Simpósio de Excelência em Gestão e Tecnologia
XXI SEGeT
GOVERNANÇA, RESPONSABILIDADE SOCIAL E O MEIO AMBIENTE
Desafios para uma Gestão Social, Financeira e Sustentabilidade Empresarial
Realização: UniDomBosco Centro Universitário Dom Bosco do Rio de Janeiro unesp
Patrocínio: INB

Data Mapping e Data Inventory de Dados de Crianças e Adolescentes: Identificação de Pontos Críticos em Processo de Adequação a LGPD em Instituição de Ensino

Dacyr Dante de Oliveira Gatto
dacyrgatto@terra.com.br
UNINOVE

Nityananda Portellada
nityananda.portellada@gmail.com
UNINOVE

Renato José Sassi
sassi@uni9.pro.br
UNINOVE

Resumo:A Lei Geral de Proteção de Dados (LGPD) estabelece que dados pessoais de crianças e adolescentes requerem proteção adicional para garantir sua privacidade. A conformidade com a LGPD em instituições de ensino infantil e médio deve considerar os riscos envolvidos. Atividades de Data Mapping e Data Inventory são essenciais para um processo de conformidade eficaz. Este artigo tem como objetivo identificar pontos críticos nos processos de mapeamento e inventário de dados pessoais em um caso real de adequação à LGPD em uma instituição de ensino infantil e médio. A metodologia de pesquisa adotada é descritiva e exploratória e a abordagem da pesquisa é qualitativa, utilizando a análise documental para obter as evidências necessÃ¡rias. Como procedimento metodológico, foi adotada a pesquisa de campo como método de coleta de dados, que envolveu entrevistas com as pessoas em seu ambiente natural. A instituição em foco administra escolas distribuídas por todo o território nacional e iniciou a adequação à LGPD com o apoio de uma consultoria de segurança da informação e privacidade. O processo seguiu quatro fases: Data Inventory, Gap Analysis e Roadmap, Program Design e Program Implementation. Com as atividades do processo de adequação à LGPD em execução, foram identificados dois pontos críticos que comprometeram

parcialmente o andamento do processo.

Palavras Chave: LGPD - Data Mapping - Data Inventory - Conformidade - Privacidade

1. INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD), sancionada em agosto de 2018 e em vigor desde setembro de 2020, representa um marco regulatório significativo na proteção de dados pessoais no Brasil. Com seu texto baseado no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD estabelece diretrizes rigorosas para o tratamento de dados pessoais, com o objetivo de garantir a privacidade e a segurança dos titulares de dados pessoais. Este novo cenário impõe às organizações a necessidade de reestruturar seus processos e sistemas para atender às exigências legais, prevenindo infrações e protegendo os direitos dos titulares dos dados (BRASIL, 2018).

Cada organização deve compreender o quão crítico o tratamento de dados pessoais é para o seu negócio, diante desse cenário regulatório. Instituições de ensino infantil e médio tem neste contexto um grande desafio, pois os dados pessoais que essas instituições tratam, para fornecer seus serviços, em sua maior parte, são de crianças e adolescentes (FERRÃO *et al.*, 2024).

A LGPD entende que estes dados pessoais requerem proteção adicional, por pertencerem a um grupo de titulares considerado vulnerável. Informações como nome, endereço, dados de saúde, entre outros, são frequentemente coletadas e processadas, exigindo um cuidado específico 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 crucial para manter a confiança dos pais e responsáveis, além de assegurar o cumprimento das obrigações legais (CANDIANI; PEREIRA, 2024)

A criticidade no processo de adequação à LGPD em instituições de ensino infantil e médio não pode ser subestimada, dado os riscos envolvidos. A ausência de conformidade pode resultar em sérias consequências, incluindo sanções administrativas, danos à reputação da instituição e, mais gravemente, a exposição dos dados das crianças e adolescentes e a usos indevidos que podem comprometer sua segurança e bem-estar. A complexidade do processo de adequação envolve a revisão de políticas internas, a capacitação de colaboradores, a implementação de tecnologias de segurança da informação, a criação de mecanismos de resposta a incidentes, mapeamento de processos que tratam dados pessoais, assim o mapeamento e inventário de dados pessoais (DE ARAÚJO NETO; AGUIAR, 2024).

