INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS PEDRO II
TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

ANTONIO MARCOS BEZERRA UCHÔA

SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO EM ESCOLAS DA ZONA URBANA EM UMA CIDADE NO NORTE DO PIAUÍ

PEDRO II,
PIAUÍ 2025

ANTONIO MARCOS BEZERRA UCHÔA

SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO EM ESCOLAS DA ZONA URBANA EM UMA CIDADE NO NORTE DO PIAUÍ

Trabalho de Conclusão de Curso (artigo cientí- fico) apresentado como exigência parcial para obtenção do diploma do Curso de Análise e De- senvolvimento de Sistemas do Instituto Fede- ral de Educação, Ciência e Tecnologia do Piauí, Campus Pedro II.

Orientador: Profº. Esp. Danniel Rocha do Nas- cimento.
Coorientador: Profº. Mᵉ. Marcos Soares de Oli- veira.

PEDRO II, PIAUÍ
2025

SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO EM ESCOLAS DA ZONA URBANA EM UMA CIDADE NO NORTE DO PIAUÍ

Antonio Marcos Bezerra Uchôa[1] Profº. Esp. Danniel Rocha do Nascimento[2] Profº. Mᵉ. Marcos Soares de Oliveira[3]

RESUMO

Diante do aumento das ameaças cibernéticas e da crescente sofisticação dos ataques, instituições educacionais precisam adotar certas práticas para proteger informações sensíveis. Este trabalho analisou a segurança da informação em escolas de ensino médio e fundamental da cidade de Pedro II, localizada no norte do estado do Piauí. A pesquisa foca em alguns princípios da segurança da informação e como os mesmos estão sendo tratados dentro dessas instituições. A metodologia utilizada no estudo foi a estruturada. Foram selecionadas escolas da zona urbana com base em critérios de diversidade e representatividade, utilizando uma amostragem intencional e por conveniência. A coleta de dados foi realizada por meio de dois questionários: Um direcionado aos diretores e outro aplicado aos coordenadores pedagógicos, secretários e demais colaboradores que possuem acesso a informações sensíveis. Os questionários abordaram temas relacionados à segurança da informação no âmbito escolar. A análise dos dados combinou métodos quantitativos, para questões objetivas, e qualitativos, para questões subjetivas. A pesquisa permitiu obter uma visão mais crítica das práticas de segurança da informação nas escolas participantes, identificando suas práticas e áreas que necessitam de melhorias. Buscou-se contribuir para o aprimoramento das políticas de segurança da informação no contexto educacional, promover a conformidade com legislações pertinentes e aumentar a conscientização sobre a importância da proteção de dados entre funcionários, alunos e gestores. Contudo, a postura adotada pelos gestores, aliada ao momento político das eleições municipais, impactou negativamente os trabalhos que seriam desenvolvidos nesse sentido.

Palavras-chave: segurança da informação; instituições educacionais; ameaças cibernéticas; proteção de dados; pesquisa educacional.

ABSTRACT

Given the rise in cyber threats and the increasing sophistication of attacks, educational institutions need to adopt certain practices to protect sensitive information. This study analyzed information security in elementary and high schools in the city of Pedro II, located in the northern region of the state of Piauí. The research focuses on key principles of information security and how they are being addressed within these institutions. The methodology used in this study was structured.

---

[1] Graduando em Análise e desenvolvimento de sistemas. IFPI - Campus Pedro II. marcosuchoa586@gmail.com

[2] Especialização em Pós-graduação lato sensu. ESAB. E-mail: danniel.rocha@ifpi.edu.br.

[3] Mestrado em Computação Aplicada. USP- FFCLRP. E-mail: marcos.soares@ifpi.edu.br.

Schools in urban areas were selected based on criteria of diversity and representativeness, using intentional and convenience sampling. Data collection was conducted through two questionnaires: one directed at school principals and another applied to pedagogical coordinators, secretaries, and other staff members who have access to sensitive information. The questionnaires covered topics related to information security within the school environment. Data analysis combined quantitative methods for objective questions and qualitative methods for subjective questions. The research provided a critical view of the information security practices in the participating schools, identifying both existing practices and areas that require improvement. The aim was to contribute to the enhancement of information security policies in the educational context, promote compliance with relevant legislation, and raise awareness among staff, students, and administrators about the importance of data protection. However, the stance adopted by school administrators, along with the political climate of the municipal elections, negatively impacted the efforts that were to be developed in this regard.
keywords: information security; educational institutions; cyber threats; data Protection; Educati- onal Research; Security Challenges; Data Protection.

