnpq.br/2980113132269496

Maria Fátima Baptista Marques
Mestre em Engenharia da Computação
Instituição: Universidade Nove de Julho (UNINOVE)
E-mail: marques.fatimavb@gmail.com
Orcid: https://orcid.org/0009-0002-2653-0774
Lattes: http://lattes.cnpq.br/3875168344885954

Fernanda Pereira Gomes
Especialista em Gestão e Governança da Tecnologia da Informação
Instituição: Universidade Nove de Julho (UNINOVE)
E-mail: fernanda.gomes79@etec.sp.gov.br
Orcid: https://orcid.org/0009-0004-7889-5366
Lattes: http://lattes.cnpq.br/7606831553315054

Renato José Sassi
Doutor em Engenharia Elétrica
Instituição: Universidade Nove de Julho (UNINOVE)
E-mail: sassi@uni9.pro.br
Orcid: https://orcid.org/0000-0001-5276-4895
Lattes: http://lattes.cnpq.br/8750334661789610

RESUMO
A Lei Geral de Proteção de Dados (LGPD) adequada para instituições de ensino infantil e médio requer que dados pessoais de crianças e adolescentes tenham proteção adicional. É importante identificar

pontos críticos no processo de adequação com Mapeamento de Dados e Inventário de Dados, para minimizar os riscos de impacto à privacidade. O objetivo deste trabalho é identificar pontos críticos nos processos de Mapeamento de Dados e Inventário de Dados em um caso real de adequação à LGPD em uma instituição de ensino infantil e médio, descrevendo os resultados decorrentes da execução desses processos. Considera-se o processo de adequação bem sucedido, uma vez que os dados pessoais de crianças e adolescentes foram inventariados e seu fluxo mapeado, apesar da identificação de pontos críticos que foram a falta de controles de segurança da informação e privacidade sem processos definidos e a falta de engajamento de parte dos colaboradores no processo de Mapeamento de Dados.

Palavras-chave: Ensino Infantil e Médio. LGPD. Dados Sensíveis. Mapeamento de Dados. Inventário de Dados.

ABSTRACT

The General Data Protection Law (LGPD) applicable to early childhood and secondary education institutions requires that the personal data of children and adolescents receive additional protection. It is important to identify critical points in the compliance process through Data Mapping and Data Inventory in order to minimize risks to privacy. The objective of this study is to identify critical points in the Data Mapping and Data Inventory processes in a real case of LGPD compliance in an early childhood and secondary education institution, describing the results derived from the execution of these processes. The compliance process is considered successful, since the personal data of children and adolescents were inventoried and their flow was mapped, despite the identification of critical points, namely the lack of information security and privacy controls with defined processes and the lack of engagement of part of the staff in the Data Mapping process.

Keywords: Early Childhood and Secondary Education. LGPD. Sensitive Data. Mapeamento de Dados. Inventário de Dados.

RESUMEN

La Ley General de Protección de Datos (LGPD) aplicable a las instituciones de educación infantil y secundaria requiere que los datos personales de niños y adolescentes reciban una protección adicional. Es importante identificar puntos críticos en el proceso de adecuación mediante el Mapeo de Datos y el Inventario de Datos, con el fin de minimizar los riesgos de impacto a la privacidad. El objetivo de este trabajo es identificar puntos críticos en los procesos de Mapeo de Datos e Inventario de Datos en un caso real de adecuación a la LGPD en una institución de educación infantil y secundaria, describiendo los resultados derivados de la ejecución de estos procesos. El proceso de adecuación se considera exitoso, ya que los datos personales de niños y adolescentes fueron inventariados y su flujo fue mapeado, a pesar de la identificación de puntos críticos, que fueron la falta de controles de seguridad de la información y privacidad con procesos definidos y la falta de compromiso de parte de los colaboradores en el proceso de Mapeo de Datos.

Palabras clave: Educación Infantil y Secundaria. LGPD. Datos Sensibles. Mapeo de Datos. Inventario de Datos.

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD), promulgada em agosto de 2018 e em vigor desde setembro de 2020, constitui um marco regulatório de grande relevância na proteção de dados pessoais no Brasil. Impõe diretrizes rigorosas para o tratamento de dados pessoais, com a finalidade de assegurar a privacidade e a segurança dos titulares desses dados. Este novo contexto regulatório exige que as organizações reestruturem seus processos e sistemas para atender às exigências legais, prevenindo infrações e protegendo os direitos dos titulares dos dados (Brasil, 2018; Ferrão et al., 2024).

A LGPD estabelece que esses dados pessoais de crianças e adolescente requerem proteção adicional, devido à vulnerabilidade desse grupo de titulares. Informações como nome, endereço e dados de saúde são frequentemente coletadas e processadas, exigindo cuidados específicos para evitar a exposição indevida ou o uso inadequado desses dados. A implementação de práticas que garantam a segurança e a privacidade das informações é essencial para manter a confiança dos pais e responsáveis, além de assegurar o cumprimento das obrigações legais (Candiani; Pereira, 2024).

A importância do processo de adequação à LGPD em instituições de ensino infantil e médio não pode ser subestimada, considerando os riscos envolvidos. A não conformidade pode resultar em graves consequências, incluindo sanções administrativas, danos à reputação da instituição e, mais seriamente, a exposição dos dados de crianças e adolescentes a usos indevidos que podem comprometer sua segurança e bem-estar. A complexidade do processo de adequação envolve o mapeamento e inventário de dados pessoais, entre outras ações (De Araújo Neto; Aguiar, 2024, Bassani; Cazella, 2025; Getenet, 2025).

As atividades de mapeamento e Inventário de Dados pessoais, conhecidos em inglês como Mapeamento de Dados e Inventário de Dados, são essenciais para um processo de adequação. Estes processos proporcionam uma visão abrangente dos dados pessoais tratados pela instituição, delineando o fluxo desses dados nos processos de negócios e como são efetivamente tratados (Reis et al., 2024).

