

IDENTIFICAÇÃO DE PONTOS CRÍTICOS EM PROCESSO DE ADEQUAÇÃO À LGPD EM INSTITUIÇÃO DE ENSINO INFANTIL E MÉDIO

DACYR DANTE DE OLIVEIRA GATTO- dacyr.gatto@uni9.pro.br
UNIVERSIDADE NOVE DE JULHO - UNINOVE

NITYANANDA PORTELLADA- nityananda.portellada@gmail.com
UNIVERSIDADE NOVE DE JULHO - UNINOVE

RENATO JOSÉ SASSI – sassi@uni9.pro.br
UNIVERSIDADE NOVE DE JULHO - UNINOVE

ÁREA: *6. ENGENHARIA ORGANIZACIONAL*
SUBÁREA: *6.7. - GESTÃO DA TECNOLOGIA*

RESUMO: *A LGPD DETERMINA QUE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES NECESSITAM DE PROTEÇÃO ADICIONAL A PRIVACIDADE. A ADEQUAÇÃO À LGPD EM INSTITUIÇÕES DE ENSINO INFANTIL E MÉDIO DEVE CONSIDERAR OS RISCOS ASSOCIADOS. AS ATIVIDADES DE DATA MAPPING E DATA INVENTORY SÃO CRUCIAIS PARA UM PROCESSO DE ADEQUAÇÃO 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 DE NATUREZA DESCRITIVA E EXPLORATÓRIA. A ABORDAGEM DA PESQUISA É QUALITATIVA, UTILIZANDO A ANÁLISE DOCUMENTAL COMO MEIO PARA OBTER AS EVIDÊNCIAS NECESSÁRIAS. COMO PROCEDIMENTO METODOLÓGICO, ADOTOU-SE A PESQUISA DE CAMPO COMO MÉTODO DE COLETA DE DADOS, QUE ENVOLVEU ENTREVISTAS E ENGAJAMENTO COM AS PESSOAS EM SEU AMBIENTE NATURAL. A EMPRESA EM FOCO ADMINISTRA ESCOLAS DISTRIBUÍDAS EM TODO O TERRITÓRIO NACIONAL., A INSTITUIÇÃO INICIOU A ADEQUAÇÃO À LGPD COM O APOIO DE UMA CONSULTORIA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE, A ITALTEL DO BRASIL. O PROCESSO SEGUIU EM QUATRO FASES: DATA INVENTORY, GAP ANALYSIS E ROADMAP, PROGRAM DESIGN E PROGRAM IMPLEMENTATION. DURANTE AS ATIVIDADES DO PROCESSO DE ADEQUAÇÃO À LGPD, FORAM IDENTIFICADOS DOIS PONTOS CRÍTICOS QUE COMPROMETERAM PARCIALMENTE O ANDAMENTO DO PROCESSO DE ADEQUAÇÃO.*

PALAVRAS-CHAVES: *LGPD; PRIVACIDADE; INSTITUIÇÕES DE ENSINO INFANTIL E MÉDIO; DATA MAPPING; DATA INVENTORY.*

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).

As atividades de mapeamento e inventário de dados pessoais, conhecidos em inglês como *Data Mapping* e *Data Inventory*, 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).

Este artigo objetiva, por meio de uma pesquisa de campo, identificar os pontos de criticidade nos processos de *Data Mapping* e *Data Inventory* em um caso real de adequação à LGPD em uma instituição de ensino infantil e médio, descrevendo os desafios e os resultados decorrentes da execução desses processos.

2. FUNDAMENTAÇÃO TEÓRICA

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. 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).

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. Um componente essencial 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).

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 *Data Mapping* e o *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. Ademais, o *Data Inventory* 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 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 (CANDIANI; PEREIRA, 2024).

A governança de dados e o *Data Inventory* 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 de 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 *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).

3. METODOLOGIA

Para a elaboração deste artigo, utilizou-se como referência teórica literaturas relacionadas à 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, 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 *Data Mapping* e *Data Inventory* (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 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.

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 (ITALTEL, 2024).

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.

3.1 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:

- ***Data Inventory:*** 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.
- ***Gap Analysis* e *Roadmap*:** Esta fase envolveu a identificação, análise e avaliação de riscos de privacidade baseados no Data Inventory consolidado, o que direcionou a elaboração de um Roadmap de ações recomendadas para a adequação à LGPD.
- ***Program Design*:** Esta fase consistiu na elaboração de uma Matriz de Responsabilidades (Matriz RACI), formalização de um Data Mapping consolidando os fluxos de dados pessoais dentro das áreas da instituição em sua central no Rio de Janeiro, bem como em cada escola.
- ***Program Implementation*:** Esta etapa incluiu o acompanhamento na execução do *Roadmap*, 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 *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.

4. 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.