Data de aprovação: 27 de Fevereiro de 2025

1 INTRODUÇÃO

A segurança da informação envolve um conjunto de medidas planejadas para gerenciar e prevenir riscos relacionados ao roubo, dano e perda de dados, dispositivos, servidores, sistemas e redes (Otten, 2023). Seu objetivo é detectar, documentar e enfrentar as ameaças que podem surgir ao longo do ciclo de vida das informações. De acordo com Prummer *et al.* (2024), com o desenvolvimento tecnológico e a ampliação da digitalização nas escolas, a segurança da informação tornou-se uma questão de grande importância para as instituições educacionais.

Conforme indicado por Bezerra (2023), a adoção de sistemas digitais e o uso de plataformas online para administração acadêmica, comunicação e armazenamento de dados aumentaram a vulnerabilidade das informações a vários riscos cibernéticos. Mackievicz (2022), observa que, na prática, a segurança da informação escolar envolve as técnicas realizadas em instituições de ensino, para garantir a proteção dos dados, evitar a perda e manipulação de documentos e assegurar que eles sejam acessados apenas por pessoas previamente autorizadas. Assim, além de administrar a preservação dos dados, as escolas também precisam proteger essas informações, a fim de evitar vazamentos, garantir a privacidade dos alunos e cumprir com as normativas legais relacionadas à segurança das mesmas.

Dentro da segurança da informação, é necessário que sejam seguidas algumas regras

ou princípios para garantir uma proteção eficiente. Como apontado por Neves *et al.* (2021), a implementação de políticas de segurança da informação, aliada à utilização de tecnologias adequadas e ao treinamento constante dos colaboradores são formas fundamentais de mitigação de riscos e busca pela privacidade e conformidade com as exigências legais.

Além das soluções tecnológicas, a segurança da informação nas escolas depende da conscientização e capacitação de gestores, professores e colaboradores. De acordo com Santos *et al.* (2021) boas práticas, como o uso de senhas seguras, controle de acessos e políticas de backup, são fundamentais para reduzir riscos e proteger os dados institucionais. Assim, mais do que uma necessidade técnica, a proteção das informações educacionais torna-se um compromisso essencial para a integridade e confiabilidade do ambiente escolar.

Este trabalho busca conhecer e analisar a realidade da Segurança da Informação de algumas escolas, municipais e estaduais, da zona urbana de uma cidade no norte do estado do Piauí, mais precisamente no município de Pedro II. Foram ponderadas as práticas implementadas para a proteção das informações e o entendimento dos participantes da pesquisa sobre segurança da informação, levando em consideração alguns princípios que foram citados previamente e que serão trazidos para o âmbito escolar e abordados mais intensamente ao decorrer deste trabalho.

1.1 OBJETIVOS

1.1.1 Objetivo geral

Esta pesquisa visou conhecer e analisar as práticas de Segurança da Informação de es- colas públicas, o conhecimento sobre segurança da informação no contexto escolar, comparando as práticas observadas com os pilares fundamentais da segurança da informação, trazidos para o âmbito escolar, a fim de identificar lacunas e propor melhorias para garantir a proteção de dados sensíveis nas escolas.

1.1.2 Objetivos específicos

1. Reconhecer o tema de segurança da informação no âmbito escolar.

2. Coletar dados sobre atitude e comportamento dos gestores escolares e seus colaboradoresquanto a Segurança da Informação.

3. Buscar *insights* nos dados obtidos por meio de formulários realizados com os participantes.

4. Comparar os resultados com os princípios da segurança da informação trazidos para o âmbito educacional.

5. Propor melhorias para a gestão de Segurança da Informação das instituições investigadas.

A presente pesquisa está organizada da seguinte maneira. A Seção 2 apresenta um panorama teórico, estudos e trabalhos anteriores relevantes, definições e conceitos importantes acerca da segurança da informação e seu contexto em escolas, leis e normas que devem ser adotadas para uma segurança mais robusta e os principais tipos de ataques realizados. A Seção 3 investiga a realidade das escolas estaduais em relação à segurança da informação, por meio da aplicação de um formulário com os diretores e os funcionários que possuem acesso a dados sensíveis das escolas. Os resultados da pesquisa feita nas escolas, análise crítica dos resultados comparando com os princípios da segurança da informação e sugestões de mecanismos para que o resultado obtido seja melhorado estão descritos na Seção 4. Por fim, a Seção 5 trata das conclusões obtidas por meio deste trabalho de conclusão de curso.