Assim, o objetivo deste trabalho é identificar pontos críticos nos processos de Mapeamento de Dados e Inventário de Dados em um caso real de adequação à LGPD em uma instituição de ensino infantil e médio, descrevendo os resultados decorrentes da execução desses processos.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta seção é apresentada a fundamentação teórica que aborda os temas centrais como a Lei Geral de Proteção de Dados (LGPD), Processo de Adequação À LGPD e Governança de Dados.

2.1 LEI GERAL DE PROTEÇÃO DE DADOS

A LGPD estabelece princípios e diretrizes obrigatórios para todas as organizações, sejam públicas ou privadas, que realizam operações de tratamento de dados pessoais. Entre seus principais

objetivos estão a proteção dos direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade dos indivíduos (Nascimento; Silva, 2023).

A lei introduz a figura do encarregado pelo tratamento de dados pessoais, que é responsável por garantir a conformidade com a LGPD e atua como ponto de contato entre a organização controladora dos dados, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (ANPD, 2022).

Um aspecto de destaque da LGPD é a regulamentação do tratamento de dados pessoais sensíveis, que requerem proteção adicional devido ao seu potencial de causar discriminação ou danos à privacidade dos titulares. Dados sensíveis incluem informações sobre origem racial ou étnica, convicções religiosas, opiniões políticas, filiação sindical, dados sobre saúde ou vida sexual, e dados genéticos ou biométricos (Silva; Sarkis, 2023).

No que concerne ao tratamento de dados pessoais sensíveis, os dados de crianças e adolescentes assumem uma importância crítica, dada a vulnerabilidade intrínseca deste grupo etário. Dados pessoais sensíveis de crianças e adolescentes, como informações sobre saúde, características genéticas, orientação sexual ou convicções religiosas, requerem proteção adicional devido ao potencial de causar discriminação ou outros danos significativos à privacidade e ao desenvolvimento pessoal dos menores (Shin et al., 2018).

Além disso, a lei demanda que os controladores de dados implementem medidas de segurança robustas e políticas transparentes para garantir que esses dados sejam tratados de maneira ética e segura, assegurando que o direito à privacidade e a proteção integral dos direitos dos menores sejam resguardados, conforme os princípios estabelecidos no Estatuto da Criança e do Adolescente (ECA) e demais normas pertinentes (Vasconcelos et al., 2023).

2.2 PROCESSO DE ADEQUAÇÃO À LGPD

O processo de adequação à LGPD imposto às organizações envolve uma série de etapas complexas e integradas que visam garantir a conformidade com as exigências legais e a proteção eficaz dos dados pessoais. Inicialmente, as organizações devem realizar um mapeamento abrangente de todos os dados pessoais que coletam, armazenam, processam e compartilham (Silva, 2024).

Este mapeamento, conhecido como Mapeamento de Dados, é crucial para identificar os fluxos de dados e as práticas atuais de tratamento, permitindo uma visão clara dos pontos críticos que necessitam de ajustes (Wendling et al., 2023).

Subsequente a esta etapa, é importante que as organizações estabeleçam um programa de governança de dados robusto, que envolva a criação de políticas internas, procedimentos operacionais e a definição de responsabilidades específicas dentro da organização. A governança de dados

desempenha um papel essencial na conformidade com a LGPD e na proteção efetiva dos dados pessoais (Reis et al., 2024).

Um componente essencial da governança de dados é a criação e manutenção de um Inventário de Dados, que funciona como um registro detalhado de todos os dados pessoais coletados, armazenados, processados e compartilhados pela organização (Santos Filho; De Jesus, 2023).

Esse inventário detalhado é fundamental para identificar quais dados são considerados sensíveis, conforme definido pela LGPD, e garantir que esses dados sejam tratados com as devidas precauções e proteções (Silva; Sarkis, 2023).

Mantendo o Mapeamento de Dados e o Inventário de Dados atualizados, as organizações conseguem mapear precisamente os fluxos de dados, identificando todas as entradas, saídas e pontos de armazenamento. Isso permite uma avaliação precisa dos riscos associados ao tratamento de dados pessoais, facilitando a implementação de medidas de segurança adequadas para mitigar esses riscos (Wendling et al., 2023).

Ademais, o Inventário de Dados auxilia na realização de avaliações de impacto sobre a proteção de dados, identificando possíveis vulnerabilidades e áreas de não conformidade que necessitam de atenção (Reis et al., 2024).

2.3 GOVERNANÇA DE DADOS

A governança pode ser compreendida como o conjunto de mecanismos, estruturas, processos e práticas estabelecidos para direcionar, monitorar e avaliar a atuação organizacional, assegurando que os objetivos estratégicos sejam alcançados de forma eficiente, ética e em conformidade com normas e regulamentos aplicáveis (Matebese, 2025).

Matebese (2025) também aborda que no contexto organizacional, a governança envolve a definição clara de papéis e responsabilidades, a implementação de controles internos e a promoção da transparência e da prestação de contas, garantindo alinhamento entre estratégia, gestão operacional e mitigação de riscos.

A governança de dados, por sua vez, refere-se ao conjunto de políticas, procedimentos, padrões e controles que regulam a gestão dos dados ao longo de todo o seu ciclo de vida, desde a coleta até o descarte. Seu objetivo é assegurar a qualidade, integridade, disponibilidade, confidencialidade e conformidade dos dados, estabelecendo responsabilidades claras sobre sua utilização e proteção (Silva, 2024).

A governança de dados define critérios para classificação, acesso, armazenamento, compartilhamento e retenção das informações, garantindo que o tratamento de dados esteja alinhado às exigências legais, regulatórias e estratégicas da organização (DAMA International, 2017).

A importância da governança, assim como da governança de dados, reside na sua capacidade de estruturar processos decisórios e fortalecer mecanismos de controle, reduzindo riscos operacionais, jurídicos e reputacionais (Nascimento; Silva, 2023).

