CENTRO UNIVERSITÁRIO UNICARIOCA
MESTRADO PROFISSIONAL EM NOVAS TECNOLOGIAS DIGITAIS NA EDUCAÇÃO

Alexander Martins dos Santos

A UTILIZAÇÃO DE TECNOLOGIAS DIGITAIS PARA SUPERAR OS DESAFIOS DA SEGURANÇA DA INFORMAÇÃO NA EDUCAÇÃO

Rio de Janeiro

2025

Alexander Martins dos Santos

A UTILIZAÇÃO DE TECNOLOGIAS DIGITAIS PARA SUPERAR OS DESAFIOS DA SEGURANÇA DA INFORMAÇÃO NA EDUCAÇÃO

Dissertação apresentada ao Programa de Pós-Graduação em Novas Tecnologias Digitais na Educação do Centro Universitário UniCarioca como parte dos requisitos necessários para a obtenção do Título de Mestre em Novas Tecnologias Digitais na Educação.

Orientadores: Prof Hugo Cesar Bellas, titulação (D. Sc.)
Prof Jorge E Mansur Serzedello, titulação (D. Sc.)

Rio de Janeiro

2025

S231g Santos, Alexander Martins dos
A utilização de tecnologias digitais para superar os desafios da segurança da informação na educação / Alexander Martins dos Santos; orientador: Hugo Cesar Bellas; coorientador: Jorge Eduardo Mansur Serzedello. – Rio de Janeiro, 2026.
102 f.

Dissertação (Mestrado Profissional em Novas Tecnologias Digitais na Educação) – Centro Universitário UniCarioca, Rio de Janeiro, 2026.

1.Tecnologias digitais. 2. Segurança da informação. 3. Segurança de dados em educação. 4. Lei geral de proteção de dados; Capacitação profissional. I. Bellas, Hugo Cesar, prof. orient. II. Serzedello, Jorge Eduardo Mansur, prof. coorient. III. Título.

CDD: 371.344

ALEXANDER MARTINS DOS SANTOS

A UTILIZAÇÃO DE TECNOLOGIAS DIGITAIS PARA SUPERAR OS DESAFIOS DA SEGURANÇA DA INFORMAÇÃO NA EDUCAÇÃO

Dissertação apresentada ao Programa de Pós-Graduação em Novas Tecnologias Digitais na Educação do Centro Universitário UniCarioca como parte dos requisitos necessários para a obtenção do Título de Mestre em Novas Tecnologias Digitais na Educação.

O Presidente da Banca, abaixo assinado, atesta que os membros da banca participaram desta defesa de dissertação.

Examinado por:

gov.br
Documento assinado digitalmente
HUGO CESAR BELLAS
Data: 30/12/2025 10:17:23-0300
Verifique em https://validar.iti.gov.br

Prof. Hugo Cesar Bellas, D. Sc. (UniCarioca)
Presidente da Comissão Examinadora

Prof. Paulo Victor Rodrigues de Carvalho, D. Sc. (UniCarioca)

Profa. Bárbara Bulhões Lopes de Andrade, D. Sc. (FIOCRUZ)

Rio de Janeiro
2025

DEDICATÓRIA

A ti, Deus, toda honra e toda glória. Por me guiar, me fortalecer e por tornar este sonho possível.

Ao meu pai, Pedro, que partiu antes que pudesse ver este dia, mas que, em memória, esteve comigo em cada linha escrita. cujo exemplo de retidão e amor, sempre será minha maior inspiração. Que no céu, saiba que seu legado vive em mim.

E minha mãe, Léa, minha primeira professora, meu maior exemplo de força e dedicação, por seu amor incondicional, seus sacrifícios silenciosos e por ser a base de tudo. Obrigado por nunca me deixar desistir.

À minha amada esposa, Renata, por sua paciência infinita com minhas horas de ausência, pela compreensão nos momentos difíceis e por ser meu apoio constante meu porto seguro, minha cúmplice e companheira de vida. Obrigado por ter caminhado ao meu lado em cada desafio, por todo amor e por ser a razão pela qual cada esforço valeu a pena.

Às minhas queridas filhas, Raianny e Raphaella, que com seus sorrisos iluminaram os dias mais cansativos e me deram a maior motivação para construir um futuro melhor. Dedico a vocês cada página, como uma promessa do futuro que estamos construindo juntos.

Aos meus irmãos, Alessandra e Alessandro, meus amigos de uma vida, obrigado pelo apoio constante e pela certeza de que eu nunca estava sozinho.
A todos, minha eterna gratidão.

AGRADECIMENTOS

Toda a minha gratidão a Deus. Pela força nas dificuldades, pela clareza nas incertezas e pela fé necessárias para percorrer esta longa e, por vezes, árdua jornada acadêmica. Sem a Sua força, esta conquista não seria possível, renovou minhas energias e me permitiu chegar até aqui.

Agradeço de coração ao meu orientador, Professor D. Hugo Cesar Bellas e Coorientador Professor D. Jorge E Mansur Serzedello, meu mais sincero e afetuoso agradecimento. Sou imensamente grato por sua paciência infinita e por sua presença serena, que me trouxeram segurança e tranquilidade nos inúmeros momentos de dúvida que surgiram nesta jornada. Mais do que um orientador, você foi um mentor que acreditou no meu potencial e me incentivou a ir além. Obrigado pela confiança e por tornar este caminho muito mais leve.

A todos os professores que cruzaram meu caminho no mestrado, meu muito obrigado pelo conhecimento compartilhado, que moldou minha visão como pesquisador.

Nesta página, preciso registrar o meu mais sincero e comovido agradecimento a quatro pessoas que foram essenciais para que este trabalho não fosse interrompido pela dor: minhas queridas amigas Michele Bitencourt Marques, Renata Marques Costa, Simone Marques Costa e Taís Ferraz Duarte. Vocês estiveram ao meu lado no pior momento da minha vida, a perda do meu amado pai. Quando pensei em desistir, quando o luto parecia maior que minhas forças, foi a amizade, o carinho e o apoio incansável de vocês que me reergueram e me lembraram do meu propósito. Esta dissertação só foi concluída porque vocês não me deixaram parar. Recebam meu eterno carinho e gratidão.

RESUMO

Esta dissertação aborda a utilização de tecnologias digitais como estratégia para a capacitação de profissionais da educação frente aos desafios da segurança da informação, em um contexto marcado pela crescente digitalização e pela vigência da Lei Geral de Proteção de Dados (LGPD). O problema de pesquisa parte da vulnerabilidade das instituições de ensino a ataques cibernéticos e da necessidade de formar educadores para utilizarem de modo seguro os dados pessoais e institucionais, preenchendo uma lacuna de conhecimento prático nesta área. O objetivo geral do estudo foi elaborar e aplicar um curso online sobre segurança da informação e LGPD, destinado a profissionais do ambiente educacional. Como objetivos específicos, capacitar os participantes nos conceitos básicos de segurança e da legislação, e aprimorar seus conhecimentos para a proteção de dados no cotidiano. A metodologia consistiu na concepção, aplicação e avaliação de um curso de capacitação online, utilizando as plataformas Microsoft PowerPoint para exposição de conteúdo e Microsoft Teams para a realização das aulas. O estudo contou com 14 participantes, incluindo professores, gestores e pessoal administrativo da educação básica. A avaliação do treinamento foi realizada por meio de um questionário aplicado ao final do curso. Os resultados indicam uma eficácia e satisfação com o curso proposto. A maioria dos participantes (92%) relatou um aumento significativo no conhecimento sobre segurança de dados e LGPD e uma percepção de maior segurança em suas práticas digitais. A totalidade dos respondentes (100%) considerou o conteúdo bom, a duração adequada e recomendaria o treinamento. Foram identificados pontos para aprofundamento futuro, como procedimentos práticos de reporte de incidentes e a apresentação de mais ferramentas tecnológicas de apoio. Conclui-se que a capacitação mediada por tecnologias digitais é uma abordagem metodológica eficaz para preparar profissionais da educação para os desafios atuais da segurança da informação. O estudo demonstra que o treinamento melhorou o conhecimento técnico e uma cultura de segurança e responsabilidade, contribuindo para a construção de ambientes educacionais mais seguros e em conformidade com as diretrizes da LGPD.

Palavras-chave: Tecnologias Digitais; Segurança da informação; Segurança de dados em educação; Lei Geral de Proteção de Dados; Capacitação profissional.

ABSTRACT

This dissertation addresses the use of digital technologies as a strategy for training education professionals in the face of information security challenges, in a context marked by increasing digitization and the enforcement of the General Data Protection Law (LGPD). The research problem stems from the vulnerability of educational institutions to cyber attacks and the need to train educators to use personal and institutional data safely, filling a gap in practical knowledge in this area. The overall objective of the study was to develop and implement an online course on information security and LGPD, aimed at professionals in the educational environment. The specific objectives were to train participants in the basic concepts of security and legislation and to improve their knowledge of data protection in everyday life. The methodology consisted of the design, application, and evaluation of an online training course, using Microsoft PowerPoint for content presentation and Microsoft Teams for conducting classes. The study had 14 participants, including teachers, managers, and administrative staff from basic education. The training was evaluated through a questionnaire administered at the end of the course. The results indicate the effectiveness of and satisfaction with the proposed course. Most participants (92%) reported a significant increase in knowledge about data security and the LGPD and a perception of greater security in their digital practices. All respondents (100%) considered the content to be good, the duration to be adequate, and would recommend the training. Points for future development were identified, such as practical incident reporting procedures and the presentation of more technological support tools. It was concluded that training mediated by digital technologies is an effective methodological approach to preparing education professionals for the current challenges of information security. The study demonstrates that the training improved technical knowledge and a culture of security and responsibility, contributing to the construction of safer educational environments in compliance with LGPD guidelines.

Keywords: Digital Technologies; Information Security; Data Security in Education; Brazilian General Data Protection Law (LGPD); Professional Training.

SUMÁRIO

1. INTRODUÇÃO 12
1.1. Inquietação 15
1.2. Caracterização do Problema 17
1.3. Tecnologia na Educação 18
1.4. Relevância 19
1.5. Objetivos 20
1.5.1. Objetivo Geral 20
1.5.2. Objetivos Específicos 21
2. FUNDAMENTAÇÃO TEÓRICA 22
2.1. O Paradigma da Segurança da Informação na Sociedade Digital 22
2.2. A Lei Geral de Proteção de Dados (LGPD) como Marco Regulatório no Brasil 22
2.3. A Intersecção entre LGPD e o Ambiente Escolar: Desafios e Responsabilidades 23
3. PERCURSO METODOLÓGICO 24
3.1. Concepção e Estruturação do Curso: 27
3.2. Desenvolvimento do Conteúdo em PowerPoint: 28
3.3. Aplicação do Curso via Microsoft Teams: 30
4. ETAPAS DO PERCURSO METODOLÓGICO COM A DESCRIÇÃO DOS RESULTADOS 30
5. Recursos Didáticos e o Ambiente Virtual de Aprendizagem 69
5.1. Estrutura do Material Didático 70
5.2. Resultados 71
6. ANÁLISE DOS DADOS E DISCUSSÃO 94
6.1. Eficácia da Intervenção e o Aumento da Percepção de Segurança 95
6.2. Transferência de Aprendizagem e o Letramento Digital no Contexto Educacional 96
6.3. Avaliação da formação 96
7. CONCLUSÃO 97
REFERÊNCIAS BIBLIOGRÁFICAS 99

LISTA DE GRÁFICOS

Gráfico 1 – Gênero 72
Gráfico 2 - Faixa etária 73
Gráfico 3 - Perfil dos participantes 74
Gráfico 4 - Experiencia profissional dos participantes 75
Gráfico 5 - Área de atuação dos participantes 76
Gráfico 6 - Segmentação escolar dos participantes 77
Gráfico 7 - Expectativa do treinamento 78
Gráfico 8 - Resultado sobre o conteúdo abordado 79
Gráfico 9 - Resultado sobre a segurança dos dados após o treinamento 80
Gráfico 10 - Resultado sobre a compreensão dos participantes na aplicação do treinamento 81
Gráfico 11 - Resultado sobre o aumento conhecimento sobre a LGPD 82
Gráfico 12 - Resultado sobre o aumento conhecimento sobre segurança de dados 83
Gráfico 13 - Resultado de como os usuário se sentem seguros após o treinamento 84
Gráfico 14 - Resultado se com o treinamento ajudará melhorar a segurança no seu ambiente de trabalho ou em casa 85
Gráfico 15 - Recomendação do treinamento para outras pessoas 86
Gráfico 16 - O gráfico demostra a profundidade do conteúdo abordado 87
Gráfico 17 - Relacionado a pergunta anterior, a imagem abaixo apresenta a sugestão do participante 88
Gráfico 18 - Resultado sobre a duração do treinamento 89
Gráfico 19 - Avaliação se haveria necessidade de mais algum conteúdo para ser abordado 90
Gráfico 20 - Relacionado a pergunta anterior, a imagem abaixo apresenta a sugestão do participante 91
Gráfico 21 - O tempo de treinamento foi adequado? 92
Gráfico 22 - Notas para avaliação do treinamento 93

LISTA DE FIGURAS

Figura 1 - Percurso metodológico 25
Figura 2 – Primeiro slide do treinamento 33
Figura 3 - Dados importantes 34
Figura 4 - Tipos de dadosFonte: Autoria própria (2025) 36
Figura 5 - Slide sobre a importância da segurança de dados 38
Figura 6 - Criptografia e Autenticação 44
Figura 7 - formas de segurança em dispositivos móveis 46
Figura 8 - Redes Sociais e Internet 48
Figura 9 - Segurança e resposta aos incidentes 50
Figura 10 - LGPD 52
Figura 11 - O que é a LGPD 54
Figura 12 - Os direitos do titular dos dados 55
Figura 13 - Dados Pessoais 57
Figura 14 - Seus direitos 59
Figura 15 - Utilização dos seus dados 61
Figura 16 - Protegendo seus dados pessoais 62
Figura 17 - Vazamentos de dados 64
Figura 18 - Impacto da LGPD 65
Figura 19 - Conclusão 67

LISTA DE QUADROS

Quadro 1 - Etapas do percurso metodológico..... 30

LISTA DE ABREVIATURAS E SIGLAS

SIGLA	SIGNIFICADO
ARPANET	Advanced Research and Projects Agency Network
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
CID	Confidencialidade, Integridade e Disponibilidade
LGPD	Lei Geral de Proteção de Dados

1. INTRODUÇÃO

A evolução da segurança da informação mostra que, antes da digitalização dos processos, a proteção de dados se apoiava quase exclusivamente em mecanismos físicos. Nessa fase, o foco estava em limitar o acesso a documentos, controlar ambientes e evitar que o conteúdo circulasse sem autorização. Assim, a noção de segurança era associada principalmente à guarda material dos registros e ao controle das condições de acesso (Camello; Alves, 2021).

O surgimento dos computadores representa uma grande mudança para a área de segurança da informação. A partir desse avanço tecnológico, tornou-se necessário ampliar o foco da proteção, que antes se concentrava em documentos físicos, para abranger também arquivos, sistemas e processos digitais. Esse movimento inaugura o cenário em que se estabelecem as bases da cibersegurança contemporânea (Beppler, 2021).

Durante as décadas de 1950 e 1960, o contexto da Guerra Fria ampliou de maneira significativa ferramentas à proteção da informação. Além das tradicionais barreiras físicas, tornou-se necessário adotar mecanismos mais rigorosos de controle de acesso, para evitar vazamentos decorrentes de infiltrações e espionagem interna (KAHN, 1996). Nesse mesmo período, descobriu-se que equipamentos eletrônicos podiam emitir sinais captáveis à distância, o que levou ao desenvolvimento de medidas de contenção de emissões eletromagnéticas, posteriormente consolidadas no programa TEMPEST da NSA (NSA, 2008). Em resposta às novas ameaças, surgiram também técnicas e tecnologias mais sofisticadas, como o uso ampliado de criptografia de alta segurança — incluindo o One-Time Pad e máquinas eletromecânicas como o KL-7 empregadas pela OTAN — além de sistemas seguros de voz e métodos avançados de análise de tráfego para identificar padrões de comunicação mesmo sem acesso ao conteúdo das mensagens (ANDREW, 2018; ANDREW; MITROKHIN, 1999). Esses avanços estabeleceram bases estratégicas que influenciariam diretamente o desenvolvimento posterior da segurança no ambiente digital. (Pinheiro, 2022).

A popularização da internet nos anos 1990 transformou profundamente o cenário da segurança da informação. Redes que até então operavam em ambientes controlados, como a ARPANET de origem militar (GARCIA, 2002), passaram a integrar um espaço aberto e global, marcado pela diversidade de atores e pela ausência de relações de confiança. Com essa abertura, os limites de proteção que antes eram bem definidos deixaram de existir, e a

necessidade de segurança ultrapassou o setor governamental, alcançando empresas, provedores e usuários comuns que começavam a explorar o novo ambiente digital.

A abertura da internet ao público ampliou rapidamente o repertório de riscos digitais. A partir desse período, diferentes tipos de software malicioso passaram a circular com mais facilidade, aproveitando brechas presentes em sistemas amplamente utilizados. Alterações indevidas em páginas da web se tornaram frequentes como forma de provocação ou ataque simbólico, enquanto práticas como envio de mensagens enganosas e golpes eletrônicos começaram a ganhar espaço. Paralelamente, o perfil dos agentes envolvidos na exploração dessas vulnerabilidades também se diversificou, abrangendo desde indivíduos movidos por curiosidade ou desafio até grupos organizados com fins econômicos (BEPPLER, 2021; CANAZARO, 2022).

A ampliação das ameaças digitais levou o setor tecnológico a criar produtos voltados ao fortalecimento da proteção dos usuários. Entre essas iniciativas, os antivírus passaram a desempenhar um importante papel na defesa de computadores pessoais, enquanto os firewalls foram aprimorados para bloquear tentativas de acesso indevido vindas da internet. Nesse mesmo período, surgiram protocolos de criptografia para garantir a confidencialidade das informações em circulação, como o SSL, responsável por abrir caminho para o HTTPS e possibilitar transações eletrônicas mais seguras. (SLEIGH, 2023).

No início do século XXI, o volume de informações digitais cresceu de forma acelerada, impulsionado pelo avanço da computação em nuvem e pela popularização de dispositivos conectados no contexto da Internet das Coisas (IoT). Esse novo ambiente tecnológico ampliou as possibilidades de inovação, mas também aumentou significativamente os riscos relacionados ao uso e à circulação de dados. Nesse cenário, a segurança da informação passou a incorporar uma perspectiva mais ampla, consolidando-se no campo da cibersegurança, que hoje desempenha um papel importante não apenas na proteção de infraestruturas e serviços, mas também na defesa da privacidade e dos dados pessoais. (DONEDA, 2023).

Durante o período da pandemia e nos anos seguintes, o cibercrime ganhou relevância e tornou-se um dos tipos de delito mais frequentes, afetando especialmente pequenas e médias empresas. Esses negócios, muitas vezes, não possuem estruturas maduras de proteção, o que os torna mais vulneráveis a ataques e incidentes digitais. Estudos apontam que organizações com políticas de segurança pouco desenvolvidas enfrentaram prejuízos significativos nesse período (DE ABREU, 2022).

No ambiente da economia digital, a segurança da informação passou a ocupar posição estratégica dentro da governança corporativa. A adoção inadequada de práticas de proteção expõe as organizações a riscos significativos, que se manifestam em prejuízos financeiros e em danos à imagem institucional. Episódios como vazamentos de dados e falhas operacionais comprometem a percepção do público e podem afetar a confiança dos consumidores, com impacto direto sobre o valor da marca e a manutenção de relacionamentos de longo prazo (MONTEIRO; MENDES SILVA, 2022).