Dentre as atividades de um processo de adequação, os processos de mapeamento e de inventário de dados pessoais, também conhecidos, do inglês, como *Data Mapping* e *Data Inventory*, são uns dos mais trabalhosos, e também uns dos mais importantes para o processo de adequação, pois fornece uma visão de quais são os dados pessoais tratados pela instituição, por onde estes dados fluem nos processos de negócios e como eles são efetivamente tratados (REIS *et al*, 2024).

Esse artigo busca apresentar por meio de uma pesquisa de campo, a identificação dos pontos de criticidade dos processos de *Data Mapping* e *Data Inventory*, em um caso real de adequação a LGPD em uma instituição de ensino infantil e médio, descrevendo os desafios e resultados na execução desses processos.

2. PROBLEMA DE PESQUISA E OBJETIVO

O problema de pesquisa deste artigo, é explorar e analisar como foram executados os processos de *Data Mapping* e *Data Inventory* em uma instituição de ensino infantil e médio, composta por várias escolas, em diferentes localidades geográficas do Brasil. Outro ponto a se considerar é o fato da instituição ser gerida por um grupo educacional situado na União Europeia, o que indica que a cultura de proteção de dados, teoricamente, deveria existir no contexto organizacional.

O objetivo deste trabalho foi identificar os pontos críticos do processo de *Data Mapping* e *Data Inventory* em uma instituição de ensino infantil e médio e verificar se os resultados esperados por esses processos, no contexto de um processo de adequação a LGPD, foram alcançados.

3. FUNDAMENTAÇÃO TEÓRICA

3.1. LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei Geral de Proteção de Dados (LGPD), instituída pela Lei nº 13.709, de 14 de agosto de 2018, representa um marco regulatório significativo no ordenamento jurídico brasileiro, delineando um conjunto abrangente de normas para o tratamento de dados pessoais. Esta legislação surge em um contexto global de crescente preocupação com a privacidade e a segurança dos dados, alinhando-se com tendências internacionais como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia (BRASIL, 2018).

A LGPD estabelece princípios e diretrizes que devem ser observados por todas as organizações, 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 e o livre desenvolvimento da personalidade dos indivíduos. A lei define dados pessoais como informações relacionadas a uma pessoa natural identificada ou identificável, abrangendo uma vasta gama de informações que podem ser utilizadas para identificar um indivíduo (NASCIMENTO; SILVA, 2023).

Uma das bases-legais da LGPD é o consentimento, que deve ser fornecido de forma livre, informada e inequívoca pelo titular dos dados. A legislação também impõe a necessidade de transparência nas operações de tratamento, exigindo que as finalidades para as quais os dados são coletados sejam claramente comunicadas aos titulares. Além disso, a lei introduz a figura do encarregado pelo tratamento de dados pessoais, também conhecido como *Data Protection Officer (*DPO), nomenclatura oriunda da GDPR. O encarregado pelo tratamento de dados pessoais é responsável por garantir a conformidade com a LGPD e atua como ponto de contato entre a organização, denominada controladora dos dados, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (ANPD, 2022).

Outro aspecto relevante da LGPD é o tratamento de dados pessoais sensíveis, que merecem uma proteção adicional devido ao seu potencial de causar discriminação ou danos à privacidade dos titulares. Dados sensíveis incluem informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico (SILVA; SARKIS, 2023)

Dentro do contexto de tratamento de dados pessoais sensíveis, tem-se os dados relacionados a crianças e adolescentes que passam a ter uma importância crítica, dada a vulnerabilidade inerente deste grupo etário. A LGPD estipula que o tratamento de dados pessoais de crianças e adolescentes deve ser realizado em seu melhor interesse, sendo necessário o consentimento específico e destacado, dado por pelo menos um dos pais ou pelo responsável legal. 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 exige que controladores 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 de acordo com os princípios estabelecidos no Estatuto da

Criança e do Adolescente (ECA) e demais normas pertinentes (VASCONCELOS *et al.*, 2023).

3.2. 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. Este mapeamento, conhecido como *Data Mapping*, 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).

Em sequência a este processo, convém que seja estabelecido um programa de governança de dados robusto, envolvendo 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. Um componente crucial da governança de dados é a criação e manutenção de um *Data Inventory*, que funciona como um registro detalhado de todos os dados pessoais coletados, armazenados, processados e compartilhados pela organização (SANTOS FILHO, 2023).