No contexto da proteção de dados e da segurança da informação, a governança permite maior previsibilidade, rastreabilidade e controle sobre os ativos informacionais, promovendo conformidade normativa e melhoria contínua. Ao estabelecer diretrizes claras e mecanismos de monitoramento, a governança contribui para a sustentabilidade organizacional, aumento da confiança de stakeholders e suporte à inovação com responsabilidade (Silva, 2024).

A Governança de Dados, suportada por um Inventário de Dados, também facilita a gestão de consentimento e o atendimento aos direitos dos titulares de dados. Com um inventário bem estruturado, as organizações podem rapidamente localizar e acessar dados específicos, permitindo responder de maneira eficiente a solicitações de acesso, correção, exclusão e portabilidade dos dados (Candiani; Pereira, 2024).

A Governança de Dados e o Inventário de Dados são essenciais para a implementação de políticas de minimização de dados, um princípio central da LGPD. Compreendendo exatamente quais dados são coletados e por quê, as organizações podem avaliar a necessidade e a relevância de cada conjunto d dados, reduzindo a coleta e o armazenamento de informações desnecessárias, minimizando assim o risco de exposição a violações de dados (Wendling et al., 2023).

Outro aspecto crítico é a capacidade de monitorar e auditar o uso de dados pessoais. Com um Inventário de Dados abrangente, as organizações podem realizar auditorias regulares para assegurar que todas as práticas de tratamento de dados estão em conformidade com as políticas internas e os requisitos legais. Isso fortalece a governança de dados, proporcionando uma camada adicional de segurança e conformidade contínua (Nascimento; Silva, 2023)

3 METODOLOGIA

Nesta seção são apresentadas a caracterização metodológica, a caracterização do cenário da empresa e a caracterização do problema.

3.1 CARACTERIZAÇÃO METODOLÓGICA

Para a elaboração deste artigo, utilizou-se como referência teórica literaturas relacionadas à Lei Geral de Proteção de Dados, Mapeamento de Dados, Inventário de Dados e Governança de Dados. Os artigos de periódicos pesquisados foram obtidos das bases de conhecimento *Scielo*, *Science Direct* e *Research Gate*, enquanto as obras consultadas são de autores com relevância no referencial teórico da pesquisa.

A metodologia de pesquisa adotada foi de natureza descritiva e exploratória, objetivando descrever sistematicamente a situação e o problema identificado, bem como investigar as possibilidades emergentes, elucidando os conceitos teóricos apresentados no referencial teórico. A abordagem da pesquisa foi qualitativa, centrada no estudo de uma instituição de ensino infantil e médio, utilizando a análise documental como meio de obtenção das evidências necessárias para abordar a criticidade dos processos de Mapeamento de Dados e Inventário de Dados (Kumar, 2019).

Como procedimento metodológico, adotou-se a pesquisa de campo como método de coleta de dados, que envolveu entrevistas e o engajamento com as pessoas em seu ambiente natural (Gil, 2019; Kumar, 2019).

Foram realizadas entrevistas com pontos focais indicados pela área de gestão da instituição, bem como solicitado o preenchimento de um mapeamento para os processos de negócios e os respectivos tipos de dados pessoais envolvidos nesses processos, durante o período de janeiro a maio de 2024. Devido ao caráter sigiloso do processo para a organização, não foi autorizada a divulgação do nome da empresa, sendo divulgados apenas os resultados obtidos.

Outro aspecto importante desta pesquisa, é o fato de que apenas os tipos de dados pessoais foram abordados, sem que houvesse acesso, tratamento ou manipulação de dados pessoais reais pertencentes a indivíduos identificados ou identificáveis, o que não implicou na necessidade de anonimização, ou outra forma de mascaramento de dados.

3.2 CARACTERIZAÇÃO DO CENÁRIO DA EMPRESA

A empresa foco do estudo é uma instituição de ensino infantil e médio que administra escolas distribuídas em todo o território nacional, atendendo principalmente crianças e adolescentes. Como parte do seu projeto de conformidade, a instituição iniciou a adequação à Lei Geral de Proteção de Dados, com o apoio de uma consultoria de Segurança da Informação e Privacidade, a ITALTEL do Brasil, que autorizou o uso do seu ambiente organizacional para realizar a pesquisa.

O processo de adequação à LGPD foi direcionado para a central da instituição, situada na cidade do Rio de Janeiro, e para 11 escolas distribuídas no Rio de Janeiro, São Paulo, Recife e Brasília. Apesar da empresa ser vinculada à sua sede internacional na União Europeia, onde possui um processo de adequação ao GDPR mais avançado, pouco do que foi implementado internacionalmente pôde ser aproveitado na instituição em território brasileiro. Isso se deve, em parte, à limitação de comunicação entre o encarregado pelo tratamento de dados pessoais da instituição na Europa e, em parte, à necessidade de adaptação de documentos, entre políticas e procedimentos, ao cenário brasileiro e às demais legislações e regulações do setor educacional.