A inadequada segurança da informação inflige danos reputacionais a uma organização. Uma violação de dados, ao expor a vulnerabilidade da empresa, corrói diretamente a confiança do cliente, um ativo de valor muita das vezes se incalculável. Essa quebra de confiança eleva a percepção de risco por parte dos consumidores, que podem hesitar em manter ou iniciar relações comerciais com uma entidade vista como incapaz de tutelar suas informações pessoais. Tal hesitação pode culminar na evasão da base de clientes existente, na dificuldade de atrair novos negócios (LUCAS; MEIRELLES, 2021).

Nesse contexto, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018 (BRASIL, 2018), representa um marco regulatório importante no cenário jurídico brasileiro, estabelecendo uma nova forma para o tratamento de dados pessoais no país. Inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD surge em um contexto global de crescente preocupação com a privacidade e o controle dos dados pessoais em decorrência com a expansão da economia digital e da intensificação da coleta e uso de informações por organizações de todos os portes.

A LGPD também se revela a sua importância para o desenvolvimento econômico sustentável do Brasil na era digital. A (SERASA EXPERIAN) salienta que " A LGPD é um importante marco regulatório que estabelece princípios, direitos e responsabilidades no tratamento de dados pessoais. O objetivo é levar transparência aos titulares em relação aos seus direitos, bem como mais detalhes sobre em quais situações e de que forma os seus dados pessoais podem ser tratados." Ao alinhar o Brasil com as normas globais de proteção de dados, a LGPD fortalece a confiança no ambiente de negócios digital brasileiro, facilitando o comércio internacional e a colaboração com parceiros estrangeiros.

A crescente digitalização das documentações nas escolas e com a grande utilização de tecnologias, têm intensificado a coleta e o processamento de dados pessoais nas instituições de ensino. A proteção dessas informações tornou-se um tema de grande importância, especialmente com a vigência da Lei Geral de Proteção de Dados (LGPD).

Nesse sentido, as instituições de ensino podem implementar práticas de segurança da informação alinhadas às exigências legais, buscando proteger os dados de alunos, professores e colaboradores. O estudo explora os principais desafios enfrentados pelas escolas, universidades e demais instituições educacionais, incluindo a conscientização sobre privacidade, o uso ético de dados, a adoção de medidas técnicas e administrativas para prevenir vazamentos, e a responsabilização por violações. Além disso, destaca a importância de políticas internas claras, treinamento contínuo e a criação de uma cultura organizacional voltada à proteção de dados. Conclui-se que a formação oferecida sobre segurança de dados e LGPD pode aumentar a confiança dos profissionais das instituições de ensino e seus públicos, promovendo um ambiente seguro e ético para a gestão de informações pessoais.

1.1. Inquietação

A incorporação de tecnologias digitais no ambiente de ensino deixou de ser uma tendência para transformar em um elemento essencial, prometendo otimizar a gestão administrativa, personalizar as trajetórias de aprendizagem e democratizar o acesso ao conhecimento. As Plataformas de ensino, sistemas de gestão acadêmica, repositórios de conteúdo e ferramentas de comunicação online compõem um novo ecossistema, ao mesmo tempo em que gera valor, cria uma superfície de vulnerabilidade para as informações que são manipuladas e armazenadas.

As instituições de ensino, por sua natureza, tornaram-se repositórios de um grande volume de informações pessoais. O tratamento dessas informações inicia desde dados cadastrais de alunos, pais e colaboradores (nomes, endereços, documentos de identificação); dados de desempenho acadêmico (notas, frequência, avaliações pedagógicas); dados financeiros (informações de pagamento e faturamento); incluindo dados pessoais sensíveis. Esta última categoria incluí informações sobre a saúde dos estudantes (históricos médicos, laudos, necessidades especiais), dados biométricos para controle de acesso, e, em muitos casos, informações sobre convicções religiosas ou origem étnica. A particularidade do setor reside no fato de que uma parcela significativa desses dados pertence a crianças e adolescentes, um grupo que a legislação brasileira trata com especial proteção, elevando a responsabilidade das instituições.

Com a manipulação e armazenamento de dados valiosos e sensíveis tornou as instituições de ensino alvos atrativos para uma gama diversificada de ameaças cibernéticas.

Por um lado, existem as ameaças externas, perpetradas por agentes maliciosos com motivações variadas. Ataques de *ransomware*, capazes de paralisar toda a operação de uma escola ao criptografar seus dados e exigir um resgate, representam um risco direto à continuidade dos serviços.

Campanhas de *phishing* direcionadas a funcionários e famílias buscam o roubo de credenciais para acesso indevido a sistemas ou para a realização de fraudes financeiras. Por outro lado, existem as ameaças internas involuntárias. Estas não decorrem de má-fé, mas da falta de conhecimento e preparo dos profissionais que manuseiam os dados diariamente. A utilização de senhas fracas, o compartilhamento de informações sensíveis por canais inseguros (como aplicativos de mensagens instantâneas), o uso de redes Wi-Fi públicas sem as devidas precauções e o clique em links maliciosos são exemplos de falhas humanas que podem originar incidentes de segurança de graves proporções.

Nesse contexto de risco, a promulgação da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, funcionou como um divisor de águas regulatório no Brasil. A LGPD formalizou a proteção de dados pessoais como um direito fundamental e estabeleceu um regime de responsabilidade clara para todas as organizações que tratam esses dados, incluindo as do setor educacional. A lei impôs a adoção de medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas. Com isso, a segurança da informação deixou de ser uma mera recomendação de boas práticas para se tornar um dever legal, cujo descumprimento acarreta sanções severas.

Contudo, observa-se uma dificuldade entre a exigência legal e a realidade prática de muitas instituições de ensino. A conformidade com a LGPD sobressai a elaboração de políticas de privacidade e a nomeação de um Encarregado de Proteção de Dados (DPO). Ela demanda uma transformação cultural e operacional, que só se materializa quando cada indivíduo dentro da organização compreende e aplica os princípios de segurança em suas rotinas de trabalho. É precisamente neste ponto que reside a maior fragilidade do setor: a carência de uma capacitação específica e contínua direcionada aos profissionais da educação. Professores, gestores e pessoal administrativo, embora especialistas em suas respectivas áreas, frequentemente não possuem o conhecimento necessário para identificar riscos, adotar comportamentos seguros e compreender suas responsabilidades no ciclo de vida dos dados.

Diante desse cenário, surge uma grande inquietação quanto ao descompasso entre a sofisticação das ameaças digitais e a fragilidade da conscientização humana nas escolas. Torna-se preocupante constatar que, mesmo guardando dados tão valiosos, as instituições permanecem expostas justamente pela fragilidade do 'fator humano', permanece sendo o elo mais fraco, muitas vezes por simples desinformação. Essa discrepância me leva a questionar: como podemos garantir a integridade dos alunos se os próprios educadores, peças-chave nessa engrenagem, desconhecem os riscos de suas ações digitais cotidianas? A segurança não pode ser apenas um protocolo de TI; ela precisa ser uma vivência diária

A ausência de um treinamento direcionado, que traduza os conceitos técnicos da cibersegurança e os requisitos da LGPD para a realidade concreta do ambiente escolar, impede a construção de uma cultura de segurança. As melhores ferramentas tecnológicas de proteção perdem sua eficácia se os usuários não estiverem preparados para utilizá-las corretamente e para reconhecer as ameaças que exploram, justamente, a confiança e a desinformação.

A adoção do formato de ensino a distância (EAD) para este plano de aula foi escolhida pela necessidade de flexibilidade e abrangência, permitindo a participação de profissionais com agendas e localizações geográficas diversas. Essa modalidade rompe barreiras físicas, democratizando o acesso ao conhecimento e facilitando a capacitação nos temas segurança de dados e LGPD, sem comprometer a qualidade do conteúdo.

1.2. Caracterização do Problema

A vulnerabilidade de sistemas educacionais à ataques cibernéticos é uma preocupação importante. Dessa forma os Hackers (CANAZARO, 2022) podem atacar os sistemas das instituições educacionais para roubar dados valiosos, interromper operações ou mesmo vender os dados. Esses ataques não apenas prejudicam o funcionamento regular das instituições, mas também podem resultar na perda de dados importantes, interrupções no ensino e na exposição de informações confidenciais.

Desde a popularização da internet nos anos 90 (GOMES, 2022), houve um aumento significativo na incidência de crimes cibernéticos. A educação, como muitos outros setores, começou a integrar tecnologias digitais em suas práticas, o que trouxe consigo novas vulnerabilidades. Um exemplo notável foi o incidente de 2017, conhecido como o ataque

WannaCry (SYMANTEC, 2017), que afetou várias organizações educacionais ao redor do mundo, incluindo universidades e escolas, paralisando suas redes e exigindo pagamentos em criptomoeda para liberar os dados sequestrados.

Além disso, a implementação da Lei Geral de Proteção de Dados (LGPD), (BRASIL, 2018) no Brasil, que entrou em vigor em setembro de 2020, trouxe um novo foco na importância da segurança cibernética, incluindo o setor educacional. A LGPD estabelece diretrizes claras para a coleta, armazenamento e tratamento de dados pessoais, incluindo os de alunos e funcionários, e impõe multas severas para o não cumprimento dessas normas. Essa regulamentação impulsionou as instituições de ensino a revisar e fortalecer suas práticas de segurança da informação de forma a atender as normas nessa nova legislação.

Portanto, é importante entender essas novas necessidades e disseminá-las internamente nas instituições fim de que possam se prevenir e cumprirem com suas obrigações legais

1.3. Tecnologia na Educação

A atenção à segurança da informação tem aumentado significativamente nos últimos anos, especialmente com a crescente digitalização e interconectividade. Segundo (Silva, 2025), "a implementação de medidas de segurança cibernética no ambiente educacional é essencial para proteger dados sensíveis". Além disso, Almeida (2023) destaca que "a capacitação contínua em segurança da informação é importante para mitigar riscos". A Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018), também tem desempenhado um papel importante, conforme observado por Magalhães e (Pereira, 2024), ao estabelecer diretrizes claras para a proteção de dados pessoais. Portanto, as instituições devem investir em tecnologias avançadas e treinamento para garantir a segurança da informação A expansão dos dispositivos conectada à internet e cada dia mais interligada, vem atraindo pessoas mal-intencionadas. As corporações estão em busca diária de melhorias e os investimentos em seus equipamentos de última geração, como firewall e soluções de criptografia. As investidas de criminosos utilizando da engenharia social, tem impulsionado as empresas a procurarem investir na capacitação contínua de mão de obra humana nos últimos anos.

A crescente conscientização sobre a segurança da informação tem impulsionado um aumento significativo nos esforços para proteger os dados. Com a proliferação de dispositivos interconectados e a dependência cada vez maior da internet, as ameaças cibernéticas se tornaram mais sofisticadas e frequentes, atraindo indivíduos mal-intencionados que buscam explorar vulnerabilidades.

Empresas de todos os setores estão com investimentos constantes em soluções de ponta, como firewalls e tecnologias de criptografia (GARCIA, 2021), para mitigar os riscos associados a ataques cibernéticos. A engenharia social uma técnica que manipula indivíduos para revelar informações confidenciais, tem sido uma tática comum entre os criminosos cibernéticos, destacando a necessidade de capacitação contínua dos profissionais (JUNIOR, 2022).

Além dos investimentos em tecnologia, as organizações estão cada vez mais reconhecendo a importância de educar seus funcionários sobre práticas seguras de navegação e manuseio de dados. Programas de treinamento e workshops são implementados regularmente para garantir que todos estejam cientes das melhores práticas de segurança e das políticas internas de proteção de dados (BOTELHO; DE ANDRADE, 2021).

Essa abordagem integrada, que combina tecnologia avançada com a educação do usuário, é de muita importância para enfrentar os desafios crescentes no campo da segurança cibernética. Ao adotar essas medidas, as instituições não só protegem suas informações, mas também criam um ambiente mais seguro contra as ameaças cibernéticas (MARCELINO, 2021).

A crescente conscientização sobre a segurança da informação tem impulsionado um aumento significativo nos esforços para proteger os dados. Com a proliferação de dispositivos interconectados e a dependência cada vez maior da internet, as ameaças cibernéticas se tornaram mais sofisticadas e frequentes, atraindo indivíduos mal-intencionados que buscam explorar vulnerabilidades (COSTA; DE OLIVEIRA, 2022).

1.4. Relevância

A tecnologia atualmente é marcada por uma rápida e contínua evolução tecnológica (BRUNO et al., 2021), que tem se infiltrado em todos os aspectos de nossas vidas, a educação não se distancia desse cenário. O crescente aumento do volume de dados que inicialmente não eram digitais e posteriormente foram sendo digitalizadas de forma local, agora com o crescimento e utilização da rede compartilhada que vem ocorrendo também no ambiente educacional, trouxe uma série de benefícios, mas também ficou em evidência uma grande preocupação com a segurança das informações.

Nesse cenário, a relevância da segurança de dados no ambiente educacional se destaca, uma vez que abrange uma série de aspectos importantes, desde a proteção da privacidade dos alunos até a integridade do processo de ensino (NASCIMENTO; BAPTISTA, 2023).

A inserção de tecnologias digitais nas escolas trouxe grandes benefícios, como a facilidade de acesso ao conhecimento e a possibilidade de personalização do ensino. No entanto, essa digitalização também trouxe preocupações com a segurança dos dados. Proteger a privacidade dos alunos e garantir a integridade do processo educativo são aspectos importantes que não podem ser negligenciados.

Nesse cenário, é importante que as instituições de ensino implementem medidas de segurança cibernética (MARCELINO, 2021). Isso inclui a adoção de políticas rigorosas de proteção de dados, a atualização contínua dos sistemas e a capacitação permanente de professores, alunos e funcionários em práticas seguras de navegação e manuseio de informações. Além disso, a seleção criteriosa de fornecedores de tecnologia confiáveis é de suma importância para a diminuição de riscos.

A colaboração entre educadores, administradores e especialistas em segurança da informação é de muita relevância para enfrentar esses desafios (COSTA; DE OLIVEIRA, 2022).

Apenas com um esforço conjunto é possível assegurar que os benefícios da tecnologia na educação possam ser aproveitados (DA SILVA; BEHRENS, 2021), sem comprometer a privacidade e a integridade dos dados. Dessa forma, cria-se um ambiente educacional mais seguro, capaz de proteger as informações e promover um ensino de qualidade.

1.5. Objetivos

Este trabalho tem como finalidade integrar a pesquisa acadêmica à prática pedagógica, resultando na criação de um Produto Educacional fundamentado teoricamente.

1.5.1. Objetivo Geral

Desenvolver e aplicar um Produto Educacional, no formato de curso EAD, sobre segurança da informação e LGPD para a área educacional, fundamentado em um levantamento teórico e normativo.

1.5.2. Objetivos Específicos

Realizar a revisão da literatura para construir a fundamentação teórica sobre os conceitos de segurança de redes e as exigências da Lei Geral de Proteção de Dados (LGPD).

Elaborar o material didático e o plano de aula na modalidade EAD, adequando a linguagem técnica para a realidade dos profissionais da educação.

Capacitar os professores e gestores sobre as vulnerabilidades no tratamento de dados e as boas práticas de segurança.

Avaliar a relevância e a aplicabilidade do curso proposto a partir da percepção dos participantes.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. O Paradigma da Segurança da Informação na Sociedade Digital

A segurança da informação é a disciplina que visa proteger os dados contra uma gama de ameaças, a fim de garantir a continuidade dos negócios, minimizar riscos e maximizar o retorno sobre os investimentos. Sua base conceitual é tradicionalmente sustentada pela tríade CID: Confidencialidade, que assegura que a informação seja acessível apenas por entidades autorizadas; Integridade, que garante a exatidão e a completude da informação; e Disponibilidade, que assegura o acesso à informação sempre que necessário por usuários autorizados (DINIZ, 2020). Estes pilares constituem a base para o desenvolvimento de qualquer política ou sistema de gestão da segurança.

Contudo, a proteção de dados transcende a dimensão puramente tecnológica. A literatura contemporânea aponta o fator humano como um dos elementos mais críticos e vulneráveis na cadeia de segurança. As ações dos colaboradores, sejam elas intencionais ou acidentais, como o clique em um link de phishing ou o compartilhamento indevido de credenciais, são frequentemente a porta de entrada para incidentes de segurança. Desta forma, a eficácia de qualquer estratégia de proteção não reside apenas na robustez das ferramentas tecnológicas, mas na conscientização e no treinamento contínuo das pessoas que interagem com os dados (SILVA; GOMES, 2022).

2.2. A Lei Geral de Proteção de Dados (LGPD) como Marco Regulatório no Brasil

No Brasil, a discussão sobre segurança da informação adquiriu um caráter jurídico com a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018. Este marco regulatório não apenas estabelece regras para o tratamento de dados pessoais por organizações públicas e privadas, mas também eleva a proteção da privacidade a um direito fundamental. O propósito da LGPD é assegurar a autodeterminação informativa do indivíduo, fortalecendo o cidadão como o verdadeiro titular de suas informações (LIMA, 2021).

Para operacionalizar esse objetivo, a LGPD se baseia em um conjunto de princípios que devem nortear todo o ciclo de vida do tratamento de dados, como os da finalidade,

adequação e necessidade, que limitam a coleta e o uso de dados ao estritamente essencial para os propósitos informados. Dentre eles, destaca-se o princípio da responsabilização e prestação de contas (accountability), que exige das organizações uma postura proativa. Não basta apenas cumprir a lei; é preciso ser capaz de demonstrar a adoção de medidas eficazes e aptas a comprovar a conformidade com as normas de proteção de dados (MARTINS; FONSECA, 2023). Assim, a LGPD transformou a segurança da informação de uma boa prática em um requisito de conformidade legal.

2.3. A Intersecção entre LGPD e o Ambiente Escolar: Desafios e Responsabilidades

A aplicação da LGPD no ambiente escolar apresenta desafios únicos e de alta complexidade, dada a natureza dos dados tratados. O principal deles reside no tratamento de dados de crianças e adolescentes, que, conforme o Art. 14 da LGPD, exige um regime de proteção especial. Todo tratamento de dados de crianças deve ser realizado com o consentimento específico de, pelo menos, um dos pais ou do responsável legal, e sempre considerando o seu melhor interesse (RODRIGUES; BITTENCOURT, 2022). Esta exigência impõe às escolas um rigoroso dever de transparência e gestão do consentimento.

Adicionalmente, as instituições de ensino frequentemente coletam e armazenam dados pessoais sensíveis, como informações de saúde (fichas médicas, alergias, laudos de necessidades especiais), dados biométricos para controle de acesso ou mesmo informações sobre a convicção religiosa. A LGPD impõe regras ainda mais estritas para o tratamento desses dados, devido ao seu elevado potencial discriminatório. A gestão inadequada dessas informações pode gerar riscos significativos não apenas para a instituição, mas, principalmente, para a segurança e o bem-estar dos alunos (OLIVEIRA, 2021).

Nesse contexto, os profissionais da educação gestores, professores e pessoal administrativo atuam na linha de frente como agentes de tratamento. A ausência de uma capacitação direcionada sobre suas responsabilidades sob a LGPD e sobre as práticas de segurança de dados os torna um ponto de vulnerabilidade crítica. Portanto, a implementação de uma cultura de proteção de dados nas escolas, por meio de treinamentos contínuos e eficazes, não é apenas uma recomendação, mas uma condição de suma importância para a

conformidade legal e para a garantia de um ambiente escolar seguro e ético (ALMEIDA; SANTOS, 2021).