2 FUNDAMENTAÇÃO TEÓRICA

Esta seção apresenta conceitos relevantes para a compreensão deste projeto de pesquisa, como a história da segurança da informação, os conceitos que a envolvem, o contexto da segurança da informação na educação, os princípios fundamentais, as principais ameaças à segurança da informação em escolas, leis e normas que a regem, além de trabalhos relacionados ao tema. O objetivo é oferecer uma visão panorâmica do conteúdo utilizado neste trabalho.

2.1 SEGURANÇA DA INFORMAÇÃO

A informação sempre foi algo de grande relevância, tanto pelo que guarda quanto pelo que pode gerar, como visto em Coadic (2004). A segurança da informação está presente desde os primórdios da computação. Entre os anos de 1950 e 1969, surgiram os primeiros

computadores e dados digitais, marcando o início da segurança da informação. Contudo, foi apenas entre 1970 e 1980 que a segurança da informação foi consolidada e formalizada, com o surgimento dos primeiros padrões de segurança, como o *Data Encryption Standard* (NIST, 2001).

A partir de 2010, houve uma intensificação na proteção avançada e na resposta a inci- dentes, marcada pelo uso de tecnologias como criptografia avançada, autenticação multifatorial e inteligência artificial para detectar e responder a ameaças. Eventos de alto impacto, como o ataque de *ransomware WannaCry* em 2017, chamaram a atenção para a importância da segurança da informação. De acordo com Latto (2020), mais de 230.000 computadores com *Windows* foram infectados em 150 países em um único dia, afetando agências governamentais e hospitais.

Ao longo do tempo, a segurança da informação foi aplicada a diversos campos, mas, para que seja eficaz, é essencial seguir boas práticas. A implementação de boas práticas como o uso de senhas fortes, a atualização regular de software, a análise de links suspeitos e a ativação da autenticação multifatorial são passos básicos para melhorar a segurança online (Estados Unidos, 2021).

A segurança da informação busca proteger dados e sistemas contra ameaças e vul- nerabilidades. Conforme indicado por Alkhudhayr *et al.* (2019), seus pilares fundamentais podem ser resumidos em quatro princípios principais : O primeiro sendo a **Con- fidencialidade**, que protege as informações para que somente pessoas autorizadas possam acessá-las, utilizando técnicas como criptografia e controle de acesso, ponto que também é reforçado por Conceição (2019). O segundo , **Integridade**, garante que os dados não sejam alterados de forma não autorizada, empregando mecanismos como checksums e assinaturas digitais, sendo abordado também por Coutinho *et al.* (2017). O terceiro trata-se da **Disponibilidade**, onde ela age assegurando que as informações estejam acessíveis para usuários autorizados sempre que necessário, por meio de sistemas de backup e redundância, garantindo uma resposta eficaz e em tempo hábil, Sousa *et al.* (2020) também destaca a importância desse princípio. O último pilar se trata da **Autenticidade**, que valida a identidade de usuários autorizados por meio de senhas, logins e autenticação biométrica, prote- gendo contra fraudes e acessos não autorizados (Oliveira; Filgueiras, 2022).

2.1.1 Princípios da segurança da informação

Dentre os diversos livros e artigos sobre Segurança da Informação, *Computer*

Security: Principles and Practice (Stallings; Brown, 2014), trata de práticas e princípios, com base em quatro pilares: Confidencialidade, Integridade, Disponibilidade e Autenticidade, apresentados anteriormente e estão detalhados resumidamente na Tabela 1 (Princípios básicos da segurança da informação):

Tabela 1 – Princípios básicos da segurança da informação.