O *Data Inventory* proporciona uma base sólida para a governança de dados, oferecendo visibilidade e controle sobre o ciclo de vida dos dados dentro da organização. Este 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).

Ao manter um *Data Mapping* e um *Data Inventory* 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. Além disso, o *Data Inventory* auxilia na realização de avaliações de impacto sobre a proteção de dados (AIPD), identificando possíveis vulnerabilidades e áreas de não conformidade que necessitam de atenção (REIS *et al*, 2024)..

3.3. GOVERNANÇA DE DADOS

A governança de dados, suportada por um *Data Inventory*, 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. Isso não apenas assegura a conformidade com a LGPD, mas também promove a transparência e a confiança dos seus clientes, ao demonstrar que a organização possui um controle rigoroso sobre os dados pessoais que manipula (CANDIANI; PEREIRA, 2024).

Além disso, a governança de dados e o *Data Inventory* são vitais para a implementação de políticas de minimização de dados, um princípio central da LGPD. Ao entender exatamente quais dados são coletados e por quê, as organizações podem avaliar a necessidade e a relevância de cada conjunto de dados, reduzindo a coleta e o armazenamento de dados desnecessários e, assim, minimizando 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 *Data Inventory* 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).

4. METODOLOGIA

4.1 CARACTERIZAÇÃO METÓDOLÓGICA

Para a elaboração deste artigo foram utilizadas como referência teórica literaturas (artigos de periódicos, congressos e obras) referente a Lei Geral de Proteção de Dados, *Data Mapping*, *Data Inventory* e Governança de Dados. Os artigos de periódicos pesquisados, foram obtidos das bases de conhecimento Scielo, Science Direct e ResearchGate, e as obras utilizadas são de autores relacionados ao referencial teórico da pesquisa.

A metodologia de pesquisa adotada foi descritiva e exploratória, com o objetivo de 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 análise documental como meio de obtenção das evidências necessárias para abordar a criticidade dos processos de *Data Mapping* e de *Data Inventory* (KUMAR, 2019).

Como procedimento metodológico, abordou-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 executadas entrevistas com pontos focais indicados pela área de gestão da instituição, assim como solicitado o preenchimento de um mapeamento para os processos de negócio e os respectivos dados pessoais envolvidos nesses processos, ao longo do 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.

4.2 CARACTERIZAÇÃO DA EMPRESA

A empresa foco do estudo, é uma instituição de ensino infantil e médio, que administra escolas distribuídas em todo território nacional, contemplando crianças e adolescentes como seu principal público-alvo. A instituição, como parte do seu projeto de atendimento a compliance, iniciou a adequação a Lei Geral de Proteção de Dados, com o apoio de uma consultoria de Segurança da Informação e Privacidade, a ITALTEL do Brasil (ITALTEL, 2024).

O processo de adequação a LGPD foi direcionado para a Central da Instituição, situado na cidade do Rio de Janeiro, e com 11 escolas distribuídas no Rio de Janeiro, São Paulo, Recife e Brasília.

Apesar da empresa ser vinculada a sua sede internacional na União Europeia, e esta possuir um processo de adequação a GDPR mais avançado, pouco do que se foi adequado internacionalmente pode ser aproveitado na instituição em território brasileiro, parte por limitação de comunicação entre o DPO da instituição na Europa, parte por necessitar de documentos, entre políticas e procedimentos, traduzidos e aderentes ao cenário brasileiro, em relação a outras legislações e regulações do setor educacional.

4.3 CARACTERIZAÇÃO DO PROBLEMA

Diante deste cenário, então o processo de adequação a 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 a abordagem metodológica aplicada.

Para a execução do processo de adequação, definiu-se então as seguintes fases de execução do processo:

— ***Data Inventory***: Esta etapa consistiu no mapeamento dos fluxos dos processos negócios que tratam dados pessoais, através de entrevistas, assim como o mapeamento de repositórios de dados e tipos de dados pessoais tratados;

— ***Gap Analysis e Roadmap***: Esta etapa consistiu na identificação, análise e avaliação de riscos de privacidade baseado no *Data Inventory* consolidado, o que direcionou a elaboração de um *Roadmap* de ações recomendadas para a adequação a LGPD;

— ***Program Design***: Esta etapa consistiu na elaboração de uma Matriz de Responsabilidades (Matriz RACI), formalização de um *Data Mapping* conslidadando os fluxos de dados pessoais dentro das áreas da instituição em sua central no Rio de Janeiro, assim como por escola;

— ***Program Implementation***: Esta etapa constituiu no acompanhamento na execução do *Roadmap*, junto ao encarregado pelo tratamento de dados pessoais da instituição e também na execução de *Workshops* de conscientização junto aos colaboradores da instituição.