3. PERCURSO METODOLÓGICO

O percurso metodológico adotado foi utilizado para a concepção e aplicação de um curso focado na Segurança de Dados (*Ministério da Educação. (2021),* nas diretrizes para a Implementação da Segurança da Informação nas Escolas e na Lei Geral de Proteção de Dados (LGPD) **(***BRASIL. Lei Geral de Proteção de Dados. 2018.)*

O objetivo do curso foi de ensinar professores e demais profissionais do ambiente educacional como proteger seus dados, como navegar com segurança nas redes e como se proteger de um ataque e como agir em caso de suspeita de um ataque cibernético.

A seleção dos participantes pautou-se pela heterogeneidade, visando abranger profissionais atuantes em diferentes setores da instituição de ensino. Para a composição dessa amostra, realizou-se uma única convocação, direcionada estrategicamente para alcançar desde o corpo docente até as equipes de gestão e apoio administrativo. Essa abordagem permitiu assegurar a representatividade das diversas funções escolares, garantindo uma visão sistêmica sobre os desafios da segurança da informação.

O conteúdo foi organizado de forma modular, seguindo uma progressão lógica que se inicia com os fundamentos e avança para temas práticos e específicos. A estrutura temática abrangeu os seguintes tópicos:

Fundamentos: Conceitos de Segurança de Dados e LGPD, a definição de dados, sua importância e exemplos de dados sensíveis.

Ameaças e Contramedidas: Abordagem sobre as principais ameaças cibernéticas, medidas básicas de proteção, e os pilares tecnológicos de criptografia e autenticação.

Aplicações Práticas: Orientações sobre segurança em dispositivos móveis e em redes sociais.

Foco na LGPD: Explanação sobre os direitos do titular dos dados, as definições de dados pessoais e sensíveis, as regras de utilização de dados, e as formas de proteção e ação em caso de vazamento de dados.

A execução do curso foi viabilizada pelo uso estratégico de duas ferramentas principais do ecossistema Microsoft: o PowerPoint e o Teams.

Todo o conteúdo programático foi desenvolvido em apresentações no Microsoft PowerPoint. A criação dos slides com objetivos específicos, como a apresentação clara e objetiva dos conceitos, o uso de recursos visuais para facilitar a compreensão de temas, a cobertura abrangente dos aspectos legais (LGPD) e práticos da segurança de dados, e a inclusão de pontos para a discussão e dúvidas entre os participantes.

A plataforma Microsoft Teams foi selecionada como o ambiente virtual de aprendizagem para a realização do curso. A escolha desta ferramenta foi motivada pela sua capacidade de reunir participantes de diversas localidades. As aulas foram conduzidas ao vivo por meio do recurso de videoconferência, no qual os slides do PowerPoint eram apresentados e se promoviam debates sobre os temas.

Além da exposição, a plataforma foi utilizada para interação em tempo real, com o uso do chat para esclarecimento de dúvidas e disponibilização de links para os conteúdos em cada slide. Ao final do curso, foi aplicado um questionário para avaliar a percepção dos participantes sobre o conteúdo ministrado.

Figura 1 - Percurso metodológico



Quadro 1 – Etapas da aplicação do curso

Etapa	Descrição	Ferramentas e Estratégias	Referências Principais
1. Introdução e Contextualização	Apresentação dos objetivos e a importância da segurança de dados e da LGPD no ambiente educacional.	PowerPoint: Visão geral, de forma simplificada para uma melhor compreensão. Teams: Apresentação dos slides e bate-papo.	LGPD, Almeida (2023)
2. Fundamentos da Segurança de Dados e LGPD	Demonstração dos princípios da segurança da informação), conceitos básicos da LGPD.	Teams: Discussão sobre a aplicação dos conteúdos aplicados.	Almeida (2023)
3. Segurança Cibernética: Ameaças e Riscos	Análise dos principais tipos de ameaças cibernéticas (ransomware, phishing, etc.), com foco no caso WannaCry e riscos no setor educacional.	PowerPoint: Maneira simplificada tipos de malware. Teams: discussão sobre identificação de riscos.	Symantec (2017),
4. Medidas de Segurança de Dados	Discussão sobre a implementação de medidas técnicas (ex: criptografia, firewalls) e organizacionais (treinamentos contínuos) para garantir a segurança.	PowerPoint: Boas práticas. Teams: discussão de como implementar medidas de segurança e a importância contínua de treinamento.	Symantec (2017),
5. Gestão de Incidentes	Apresentação de como criar um plano de resposta a incidentes de segurança de dados.	PowerPoint: identificação de incidentes. Teams: discussão quando identificar incidente, resposta imediata e documentar os incidentes e as soluções aplicadas para correção.	

Fonte: Autoria própria (2025)

O curso foi desenvolvido seguindo uma sequência de cinco etapas principais, conforme descrito a seguir:

1. Introdução e Contextualização: A primeira etapa foi apresentar os objetivos do curso e contextualizar a importância da segurança de dados e da LGPD no ambiente educacional. A estratégia utilizada foi PowerPoint para uma visão geral simplificada e o Teams para a apresentação e um bate-papo inicial.
2. Fundamentos da Segurança de Dados e LGPD: Na segunda etapa, foram mostrados os princípios da segurança da informação e os conceitos básicos da LGPD. A interação se deu por meio de discussões na plataforma Teams sobre a aplicação prática dos conteúdos apresentados.
3. Segurança Cibernética: Ameaças e Riscos: A terceira etapa consistiu na análise dos principais tipos de ameaças cibernéticas (como ransomware e phishing), utilizando o caso WannaCry como exemplo prático. Empregaram-se slides para apresentar os tipos de malware de forma simplificada e o Teams para explicar como identificar os riscos no setor educacional.
4. Medidas de Segurança de Dados: A quarta etapa foi mostrado a implementação de medidas de segurança técnicas e organizacionais. Com o suporte do PowerPoint para apresentar boas práticas, no Teams foi apresentado como implementar essas medidas e na importância do treinamento contínuo para garantir a segurança.
5. Gestão de Incidentes: A etapa final foi apresentada como criar um plano de resposta a incidentes de segurança de dados e mostrado como agir ao identificar um incidente, a importância da resposta imediata e da documentação dos eventos e das soluções aplicadas para a correção.

A metodologia utilizada teve a utilização das ferramentas Microsoft PowerPoint para a explicação do conteúdo e Microsoft Teams como plataforma para a realização do curso, seguindo a seguinte sequência.

3.1. Concepção e Estruturação do Curso:

O curso foi estruturado em módulos, seguindo os conceitos de Segurança de Dados e da LGPD, avança com a demonstração de que são dados e porque são importantes com alguns exemplos de dados sensíveis, com abordagem de algumas ameaças, medidas básicas de

proteção, criptografia e autenticação, segurança em dispositivos móveis e redes sociais, informações básicas LGPD, como: Direito do titular dos dados, dados pessoais e sensíveis, utilização, como proteger e o que fazer em caso de vazamento dos seus dados.

3.2. Desenvolvimento do Conteúdo em PowerPoint:

Para cada módulo do curso, foram desenvolvidas apresentações em Microsoft PowerPoint com os seguintes objetivos:

Apresentação clara e objetiva: Utilização de slides com linguagem de fácil compreensão, tópicos bem definidos e quantidade equilibrada de texto para facilitar a compreensão dos conceitos de segurança de dados e a LGPD, por vezes complexos, fossem de fácil compreensão para o curso aplicado. Para alcançar essa clareza, foi utilizada a estratégia se desdobrou em três assuntos principais:

Linguagem de Fácil Compreensão: Utilizando uma linguagem direta, que traduzisse termos técnicos e jurídicos de uma forma de fácil assimilação. Por exemplo, ao invés de se ater a definições puramente legais, conceitos como "Dado Pessoal" e "Dado Sensível" foram explicados com base em exemplos práticos e diretamente relacionados ao cotidiano dos participantes, como nome, CPF, endereço, informações médicas e dados biométricos. Essa abordagem criou uma ponte entre a teoria e a realidade prática do ambiente educacional.

Tópicos Bem Definidos: A estrutura do conteúdo foi organizada em tópicos e subtópicos bem definidos que promoveu uma aprendizagem sequencial e lógica. Temas amplos, como os "Direitos do Titular dos Dados", foram segmentados em itens específicos e de fácil percepção, como "Direito de acesso aos dados", "Direito de retificação e exclusão" e "Revogação do consentimento". Essa segmentação permitiu que os participantes focassem em um conceito de cada vez, facilitando a construção do conhecimento.

Quantidade Equilibrada de Texto: Evitando a sobrecarga cognitiva e manter o engajamento, os slides foram projetados com uma quantidade equilibrada de texto. Priorizou-se o uso de sentenças curtas, listas pontuadas e o apoio de recursos visuais, em detrimento de parágrafos longo. Essa escolha de design destacou as informações mais importantes e serviu como um guia para a exposição oral e para as discussões, em vez de funcionar como um repositório exaustivo de informações.

A combinação dessas três práticas teve como finalidade última facilitar a compreensão dos conceitos essenciais de segurança de dados e da LGPD, garantindo que a mensagem do curso fosse transmitida de forma eficaz e retida pelos participantes.

Recursos Visuais: Inclusão de imagens para facilitar os conceitos complexos (como princípios de segurança - Confidencialidade, Integridade, Disponibilidade) e tornar o conteúdo mais atrativo e didático, essa estratégia se materializou na prática através de duas frentes principais.

Facilitação de conceitos complexos, conforme planejado, a abordagem visual foi pensada para auxiliar na explanação de temas abstratos, como os "princípios de segurança - Confidencialidade, Integridade, Disponibilidade". Ao associar um conceito teórico a uma imagem ou a um elemento gráfico, criou uma forma visual que facilitou a compreensão e a memorização de um público não especializado. O intuito foi quebrar a dificuldade da compreensão de temas técnicos e jurídicos, tornando-os mais palatáveis.

Conteúdo atrativo e didático, tornou a experiência de aprendizagem mais dinâmica e engajadora, foram inseridas imagens temáticas para introduzir os principais módulos do curso. Por exemplo, a seção sobre a Lei Geral de Proteção de Dados (LGPD) foi ilustrada com imagens que remetem ao universo jurídico, como a balança da justiça e um martelo de juiz. Adicionalmente, utilizou-se um gráfico estilizado de um ambiente computacional como plano de fundo consistente em diversas seções, como em "Introdução à Segurança de Dados" e "Incidentes de Segurança e Resposta", reforçando visualmente o contexto digital do treinamento.

Ao complementar o conteúdo textual com esses recursos visuais, a metodologia estimulou um maior engajamento, contribuindo para a eficácia do processo de ensino/aprendizagem

Abordagem Abrangente: Cobertura tanto dos aspectos legais (LGPD) quanto dos princípios e práticas de segurança de dados.

Pontos de Reflexão e Discussão: Conversas para estimular a reflexão e a participação dos alunos, essa integração se materializou da seguinte forma:

O curso dedicou módulos para desvendar a Lei Geral de Proteção de Dados. Foram abordados o propósito central da lei, a definição e a importância da distinção entre dados pessoais e dados sensíveis, os direitos fundamentais dos titulares, as regras sobre como os dados podem ser utilizados, e as ações a serem tomadas em caso de vazamento de dados.

Paralelamente, o conteúdo cobriu os fundamentos práticos da segurança. Isso incluiu a explanação sobre os pilares da segurança (Confidencialidade, Integridade, Disponibilidade), o estudo das principais ameaças cibernéticas como phishing e ransomware, e o ensino de medidas de proteção, como a criação de senhas fortes, a ativação da autenticação de múltiplos fatores (MFA) e os conceitos de criptografia e autenticação.

3.3. Aplicação do Curso via Microsoft Teams:

A plataforma Microsoft Teams foi selecionada como ambiente virtual de aprendizagem, devido a facilidade em reunião pessoas de diversas localidades:

Realizações de aulas ao vivo, utilizando o recurso de videoconferência do Teams., apresentando os slides em PowerPoint, promovendo conversas sobre segurança de dados e a LGPD, esclarecendo algumas dúvidas.

Além disso foi utilizado chat para discussões e esclarecimento de dúvidas em tempo real. Aplicado um questionário para avaliação do conteúdo aplicado sobre os principais temas abordados nas aulas.

4. ETAPAS DO PERCURSO METODOLÓGICO COM A DESCRIÇÃO DOS RESULTADOS

O treinamento foi desenvolvido seguindo as seguintes etapas sequenciais descritas no quadro 1:

Quadro 1 - Etapas do percurso metodológico

Etapa	Descrição	Ferramentas e Estratégias	Referências Principais
1. Introdução e Contextualização	Apresentação dos objetivos e a importância da segurança de dados e da LGPD no ambiente educacional.	PowerPoint: Visão geral, de forma simplificada para uma melhor compreensão. Teams:	LGPD, Almeida (2023)

		Apresentação dos slides e bate-papo.	
2. Fundamentos da Segurança de Dados e LGPD	Demonstração dos princípios da segurança da informação), conceitos básicos da LGPD.	Teams: Discussão sobre a aplicação dos conteúdos aplicados.	Almeida (2023)
3. Segurança Cibernética: Ameaças e Riscos	Análise dos principais tipos de ameaças cibernéticas (ransomware, phishing, etc.), com foco no caso WannaCry e riscos no setor educacional.	PowerPoint: Maneira simplificada tipos de malware. Teams: discussão sobre identificação de riscos.	Symantec (2017),
4. Medidas de Segurança de Dados	Discussão sobre a implementação de medidas técnicas (ex: criptografia, firewalls) e organizacionais (treinamentos contínuos) para garantir a segurança.	PowerPoint: Boas práticas. Teams: discussão de como implementar medidas de segurança e a importância contínua de treinamento.	Symantec (2017),
5. Gestão de Incidentes	Apresentação de como criar um plano de resposta a incidentes de segurança de dados.	PowerPoint: identificação de incidentes. Teams: discussão quando identificar incidente, resposta imediata e documentar os incidentes e as soluções aplicadas para correção.	

Fonte: Autoria própria (2025)

A segurança de dados, no atual cenário com a expansão conectividade, expande-se para o domínio da segurança cibernética, que se dedica a proteger sistemas, redes e programas de ataques digitais. A crescente sofisticação e o volume de ameaças tornam a implementação de uma estratégia de defesa um fator importante para a integridade e a continuidade operacional de qualquer organização. A proliferação de vetores de ataque, como *malwares* e o *phishing* que explora a engenharia social para enganar usuários e obter informações

confidenciais, exige uma vigilância constante e uma abordagem de segurança em múltiplas camadas (BEPPLER, Tamy, 2021).

Diante desse panorama, a proteção de dados inicia-se com a adoção de medidas de proteção básicas, que constituem a primeira linha de defesa e envolvem tanto o comportamento do usuário quanto configurações essenciais. Práticas como a criação de senhas fortes, a ativação da autenticação de múltiplos fatores (MFA) e a cautela na abertura de e-mails e links suspeitos são fundamentais para mitigar os riscos mais comuns (MENEZES, Marcelo Nascimento Silva de Souza, 2023).

Contudo, a base tecnológica para uma proteção de dados repousa sobre dois pilares: a criptografia e a autenticação. A criptografia atua como um mecanismo de confidencialidade, codificando os dados de modo que se tornem ilegíveis para indivíduos não autorizados, tanto em trânsito quanto em repouso. Por sua vez, a autenticação é o processo que verifica e valida a identidade de um usuário, garantindo que apenas pessoas previamente autorizadas acessem sistemas e informações. A combinação desses dois mecanismos é importante para construir um ambiente digital seguro e confiável (DA SILVA, Marta Vieira; EVANGELISTA, 2022). Figura 2 demonstra o primeiro slide do treinamento para introdução à segurança de dados, realizado em ambiente virtual utilizando a ferramenta Microsoft Teams.

Figura 2 – Primeiro slide do treinamento



Fonte: Autoria própria (2025)

1. **Compreender a criticidade da segurança de dados:** Proteger a privacidade dos seus dados, dos alunos e funcionários, a reputação da instituição e garantir a continuidade das atividades. Que dados são ativos valiosos que exigem cuidado constante.

2. **Entender os conceitos fundamentais:**

A forma clara e simples a segurança da informação, confidencialidade, integridade e disponibilidade, e como eles se aplicam na prática. Além disso, diferenciamos dados pessoais, dados sensíveis e o porquê dessa distinção ser muito importante para todos.

3. **Reconhecer e diminuir riscos e ameaças:**

A identificar as ameaças cibernéticas mais comuns que rondam o ambiente educacional, como phishing, ransomware e outras vulnerabilidades. O objetivo foi como ações simples e conscientes, podem reduzir significativamente esses riscos.

4. **Fomentar uma cultura de segurança proativa:**

Mais do que apenas transmitir informações, uma mudança de mentalidade: a de que a segurança de dados é uma responsabilidade de todos, não apenas da equipe de tecnologia. Uma postura de alerta e proativa na proteção das informações.

Conscientizar sobre a grande importância da segurança de dados.

Capacitar com conhecimentos essenciais para proteger informações.

Promover uma cultura de segurança e responsabilidade no ambiente escolar.

A figura 3 apresenta a importância dos dados, coletas e armazenamento.

Figura 3 - Dados importantes



Fonte: Autoria própria (2025)

1. **Dados são mais do que números ou bytes:**

Que 'dados' não são apenas informações técnicas ou abstratas. São fragmentos de realidade: nomes, endereços, históricos escolares, informações de saúde, preferências, fotos, avaliações de desempenho de alunos e colaboradores. A diversidade como em muitos casos existe uma grande quantidade de dados que manuseamos nosso dia a dia educacional.

2. **No ambiente escolar, lidamos com uma grande quantidade de dados (grande parte deles sensíveis):**

Que em uma instituição de ensino, estamos constantemente coletando, processando e armazenando uma grande quantidade de informações. Desde informações cadastrais básicas e inclusive dados sensíveis, como os relacionados a crianças e adolescentes, ou informações de saúde.

3. **A importância dos dados gera responsabilidade:**

Ao compreenderem o valor e, em muitos casos, a sensibilidade desses dados, a consequência natural é a conscientização sobre a responsabilidade em manuseá-los e protegê-los corretamente.

4. **Dados bem cuidados fortalecem a confiança:**

A gestão adequada e segura dos dados é importante para construir e manter a confiança da instituição escolar, alunos, pais, responsáveis e colaboradores.

A figura 4 apresenta os tipos de dados

Figura 4 - Tipos de dados



Fonte: Autoria própria (2025)

1. **Que os Dados Não São Todos Iguais em criticidade:**

Embora todos os dados mereçam cuidado, eles não são homogêneos. Existem categorias distintas, e cada uma carrega um potencial de impacto diferente caso seja mal utilizada ou exposta. O primeiro passo para proteger é saber o que se tem em mãos.

2. **A Definição de Dado Pessoal:**

O conceito de dado pessoal, qualquer informação que, isoladamente ou em conjunto com outras, possa identificar uma pessoa natural (um aluno, um pai, um professor, um funcionário). Exemplos práticos como nome, RG, CPF, endereço, e-mail, foto, para tornar o conceito de fácil compreensão.