Princípio	**Definição**	**Objetivo**
Confidencialidade	Garante que as informações sejam acessadas apenas por pessoas autorizadas.	Evitar que dados sensíveis, como informações pessoais ou financeiras, sejam divulgados a pessoas não autorizadas.
Integridade	Assegura que as informações não sejam alteradas de maneira não autorizada, acidental ou maliciosa.	Garantir que os dados sejam confiáveis e precisos.
Disponibilidade	Garante que as informações e os sistemas estejam disponíveis sempre que necessário.	Minimizar interrupções no acesso às informações ou serviços.
Autenticidade	Assegura que os usuários ou sistemas sejam quem dizem ser.	Evitar acesso não autorizado por indivíduos ou sistemas falsos. .

Fonte: Elaborado pelo autor.

É importante ressaltar que o livro de Stallings e brown (2014) possui outras edições. No entanto, a escolha da 3ª edição para esta pesquisa se deve ao fato de que ela se encaixa melhor no tema central do trabalho. Essa edição apresenta os quatro princípios fundamentais da segurança da informação de maneira mais adaptável ao contexto educacional, proporcionando uma abordagem mais clara e estruturada para aplicação nas instituições de ensino. Além disso, a organização dos conteúdos e a forma didática como os autores exploram esses princípios facilitaram a compreensão e análise crítica do tema.

Os princípios apresentados por Stallings e brown (2014), representam os fundamentos essenciais para a implementação eficaz da segurança da informação. No contexto educacional, esses princípios se desdobram em aspectos específicos que demandam atenção, como a proteção dos dados de alunos e funcionários, o controle de acesso a registros acadêmicos e administrativos, a segurança no uso de dispositivos compartilhados e a capacitação contínua de professores e colaboradores para práticas seguras no ambiente escolar. Esses pontos, juntamente com outros fatores relevantes, serão explorados no tópico seguinte.

2.2 CONTEXTO DE SEGURANÇA DA INFORMAÇÃO NA EDUCAÇÃO

No contexto educacional, o avanço da digitalização e o uso crescente das Tecnologias da Informação e Comunicação transformaram significativamente a gestão e o acesso às informações. Com essa evolução, a segurança da informação tornou-se uma preocupação essencial, especialmente diante do aumento da dependência de plataformas digitais para ensino, administração e armazenamento de dados sensíveis. Ao longo dos últimos anos, e de forma acentuada na atualidade, as instituições educacionais enfrentam desafios cada vez mais complexos para proteger os dados de alunos, docentes e funcionários administrativos, garantindo, ao mesmo tempo, acessibilidade, privacidade e a continuidade segura das operações escolares.

Para garantir a segurança da informação no ambiente escolar, é fundamental considerar alguns princípios essenciais. Esses princípios foram formulados com base nos quatro pilares da segurança da informação, conforme apresentados por Stallings e brown (2014), e citados na Tabela 1 - Princípios básicos da segurança da informação, sendo representados a seguir.

- Conhecimento e Capacitação em Segurança da Informação;
- Políticas e Procedimentos de Segurança;
- Acesso e Controle de Informações;
- Uso e Compartilhamento de Dispositivos e Senhas;
- Práticas de Segurança no Dia a Dia;
- Incidentes de Segurança e Conscientização.

2.2.1 Conhecimento e Capacitação em Segurança da Informação

Um ponto importante a ser levado em consideração quando se trata da segurança da informação dentro do âmbito escolar e em lugares como órgãos importantes, empresas ou qualquer outro tipo de meio que trate de informações sigilosas, é o conhecimento e a capacitação

dos colaboradores/envolvidos em cargos de importância. Soares e Silva (2019),

observam que no âmbito escolar, funcionários possuem o acesso pleno a informações sigilosas, como dados de alunos, dados de professores, entre outros, que tramitam entre a direção da escolas e os setores ligados a ela.

2.2.2 Políticas e Procedimentos de Segurança

Segundo o manual desenvolvido pelo Ministério da Gestão e da Inovação em Serviços Públicos (Brasil, 2024), tal política tem como objetivo assegurar a proteção das informações, garantindo sua confidencialidade, integridade e disponibilidade. Além disso, busca promover o uso apropriado desses dados, minimizar riscos relacionados à segurança da informação e garantir a conformidade com a Lei Geral de Proteção de Dados Pessoais (2018) e demais regulamentações aplicáveis.