3.3 CARACTERIZAÇÃO DO PROBLEMA

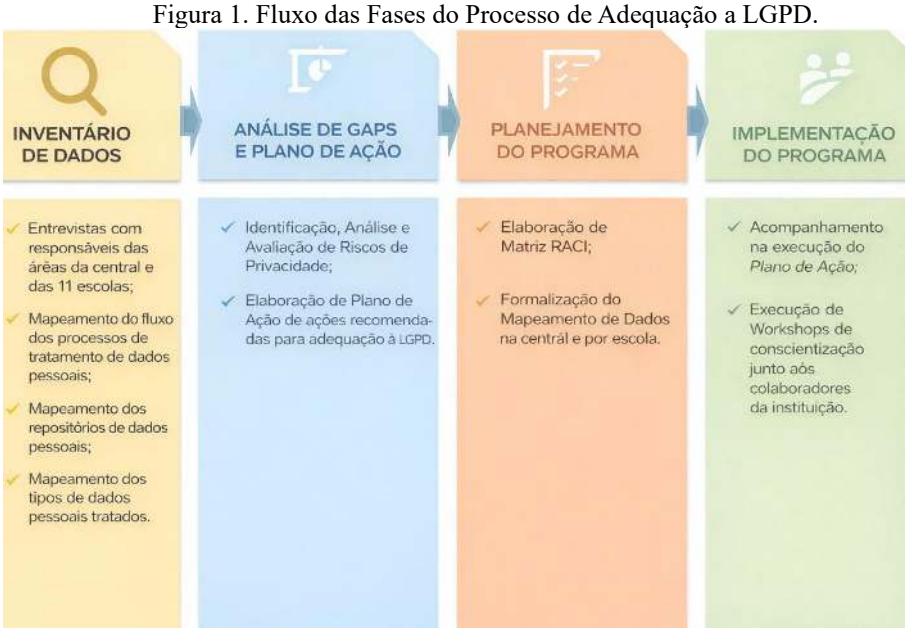
Diante desse cenário, o processo de adequação à LGPD teve que ser iniciado praticamente do zero, o que, por um lado, favoreceu que o processo pudesse ser iniciado sem ressalvas ou restrições em relação à abordagem metodológica aplicada.

Para a execução do processo de adequação, foram definidas as seguintes fases:

- **Inventário de Dados*:*** Esta etapa consistiu no mapeamento dos fluxos dos processos de negócios que tratam dados pessoais, por meio de entrevistas, bem como no mapeamento de repositórios de dados e tipos de dados pessoais tratados.
- **Análise de *Gaps* e Plano de Ação:** Esta fase envolveu a identificação, análise e avaliação de riscos de privacidade baseados no Inventário de Dados consolidado, o que direcionou a elaboração de um Plano de Ação recomendado para a adequação à LGPD.
- **Planejamento do Programa:** Esta fase consistiu na elaboração de uma Matriz de Responsabilidades (Matriz RACI), formalização de um Mapeamento de Dados consolidando os fluxos de dados pessoais dentro das áreas da instituição em sua central no Rio de Janeiro, bem como em cada escola.
- **Implementação do Programa:** Esta etapa incluiu o acompanhamento na execução do Plano de Ação, junto ao encarregado pelo tratamento de dados pessoais da instituição, e também a realização de workshops de conscientização com os colaboradores da instituição.

O fluxo do processo, assim como das atividades do processo são apresentados na Figura 1.

Figura 1. Fluxo das Fases do Processo de Adequação a LGPD.



Fonte: ITALTEL (2024)

Durante a execução do processo de adequação, um ponto chamou a atenção na Fase de Inventário de Dados. A falta de engajamento dos colaboradores em levantar os processos de negócios para iniciar o mapeamento dos fluxos e por consequência os tipos de dados pessoais, foi identificado já no início das entrevistas. Esta falta de engajamento, muitas das vezes foi justificada pela falta de tempo dos colaboradores em conciliar as atividades do processo de adequação com suas atividades cotidianas de suas respectivas áreas.

4 APRESENTAÇÃO E ANÁLISE DE RESULTADOS

Com a Fase de Inventário de Dados, iniciou-se a atividade de entrevistas com os 42 colaboradores designados pelo encarregado pelo tratamento de dados pessoais da instituição, atuando diretamente da central da organização.

Foi elaborado então um calendário com *"slots"* de horários a serem disponibilizados para as entrevistas, para que os 42 colaboradores designados escolhessem o melhor horário que se encaixasse em suas agendas. Foram então selecionados colaboradores atuantes nas áreas de Admissões, Expansões, Financeiro, Jurídico, Marketing, Operações, Pedagógico, RH e Tecnologia da central. Para as demais escolas foram selecionados apenas colaboradores das áreas de Admissões, Operações e Pedagógico, uma vez que as demais áreas eram centralizadas na central da instituição.

Conforme os slots eram preenchidos, invites eram elaborados e encaminhados para formalizar a data e a hora de cada entrevista. A entrevista era dividida em duas etapas:

- **Questionário:** a primeira etapa consistiu na aplicação de um conjunto de perguntas abrangentes sobre segurança da informação e privacidade para obter a percepção inicial de cada colaborador sobre os temas, assim como obter uma visão do nível de implantação que cada aspecto questionado estava implantado, ou se não estava implantado. Após o colaborador esboçar sua resposta ele era convidado então a atribuir uma nota de 1 a 4 em relação ao nível de implantação, ou se o aspecto questionado não se aplicava a sua área. A escala das notas e suas respectivas descrições encontram-se apresentadas na Tabela 1.

Tabela 1. Escala de Notas e Descrições

Respostas	Descrição
1	O controle de segurança da informação e privacidade não está em vigor.
2	O controle de segurança da informação e privacidade não existe, mas é praticado reativamente com base em cenários. O objetivo de praticar o controle é atingir um objetivo específico sem um processo passo a passo para alcançá-lo.
3	O controle de segurança da informação e privacidade está implementado e executado com base em políticas, padrões e processos documentados e definidos.
4	O controle de segurança da informação e privacidade é definido por políticas e processos baseados em padrões internacionais ajustados às necessidades, experiências e capacidades da instituição dentro de um Sistema de Gestão da Segurança da Informação formalizado sujeito à Melhoria Contínua e Gestão da Qualidade.
N/A	O controle de segurança da informação e privacidade não se aplica a área

Fonte: Autores (2026)

As 42 entrevistas, que avaliaram a percepção da Segurança da Informação e Privacidade em 6 Domínios: Planejamento, Programa de Governança, Descoberta de Dados, Mapeamento de Controles, Plano de Ação e Ação Emergencial. Ao término os dados foram consolidados de forma a se obter uma visão do nível de implantação dos domínios de Segurança da Informação e Privacidade avaliados, obtendo-se o seguinte resultado demonstrado na Figura 2.

Figura 2. Nível de Implantação dos Domínios de Segurança da Informação e Privacidade

Fonte: Autores (2026)

Baseado na escala utilizada, observou-se que todos os domínios de Segurança e Privacidade se encontravam abaixo da nota 2, o que representava, segundo a descrição da respectiva nota, que os controles de segurança da informação e privacidade não existem, mas são praticados reativamente com base em cenários, porém sem processos definidos, o que apresentou o primeiro ponto crítico do processo de adequação.