3. **A Importância e o Cuidado Redobrado com Dados Pessoais Sensíveis:**

Um dos focos principais foi nos dados pessoais sensíveis. Expliquei a gravidade e a necessidade de proteção adicional para informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos. Expliquei que a LGPD impõe um tratamento muito mais rigoroso para esses dados devido ao alto risco de discriminação e dano que seu vazamento pode causar.

4. **O cuidado no Tratamento de Dados de Crianças e Adolescentes:**

Considerando nosso contexto educacional, atenção especial aos dados de crianças e adolescentes. Que a LGPD estabelece regras específicas para esses dados, sempre priorizando o seu melhor interesse e, na maioria dos casos, exigindo o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

5. **A Existência de Outras Categorias e Seus Impactos:**

Os dados anonimizados (aqueles que não permitem mais a identificação do titular), os dados pseudonimizados (que dificultam a associação direta), e os dados públicos (aqueles tornados manifestamente públicos pelo titular), para tivessem uma visão mais ampla e entendessem que, mesmo para esses, existem considerações de segurança e privacidade.

Além disso, foi pontuado a existência de dados corporativos ou institucionais (financeiros, administrativos etc.), que, embora não sejam pessoais, são importantes para a instituição e exigem proteção.

6. **Como a Classificação dos Dados Direciona as Ações de Proteção e Conformidade:**

Cada categoria de dado às obrigações específicas impostas pela LGPD e às medidas de segurança adequadas. Entender o tipo de dado é o que nos permite definir, por exemplo, qual base legal utilizar para o tratamento, quem pode ter acesso, por quanto tempo e de que forma pode ser armazenado e que tipo de controle de segurança é mais eficiente.

A figura 5 apresenta conteúdo sobre a importância segurança de dados para os usuários

Figura 5 - Slide sobre a importância da segurança de dados



Fonte: Autoria própria (2025)

1. **As Consequências em Falhas de Segurança:**

Os impactos quando dados pessoais, especialmente as sensíveis ou de crianças e adolescentes, são comprometidos. Falamos sobre roubo de identidade, fraudes financeiras, exposição que pode levar a cyberbullying, discriminação, danos emocionais e constrangimentos.

O peso da responsabilidade que temos ao lidar com informações que representam pessoas, com suas vulnerabilidades e direitos.

2. **Os Riscos para a Instituição Educacional:**

As falhas de segurança de dados podem significar no âmbito escolar.

Perda de reputação e confiança: Pais, alunos e colaboradores podem deixar de confiar na capacidade de proteger suas informações.

Sanções legais e multas (LGPD): Que podem comprometer financeiramente a instituição.

Interrupção das operações: Ataques podem paralisar sistemas essenciais para o ensino e a administração.

3. **Segurança de Dados como base da Confiança:**

A maneira como cuidamos dos dados é um termômetro da confiança que para instituição. Uma segurança aplicada fortalece essa confiança; a negligência a destrói rapidamente.

4. **A Proteção da Privacidade como um Dever Ético e um Direito Fundamental:**

A discussão para além das penalidades, mostrando que zelar pela privacidade e pela segurança dos dados é um compromisso ético e um respeito aos direitos humanos básicos. A figura 6 descreve alguns tipos de ameaças à segurança de dados

Figura 6: Principais ameaças à segurança de dados



Fonte: Autoria própria (2025)

1. **A Diversidade das Ameaças Existentes:**

As ameaças não se limitam a um único tipo. Apresentei um panorama que inclui Malware (como o Ransomware – lembrando o impacto do WannaCry, vírus, spyware), Phishing e suas variações (e-mails fraudulentos, mensagens falsas), Engenharia Social (manipulação psicológica), Ataques de Negação de Serviço (DDoS), e outros.

2. **O *Modus Operandi* de Cada Ameaça:**

Para cada ameaça, foi explicado de forma simples como ela funciona na prática. Por exemplo, como o phishing tenta enganar o usuário para que ele clique em um link malicioso ou forneça informações confidenciais, ou como o ransomware 'sequestra' os dados exigindo um resgate.

3. **O Humano muitas vezes é o ponto mais fraco (e Não Apenas a Tecnologia):**

Embora existam ameaças técnicas, muitas delas, como a Engenharia Social e o Phishing, exploram a psicologia humana, a desatenção ou a falta de conhecimento. Além disso, foi ressaltado as ameaças internas, que podem ser intencionais, mas frequentemente são resultado de negligência, como senhas fracas, compartilhamento indevido de credenciais ou clique em links perigosos.

4. **A Importância de Reconhecer Sinais de Alerta:**

Capacitá-los a identificar os sinais de alerta de cada ameaça. Como desconfiar de um e-mail (remetente desconhecido, erros de escrita, senso de urgência), como identificar um site falso, ou os comportamentos estranhos em um computador que podem indicar uma infecção por malware.

5. **A Relevância das Ameaças no Contexto Educacional:**

Como essas ameaças poderiam se manifestar especificamente no ambiente escolar: um phishing direcionado a obter credenciais de acesso ao portal do aluno/professor, um ransomware que paralise os sistemas da secretaria, ou o vazamento de dados de avaliações ou médicas.

6. **O Conhecimento é a Primeira Linha de Defesa:**

Ao entenderem as ameaças, tornam mais preparados para evitá-las. Mostrei que a informação e a atenção são ferramentas preciosas contra muitos desses ataques, preparando o terreno para as medidas preventivas.

A figura 7 apresenta algumas medidas e ferramentas para proteção de dados

Figura 7: Proteções básicas



Fonte: Autoria própria (2025)

1. **Construir e gerenciar senhas fortes:**

Senhas fortes, longas, complexas e únicas para cada conta são a primeira linha de defesa. Ensinado como criá-las, a importância de não anotá-las em locais óbvios, de não reutilizá-las e sugeri o uso de gerenciadores de senhas para facilitar esse processo.

2. **Adotar a autenticação de dois fatores (MFA/2FA) sempre que possível:**

A autenticação de dois ou múltiplos fatores e como ela adiciona uma camada extra de segurança, mesmo que sua senha seja comprometida. A importância da ativação dessa funcionalidade em todos os serviços que a oferecem (e-mail, redes sociais, sistemas da instituição onde trabalham).

3. **Ter cuidado máximo com e-mails e mensagens (combate ao phishing):**

Uma postura cética e atenta ao lidar com e-mails e mensagens. Ensinado a identificar sinais de phishing: verificar o remetente, desconfiar de links e anexos inesperados, não ceder a pressões de urgência e nunca fornecer informações confidenciais por esses canais sem confirmação.

4. **Manter softwares e sistemas sempre atualizados:**

Atualizar o sistema operacional, navegadores, antivírus e todos os aplicativos. Essas atualizações frequentemente corrigem vulnerabilidades conhecidas que são exploradas por criminosos.

5. **Praticar a navegação segura e o uso consciente de redes:**

A importância de verificar se os sites utilizam https (o cadeado de segurança), evitar downloads de fontes não confiáveis e ter cuidado redobrado ao usar redes WI-FI públicas para acessar informações sensíveis.

6. **A importância dos backups de dados:**

A importância de manter cópias de segurança (backups) regulares de seus dados, como uma forma de se proteger contra perdas por falhas de hardware, exclusão acidental ou ataques como o ransomware.

7. **Proteger dispositivos físicos:**

Necessidade de proteger nossos computadores, celulares e tablets com senhas, pins ou biometria, e de ter cuidado com quem tem acesso físico a eles, além de reportar imediatamente perdas ou roubos.

8. **Utilizar software de segurança (antivírus/antimalware):**

A importância de ter um bom programa antivírus e antimalware instalado, ativo e atualizado em seus dispositivos, como uma camada adicional de detecção e proteção.

9. **O descarte seguro de informações:**

Necessidade de descartar informações de forma segura, seja triturando documentos físicos que contenham dados pessoais ou apagando de forma definitiva os dados de dispositivos eletrônicos antes de se desfazer deles.

A figura 8 descreve as funções da criptografia e autentificação

Figura 8 - Criptografia e Autenticação



Fonte: Autoria própria (2025)

1. **O Que é e Como Proteger (Confidencialidade):**

A criptografia é a arte de 'embaralhar' os dados de forma que apenas quem possui a 'chave' correta consiga 'desembaralhá-los' e ler a informação original. O principal objetivo aqui é garantir a confidencialidade: mesmo que alguém intercepte os dados, não conseguirá entendê-los.

2. **Sua Aplicação em Dados (tráfego e armazenamento):**

A criptografia é importante para proteger dados quando eles estão sendo transmitidos por exemplo, ao navegar em sites com HTTPS (Hypertext Transfer Protocol Secure), enviar e-mails ou usar aplicativos de mensagens com criptografia de ponta a ponta quando estão armazenados (em discos rígidos de computadores, pen drives, ou em bancos de dados).

3. **Exemplos Práticos:**

Como o HTTPS (Hypertext Transfer Protocol Secure) que vemos em sites de bancos e lojas online, e a criptografia em aplicativos de mensagens, para tornar o conceito mais compreensível.

4. O Que é e Por Que é Essencial a Verificação de Identidade):

Autenticação é o processo de confirmar se você é realmente quem você diz ser antes de permitir o acesso a um sistema, dispositivo ou informação. É o 'portão de entrada' que controla o acesso.

5. Os Diferentes Fatores de Autenticação:

Senhas, frases secretas e PINs.

Um token físico, um cartão inteligente, um celular para receber códigos (como na Autenticação de Múltiplos Fatores - MFA).

Biometria, como impressão digital, reconhecimento facial ou de voz.

6. A Força da Autenticação de Múltiplos Fatores (MFA):

Como a MFA, que combina dois ou mais desses fatores, aumenta a segurança, tornando muito mais difícil para um invasor obter acesso, mesmo que uma senha seja comprometida. Ligamos isso às medidas básicas que já havíamos discutido.

7. Criptografia e Autenticação como Aliadas:

Essas duas tecnologias trabalham em conjunto para uma segurança forte. A autenticação garante que a pessoa certa está acessando, e a criptografia protege os dados contra acesso não autorizado ou interceptação, mesmo que outras barreiras falhem.
A figura 9 apresenta os riscos, configurações e as permissões para os dispositivos móveis

Figura 9 - formas de segurança em dispositivos móveis



Fonte: Autoria própria (2025)

1. **Bloqueio de tela:**

A primeira e mais importante barreira de defesa é um bloqueio de tela forte: seja senha difícil de adivinhar ou biometria (digital/facial). Sem isso, seu dispositivo perdido ou roubado estará vulnerável.

2. **Aplicativos: fontes confiáveis e permissões restritas:**

A importância em baixar aplicativos somente de lojas oficiais (google play, apple app store). Além disso, enfatizei a importância de analisar criticamente as permissões que cada app solicita, ele realmente precisa de acesso à sua câmera, microfone ou contatos o tempo todo? Revise e restrinja.

3. **Atualizações constantes (sistema e apps):**

Ignorar atualizações é abrir portas para invasores. Manter o sistema operacional do dispositivo e todos os aplicativos sempre na última versão é importante para corrigir falhas de segurança que são ativamente exploradas.

4. **Conexões WI-FI e Bluetooth seguras:**

Os riscos de redes WI-FI públicas e desconhecidas, recomendando evitá-las para atividades sensíveis ou utilizar uma VPN. Recomendei desligar WI-FI e bluetooth quando não estiverem em uso para minimizar a exposição.

5. **Prepare-se para perda ou roubo (localização e bloqueio remoto):**

A importância de ativar e configurar os recursos de localização remota (como 'encontre meu dispositivo' ou 'buscar iphone'). Saber como localizar, bloquear ou apagar os dados do seu aparelho à distância.

6. **Vigilância contra golpes nos dispositivos móveis(phishing/smishing):**

Os celulares são alvos constantes de phishing via SMS(smishing) ou aplicativos de mensagens e sempre desconfiar de links e solicitações inesperadas, mesmo que pareçam de fontes conhecidas.

7. **Backups sempre que possível:**

Fazer backups regulares dos dados do celular (fotos, contatos, arquivos importantes) é importante para evitar perdas em caso de falha, roubo ou perda do aparelho.

8. **Cuidado com o acesso físico e o descarte:**

A importância de não deixar o aparelho desatendido e, caso vá se desfazer dele, garantir que todos os dados sejam apagados de forma segura e completa.

A figura 10 apresenta como proteger a privacidade e os riscos de segurança nas redes sociais e internet

Figura 10 - Redes Sociais e Internet



Fonte: Autoria própria (2025)

1. **Dominar suas configurações de privacidade em redes sociais:**

As configurações de privacidade são importantes para sua proteção. O ponto observado foi: avaliem quem pode ver suas postagens, suas fotos, sua lista de amigos e suas informações pessoais. Revise e ajuste essas configurações constantemente.

2. **Pensar (muito) antes de compartilhar (o perigo do oversharing):**

Sempre repensar a real necessidade de cada compartilhamento. Informações sobre sua localização exata, rotina detalhada, planos de viagem ou dados muito pessoais podem se tornar armas para maus intencionados.

3. **Construir e proteger sua reputação online:**

O que postamos, curtimos ou comentamos contribui para nossa reputação online, que pode ter impactos reais na vida pessoal e profissional.

4. **Identificar e evitar armadilhas digitais (golpes, perfis falsos):**

Foram capacitados a desenvolver um olhar crítico para identificar perfis falsos, propostas fraudulentas e links suspeitos. A meta foi fortalecer o 'filtro de desconfiança' saudável.

5. **Gerenciar seu rastro digital:**

Deixamos rastros por toda a internet. Entender que essas informações podem ser coletadas e persistir por muito tempo é importante para um comportamento online mais responsável.

6. **Navegar e realizar transações na internet com mais segurança:**

Práticas como verificar a segurança de sites (https), preferir downloads de fontes oficiais, e ter cautela ao fornecer dados em formulários ou durante compras online.

7. **Segurança em senhas e acesso (específico para contas online):**

A importância de senhas únicas e fortes para cada rede social e serviço online, e de ativar a autenticação de dois fatores sempre que disponível.

A figura 11 apresenta algumas formas reconhecer incidentes de segurança, resposta para esses incidentes e a comunicação e transparência na com os envolvidos e as autoridades competentes.

Figura 11 - Segurança e resposta aos incidentes



Fonte: Autoria própria (2025)

1. **Reconhecer um incidente de segurança:**

Compreensão de que um incidente de segurança vai além de um ataque hacker cinematográfico. Pode ser a perda de um pen drive com dados institucionais, um acesso suspeito à sua conta, um e-mail de phishing que infelizmente foi aberto, ou um comportamento estranho no seu computador.

Reportar imediatamente:

Ao suspeitar de um incidente, a ação importante é reportar imediatamente. (seja o departamento de TI ou seu superior imediato, conforme definido pela instituição). Foi abordado que o tempo é um fator de muita importância; a agilidade no reporte pode definir o tamanho do prejuízo causado.

2. **Evitar ações impulsivas:**

A importância de não tentar 'resolver' o problema por conta própria sem orientação. Ações como desligar o computador de forma inadequada, apagar e-mails ou arquivos suspeitos podem destruir evidências de grande valor ou, pior, espalhar uma ameaça. A instrução foi: contenha a vontade de agir e aguarde orientação especializada.

3. **Manter a calma e fornecer informações claras:**

A necessidade de manter a calma para poder descrever o ocorrido com o máximo de detalhes úteis para a equipe de resposta: o que aconteceu, quando, como percebeu, quais sistemas ou dados parecem afetados.

4. **Entender o fluxo básico de uma resposta a incidentes:**

Uma visão geral sobre as etapas que geralmente compõem uma resposta a incidentes, como contenção, erradicação e recuperação para que entendessem que existe um processo e que a sua colaboração inicial é importante para que ele funcione bem.

5. **A importância de seguir as instruções pós-reporte:**

Após o reporte, é necessário seguir as instruções da equipe de TI. Eles conduzirão a investigação e as ações de correção.

A figura 12 apresenta o introdutório à LGPD

Figura 12- LGPD



Fonte: Autoria própria (2025)

1. **Desvendando a LGPD: o que é e qual seu propósito central:**

Compreendendo o que exatamente é a lei geral de proteção de dados pessoais (lei nº 13.709/2018), seu objetivo de resguardar nossos direitos fundamentais de liberdade e privacidade, e por que ela se tornou um marco no brasil.

2. **Seus direitos fundamentais na LGPD:**

Em seus direitos sobre a LGPD, quais são esses direitos de acesso, correção, eliminação de dados, e o direito à informação.

3. **Dados pessoais e. Dados sensíveis: entendendo a distinção:**

Distinguir entre dados pessoais e dados pessoais sensíveis, analisando por que a LGPD confere uma proteção ainda mais rigorosa a esta última categoria, dado seu potencial impacto.

4. **Como seus dados podem ser utilizados:**

Como seus dados podem ser usados legalmente, sobre os princípios da LGPD (como finalidade, necessidade, transparência.

5. **A LGPD na prática:**

De que forma a LGPD impacta no seu dia a dia, identificando as mudanças que a lei trouxe para suas interações com serviços, empresas e plataformas digitais.

6. **Protegendo seus dados com a LGPD:**

Como proteger seus dados utilizando a LGPD, focando em como seus direitos e o conhecimento da lei se convertem em ações eficazes de autoproteção.

7. **Vazamento de dados e a resposta:**

Um tema crítico: o que fazer em caso de vazamento de dados, utilizando a LGPD como um guia para entender seus direitos e as obrigações das organizações nessas situações. A figura 13 mostra o que é a LGPD e seu objetivo principal

Figura 13 - O que é a LGPD



Fonte: Autoria própria (2025)

1. **A LGPD**

(Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018) é a legislação brasileira que estabelece um conjunto de regras claras para a coleta, armazenamento, uso e compartilhamento de dados pessoais de indivíduos, tanto por empresas quanto por órgãos públicos.

2. **Seu objetivo principal**

Proteger os direitos fundamentais de liberdade e de privacidade das pessoas, assegurando maior controle sobre suas informações e impondo responsabilidades às organizações que tratam esses dados, visando um uso mais ético, seguro e transparente.

A figura 14 detalha os direitos do titular com o tratamento dos seus dados

Figura 14 - Os direitos do titular dos dados



Fonte: Autoria própria (2025)

1. **Direito à confirmação e acesso:**

Você tem o direito fundamental de confirmar se seus dados são tratados por uma organização e, em caso afirmativo, o direito de acessá-los integralmente.

2. **Direito à correção:**

Seu direito de solicitar a correção de dados que estejam incompletos, inexatos ou desatualizados.

3. **Controle sobre a necessidade e conformidade dos dados:**

Você pode requisitar a anonimização, o bloqueio ou a eliminação de dados que considere desnecessários, excessivos ou que estejam sendo tratados em desacordo com a LGPD.

4. **Direito à eliminação de dados:**

O direito à eliminação dos seus dados pessoais quando o tratamento foi baseado no seu consentimento, ressalvadas as hipóteses legais que permitem a manutenção desses dados pela organização.

5. **Portabilidade: liberdade para levar seus dados:**

O direito à portabilidade dos seus dados para outro fornecedor de serviço ou produto, conforme sua solicitação, o que incentiva a livre concorrência e sua autonomia.

6. **Transparência no compartilhamento e no consentimento:**

Seu direito de ser informado sobre as entidades, públicas ou privadas, com as quais o controlador compartilhou seus dados.

7. **Revogação do consentimento:**

O seu poder de revogar o consentimento a qualquer momento, de maneira simples e gratuita.

A figura 15 apresenta o que são dados pessoais e sensíveis, proteção desses dados e as implicações.