2.2.3 Acesso e Controle de Informações

Sfredd e Flores (2009), sugerem que o controle de acesso protege as informações sensíveis, cumpre regulamentações, previne ameaças internas e externas, garante a integridade e confidencialidade dos dados e busca facilitar auditorias e reduzir custos com os incidentes de segurança. No âmbito educacional, o controle de acesso protege não só dados de alunos e professores, mas dados sensíveis de forma geral, garantindo a segurança de sistemas e plataformas, preservando a privacidade, controlando o acesso físico a instalações e permite o rastreamento de atividades, contribuindo assim para um ambiente acadêmico seguro e eficiente.

2.2.4 Uso e Compartilhamento de Dispositivos e Senhas

O uso e compartilhamento de dispositivos e senhas no ambiente educacional representa riscos como vazamento de dados, acessos não autorizados e ataques cibernéticos, comprometendo a segurança e a privacidade de informações sensíveis. Sousa *et al.* (2020) ressaltam que para mitigar esses problemas, é fundamental implementar políticas claras, educação digital, uso de ferramentas como gerenciadores de senhas e autenticação multifator, além de auditorias regulares.

2.2.5 Práticas de Segurança no Dia a Dia

Ações diárias são necessárias para garantir a proteção das informações, seja

verificando e-mails suspeitos, armazenando documentos de forma segura ou em outro tipo de ação. É importante destacar que essas simples práticas cotidianas podem diminuir consideravelmente os riscos à segurança. Adotar essas práticas no contexto escolar contribui para a formação de uma cultura de segurança constante, protegendo dados sensíveis e aprimorando a prevenção contra ataques, como ressaltado no manual feito pela Secretaria da Educação, Governo do Estado do Espírito Santo (2024).

2.2.6 Incidentes de Segurança e Conscientização

Incidentes de segurança são imprevisíveis e podem ocorrer rapidamente e o processo de identificar, responder e prevenir incidentes de segurança é importante no quesito de segurança da informação. De acordo com Marinho e Bodê (2022), é fundamental que haja conscientização sobre as ameaças e protocolos bem definidos para lidar com essas situações, a fim de proteger os dados. Respostas rápidas a incidentes ajudam a minimizar os danos e a assegurar que as ações corretivas sejam tomadas. A conscientização dos funcionários é vital para identificar potenciais problemas antes que eles se materializem, como enfatizado por Kanagusku e Gaseta (2023).

2.3 LEIS E NORMAS DA SEGURANÇA DA INFORMAÇÃO

Garantir a segurança da informação é essencial para que não haja incidentes que acabem acarretando o mau uso das informações de indivíduos. Para reforçar a privacidade de dados, leis estão dispostas no sentido de nortear como se deve aplicar a segurança da informação. A Lei Geral de Proteção de Dados nº 13.709/2018 (2018) dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. No âmbito educacional, esta lei regula o tratamento de dados pessoais, incluindo os dados de estudantes, funcionários e colaboradores em instituições educacionais.

Conhecida como Marco Civil da Internet, a Lei nº 12.965/2014 (BRASIL, 2014) estabelece princípios, direitos e deveres para o uso da internet no Brasil. Quando aplicada ao âmbito educacional, visa assegurar a proteção dos dados pessoais dos alunos. Ela exige que as instituições de ensino obtenham consentimento explícito para a coleta e uso de informações, além de garantir a confidencialidade das comunicações. As escolas devem adotar políticas claras para o uso da internet, manter registros de acesso e promover a educação sobre segurança online. Dessa forma, a lei contribui para um ambiente digital mais

seguro e transparente, equilibrando o avanço tecnológico com a proteção dos direitos dos alunos.

Segundo a Associação Brasileira de Normas Técnicas (2013), a ABNT NBR ISO/IEC 27001 estabelece os requisitos para um Sistema de Gestão de Segurança da Informação, com ênfase na proteção da confidencialidade, integridade e disponibilidade das informações. A norma propõe um modelo estruturado para identificação, avaliação e tratamento de riscos, envolvendo planejamento, execução, monitoramento e melhoria contínua, o que evidencia a necessidade de as escolas implementarem políticas claras de proteção de dados, controle de acesso às informações e resposta a incidentes de segurança.