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

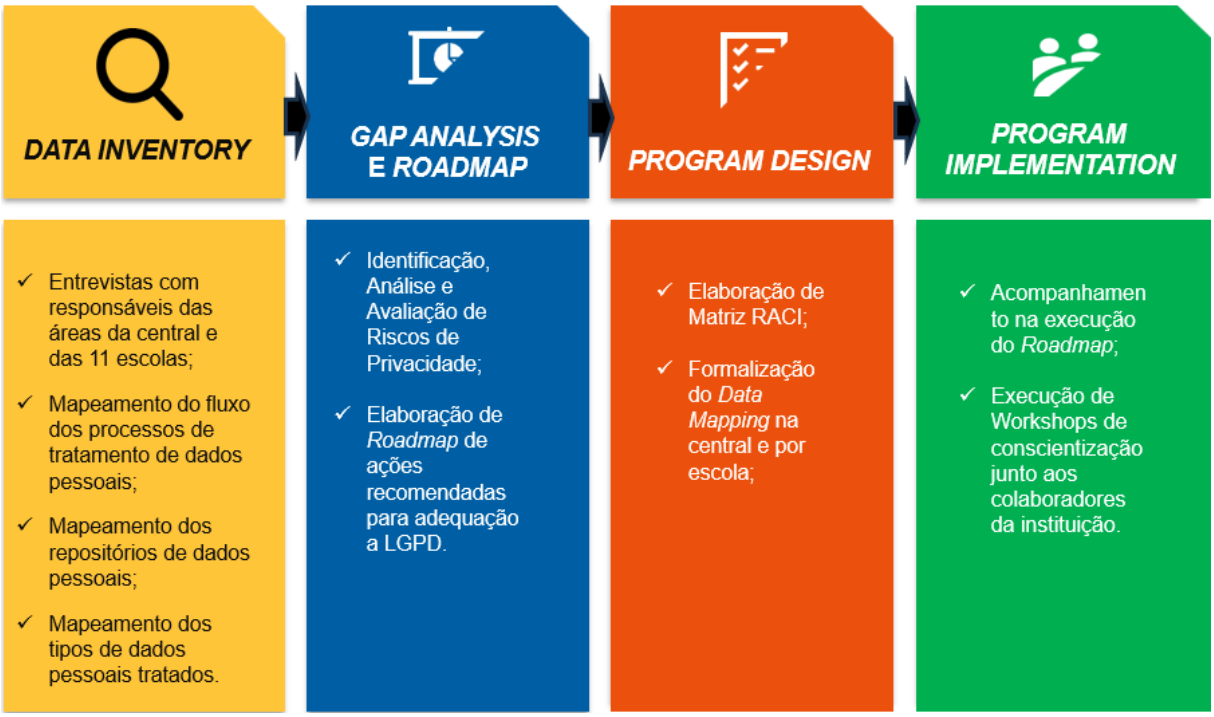

Figura 1: Fluxo das Fases do Processo de Adequação a LGPD.
Fonte: ITALTEL (2024)

Durante a execução do processo de adequação, um ponto chamou a atenção na Fase de *Data Inventory*. 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.

5. ANÁLISE DE RESULTADOS

Com a Fase de *Data Inventory*, 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: ITALTEL (2024)

As 42 entrevistas, que avaliaram a percepção da Segurança da Informação e Privacidade em 6 Domínios: Planejamento, Programa de Governança, Discovery 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.

Planejamento	1,7
Programa de Governança	1,7
Discovery de Dados	2,0
Mapeamento de Controles	1,9
Plano de Ação	1,5
Ação Emergencial	1,3

Figura 2: Nível de Implantação dos Domínios de Segurança da Informação e Privacidade
Fonte: ITALTEL (2024)

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 de criticidade dos processos de adequação.