- **Mapeamento dos Fluxos de Processos:** a segunda etapa consistiu em apresentar um guia oferecido pela ITALTEL do Brasil (ITALTEL, 2024), no qual o colaborador alimentaria com todas as informações referente aos processos que tratavam em alguma proporção dados pessoais, repositórios, e tipos de dados pessoais tratados. O referido guia apresentava quais informações seriam necessárias para efetuar o mapeamento, assim como também apresentava um guia de referência sobre todos os dados pessoais mais comuns que poderiam ser encontrados em um processo de negócio. Cada colaborador ao participar da entrevista respondeu então ao questionário inicial sobre Segurança da Informação e Privacidade, e na sequência era apresentado ao guia, recebendo então orientações de como preenchê-lo. Foi dada orientação que o colaborador buscasse apoio dos membros de sua equipe para poder preencher o guia com o maio número de informações possíveis. Foi dado um prazo de 15 dias para que o colaborador devolvesse o guia preenchido.

Dos 42 colaboradores entrevistados, apenas 23 colaboradores devolveram o guia minimamente preenchido dentro do prazo definido. Dezenove colaboradores ficaram pendentes de entregar o referido guia preenchido, o que levantou um alerta que impactou no Inventário de Dados proposto no processo de adequação. Deu-se então o segundo ponto crítico no processo de adequação.

Em acordo com o encarregado pelo tratamento de dados pessoais da instituição, ficou-se definido que este processo continuaria com as pendências e conforme os guias fossem retornando, o Inventário de Dados seria então atualizado, pelo próprio encarregado.

Na sequência iniciou-se o a Fase do Análise de Gaps e Plano de Ação, utilizando como referência a norma ISO/ABNT 27701 (ABNT, 2019) para linha de base aos potenciais riscos de segurança a informação e privacidade, assim como ao tratamento de dados como controlador e tratamento de dados como operador. Para efeito dos riscos de tratamento de dados, não foram identificados riscos relacionados à instituição, como operadora de dados pessoais, apenas como controladora. Com base no Anexo N/A da referida norma, que apresenta todos os controles de segurança da informação e privacidade relacionados aos artigos da LGPD, que respectivamente atendem, foi executada a Identificação, Análise e Avaliação dos Riscos de Privacidade encontrados nas entrevistas como no Inventário de Dados, conforme demonstrado no Quadro 1.

Quadro 1. Recorte da Identificação, Análise e Avaliação de Riscos de Segurança da Informação e Privacidade.

Descrição do Risco/Situação de Risco	Tipo do Risco	Probabilidade do Risco	Impacto do Risco	Avaliação de Risco
Segurança da Informação e Privacidade				
Políticas de Segurança da Informação não contemplam todos os aspectos de privacidade	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Alto**	**Alto**	**Alto**
Responsabilidades e papéis da segurança da informação não definidos formalmente	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Alto**	**Alto**	**Alto**
Política para o uso de dispositivo móvel não definida	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Baixo**	**Baixo**	**Baixo**
Conscientização, educação e treinamento em segurança da informação não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Alto**	**Alto**	**Alto**
Classificação da informação não formalizada	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Alto**	**Alto**	**Alto**
Gerenciamento de mídias removíveis não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Médio**	**Baixo**	**Baixo**
Descarte de mídias não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Médio**	**Baixo**	**Baixo**

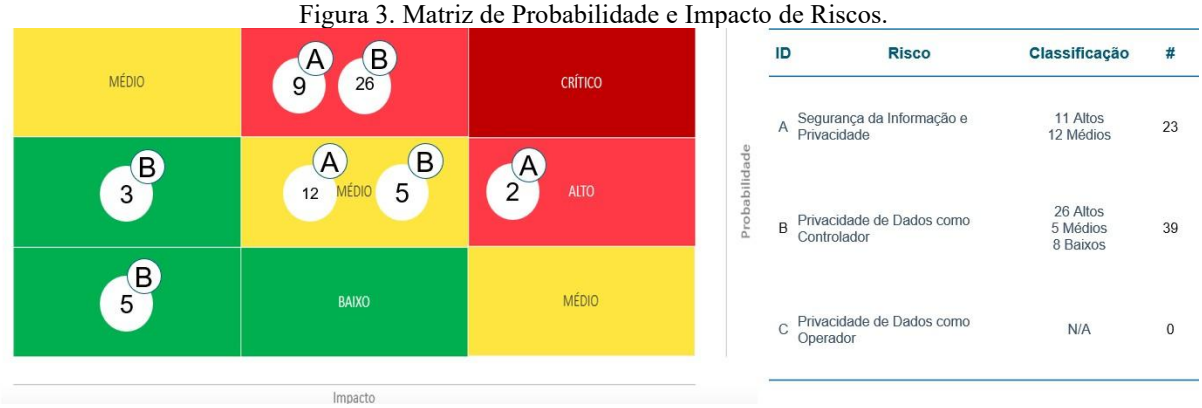
Transferência física de mídias não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Médio**	**Baixo**	**Baixo**
Registro e cancelamento de usuário não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Médio**	**Médio**	**Médio**
Provisionamento para acesso de usuário não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Baixo**	**Baixo**	**Baixo**
Procedimentos seguros de entrada no sistema (*log-on*) não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Baixo**	**Baixo**	**Baixo**
Política para o uso de controles criptográficos não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Alto**	**Alto**	**Alto**
Reutilização ou descarte seguro de equipamentos não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Baixo**	**Baixo**	**Baixo**
Política de mesa limpa e tela limpa não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Alto**	**Alto**	**Alto**
Cópias de segurança das informações não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Alto**	**Alto**	**Alto**
Registros de eventos (logs) não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Médio**	**Alto**	**Alto**
Proteção das informações dos registros de eventos (logs) não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Médio**	**Alto**	**Alto**
Políticas e procedimentos para transferência de informações não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Alto**	**Alto**	**Alto**
Acordos de confidencialidade e não divulgação não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Alto**	**Alto**	**Alto**
Serviços de aplicação seguros em redes públicas não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Médio**	**Médio**	**Médio**
Política de desenvolvimento seguro não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de	**Baixo**	**Baixo**	**Baixo**
Princípios para projetar sistemas seguros não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Médio**	**Médio**	**Médio**
Desenvolvimento terceirizado não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Médio**	**Médio**	**Médio**