Figura 15 - Dados Pessoais



Fonte: Autoria própria (2025)

1. **Dado pessoal:**

Toda informação que permite identificar uma pessoa natural ou que a torna identificável. Exemplificado com nome, CPF, endereço, e-mail, placa de carro, IP do computador etc.

2. **Dado pessoal sensível:**

Dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, e dados genéticos ou biométricos quando vinculados a uma pessoa natural.

3. **A razão da proteção adicional aos dados sensíveis:**

A LGPD trata os dados sensíveis com maior rigor porque seu tratamento indevido possui um potencial maior de resultar em discriminação, exclusão ou violação de direitos fundamentais do titular.

4. **Implicações legais e práticas da distinção:**

Essa classificação tem consequências diretas:

As bases legais para o tratamento de dados pessoais sensíveis são mais restritas e específicas do que para dados pessoais comuns (conforme art. 11 da LGPD).

Exige-se a adoção de medidas de segurança técnicas e administrativas ainda mais fortes para protegê-los.

Qualquer incidente envolvendo dados sensíveis tende a ter um impacto e uma gravidade maior.

5. **Como identificar no dia a dia (especialmente no contexto educacional):**

Os tipos de dados sensíveis que podem ser manuseados em nosso ambiente, como informações de saúde de alunos para o departamento médico, dados biométricos para controle de acesso, ou informações sobre necessidades educacionais especiais que possam revelar dados sensíveis.

A figura 16 explica seus direitos de correção, transparência e até a exclusão dos seus dados.

Figura 16 - Seus direitos



Fonte: Autoria própria (2025)

1. **Confirmação e acesso:**

É seu direito fundamental confirmar se uma organização utiliza seus dados pessoais e, em caso afirmativo, acessar todas essas informações.

2. **Correção:**

É seu direito exigir a correção de qualquer dado seu que esteja incompleto, incorreto ou desatualizado.

3. **Controle sobre o tratamento e uso indevido:**

É seu direito solicitar a anonimização, o bloqueio ou a eliminação de dados que sejam desnecessários ou que estejam sendo tratados em não conformidade com a LGPD.

4. **Exclusão de dados:**

É seu direito pedir a exclusão dos seus dados pessoais quando o tratamento se baseou no seu consentimento (e você o revogou), ou quando os dados não são mais necessários para a finalidade para a qual foram coletados, observadas as exceções legais.

5. **Transparência total: informação é seu direito:**

É seu direito ser informado de maneira clara sobre com quais entidades seus dados são compartilhados, sobre a possibilidade de não fornecer consentimento.

A figura 17 apresenta como as empresas devem utilizar seus dados e seus direitos de revogação e oposição à utilização dos dados.

.

Figura 6 - Utilização dos seus dados



Fonte: Autoria própria (2025)

1) **Portabilidade:**

O seu direito de solicitar a portabilidade dos seus dados para outro prestador de serviço ou produto.

2) **Transparência total: informação é seu direito:**

É seu direito ser informado de maneira clara sobre com quais entidades seus dados são compartilhados, sobre a possibilidade de não fornecer consentimento.

3) **Revogação do consentimento:**

O poder de revogar, a qualquer momento e de forma facilitada, o consentimento que você possa ter dado anteriormente para o tratamento de seus dados.

4) **Oposição e reclamação:**

É seu direito se opor a um tratamento de dados realizado com base em outras hipóteses legais que não o consentimento.

A figura 18 os cuidados que devemos ter com a utilização dos dados.

Figura 18 - Protegendo seus dados pessoais



Fonte: Autoria própria (2025)

1. **Proteção das suas contas digitais:**

A necessidade de utilizar senhas fortes, únicas para cada serviço, e de ativar a autenticação de dois ou múltiplos fatores (MFA) em todas as contas que oferecem esse recurso.

2. **Cuidado com compartilhamento:**

A importância de refletir antes de compartilhar qualquer dado pessoal online ou offline. A pergunta deve ser sempre: 'esta informação é realmente necessária para este fim? Confio em quem está solicitando?' Isso se aplica a redes sociais, formulários, e-mails e qualquer interação.

3. **Configurações de privacidade:**

A exploração e o ajuste ativo das configurações de privacidade em seus dispositivos (celulares, computadores), aplicativos e plataformas online.

4. **Cuidado contra fraudes:**

A identificação sinais de alerta para golpes de phishing, engenharia social e outras armadilhas digitais.

5. **O conhecimento dos seus direitos LGPD:**

Exercer os direitos garantidos pela LGPD (como solicitar acesso, correção ou eliminação de dados).

A figura 19 orienta as ações tomadas após os vazamentos dos dados

Figura 19 - Vazamentos de dados



Fonte: Autoria própria (2025)

1. **O dever de comunicação do incidente (art. 48 da LGPD):**

A LGPD, em seu artigo 48, obriga a organização (controlador) a comunicar à autoridade nacional de proteção de dados (ANPD) e ao titular, a ocorrência de um incidente de segurança que possa acarretar risco ou danos.

2. **Avaliação da responsabilidade da organização:**

Nos princípios da LGPD (como os da segurança, prevenção, e responsabilização – artigo 6º), você pode avaliar a conduta da organização antes e depois do incidente. A lei exige que medidas adequadas sejam tomadas para proteger os dados.

3. **Ações de proteção pessoal imediatas:**

Medidas práticas de autoproteção digital são necessárias: alterar senhas de contas expostas e correlatas, ativar autenticação de múltiplos fatores, monitorar atividades financeiras e ficar alerta a golpes que utilizem os dados vazados.

A figura 20 é apresentado como a LGPD impacta no dia a dia e como ela pode proteger seus dados

Figura 20 - Impacto da LGPD



Fonte: Autoria própria (2025)

1. **Tudo que envolve seus dados:**

Um dos impactos mais visíveis é o aumento da transparência. Isso se reflete em políticas de privacidade mais claras e compreensíveis, avisos de coleta de dados mais detalhados no momento do cadastro em sites ou apps, e termos de consentimento que explicam melhor para que suas informações serão usadas.

2. **Mais controle sobre o consentimento que você fornece:**

A LGPD mudou a forma como o seu consentimento é solicitado e gerenciado. Agora, ele precisa ser livre, informado para finalidades específicas. Você também tem mais clareza sobre como pode revogá-lo.

3. **Empresas mais criteriosas e responsáveis com seus dados:**

A lei incentiva (e obriga) as organizações a serem mais seletivas quanto aos dados que coletam (princípio da necessidade) e a investirem mais na segurança dessas informações.

4. **Exercício facilitado dos seus direitos de titular:**

Hoje está mais fácil exercer seus direitos de acessar seus dados, solicitar correções, pedir a eliminação, entre outros. As empresas precisam ter canais para atender a essas suas solicitações.

5. **Impacto em diversas interações cotidianas:**

   Ao navegar na internet (avisos de cookies mais informativos).

   Ao fazer compras online (opções claras sobre receber ou não marketing).

   Ao usar serviços de saúde (maior cuidado com seus dados sensíveis).

   Em aplicativos e redes sociais (configurações de privacidade mais fortes).

A figura 21 enfatiza alguns tópicos apresentados nas figuras anteriores

Figura 21 - Conclusão



Fonte: Autoria própria (2025)

1. **A LGPD como um Direito Fundamenta:**

A compreensão de que a LGPD é um marco legal que eleva a proteção de dados pessoais à categoria de direito fundamental, promovendo uma mudança na forma como as informações dos cidadãos são tratadas por empresas e pelo governo.

2. **O Titular dos Dados:**

O principal legado da LGPD é o fortalecimento do cidadão, o titular dos dados. Relembramos que os direitos de acesso, correção, eliminação, informação, revogação do consentimento, entre outros, são instrumentos à sua disposição.

3. **A Cultura de Privacidade como Responsabilidade de Todos:**

A efetividade da LGPD e a construção de uma verdadeira cultura de privacidade dependem não só das organizações, mas também da conscientização e da postura ativa de cada indivíduo em conhecer e exercer seus direitos, e em zelar pelas boas práticas de segurança.

4. **Os Impactos Práticos e Benéficos no Dia a Dia:**

Os princípios e regras da LGPD se traduzem em mais transparência, mais controle e mais segurança nas suas interações cotidianas que envolvem o uso de dados pessoais.

5. **A Proteção de Dados como um Processo Contínuo e Vigilante:**

A mensagem de que a proteção de dados não se esgota com o conhecimento da lei. Ela exige atenção constante, aprendizado contínuo sobre novas ameaças e a disposição para adaptar comportamentos e utilizar as ferramentas que a LGPD oferece.

5. Recursos Didáticos e o Ambiente Virtual de Aprendizagem

A seleção das ferramentas tecnológicas para a concepção do material didático e para a aplicação do treinamento foi uma decisão metodológica estratégica, pautada na necessidade de otimizar em um formato online. Diante dos temas abordados, a Lei Geral de Proteção de Dados e a segurança de dados, e do perfil dos participantes, optou-se por uma abordagem integrada que utilizou o Microsoft PowerPoint como plataforma para a estruturação do conteúdo e o Microsoft Teams como Ambiente Virtual de Aprendizagem para a ministração das aulas.

A utilização do Microsoft PowerPoint como ferramenta para a elaboração do material didático foi importante para a organização e a clareza da exposição. A natureza densa e, por vezes, abstrata dos conceitos legais e técnicos exigia um recurso que permitisse a fragmentação do conteúdo em unidades de informação concisas e de fácil assimilação. O PowerPoint viabilizou a criação de uma narrativa visual sequencial e lógica. Essa abordagem não apenas facilitou a compreensão durante a aula.

A escolha do Microsoft Teams como plataforma para a ministração das aulas respondeu diretamente às limitações logísticas identificadas, como a dispersão geográfica dos participantes e a dificuldade de conciliar agendas para um encontro presencial. O Teams proporcionou um ambiente profissional, onde a apresentação do conteúdo elaborado em PowerPoint pôde ser realizada de forma fluida através da funcionalidade de compartilhamento de tela. Essa ferramenta permitiu recriar a dinâmica de uma sala de aula, com interação direta por áudio e vídeo entre o instrutor e os participantes.

Além de viabilizar o encontro, o Microsoft Teams ofereceu recursos pedagógicos que enriqueceram a experiência de aprendizagem. A funcionalidade de chat, por exemplo, operou como um canal de comunicação paralelo, permitindo que os participantes formulassem perguntas e compartilhassem percepções em tempo real sem interromper a explanação principal.

Em suma, a sinergia entre o PowerPoint e o Microsoft Teams foi importante para o sucesso desta intervenção educacional. Enquanto o PowerPoint forneceu a estrutura, a clareza e o suporte visual necessários para um conteúdo complexo, o Teams ofereceu o ambiente

interativo, acessível e flexível para a sua efetiva transmissão e discussão. A combinação destas tecnologias não apenas superou as barreiras logísticas, mas também potencializou o processo de ensino-aprendizagem, um fator que certamente contribuiu para os resultados expressivamente positivos observados na avaliação final do treinamento.

5.1. Estrutura do Material Didático

A concepção do material didático foi pautada em uma abordagem modular e sequencial, visando construir o conhecimento de forma progressiva e garantir a assimilação dos conceitos. A estrutura foi desenhada para conduzir os participantes desde uma introdução conceitual até o seu contexto profissional. Todo o conteúdo foi uma apresentação de slides (Microsoft PowerPoint), que serviu como guia visual e roteiro para as aulas.

O treinamento foi iniciado com um módulo de Introdução à Segurança de Dados, cujo objetivo foi estabelecer uma base conceitual comum a todos os participantes. Nesta fase, foram abordados os pilares da segurança da informação, Confidencialidade, Integridade e Disponibilidade, e introduzidos os principais conceitos de segurança cibernética.

Na sequência, o segundo módulo aprofundou-se nas Ameaças Digitais e Mecanismos de Proteção. Foram mostrados os vetores de ataque mais comuns e relevantes para o cotidiano, como malwares e o phishing, por meio da análise de exemplos de e-mails e mensagens fraudulentas. A atividade didática desta etapa foi a discussão de estudos de caso, onde exibidos aos participantes os "sinais de alerta" em diferentes cenários, estimulando o desenvolvimento de um olhar preventivo.

O terceiro módulo foi dedicado inteiramente à Lei Geral de Proteção de Dados Pessoais (LGPD). A atividade inicial foi uma exposição sobre o propósito da lei, a definição de dado pessoal e dado pessoal sensível, e os papéis dos agentes de tratamento. A complexidade do tema foi mitigada pela utilização de analogias e exemplos práticos, conectando a legislação a situações do dia a dia. A principal atividade prática foi a análise de situações hipotéticas no ambiente escolar.

O módulo seguinte, intitulado "Seus Direitos e Deveres sob a LGPD", foram detalhados os direitos do titular (acesso, correção, exclusão etc.) e as responsabilidades dos agentes de tratamento em caso de incidentes. A atividade foi um exercício de simulação, no qual os participantes foram instruídos sobre como proceder diante de uma solicitação de um titular de dados ou como agir nos primeiros momentos de uma suspeita de vazamento de dados.

Visando a aplicação prática do conhecimento, o módulo "LGPD e Segurança de Dados no Ambiente Escolar" foi desenhado para contextualizar os temas anteriores na realidade profissional dos participantes. As atividades foram mostraram os desafios do ambiente escolar, como a gestão de matrículas, o tratamento de dados de saúde de alunos, o uso de imagens em eventos escolares e a segurança de plataformas educacionais online.

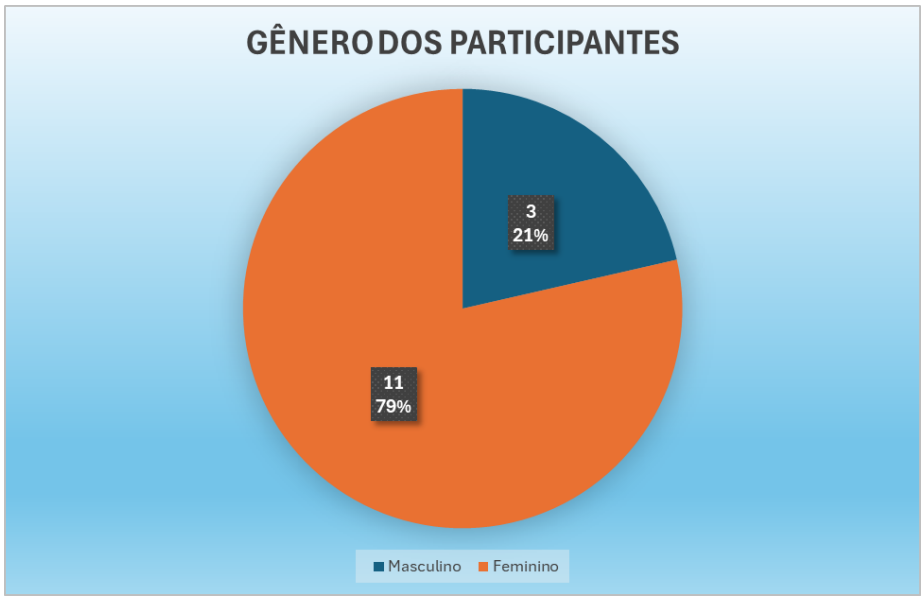
A fase final do treinamento consistiu na aplicação de um Questionário de Avaliação e Percepção, cujos dados são analisados nesta dissertação. Esta atividade não teve apenas a função de coletar dados para a pesquisa, incentivando-os a refletir sobre o conhecimento adquirido e o impacto do curso em sua percepção de segurança.

5.2. Resultados

Após o treinamento foi aplicado um questionário, respondido por de 14 (quatorze) participantes. A presente seção dedica-se à análise dos resultados obtidos com o instrumento de coleta de dados. A amostra, composta por 14 (quatorze) profissionais da educação, forneceu subsídios qualitativos que permitem traçar o perfil do grupo e avaliar a efetividade do treinamento realizado. A estratégia de captação da amostra envolveu abordagens diretas e o uso de aplicativos de mensagens, garantindo que o convite alcançasse os profissionais em suas respectivas localidades e facilitando a adesão ao curso. A apresentação dos dados segue uma ordem, iniciando pela identificação do perfil dos respondentes e avançando para a análise e percepção sobre o material didático, a metodologia aplicada e os conhecimentos adquiridos.

Quanto ao sexo revela uma participação majoritariamente feminina. Do total de 14 (quatorze) participantes, 11 (onze) são do sexo feminino, o que corresponde a aproximadamente 79%, enquanto 3 (três) são do sexo masculino, representando os 21% restantes.

Gráfico 1 – Gênero



A faixa etária dos 14 (quatorze) participantes amostra com um perfil de maturidade, marcada por uma concentração de participantes na faixa de 42 a 52 anos, composta por 11 (onze) participantes (79%). Este grupo é complementado por 2 (dois) participantes na faixa de 31 a 41 anos (14%) e 1 (um) na faixa de 53 a 63 anos (7%).

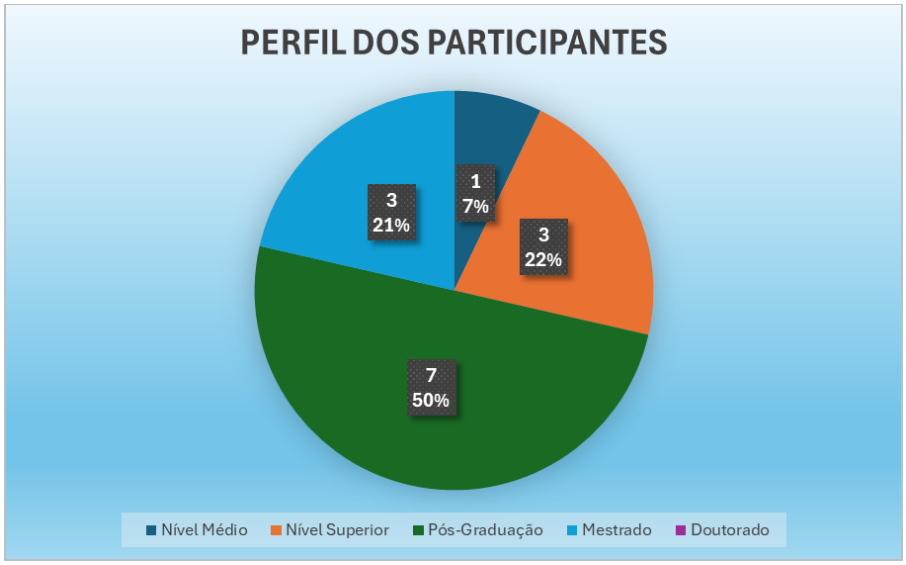
Vale notar a ausência de participantes nas faixas mais jovens (18-30 anos) e na de idade mais avançada (64 anos ou mais).

Gráfico 2 - Faixa etária



O perfil acadêmico composta por 14 (quatorze) participantes, caracteriza-se por uma qualificação educacional avançada, um fator para a análise dos dados desta pesquisa. A totalidade dos participantes concluiu o ensino médio 1 (um). A maior concentração de participantes encontra-se no nível de Pós-Graduação (*lato sensu*), com 7 (sete) participantes (50%). Os demais se distribuem equitativamente entre o Nível Superior completo e o Mestrado (*stricto sensu*), com 3 (três) participantes em cada categoria (21,5% cada).

Gráfico 3 - Perfil dos participantes



A análise estatística demonstra um tempo médio de experiência de 18,2 anos, maior quantidade de participantes é de 5 anos, com os tempos de experiência individuais variando de um mínimo de 5 anos a um máximo de 30 anos.