- **Mapeamento dos Fluxos de Processos:** a segunda etapa consistiu em apresentar um guia oferecido pela ITALTEL do Brasil, 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. Seguem exemplos das informações solicitadas no guia: Área responsável; Processo de negócio; Descrição do processo; Categorias de dados pessoais tratados; Tipos de dados pessoais por categoria; Propósito/finalidade do tratamento de dados; Método da coleta dos dados; Os dados pessoais são compartilhados?; Os dados pessoais são compartilhados com outros países?; Os dados pessoais são estruídos ao término do tratamento?; Qual o tempo de retenção do dado pessoal?; O dado pessoal é submetido a análise automatizada? O dado pessoal é utilizado em campanhas de marketing ou para finalidades diferente da informada?; Em quais repositórios os dados pessoais são armazenados?; O dado pessoal é mantido em algum tipo de formato impresso?; Existe processo ou mecanismo para que o titular possa acessar.

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

Data Inventory proposto no processo de adequação. Deu-se então o segundo ponto de criticidade 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 *Data Inventory* seria então atualizado, pelo próprio encarregado.

Na sequência iniciou-se o a Fase do *Gap Analysis e Roadmap*, 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 *Data Inventory*, conforme demonstrado na Tabela 2.

Tabela 2: 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	Não atendimento ou conformidade de um processo/controle/política	Baixo	Baixo	Baixo

como procedimento formal	com as disposições da Lei Geral de Proteção de Dados			
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 Proteção de Dados	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	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de	Médio	Médio	Médio

como procedimento formal	Proteção de Dados			
Gestão de incidentes de segurança da informação e melhorias - 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
Privacidade de Dados como Controlador				
Identificação e documentação do propósito não definido	Coleta ou processamento de dados pessoais sem transparência ou consentimento do titular da informação	Médio	Médio	Médio
Identificação de bases legais	Dado pessoal adquirido de forma ilegítima	Alto	Alto	Alto
Determinando quando e como o consentimento deve ser obtido não definido	Coleta ou processamento de dados pessoais sem transparência ou consentimento do titular da informação	Médio	Médio	Médio
Obtendo e registrando o consentimento não definido	Coleta ou processamento de dados pessoais sem transparência ou consentimento do titular da informação	Médio	Médio	Médio
Avaliação de impacto de privacidade não definido	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	Alto	Alto	Alto
Contratos com operadores de DP	Transferência insegura de dados pessoais	Alto	Alto	Alto
Controlador conjunto de DP não definido	Não atendimento de disposições jurídicas da Lei Geral de Proteção de Dados (ausência de base legal, violação de princípios e ausência de prazo de retenção)	Alto	Alto	Alto
Registros relativos ao tratamento de DP não definido	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	Alto	Alto	Alto
Determinando e cumprindo as obrigações para os titulares de DP não definido	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de	Alto	Alto	Alto

	Proteção de Dados			
Determinando as informações para os titulares de DP não definido	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	Alto	Alto	Alto
Fornecendo informações aos titulares de DP não definido	Coleta ou processamento de dados pessoais sem transparência ou consentimento do titular da informação	Alto	Alto	Alto
Fornecendo mecanismos para modificar ou cancelar o consentimento não definido	Coleta ou processamento de dados pessoais sem transparência ou consentimento do titular da informação	Médio	Médio	Médio
Fornecendo mecanismos para negar o consentimento ao tratamento de DP não definido	Coleta ou processamento de dados pessoais sem transparência ou consentimento do titular da informação	Alto	Alto	Alto
Acesso, correção e/ou exclusão não definido	Coleta ou processamento de dados pessoais sem transparência ou consentimento do titular da informação	Alto	Alto	Alto
Obrigações dos controladores de DP para informar aos terceiros	Transferência insegura de dados pessoais	Alto	Alto	Alto
Fornecendo cópia do DP tratado não definido	Coleta ou processamento de dados pessoais sem transparência ou consentimento do titular da informação	Médio	Médio	Médio
Tratamento de solicitações não definido	Não atendimento de disposições jurídicas da Lei Geral de Proteção de Dados (ausência de base legal, violação de princípios e ausência de prazo de retenção)	Alto	Alto	Alto
Tomada de decisão automatizada não definido	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	Alto	Alto	Alto
Limite de coleta não definido	Armazenamento ou retenção de dados além do necessário	Alto	Alto	Alto
Limite de tratamento não definido	Acesso ilegítimo/indevido a dados pessoais que pode viabilizar o uso inapropriado ou alteração/modificação	Alto	Alto	Alto
Precisão e qualidade não definidas	Coleta ou processamento de dados pessoais sem transparência ou consentimento do titular da informação	Alto	Alto	Alto
Objetivos de minimização de DP não definido	Não atendimento de disposições jurídicas da Lei Geral de Proteção de Dados (ausência de base legal, violação de princípios e ausência de prazo de retenção)	Alto	Alto	Alto
Anonimização e exclusão de DP ao final do tratamento não definido	Não atendimento de disposições jurídicas da Lei Geral de Proteção de Dados (ausência de base legal, violação de princípios e ausência de prazo de retenção)	Alto	Alto	Alto
Arquivos temporários não definido tempo de retenção	Armazenamento ou retenção de dados além do necessário	Alto	Alto	Alto
Retenção não definido	Armazenamento ou retenção de	Alto	Alto	Alto