Proteção dos dados para teste não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Médio**	**Médio**	**Médio**
Identificando segurança da informação nos acordos com fornecedores não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Médio**	**Médio**	**Médio**
Gestão de incidentes de segurança da informação e melhoria - Responsabilidades e procedimentos não estabelecidos como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Médio**	**Médio**	**Médio**
Gestão de incidentes de segurança da informação e melhorias - Resposta aos incidentes de segurança da informação não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Médio**	**Médio**	**Médio**
Identificação da legislação aplicável e de requisitos contratuais não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Médio**	**Médio**	**Médio**
Proteção de registros não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Médio**	**Médio**	**Médio**
Análise crítica independente da segurança da informação não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Médio**	**Médio**	**Médio**
Análise crítica técnica do compliance não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	**Médio**	**Médio**	**Médio**

Fonte: Autores (2026)

Com a Avaliação dos Riscos finalizada elaborou-se uma Matriz de Probabilidade e Impacto de Riscos, para melhor quantificação dos riscos de segurança da informação e privacidade identificados, conforme apresentado na Figura 3.

Figura 3. Matriz de Probabilidade e Impacto de Riscos.



Fonte: Autores (2026)

Com a visão dos riscos definida foi possível estabelecer um Plano de Ação de ações a serem executadas com o objetivo de tratar os riscos identificados. Essas ações foram então direcionadas as áreas da instituição por meio da Matriz de Responsabilidades (RACI), conforme apresentada da Figura 4. Essa atividade iniciou a Fase de Planejamento do Programa.

Figura 4. Recorte da Matriz RACI e Planos de Ação

Matriz RACI - Planos de Ação

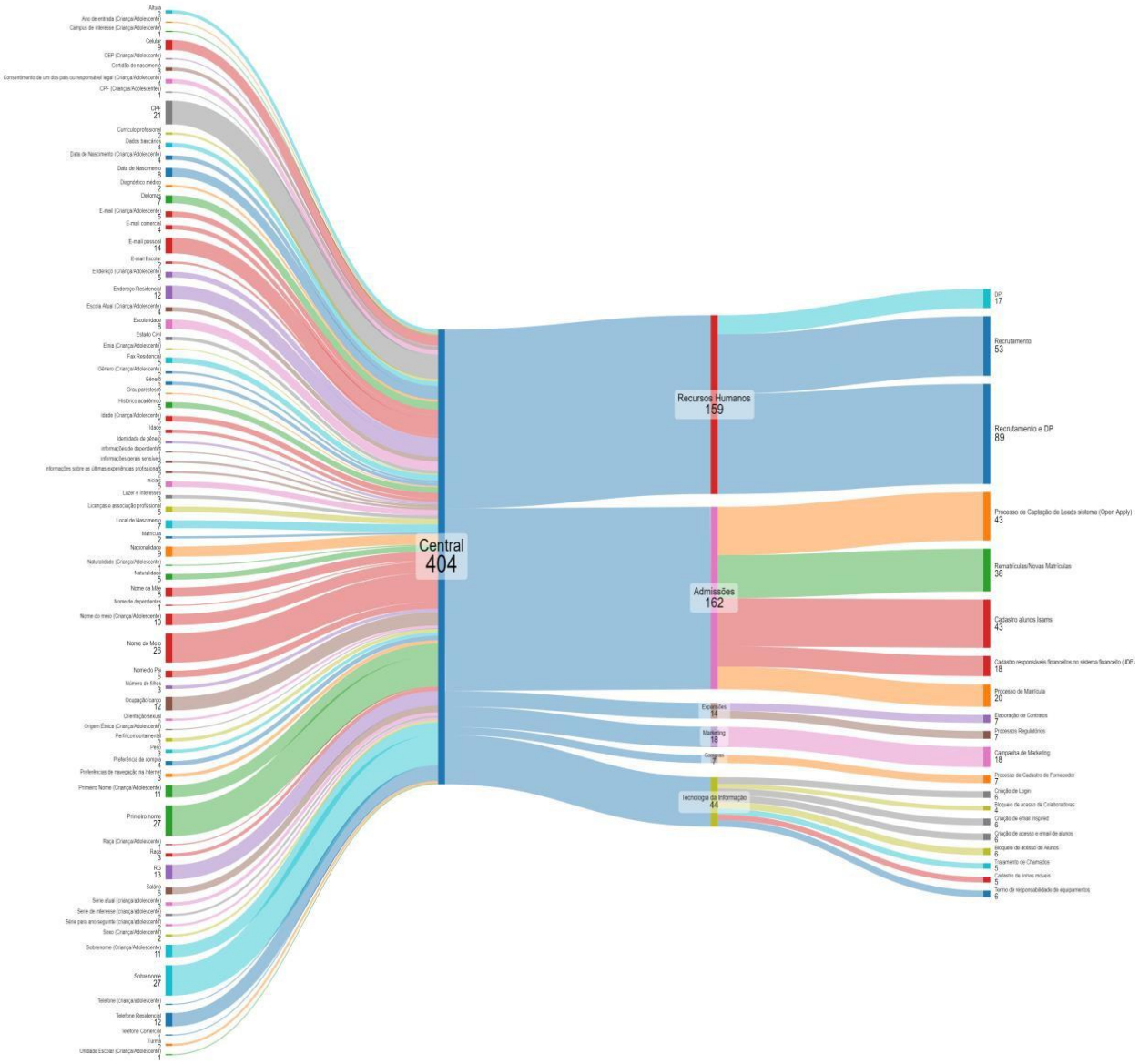
R: Responsável
A: Prestador de Contas
C: Consultado
I: Informado