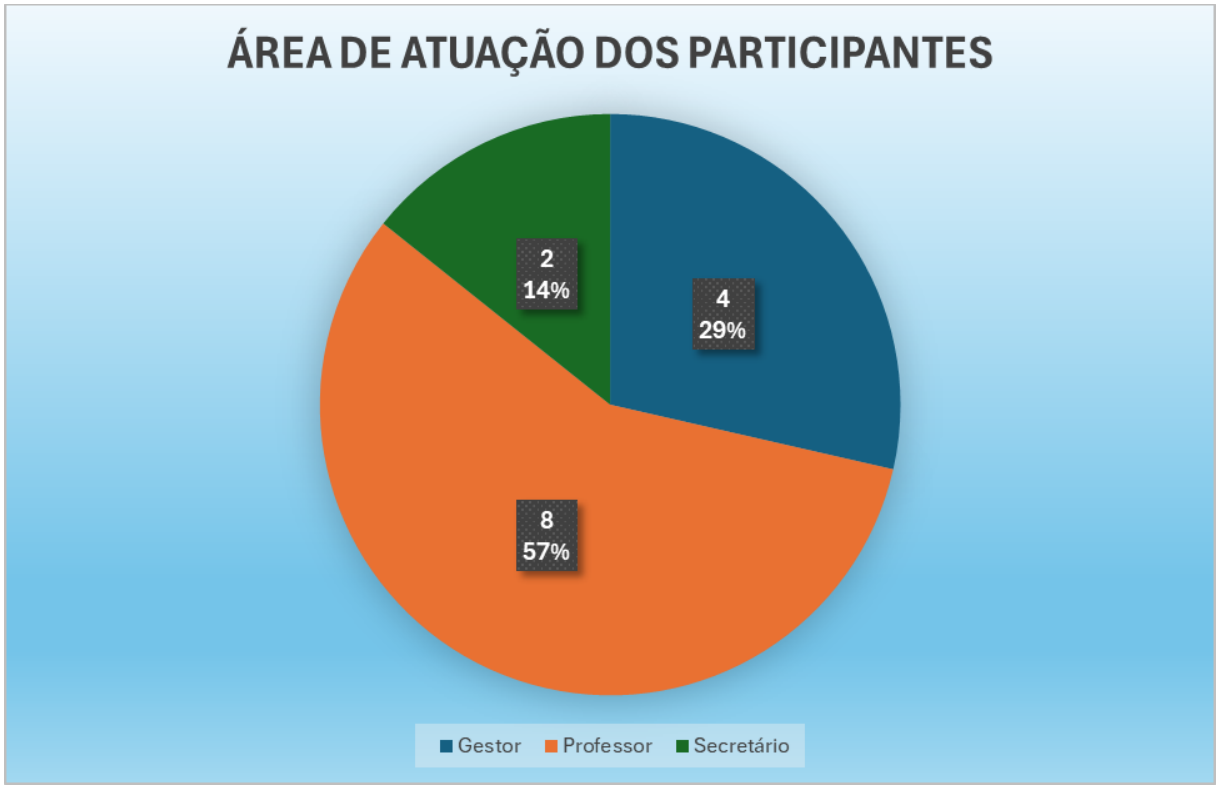
Gráfico 4 - Experiencia profissional dos participantes



A maior parte do grupo é constituída por membros do corpo docente, com 8 (oito) Professores (57%).

A equipe de gestão escolar também está representada, com 4 (quatro) Gestores (29%), enquanto o suporte administrativo é representado por 2 (dois) Secretários (14%). Essa composição heterogênea de cargos, incluindo docência, gestão e administração, enriquece o escopo do treinamento, pois permite o aprendizado a partir de múltiplos pontos dentro do ambiente educacional.

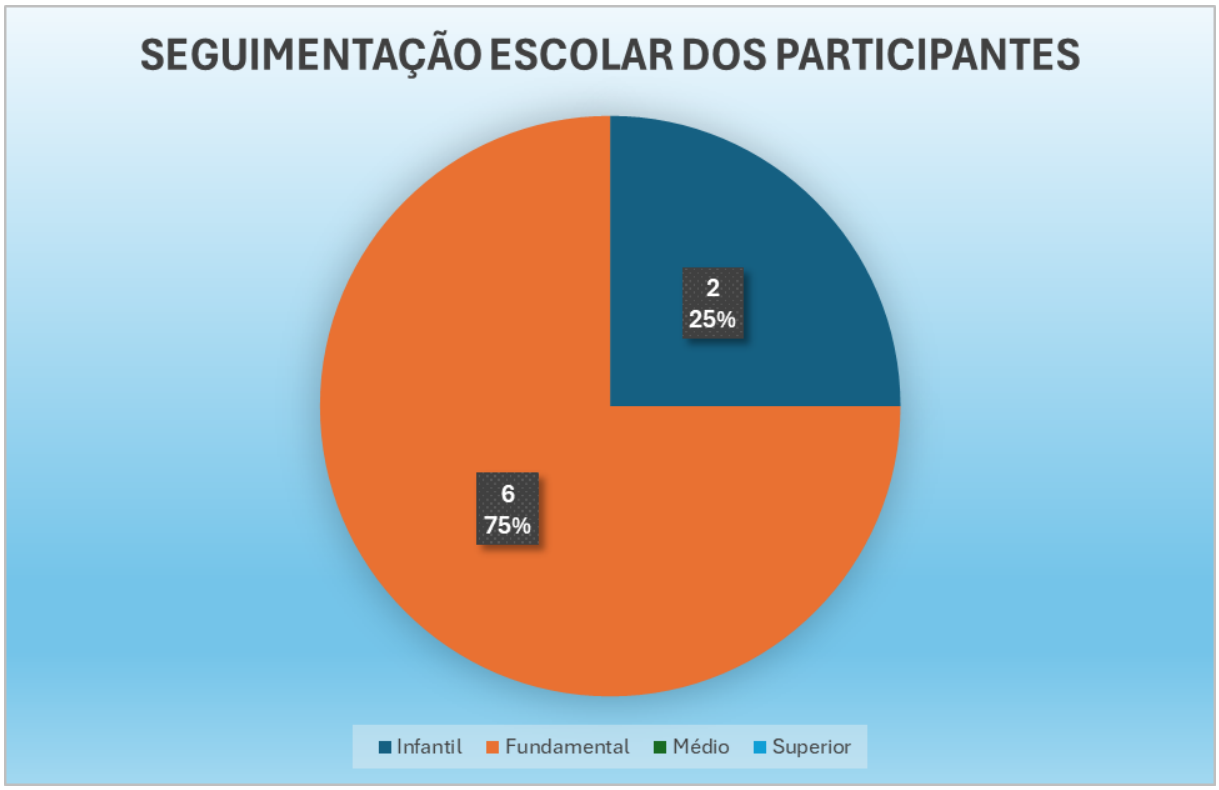
Gráfico 5 - Área de atuação dos participantes



A análise do segmento escolar de atuação dos participantes do treinamento. Dos 14 (quatorze) participantes do estudo, os 8 (oito) que exercem a função de Professor responderam a esta questão, revelando uma predominância de atuação no Ensino Fundamental, que representa 6 (seis) docentes (75%).

O Ensino Infantil é o segmento de atuação dos outros 2 (dois) professores (25%). Nenhum dos participantes a esta questão indicou atuar nos segmentos de Ensino Médio ou Superior.

Gráfico 6 - Segmentação escolar dos participantes



A avaliação geral do treinamento, a totalidade dos 14 (quatorze) participantes responderam afirmativamente. Este resultado mostra 100% consideraram que a expectativa em relação à formação foi atendida positivamente

Gráfico 7 - Expectativa do treinamento



Na avaliação do conteúdo abordado durante a formação, todos os 14 (quatorze) participantes (100%) manifestaram uma percepção positiva sobre as aulas. Este resultado mostra a relevância e a adequação do material pedagógico apresentado, indicando que esteve adequado às necessidades de aprendizagem dos participantes.

Gráfico 8 - Resultado sobre o conteúdo abordado



Após o treinamento, sentiam-se mais seguros em relação à proteção de seus dados pessoais a totalidade dos 14 (quatorze) participantes. Este resultado de (100%) aponta positivamente na aplicação do treinamento.

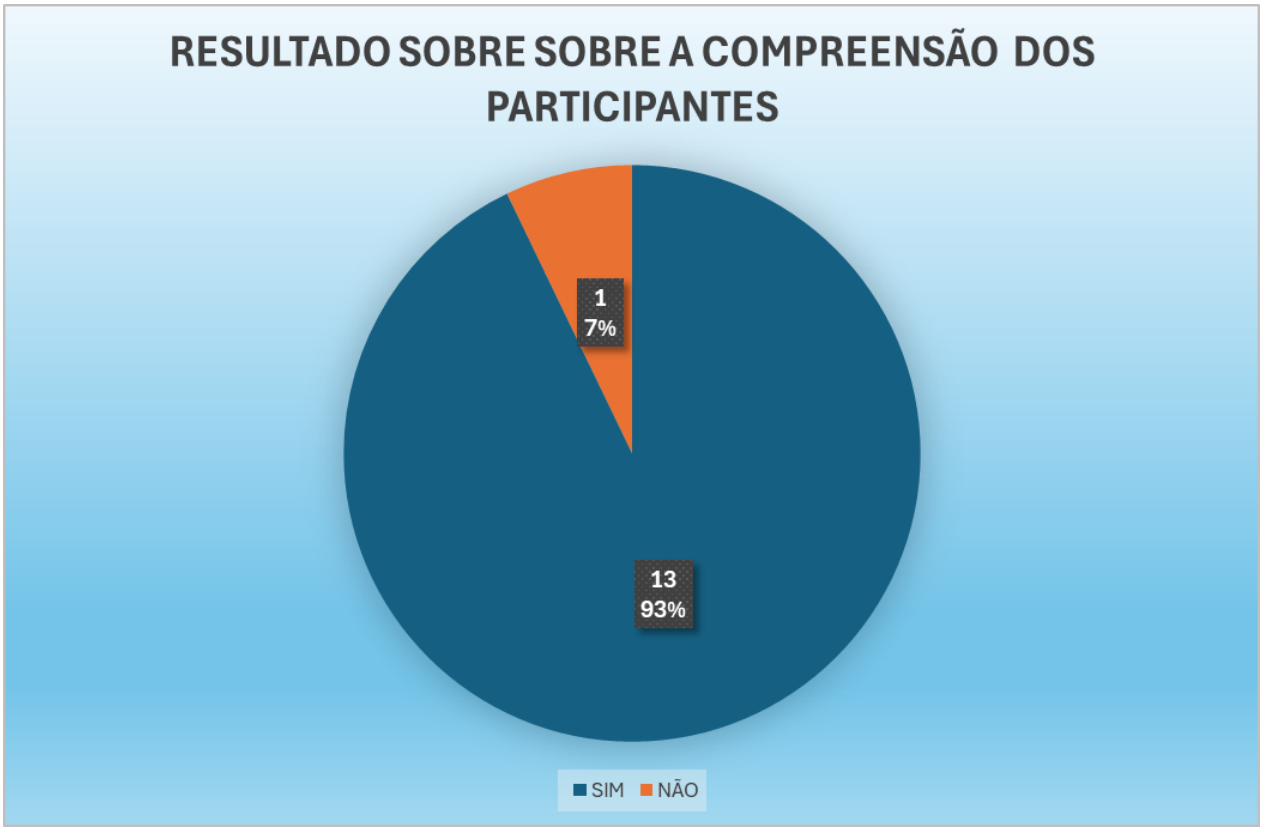
Gráfico 9 - Resultado sobre a segurança dos dados após o treinamento



A clareza do conteúdo apresentado no treinamento foi comprovada pela maioria dos participantes. Um total de 13 (treze) dos 14 (quatorze) participantes, (92%) consideraram os tópicos claros e de fácil compreensão.

Houve uma ressalva por parte de 1 (um) participante (7%), que indicou ter encontrado dificuldade na compreensão da maioria dos temas.

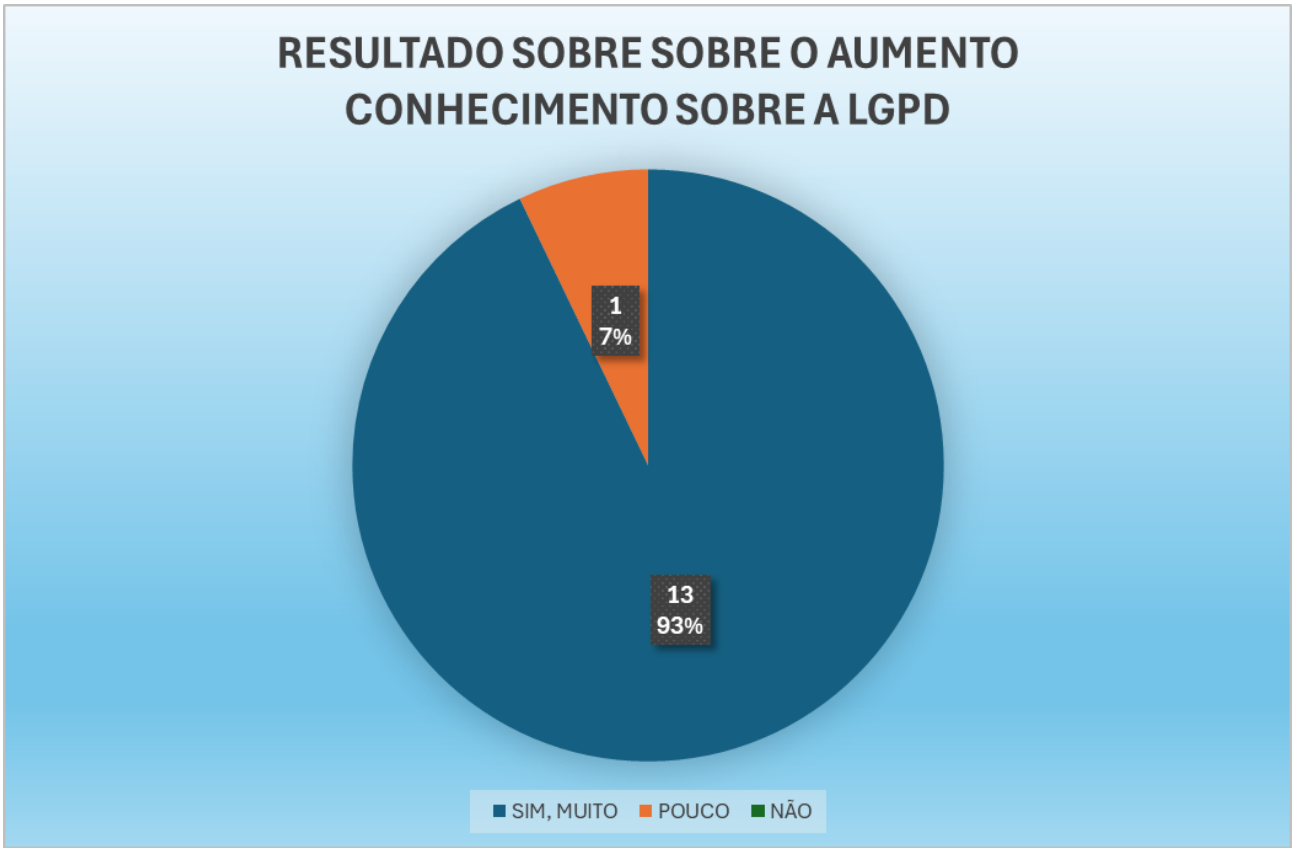
Gráfico 10 - Resultado sobre a compreensão dos participantes na aplicação do treinamento



Sobre a percepção de ganho de conhecimento sobre a LGPD, os resultados indicam um impacto positivo sobre a totalidade da amostra. Dos 14 (quatorze) participantes, 13 (treze), o que corresponde a 93%, afirmaram que o treinamento aumentou 'muito' seu conhecimento sobre o tema.

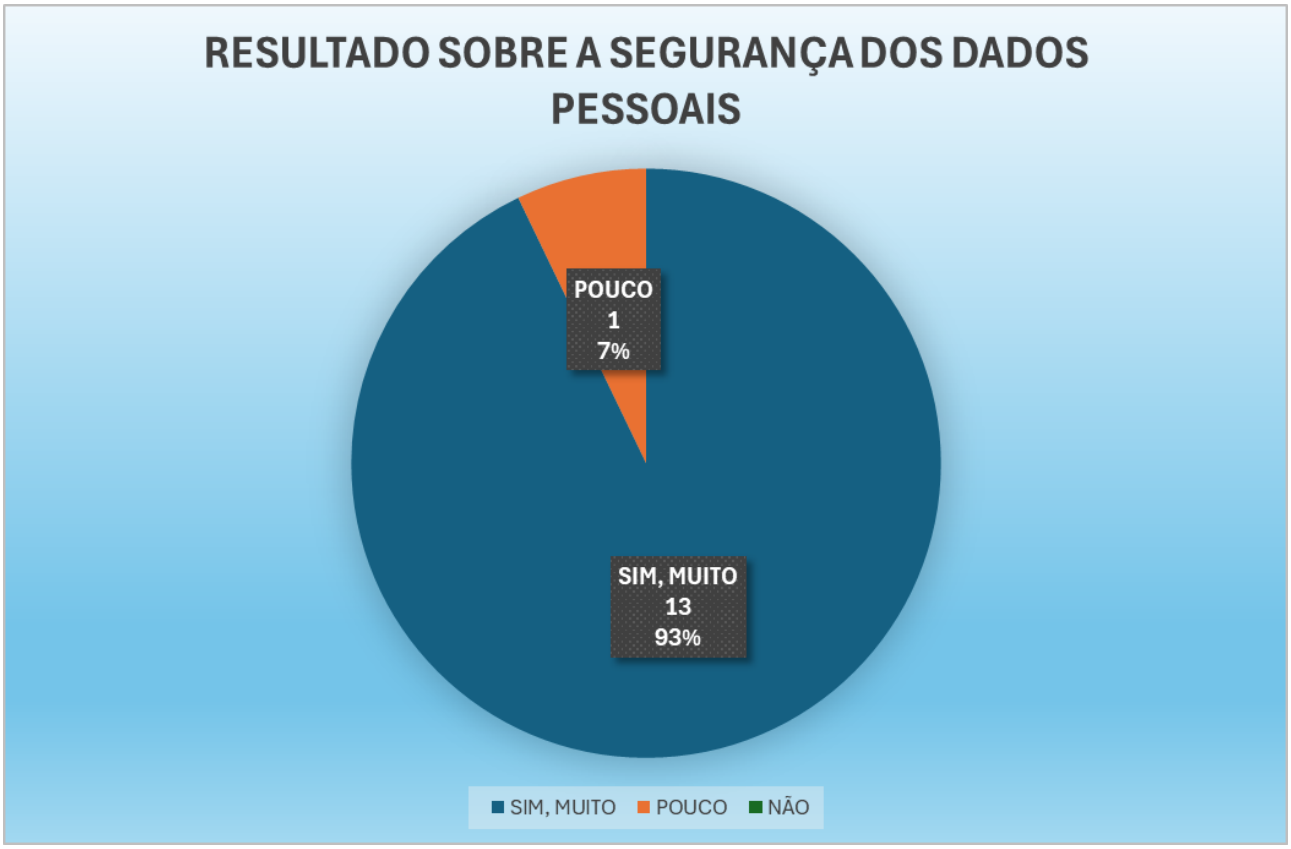
O participante restante (7%) indicou que seu conhecimento aumentou 'pouco'. Não houve respostas que indicassem ausência de ganho de conhecimento ('não').