	dados além do necessário			
Descarte não definido	Armazenamento ou retenção de dados além do necessário	Alto	Alto	Alto
Controle de transmissão de DP não definido	Transferência insegura de dados pessoais	Alto	Alto	Alto
Identificando as bases para a transferência de DP entre jurisdições	Transferência insegura de dados pessoais	Alto	Alto	Alto
Países e organizações internacionais para os quais os DP podem ser transferidos não definido	Transferência internacional de dados pessoais (sem consentimento do titular)	Alto	Alto	Alto
Registros de transferência de DP não definido	Transferência insegura de dados pessoais	Alto	Alto	Alto
Registro de divulgação de DP para terceiros não definido	Transferência insegura de dados pessoais	Alto	Alto	Alto

Fonte: ITALTEL (2024)

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.

ID	Risco	Classificação	#
A	Segurança da Informação e Privacidade	11 Altos 12 Médios	23
B	Privacidade de Dados como Controlador	26 Altos 5 Médios 8 Baixos	39
C	Privacidade de Dados como Operador	N/A	0

Figura 3: Matriz de Probabilidade e Impacto de Riscos.
Fonte: ITALTEL (2024)

Com a visão dos riscos definida foi possível estabelecer um *Roadmap* 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 *Program Design*.

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

Figura 4: Recorte da Matriz RACI e Planos de Ação
Fonte: ITALTEL (2024)

Como atividade sequencial da Etapa de *Program Design* formalizou-se o *Data Mapping*, com o mapeando dos fluxos de tratamento dos dados pessoais dentro da instituição. Na Figura 5 é apresentado um recorte do *Data Mapping* efetuado na central da instituição, mapeando os dados pessoais tratados, as áreas que tratam estes dados e os respectivos processos.