	ITALTEL	Encarregado de Dados - DPO	Central - Admissões	Central - Pedagógico	Central - Operações	Central - Marketing	Central - Tecnologia (Infra e Operações)	Central - Tecnologia (Tec. Educacional)	Central - RH (DP)	Central - RH (Recru
Plano de Ação 1 - Definição da Organização de Privacidade/Proteção de Dados										
1.1 Papéis e Responsabilidades do Encarregado de Tratamento de Dados										
Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências	C	R	I	I	I	I	I	I	I	I
Receber comunicações da autoridade nacional e adotar providências	C	R	I	I	I	I	I	I	I	I
Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais	C	R	I	I	I	I	I	I	I	I
Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.	C	R	I	I	I	I	I	I	I	I
Definir e revisar as normas de privacidades/proteção de dados e normas que possuem impacto direto em iniciativas de privacidade/proteção de dados, como por exemplo, Norma de Classificação da Informação	C	R	I	I	I	I	I	I	I	I
Governar a estratégia e o programa de proteção de dados e privacidade	C	R	I	I	I	I	I	I	I	I
Monitorar e responder tempestivamente na identificação de riscos de privacidade e proteção de dados que podem violar legislações ou causar impactos sobre o direitos dos titulares	C	R	I	I	I	I	I	I	I	I
Acompanhar a implantação de iniciativas referentes cumprimento das demandas legais ou legislações de privacidade	C	R	I	I	I	I	I	I	I	I
Monitorar, acompanhar, deliberar sobre ações de remediação e documentar incidentes de segurança que estejam relacionados a dados pessoais (vazamentos, perdas, alterações indevidas, dentre outros);	C	R	I	I	I	I	R/C	I	I	I
Atribuir responsabilidades de privacidade e proteção de dados em áreas que manuseiam dados pessoais	C	R	I	I	I	I	I	I	I	I
Elaborar e promover treinamentos de privacidade e proteção de para todos os públicos que forem necessários dentro da organização incluindo prestadores de serviços e terceiros	C	R	I	I	I	I	C/I	I	I	I
Avaliar as documentações e melhores práticas	R	C	I	I	I	I	I	I	I	I

Fonte: Autores (2026)

Como atividade sequencial da Etapa de Planejamento do Programa formalizou-se o Mapeamento de Dados, com o mapeando dos fluxos de tratamento dos dados pessoais dentro da instituição. Na Figura 5 é apresentado o Mapeamento de Dados efetuado na central da instituição, mapeando os dados pessoais tratados, as áreas que tratam estes dados e os respectivos processos.

Figura 5. Mapeamento de Dados da Central da Instituição



Fonte: Autores (2026)

Foi possível, através da compilação dos tipos de dados pessoais mapeados, elaborar um gráfico *Sankey*, que demonstra o mapa dos fluxos de cada tipo de dado pessoal, através do processos que conectam as diversas áreas da instituição.

Na primeira coluna do gráfico observa-se os tipos de dados pessoais e a quantidade de cada tipo de dado que é tratado nos processos, totalizando 404 tratamentos de tipos de dados pessoais distribuídos nos processos de tratamento. Na terceira coluna, os tipos de dados são divididos por área da instituição, e na última coluna demonstra-se os referidos processos e a quantidade de tratamentos de tipos de dados pessoais utilizados por cada processo.

5 CONCLUSÃO

Observou-se no decorrer das atividades do processo de adequação a LGPD dois pontos críticos: o primeiro no momento da consolidação dos dados das entrevistas que mostrou que a percepção da

Segurança da Informação e Privacidade para a maioria dos colaboradores era executado reativamente com base em cenários do dia a dia dos colaboradores e totalmente desprovidos de processos formais de Segurança da Informação e Privacidade. O segundo ponto crítico foi identificado no momento do preenchimento dos guias de coleta das informações sobre o Mapeamento de Dados. Neste caso o problema não foi propriamente dito em relação as informações coletadas, mas sim ao número de colaboradores que devolveram o guia preenchido, o que deixou a percepção do Inventário de Dados incompleta, mesmo tendo sido acordado com o encarregado pelo tratamento de dados pessoais que o processo seria continuado pela instituição, porém não a tempo de finalizá-lo durante o processo de adequação.

Desta foram pode-se concluir que o objetivo deste artigo foi atingido de identificar os pontos críticos dos processos de Mapeamento de Dados e Inventário de Dados, em um processo de adequação a LGPD. O cenário evidenciado nesse processo de adequação, apesar de comum em muitos projetos de adequação a LGPD, mostra que muitas das vezes as adequações são feitas de forma incompleta, e que um Plano de Ação precisa ser muito bem estruturado para que os processos necessários de Segurança da Informação e Privacidade venha a ser formalizados nas organizações.

O processo de adequação proporcionou maior conscientização organizacional acerca da importância da Segurança da Informação e da Privacidade como elementos estruturais, e não meramente reativos, da gestão institucional. A identificação dos pontos críticos no Mapeamento de Dados e no Inventário de Dados permitiu à organização reconhecer lacunas processuais e culturais, criando oportunidades para formalização de políticas, definição de responsabilidades e estabelecimento de controles mais robustos.

Este processo de adequação continuou na instituição de ensino durante a Fase de Implementação do Programa, com o intuito de levar a referida instituição a um estado de adequação minimamente aderente a LGPD, proporcionando a instituição estar então em compliance com suas obrigações legais no que diz respeito a Privacidade e atendimento aos direitos dos titulares de dados pessoais, o que é sugerido como continuidade dessa pesquisa.

Como limitação de pesquisa observou-se a falta de engajamento de parte dos entrevistados, que mesmo tendo a obrigatoriedade institucional de participar do processo de adequação, não se mostraram comprometidos com o processo, que não somente limitou a pesquisa à uma maior abrangência, mas também limitou a visão institucional para o Mapeamento de Dados e o Inventário de Dados que foram fases cruciais do processo.