Gráfico 11 - Resultado sobre o aumento conhecimento sobre a LGPD



Foi avaliada a percepção de ganho de conhecimento sobre Segurança de Dados. Os resultados foram positivos, com 13 (treze) dos 14 (quatorze) participantes (92%) afirmando que o treinamento aumentou 'muito' seu conhecimento. O participante remanescente (8%) indicou um aumento 'pouco', e não houve respostas negativas ('não').

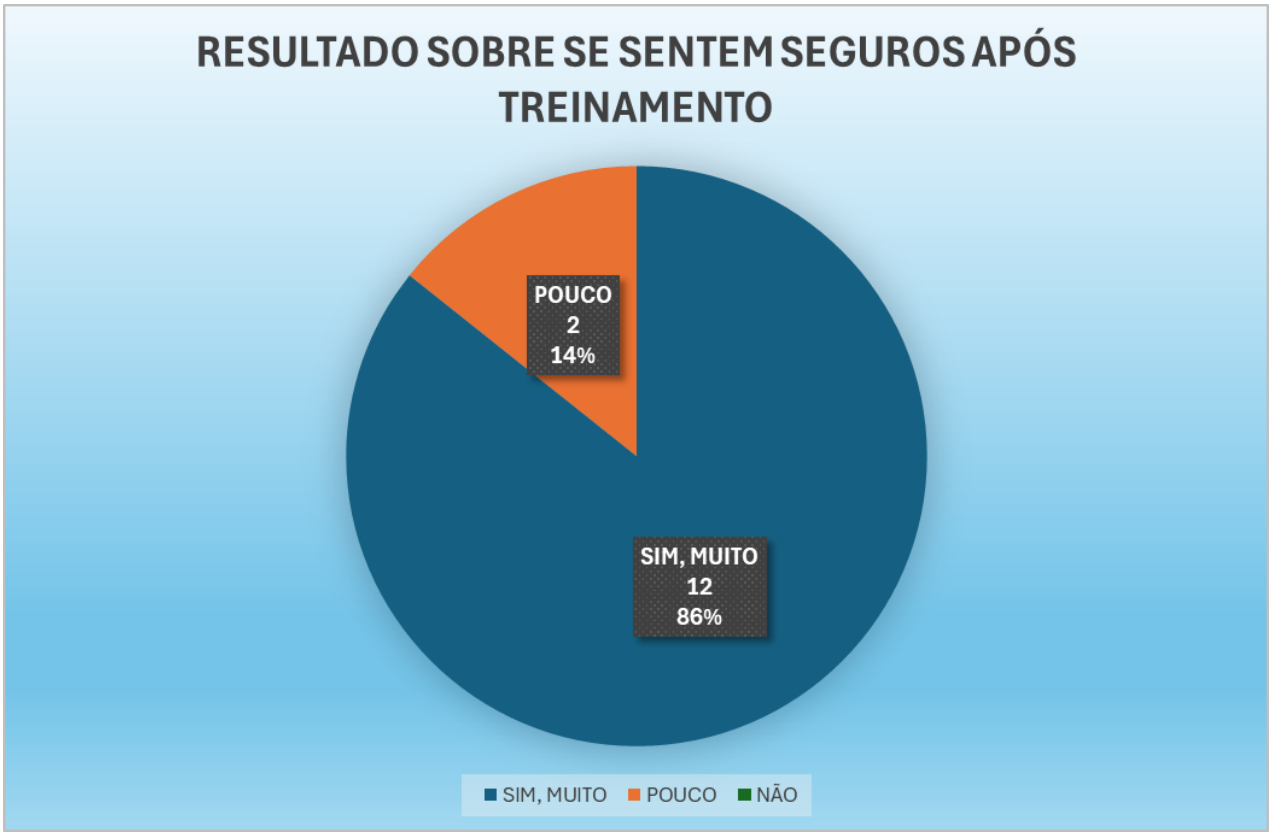
Gráfico 12 - Resultado sobre o aumento conhecimento sobre segurança de dados



Ao avaliar o impacto do treinamento na percepção de segurança para o uso específico de redes sociais e da internet, a resposta da maioria foi positiva. Dos 14 (quatorze) participantes, 12 (doze), o que equivale a 85% da amostra, indicaram sentir-se 'muito' mais seguros.

Os 2 (dois) participantes restantes (15%) afirmaram sentir-se 'pouco' mais seguros. Novamente, não houve respostas que indicassem ausência de ganho na percepção de segurança.

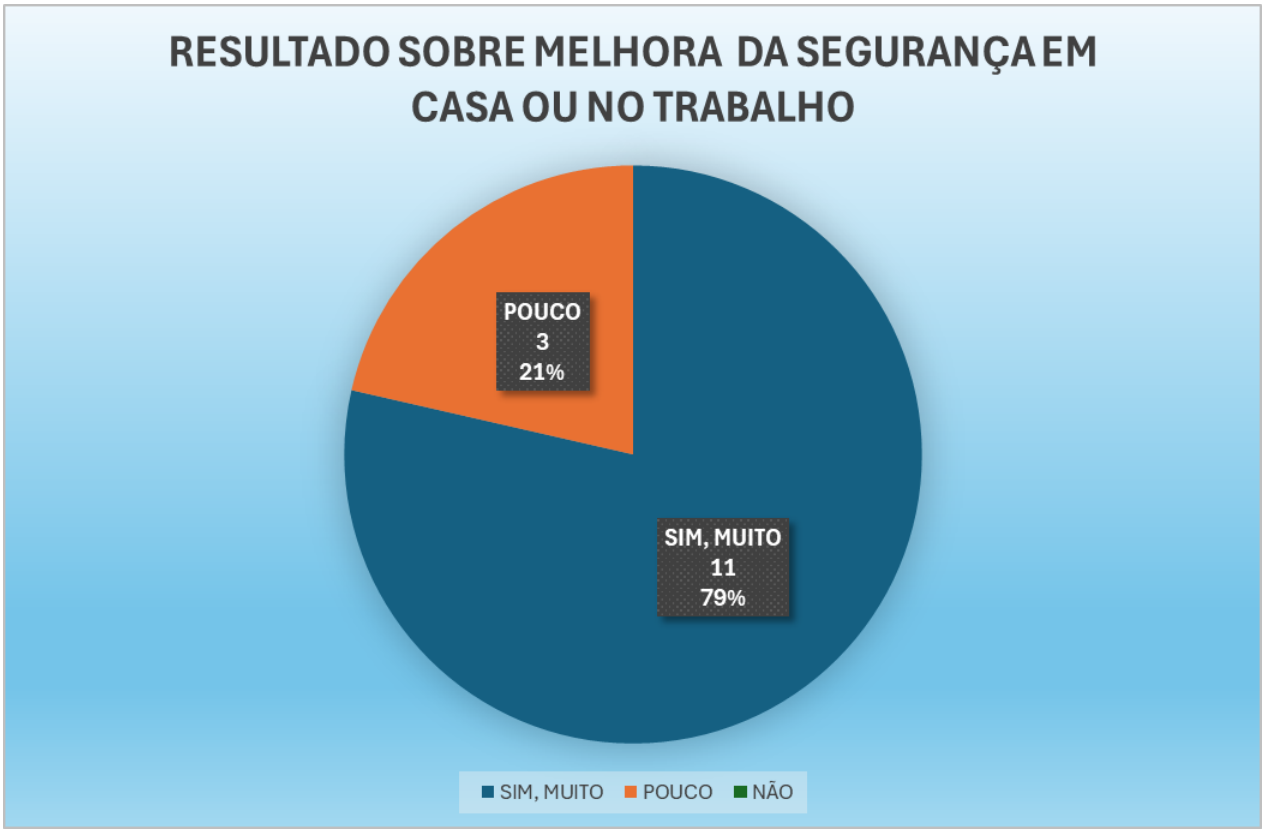
Gráfico 13 - Resultado de como os usuário se sentem seguros após o treinamento



A percepção dos participantes sobre a aplicabilidade futura do treinamento para a melhoria da segurança em seus ambientes de trabalho e doméstico. As respostas foram positivas, com 11 (onze) dos 14 (quatorze) indivíduos (79%) acreditando que o curso ajudará 'muito'.

Os 2 (dois) participantes restantes (21%) indicaram que o treinamento ajudará 'pouco'. Não houve respostas que negassem o potencial de ajuda da formação.

Gráfico 14 - Resultado se com o treinamento ajudará melhorar a segurança no seu ambiente de trabalho ou em casa



Ao serem questionados se recomendariam o treinamento para outras pessoas, a resposta foi totalmente positiva. A totalidade dos 14 (quatorze) participantes (100%) respondeu afirmativamente, o que demonstra positivamente a experiência com o treinamento.

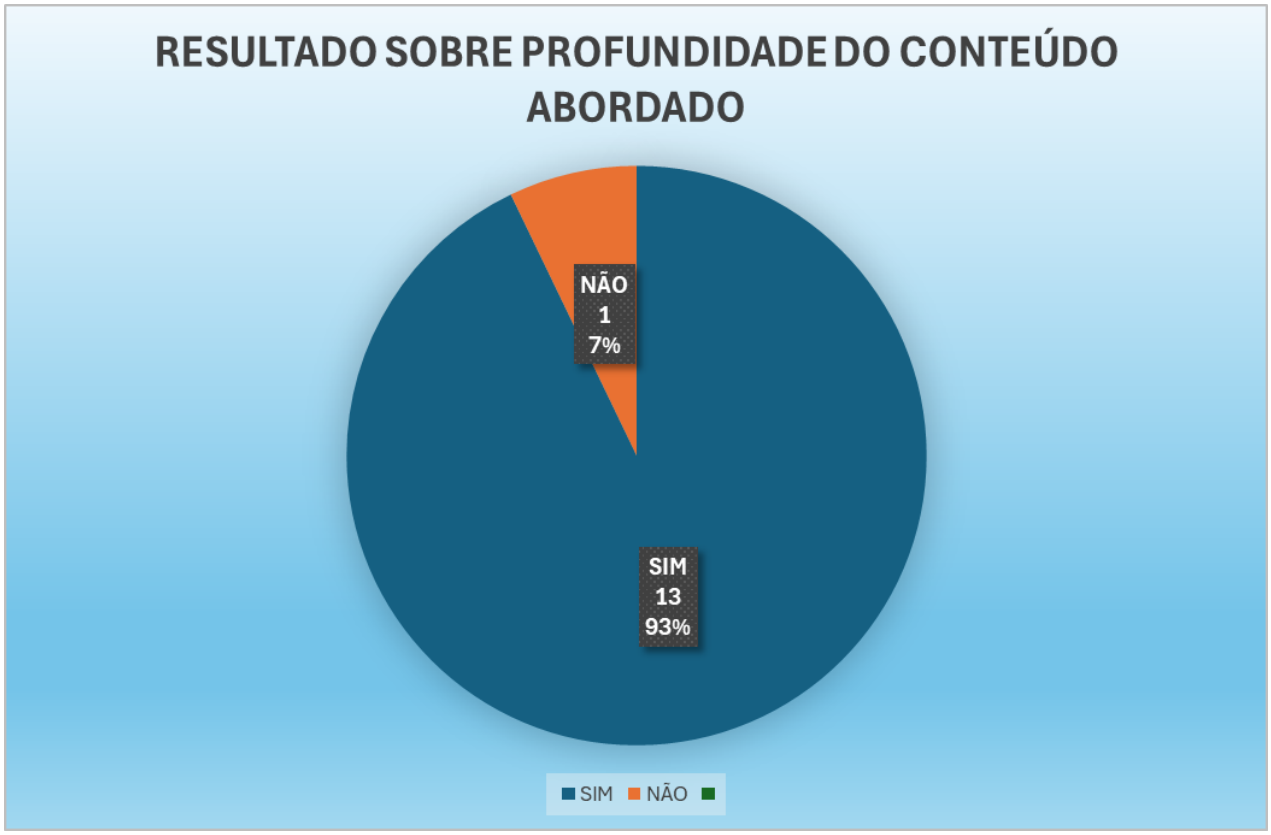
Gráfico 15 - Recomendação do treinamento para outras pessoas



Para avaliar o conteúdo dos temas abordados, questionou-se se os participantes gostariam de um maior aprofundamento em algum tópico. A grande maioria, composta por 13 (treze) dos 14 (quatorze) respondentes (93%), respondeu 'não', indicando estarem satisfeitos com o nível de detalhamento apresentado.

Houve a manifestação de 1 (um) participante (%) que respondeu 'sim', sinalizando o desejo por um maior aprofundamento em algum dos conteúdos ministrados.

Gráfico 16 - O gráfico demostra a profundidade do conteúdo abordado



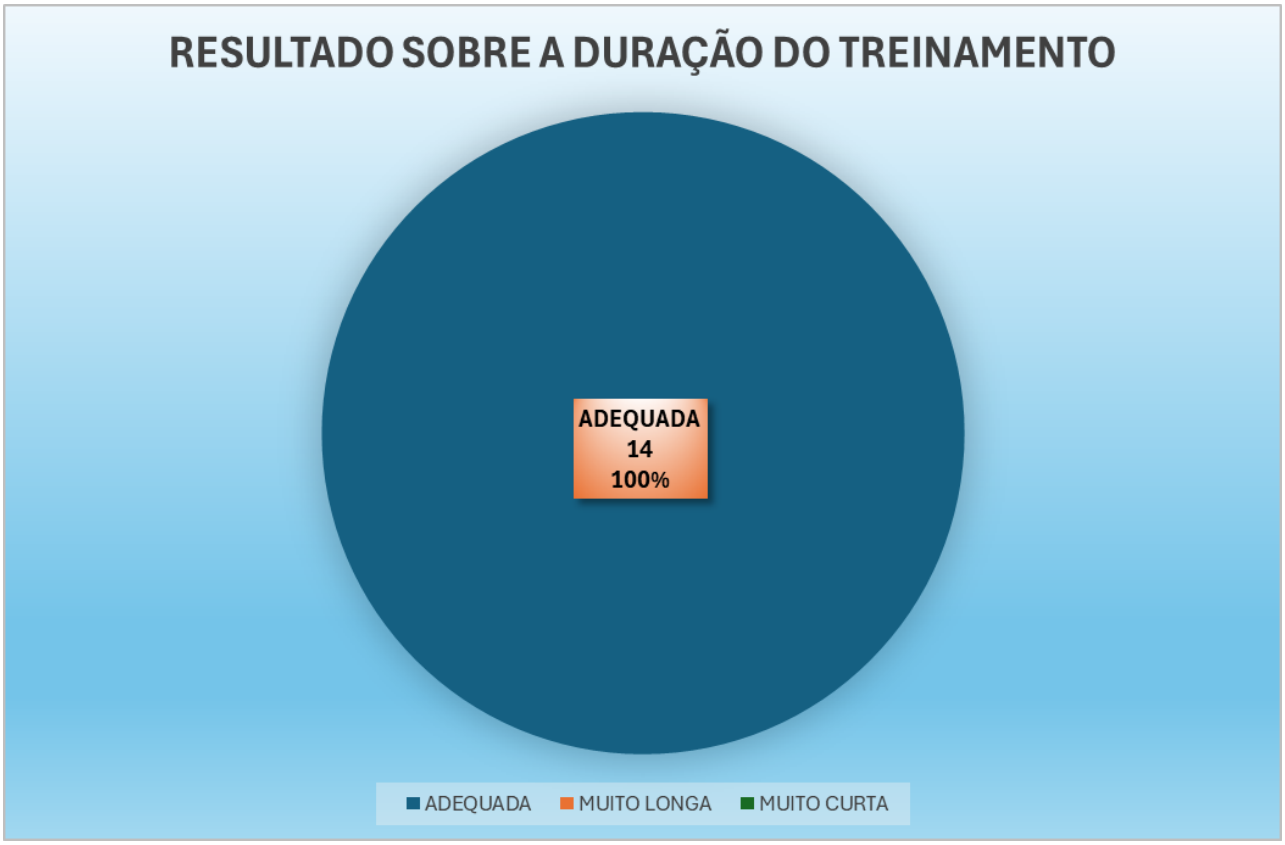
Relacionado a pergunta anterior que 1 participante respondeu sim, propondo mais aprofundamento sobre os conteúdos aplicados. A sugestão foi: "Como seguir para reportar um problema de cyber".

Gráfico 17 - Relacionado a pergunta anterior, a imagem abaixo apresenta a sugestão do participante



Ao avaliar a duração do treinamento, houve um consenso entre os participantes. A totalidade dos 14 (treze) respondentes (100%) considerou a carga horária do curso como 'adequada' para os temas propostos.

Gráfico 18 - Resultado sobre a duração do treinamento



No questionário se algum conteúdo deixou de ser abordado no treinamento, a percepção da maioria foi de que o escopo foi completo. A maioria da amostra, composta por 12 (doze) dos 13 (treze) participantes (o que corresponde a 92%), respondeu 'não'.

Em contrapartida, 1 (um) participante (8%) respondeu 'sim', indicando a percepção de que um tópico adicional poderia ter sido incluído na formação.

Gráfico 19 - Avaliação se haveria necessidade de mais algum conteúdo para ser abordado



Relacionado a pergunta anterior que 1 participante respondeu sim, propondo mais tópico adicional que poderia ser incluído no treinamento. A sugestão foi: "Apresentação de tecnologia que possa apoiar".

Gráfico 20 - Relacionado a pergunta anterior, a imagem abaixo apresenta a sugestão do participante



Gráfico 21 - O tempo de treinamento foi adequado?



A avaliação final do treinamento foi consolidada por meio de uma nota de 0 a 10 atribuída pelos participantes. O desempenho do curso foi considerado excelente, alcançando uma nota média de **8,71**.

Esta média reflete a concentração de avaliações no topo da escala: 12 (doze) dos 14 (quatorze) participantes (86%) atribuíram a nota máxima (10), enquanto os 2 (dois) participantes restantes (8%) se distribuíram igualmente entre as notas 9 e 8.

Gráfico 22 - Notas para avaliação do treinamento



6. ANÁLISE DOS DADOS E DISCUSSÃO

A análise dos resultados evidencia que a intervenção pedagógica expandiu o conhecimento dos participantes sobre o tema. A média obtida de 9,77 (em escala de 0 a 10), aliada a uma taxa de recomendação de 100%, transcende a verificação de aprendizagem; estes indicadores sugerem que a metodologia e o conteúdo foram percebidos como relevantes e aplicáveis. Tal desempenho confirma que a capacitação supre uma demanda por conhecimentos práticos em segurança da informação e LGPD, atendendo a um público que, a despeito de sua qualificação acadêmica, reconhece lacunas em sua formação específica.

Os dados corroboram o cenário descrito na literatura acerca das novas tecnologias educacionais. A insegurança inicial manifestada pelos participantes, somada à demanda por qualificação, demonstra que a inserção de ferramentas digitais nas escolas impôs ao corpo docente a necessidade de competências frequentemente não contempladas na formação inicial.

Nessa perspectiva, os resultados dialogam com os achados de (Freitas, 2023). A autora investigou as lacunas na formação docente voltada ao uso de tecnologias, apontando a carência de formação continuada como um entrave para a utilização segura e eficaz de recursos digitais. Ao indicarem que o curso proporcionou uma consciência sobre riscos e proteção de dados, os relatos dos participantes validam a premissa de Freitas de que intervenções formativas são necessárias para converter a insegurança em competência digital aplicada.