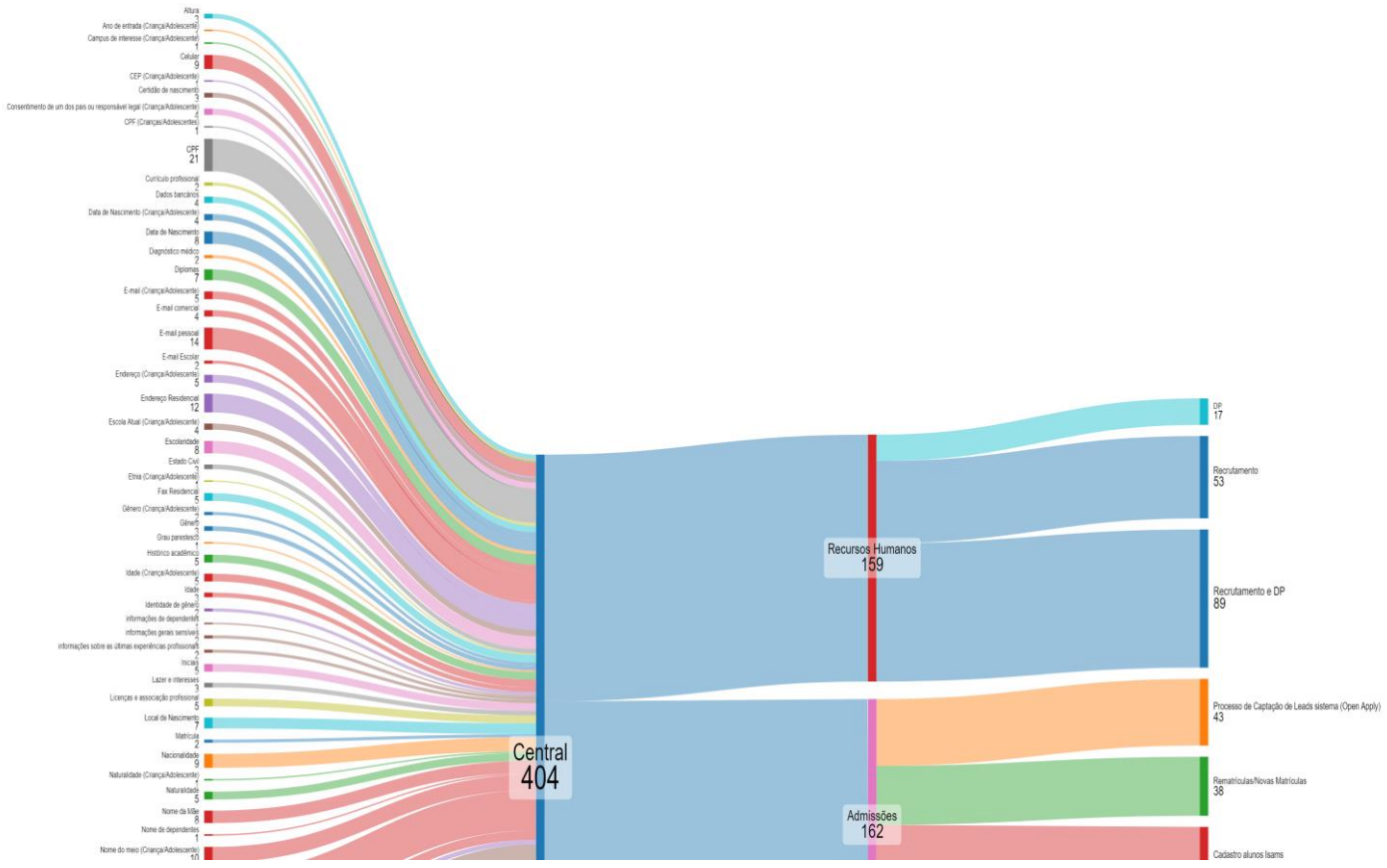

Figura 5: Recorte do Data Mapping da Central da Instituição
Fonte: ITALTEL (2024)

6. 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 *Data Mapping*. 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 *Data Inventory* 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 de criticidade dos processos de *Data Mapping* e *Data Inventory*, 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 *Roadmap* precisa ser muito bem estruturado para que os processos necessários de Segurança da Informação e Privacidade venha a ser formalizados nas organizações.

Este processo de adequação continuou na instituição de ensino infantil durante a Fase de *Program Implementation*, 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.

7. 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.

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, I.F.; PEREIRA, O. J. 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, R. J.; AGUIAR, J. J. B. The impacts of the General Data Protection Law (LGPD) on information security: a literature review. Revista de Gestão e Secretariado, [S. l.], v. 15, n. 2, p. e3442, 2024. DOI: 10.7769/gesec.v15i2.3442.

FERRÃO, S. É. R. *et al.* Towards a taxonomy of privacy requirements based on the LGPD and ISO/IEC 29100. Information and Software Technology, p. 107396, 2024.

GIL, A. C. Como elaborar projetos de pesquisa. 6. ed. São Paulo: Atlas, 2019.

KUMAR, R. 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.

NASCIMENTO, B. L. C.; SILVA, E. M. Lei Geral de Proteção de Dados (LGPD) e repositórios institucionais: reflexões e adequações. Em Questão, v. 29, p. e-127314, 2023.

REIS, S. R. F. *et al.* Desafios da LGPD quanto à privacidade em ambientes educacionais: um mapeamento sistemático. GeSec: Revista de Gestao e Secretariado, v. 15, n. 3, 2024.

SANTOS FILHO, R. F. S. F.; DE JESUS, V. B. Compliance de Dados em Instituições de Ensino Superior. Revista de Constitucionalização do Direito Brasileiro, v. 6, n. 2, p. 274-296, 2023.

SHIN, S. *et al.* Proposal for a Privacy Impact Assessment Manual Conforming to ISO/IEC 29134:2017. In: Saeed, K., Homenda, W. (eds) 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, K.; SARKIS, L. Análise de conformidade da LGPD nas Instituições Públicas de Ensino Superior no Brasil sob a perspectiva dos profissionais de TIC. In: WER. 2023.

VASCONCELOS G., F. *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, G. S. *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.