Este trabalho buscou contribuir com as instituições de ensino para darem a devida atenção aos processos de adequação à LGPD, não somente por questões regulatórias, mas também no cuidado aos dados sensíveis de crianças e adolescentes. No âmbito acadêmico, buscou-se oferecer uma visão

metodológica do uso de ferramentas, normas e processos que podem contribuir com estudos de adequação a regulações.

Como continuidade da pesquisa, pode-se considerar o aprofundamento do estudo na fase de implementação e consolidação do Programa de Adequação à LGPD, com foco na mensuração da maturidade dos processos de governança de dados e na avaliação da efetividade das medidas implementadas. Recomenda-se também investigar estratégias para aumento do engajamento institucional, incluindo ações de capacitação, cultura organizacional voltada à privacidade e mecanismos formais de responsabilização.

Estudos futuros podem também propor modelos estruturados de Plano de Ação aplicáveis a instituições de ensino, permitindo replicabilidade metodológica e comparação entre diferentes níveis de aderência normativa, contribuindo para o avanço acadêmico e prático na área de governança de dados e conformidade regulatória.

AGRADECIMENTOS

À Universidade Nove de Julho pelo apoio à pesquisa e a empresa ITALTEL por permitir o uso do seu ambiente organizacional.

REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27701 - Tecnologia da informação – 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. ABNT, 2019.

ANPD - RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022 - Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. ANPD, 2022.

BASSANI, Rafael Vescovi; CAZELLA, Silvio César. Um modelo de analítica acadêmica baseado na regulação geral de proteção de dados, na lei geral de proteção de dados pessoais e governança da informação. ETD - Educação Temática Digital, v. 27, https://doi.org/10.20396/etd.v27i00.8675203. 2025

BRASIL. Lei Nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Brasília: Congresso Nacional, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em: 16 jul. 2023.

CANDIANI, Israel Ferreira; PEREIRA, Otaviano José. Lei Geral de Proteção de Dados (LGPD) Nas Instituições De Ensino: Desafios Formativos Para Sua Aplicação E Gestão. Cadernos da FUCAMP, v. 27, 2024.

DE ARAÚJO NETO, Reinaldo Juvino; AGUIAR, Janderson Jason Barbosa. The impacts of the General Data Protection Law (LGPD) on information security: a literature review. Revista de Gestão e Secretariado, v. 15, n. 2, p. e3442, 2024. DOI: 10.7769/gesec.v15i2.3442.

DAMA INTERNATIONAL. DAMA-DMBOK: Data Management Body of Knowledge. 2. ed. Basking Ridge: Technics Publications, 2017.

FERRÃO, Sâmmara Éllen Renner et al. Towards a taxonomy of privacy requirements based on the LGPD and ISO/IEC 29100. Information and Software Technology, p. 107396, 2024.

GIL, Antônio Carlos. Como elaborar projetos de pesquisa. 6. ed. São Paulo: Atlas, 2019.

GETENET, Seyum. Mapping initial teacher education program courses with professional standards of teachers: implications for professional learning. Quality Assurance in Education, v. 33, i. 4, 2025. DOI: https://doi.org/10.1108/QAE-10-2024-0202.

KUMAR, Ranjit. Research methodology: a step-by-step guide for beginners. 5. ed. Thousand Oaks: SAGE, 2019.

ITALTEL. Privacy & Data Protection. 2024. https://www.italtel.com/br/privacy-data- protection/. Acessado em 14/07/2024.

MATEBESE, Hialele. The dynamic correlation between corporate governance and strategy to inform organisational resilience. Future Studies Research Journal: Trends and Strategies, v. 17, n. 1, e929, jun. 2025. DOI: https://doi.org/10.24023/FutureJournal/2175-5825/2025.v17i1.929

NASCIMENTO, Bruna Laís Campos do; SILVA, Edilene Maria. Lei Geral de Proteção de Dados (LGPD) e repositórios institucionais: reflexões e adequações. Em Questão, v. 29, p. e-127314, 2023.

REIS, Sálvio Roberto Freitas et al. Desafios da LGPD quanto à privacidade em ambientes educacionais: um mapeamento sistemático. GeSec: Revista de Gestão e Secretariado, v. 15, n. 3, 2024.

SANTOS FILHO, Ronaldo Fenelon; DE JESUS, Victor Borges. Compliance de Dados em Instituições de Ensino Superior. Revista de Constitucionalização do Direito Brasileiro, v. 6, n. 2, p. 274- 296, 2023.

SHIN, Sanggyu et al. Proposal for a Privacy Impact Assessment Manual Conforming to ISO/IEC 29134:2017. Computer Information Systems and Industrial Management. CISIM. Lecture Notes in Computer Science(), vol 11127. Springer, Cham, 2018. DOI: 10.1007/978-3-319-99954-8_40.

SILVA, Keyla; SARKIS, Laura. Análise de conformidade da LGPD nas Instituições Públicas de Ensino Superior no Brasil sob a perspectiva dos profissionais de TIC. In: WER. 2023.

SILVA, Lindomar Pinto da. Does Public Governance Impact Performance? An Analysis of Higher Education Institutions in Brazil. Brazilian Administration Review, v. 21, n. 2, e230181, abr. 2024. DOI: https://doi.org/10.1590/1807-7692bar2024230181

VASCONCELOS GOMES, Fabricio et al. Proteção de dados e instituições de ensino: o que fazer com dados de alunos?. Revista Brasileira de Políticas Públicas, v. 13, n. 1, 2023.

WENDLING, Gláucia Severo et al. Diagnóstico do Nível de Maturidade da Aplicação da LGPD Nas Escolas de Educação Infantil da Rede Municipal de Educação de Passo Fundo. Contribuciones A Las Ciencias Sociales, v. 16, n. 8, p. 11359-11376, 2023.