Sob a ótica da governança e da gestão escolar, os resultados reforçam a necessidade da institucionalização de tais práticas. Conforme observa (Isidorio, 2021) ao analisar os processos de mudança na educação contemporânea, a adaptação das escolas a novas realidades requer uma atuação participativa e uma gestão que fomente a cultura da formação contínua. A autora sustenta que o êxito dessas transformações depende da condução e do suporte oferecidos pela gestão à comunidade escolar.

Depreende-se, portanto, que a eficácia da intervenção transcende a transmissão de conteúdo técnico. Ela reside no preenchimento de uma lacuna estrutural destacada por (Freitas, 2023) e (Isidorio, 2021): a integração da competência digital docente a uma gestão escolar consciente, capaz de oferecer suporte frente aos desafios atuais.

Avançando na análise, os resultados dialogam com a literatura sobre o fator humano na segurança da informação. Se, por um lado, estudos de (Freitas; Gomes, 2021) identificam o profissional como o potencial "elo mais fraco" da segurança, os dados aqui apresentados

oferecem uma nova perspectiva, evidenciando-o como agente da solução. A taxa de aprendizado sugere que a vulnerabilidade humana não é uma condição imutável, mas consequência de uma lacuna formativa passível de mitigação por intervenções pedagógicas. Tal constatação alinha-se a (Costa; Leite, 2022), que defendem o letramento digital docente como condição necessária para a proteção de dados no ambiente escolar.

Adicionalmente, a intervenção configura-se como uma aplicação prática do conceito de "cultura de segurança", defendido por (Almeida; Santos, 2021). Enquanto a teoria aponta a necessidade de internalizar valores e práticas seguras, este estudo apresenta e valida uma metodologia capaz de iniciar esse processo no contexto escolar. Demonstra-se, assim, que o investimento na capacitação humana é estratégia necessária para a conformidade com a LGPD, constituindo complemento às tecnologias de proteção. Nesse sentido, (Monteiro, 2021) argumenta que a conformidade com a LGPD não se resume à implementação de medidas técnicas de TI, exigindo a adoção de medidas administrativas e organizacionais que promovam a governança de dados e a conscientização dos agentes de tratamento. O autor ressalta que o fator humano e a cultura de proteção são relevantes para a mitigação dos riscos inerentes ao tratamento de dados pessoais.

6.1. Eficácia da Intervenção e o Aumento da Percepção de Segurança

Os resultados demonstram o sucesso do treinamento. A nota média de 9,77 (de 10), a taxa de recomendação de 100% e a percepção de que a formação atendeu às expectativas são indicadores da qualidade da intervenção. Este sucesso pode ser diretamente associado à crescente conscientização sobre a relevância do tema. Autores como COSTA (2024) e OLIVEIRA (2025) destacam que a conformidade com a LGPD não é apenas uma obrigação legal, mas uma necessidade estratégica que exige a capacitação contínua dos colaboradores. Os resultados sugerem que os participantes, profissionais experientes da área da educação, reconheceram o valor prático e a urgência do conhecimento oferecido.

O aumento da percepção de segurança — com 92,3% sentindo-se "muito" mais seguros em relação aos seus dados em geral e 84,6% no uso da internet e redes sociais, alinha-se aos achados de TAKEUCHI (2023), que investigaram o impacto de treinamentos de cibersegurança e constataram que ações de capacitação bem estruturadas elevam a autoconfiança e a proatividade dos indivíduos. O treinamento, portanto, não apenas transmitiu conteúdo, mas

cumpriu um papel importante com o aumento de conhecimento dos participantes, um objetivo defendido por BRITO (2025), que posiciona a LGPD como um instrumento de fortalecimento do cidadão como titular de direitos.

6.2. Transferência de Aprendizagem e o Letramento Digital no Contexto Educacional

A percepção de que o treinamento ajudará a melhorar a segurança nos ambientes de trabalho e doméstico (com 84,6% indicando que ajudará "muito") é uma forte evidência da transferência de aprendizagem. Este conceito, valida que o conhecimento adquirido foi considerado aplicável e relevante para além do ambiente de aula. No contexto específico da educação, isso dialoga diretamente com o debate sobre o letramento digital docente. VIEGAS (2020) argumentam que a competência em proteção de dados é uma nova e indispensável dimensão do letramento digital para educadores. Os resultados indicam que o treinamento contribuiu efetivamente para o desenvolvimento dessa competência, capacitando os profissionais para uma atuação mais segura e consciente.

A especificidade do público, composto por maioria profissionais da Educação Básica, torna os resultados ainda mais relevantes. O ambiente escolar lida com um volume significativo de dados pessoais, incluindo dados sensíveis e de crianças e adolescentes, que recebem proteção especial pela LGPD). A receptividade e a avaliação positiva do curso por parte de gestores e professores demonstram a demanda a necessidade de iniciativas de formação focadas neste setor, como defende REIS (2024) em seu trabalho sobre os desafios da LGPD nas escolas.

6.3. Avaliação da formação

Apesar da aprovação, poucos participantes fizeram menções a melhorias no conteúdo, um participante que considerou os tópicos difíceis e os que desejaram maior aprofundamento ou sentiram falta de algum conteúdo, são de grande valia para aprimorar a formação e incluir novos conteúdos no futuro. Longe de invalidarem o sucesso do curso, esses pontos dissonantes corroboram a literatura sobre o fator humano na segurança da informação. ALVES

(2024) afirmam que diferentes níveis de conhecimento prévio, perfis de aprendizagem e contextos profissionais influenciam a recepção de treinamentos técnicos.

Portanto, o retorno minoritário não deve ser visto como uma falha, mas como um indicador da complexidade inerente ao processo de capacitação em temas de alta tecnicidade e um valioso subsídio para o aprimoramento contínuo da intervenção, talvez com a criação de módulos de nivelamento ou avançados. Essa percepção está alinhada com a visão de Doneda (2020), que trata a proteção de dados como um campo em constante construção, exigindo aprendizado e adaptação contínuos.

Em suma, os dados coletados validam a eficácia da intervenção educacional, mostrando que ela foi bem-sucedida em ampliar o conhecimento e a percepção de segurança de um público estratégico. A análise, confrontada com a produção acadêmica nacional, permite concluir que o treinamento não só atendeu a uma demanda real e urgente do setor educacional, como também contribuiu para o letramento digital dos participantes, em plena conformidade com os princípios e objetivos da LGPD.

7. CONCLUSÃO

A presente dissertação propôs-se a desenvolver, aplicar e avaliar uma intervenção educacional focada na Lei Geral de Proteção de Dados (LGPD) e na segurança de dados pessoais no ambiente escolar. Ao final desta jornada investigativa, conclui-se que os objetivos propostos foram alcançados, com a validação do treinamento e a coleta de percepções valiosas que demonstram a relevância e a necessidade de capacitação contínua para os profissionais da educação.

O estudo foi realizado com um grupo de 14 (quatorze) participantes, cuja base de conhecimentos se revelou um fator importante para a riqueza da análise. A amostra foi composta por profissionais de elevada qualificação, com a totalidade possuindo ensino superior e uma maioria expressiva com pós-graduação. Ademais, o grupo demonstrou uma senioridade notável, com uma média de 18,2 anos de experiência profissional, atuando em funções estratégicas como gestão e docência, majoritariamente na Educação Básica. Este perfil de alta maturidade profissional e acadêmica forneceu uma base para a assimilação do conteúdo e conferiu um peso significativo às suas avaliações positivas.

A contribuição da formação para este público foi evidenciada de forma contundente pelos resultados do questionário de avaliação. A intervenção não apenas atendeu (100%) como superou as expectativas, com o conteúdo e a abordagem sendo validados por uma nota média

final de 9,77 em 10. A aprovação em quesitos como qualidade do conteúdo e adequação da duração demonstra o sucesso do planejamento e da execução pedagógica.

Mais do que a simples satisfação, a principal contribuição do treinamento reside no impacto direto sobre a percepção de segurança e no preparo dos participantes. A totalidade da amostra afirmou sentir-se mais segura em relação à proteção de seus dados, com a maioria (92,3%) relatando um grande aumento no conhecimento sobre LGPD e Segurança de Dados.

Na maioria dos participantes ao afirmar que o treinamento foi útil para melhorar a segurança em seus ambientes de trabalho e doméstico atesta o sucesso na transferência de aprendizagem. O conhecimento não foi percebido como estanque, mas como uma ferramenta prática e transferível para os múltiplos contextos da vida profissional e pessoal, validando a proposta de valor da intervenção.

A concretização deste estudo, contudo, deparou-se com limitações de ordem logística que influenciaram diretamente a escolha do formato de aplicação. A principal dificuldade residiu na conciliação das agendas de profissionais experientes e geograficamente dispersos.

A inviabilidade de encontrar um local físico de fácil acesso para todos, somada à dificuldade de sincronizar um dia e horário comum para um encontro presencial, apresentou-se como uma barreira.

Diante dessas limitações, a melhor forma encontrada para viabilizar o treinamento foi a sua realização em formato online, utilizando a ferramenta Microsoft Teams. Esta decisão, longe de ser um demérito, revelou-se uma escolha metodológica estratégica. A modalidade a distância não apenas superou os obstáculos de espaço e tempo, mas também democratizou o acesso, permitindo que profissionais de diferentes localidades pudessem participar e contribuir com suas experiências, o que enriqueceu o alcance da pesquisa.

Embora os resultados desta dissertação demonstrem a eficiência do modelo de treinamento proposto, é importante reconhecer as limitações inerentes ao escopo da amostra.

A análise foi conduzida com um número limitado de 14 participantes. Os resultados, portanto, devem ser compreendidos como uma validação de um projeto-piloto, que aponta para um potencial de sucesso em maior escala.

Esta limitação, no entanto, serve como a principal justificativa para a necessidade de trabalhos futuros e da expansão desta iniciativa. O sucesso e a boa receptividade do treinamento, validados por um grupo qualificado de profissionais, demonstram uma demanda clara e urgente por capacitação em segurança de dados e LGPD no setor educacional. A elevada taxa de recomendação (100%) sinaliza que o modelo proposto tem grande potencial de aceitação e eficácia se aplicado a um público mais amplo.

Portanto, recomenda-se, com base nas evidências aqui consolidadas, o desenvolvimento de um programa de formação em larga escala, que possa ser institucionalizado e ofertado a um número expressivamente maior de professores, gestores e demais profissionais da educação. A presente dissertação cumpre seu papel ao não apenas analisar um problema, mas ao oferecer e validar um caminho concreto para sua solução, reforçando a premissa de que a educação é a ferramenta de suma importância para a construção de uma cultura sólida de proteção de dados no Brasil.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Beatriz Venâncio de. A estratégia de cibersegurança nas pequenas e médias empresas: uma análise exploratória dos fatores de adoção e implementação de medidas de proteção. In: CONGRESSO INTERNACIONAL DE GESTÃO E TECNOLOGIA – CINGET, 10., 2024, Porto Alegre. Anais [...]. Porto Alegre: CINGET, 2024. p. 1–15.

ALMEIDA, F.; SANTOS, C. N. Desafios e estratégias para a adequação à Lei Geral de Proteção de Dados (LGPD) em instituições de ensino. *Revista de Administração e Educação*, v. 12, n. 2, p. 88-105, 2021.

ALMEIDA, S. DO C. D. DE; SOARES, T. A. Os impactos da Lei Geral de Proteção de Dados - LGPD no cenário digital. Perspectivas em Ciência da Informação, v. 27, n. 3, p. 26–45, set. 2022.

ALVES, et al. Fator humano na segurança da informação: um mapeamento dos comportamentos de risco no ambiente digital. Texto Livre, v. 17, p. e51184, 6 set. 2024.

BEPPLER, Tamy. A evolução da segurança cibernética. Conteúdo Jurídico, Brasília-DF, 07 jun. 2021.

BOTELHO, L. L. R.; DE ANDRADE, M. T. C. A importância da conscientização e treinamento em segurança da informação nas organizações. Revista de Administração e Inovação (RAI), v. 18, n. 3, p. 1-23, 2021.

BRASIL. Lei Geral de Proteçâo de Dados. 2018**.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 04 de dez. de 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

BRITO, Alan Pinheiro. Desafios da implementação do mapeamento de dados pessoais em sistemas de informações na Administração Pública: Revisão Sistemática. In: Latin American Symposium on Digital Government (LASDiGov). SBC, 2025. p. 13-24.

BRUNO, F. et al. (Orgs.). Tecno políticas da vigilância: perspectivas da margem. 1ª ed. São Paulo: Boitempo, 2021.

CANAZARO, Fábio P. Cibercriminalidade e investigação criminal tecnológica. 2ª ed. Salvador: Editora JusPodivm, 2022.

COSTA, R. S.; LEITE, F. T. Letramento digital docente e a cultura de proteção de dados na escola. *Educação e Pesquisa*, v. 48, e245897, 2022.

COSTA, Ricardo Alexandre; CUNHA, Carlos Renato. A Lei Geral de Proteção de Dados: um estudo descritivo e exploratório da sua aplicação no Brasil e no cenário internacional. Revista JurisFIB, v. 14, n. 14, 2023.

COSTA, V. G.; DE OLIVEIRA, L. C. Desafios de segurança em Internet das Coisas (IoT) no contexto da saúde 4.0. Revista de Informática Aplicada, v. 18, n. 1, p. 55-66, 2022.

DA SILVA, K. A.; BEHRENS, M. A. O professor e o uso das tecnologias digitais: a ressignificação da prática docente. Educar em Revista, v. 37, e80119, 2021.

DE ABREU, Beatriz Venâncio. A estratégia de cibersegurança nas pequenas e médias empresas pela ótica do Google Scholar entre 2020 e 2022.

DE SOUZA SILVA, André Luis; SILVA, Regina Célia Marques Freitas. Protocolo HTTP x protocolo HTTPS. Nucleus, v. 6, n. 1, p. 1-8, 2009.

DINIZ, Maria Munique S. B. S. A segurança da informação e seus pilares para a proteção de dados pessoais na perspectiva da LGPD. *Revista Eletrônica de Iniciação Científica*, Itabuna, v. 10, n. 1, p. 94-111, 2020.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 3ª ed. rev. São Paulo: Thomson Reuters Brasil, 2023.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Revista de Direito Civil Contemporâneo, v. 23, p. 11-20, 2020.

FREITAS, Suzanne de Oliveira. [R]evolução na Educação: Formação Continuada Para Professores Sobre Novas Tecnologias Digitais na Educação. 2023. Dissertação (Mestrado Profissional em Novas Tecnologias Digitais na Educação) – Centro Universitário Carioca (UniCarioca), Rio de Janeiro, 2023.

GARCIA, J. D. C. Segurança em Redes e Invasão de Sistemas. 1ª ed. São Paulo: Editora Senac São Paulo, 2021.

GARCIA, Paulo Sérgio. A Internet como nova mídia na educação. 2001.
Disponível em:
https://web.archive.org/web/20090803040447/http://www.geocities.com/Athens/Delphi/2361/intmid.htm.
Acesso em: 5 dez. 2025.

GOMES, P. C. R. Da Contracultura à Cibercultura: A história social da internet no Brasil. Rio de Janeiro: Editora FGV, 2022.

ISIDORIO, Sheila Cristhiane de Almeida. A Educação no Século XXI: Uma Análise do papel da Inspeção Escolar nos Processos de Mudança. 2021. Dissertação (Mestrado Profissional em Novas Tecnologias Digitais na Educação) – Centro Universitário Carioca (UniCarioca), Rio de Janeiro, 2021.

JUNIOR, A. O.; REGINA, T. K. A Engenharia Social e o fator humano na Segurança da Informação. In: Salão de Iniciação Científica da UNIVATES, 22., 2022, Disponível em: https://www.univates.br/sistemas/hotsite/editor/hotsite/arquivos/51/1669830573.pdf.

LIMA, Cíntia Rosa Pereira. A Lei Geral de Proteção de Dados Pessoais (LGPD) e o fortalecimento do cidadão como titular de direitos. *Revista de Direito, Governança e Novas Tecnologias*, Salvador, v. 7, n. 1, p. 1-18, 2021.

LUCAS, I. C. L.; MEIRELLES, J. L. F. A proteção de dados pessoais como vetor de confiança e desenvolvimento na sociedade da informação. Revista de Direito, Economia e Desenvolvimento Sustentável, v. 7, n. 1, p. 110-130, 2021.

MARCELINO, Nelson. Cibersegurança, Ciberdefesa e Ciberguerra: Cenários de um mundo digital e globalizado. Rio de Janeiro: Appris Editora, 2021.

MARTINS, A. C.; FONSECA, L. S. O princípio da responsabilização e prestação de contas (accountability) na LGPD e seus impactos na governança de dados. *Revista de Direito Digital e Compliance*, v. 4, n. 1, p. 78-95, 2023.

MONTEIRO, Renato Leite. Desafios para a efetivação do direito à explicação na Lei Geral de Proteção de Dados do Brasil. 2021. 385 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021.

NASCIMENTO, A. C. S.; BAPTISTA, C. S. A Lei Geral de Proteção de Dados (LGPD) e seus impactos no ambiente escolar. Revista Thema, v. 22, n. 2, p. 333-350, 2023.

OLIVEIRA, Anderson. LGPD Essencial: Dicas e Boas Práticas para a Conformidade– Volume 1. Editora Dialética, 2025.

OLIVEIRA, M. A. O tratamento de dados sensíveis em prontuários de alunos à luz da Lei Geral de Proteção de Dados. *Anais do Congresso Brasileiro de Direito Educacional*, v. 5, p. 1-15, 2021.

PINHEIRO, Patricia Peck. Direito Digital. 8ª ed. São Paulo: Saraiva Jur, 2022.
RAPÔSO, Cláudio Filipe Lima et al. Lgpd-lei geral de proteção de dados pessoais em tecnologia da informação: Revisão sistemática. RACE-Revista de Administração do Cesmac, v. 4, p. 58-67, 2019.

REIS, Sálvio Roberto Freitas et al. Desafios da LGPD quanto à privacidade em ambientes educacionais: um mapeamento sistemático. Revista de Gestão e Secretariado, v. 15, n. 3, p. e3292-e3292, 2024.

RICHARDSON, Roberto Jarry. Pesquisa social: métodos e técnicas. 3. ed. São Paulo: Atlas, 2012.

RODRIGUES, T. F.; BITTENCOURT, J. R. O tratamento de dados de crianças e adolescentes à luz da LGPD e os desafios para o setor educacional. *Cadernos de Direito e Inovação*, v. 2, n. 1, p. 112-130, 2022.

SILVA, L. A.; GOMES, J. O. O fator humano como vetor de vulnerabilidade em segurança da informação: uma revisão sistemática. *Revista de Gestão e Sistemas de Informação*, v. 11, n. 3, p. 204-220, 2022.

SLEIGH, Ana Paula de Moraes. Manual de direito digital e segurança da informação. 3ª ed. São Paulo: Thomson Reuters Brasil, 2023.

SYMANTEC CORPORATION. WannaCry ransomware attack: technical analysis. Symantec Security Response, 2017.
Disponível em: https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/wannacry-ransomware-attack. Acesso em: 5 dez. 2025.

TAKEUCHI, E. C. Fatores humanos em cibersegurança: uma revisão sistemática da literatura. Curitiba: UFPR, 2023. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) — Universidade Federal do Paraná, 2023.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2ª ed. São Paulo: Thomson Reuters Brasil, 2021.

VIEGAS, Patrícia Peixoto Carneiro; GOULART, Ilsa do Carmo Vieira. O estado da arte da produção acadêmica sobre o letramento digital na formação docente. Revista Ibero-Americana de Estudos em Educação, p. 125-145, 2020.