FIGURA 2: Nível de Implantação dos Domínios de Segurança da Informação e Privacidade



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

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. 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: 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

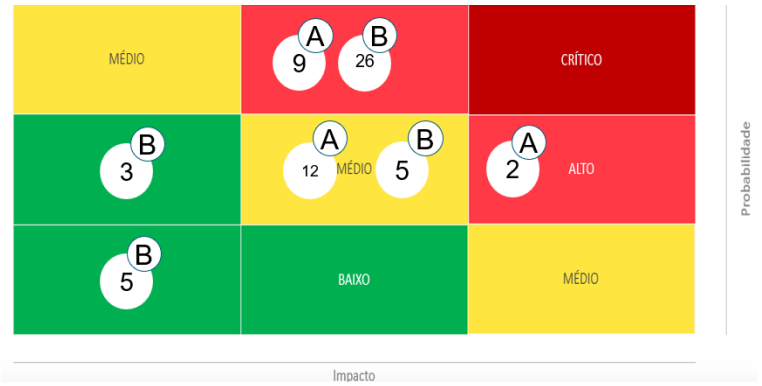
Descarte de mídias não estabelecido como procedimento formal	Não atendimento ou conformidade de um processo/controle/política com as disposições da Lei Geral de Proteção de Dados	Médio	Baixo	Baixo
Transferência física de mídias não estabelecido como procedimento formal	Não atendimento ou conformidade 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

	Proteção de Dados			
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 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

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.

Figura 3: Matriz de Probabilidade e Impacto de Riscos.



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

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*.

Figura 4: Recorte da Matriz RACI e Planos de Ação

Matriz RACI - Planos de Ação

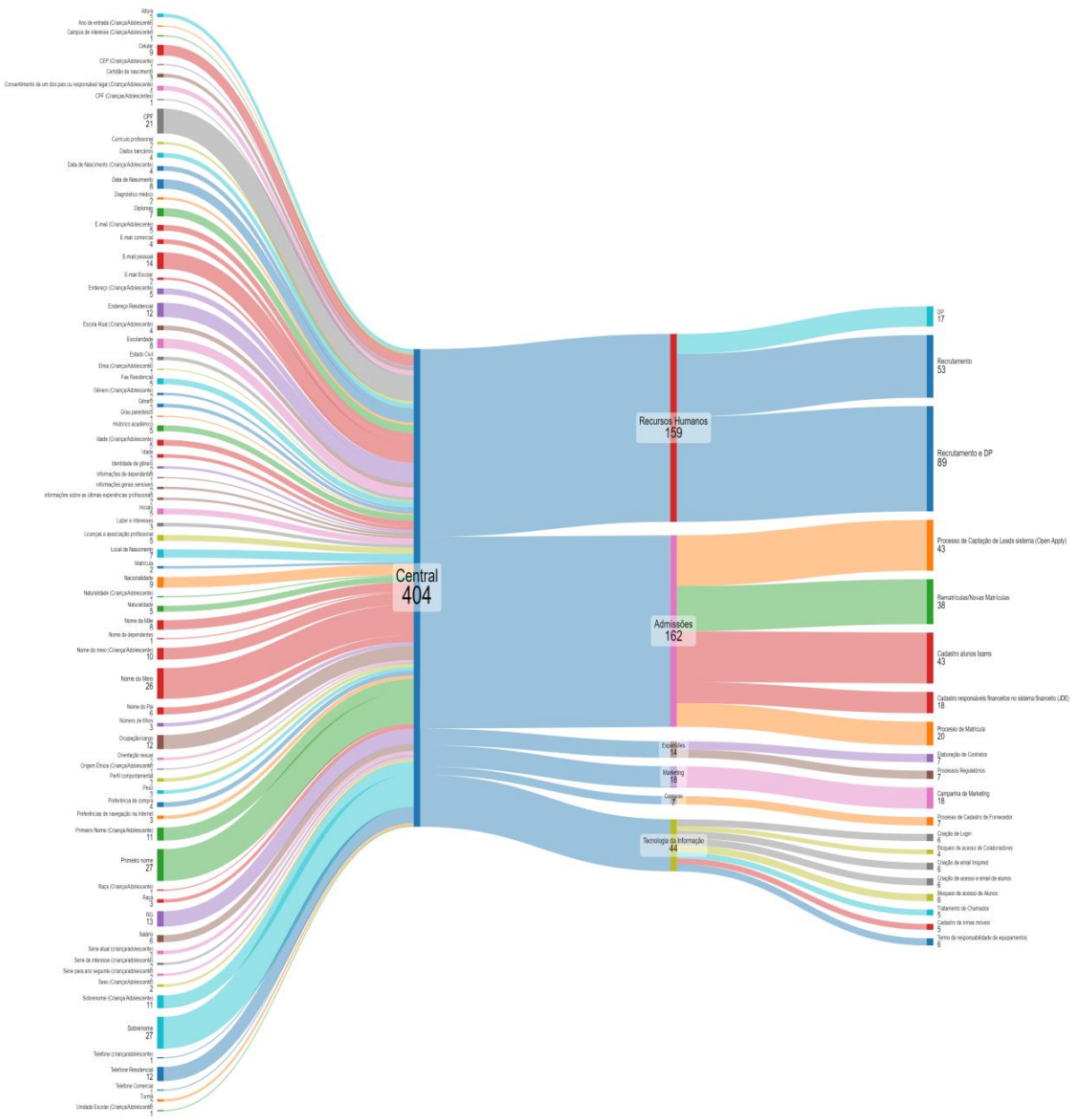
R: Responsável
A: Prestador de Contas
C: Consultado
I: Informado

	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: 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 o *Data Mapping* efetuado na central da instituição, mapeando os dados pessoais tratados, as áreas que tratam estes dados e os respectivos processos.

Figura 5: *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.

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.