2.4 AMEAÇAS DENTRO DA SEGURANÇA DA INFORMAÇÃO

Ameaças são sempre um fator a ser considerado quando se trata de segurança da informação, como apresentado por Otten (2023). Não seria diferente nas instituições de ensino, onde grandes acervos de informações são mantidos, tornando-se assim um grande atrativo para possíveis tentativas de fraudes relacionadas a esses dados. Nesse contexto, é possível categorizar algumas das principais ameaças que afetam a segurança da informação neste ambiente, como destacado por (Castanho, 2023), sendo melhor exemplificado na Tabela 2 - Duas das principais ameaças à segurança da informação, medidas de proteção e referências.

Tabela 2 – Duas das principais ameaças à segurança da informação, medidas de proteção e referências.

Tipo de Ameaça	Descrição	Medidas de Proteção	Referências
Ransomware	É um tipo de software malicioso que, ao infectar um computador ou uma rede, criptografa arquivos e dados, impedindo o acesso dos usuários até que um resgate seja pago ao criminoso responsável.	– Realizar backups frequentes dos dados importantes. – Manter o software de segurança atualizado. – Adotar autenticação robusta. – Treinar os usuários sobre práticas seguras e perigos de acessar conteúdos nocivos.	(FORNASIER; SPINATO; RIBEIRO, 2020); (SILVA, 2023)

Phishing	É uma fraude digital que usa manipulação psicológica para obter informações pessoais ou financeiras, frequentemente através de mensagens falsas que imitam instituições confiáveis, como bancos ou empresas de tecnologia.	– Implementar técnicas de detecção e mitigação aprimoradas. – Realizar pesquisas contínuas sobre a área. – Educar os usuários para reconhecer e evitar mensagens fraudulentas.	(SILVEIRA; REALAN; AMARAL, 2016); (MONTAGNER; WESTPHALL, 2022); (GUPTA; THAKRAL; CHOUDHURY, 2018)

Fonte: Elaborado pelo autor.

2.5 TRABALHOS RELACIONADOS

A segurança da informação é um tema que exige constante atenção, pois, apesar dos avanços nessa área, os tipos de ataques vêm se tornando cada vez mais sofisticados. Com o intuito de proporcionar uma visão mais ampla sobre o tema deste artigo, reunimos alguns trabalhos relacionados. A importância da segurança da informação nas organizações, desta- cando a necessidade de proteger dados contra ameaças e vulnerabilidades, além de classificar e priorizar informações críticas (Silva *et al.*, 2021). Souza *et al.* (2020), busca analisar a segurança da informação na gestão de riscos da governança de tecnologia da informação em instituições educacionais, enfatizando a importância de políticas, procedimentos e da organização de segurança para proteger os ativos e mitigar riscos. Sousa (2023), aponta a necessidade de implementar políticas de segurança da informação em instituições públicas municipais para proteger a integridade, confiabilidade e disponibilidade dos dados, especialmente diante do aumento dos incidentes de segurança.

Este trabalho buscou-se responder a questões sobre como a segurança da informação é tratada nos contextos educacionais, como se dá a compreensão dos participantes sobre o tema, os mecanismos utilizados para proteção de informações, o cumprimento de leis e normas, entre outras questões. A inovação deste projeto reside em apontar mecanismos que possam aumentar a segurança das informações armazenadas no acervo dessas escolas, reforçando a importância de seguir as leis e normas estabelecidas no campo da segurança da informação, garantindo maior integridade no armazenamento desses dados. A proposta deste artigo é proporcionar uma análise crítica com foco em possíveis melhorias, fazendo um comparação com os princípios da segurança da informação trazidas ao âmbito

educacional, além de explorar alternativas viáveis para a implementação de escolas mais seguras.

3 METODOLOGIA

Esta pesquisa visou analisar a segurança da informação em escolas da zona urbana situadas em na cidade de Pedro II, cidade que fica situada no norte do estado do Piauí. O estudo foi conduzido em instituições de ensino, a níveis municipais e estaduais, e a metodologia adotada foi estruturada para garantir uma análise crítica e abrangente das práticas, desafios e oportunidades relacionados à segurança da informação nas escolas selecionadas, fazendo um comparação com os princípios da segurança da informação no âmbito educacional. Foram levados em consideração alguns pontos para analisar a segurança da informação, que foram formulados a partir de princípios já abordados na seção anterior, sendo mostrados a seguir, de acordo com a Tabela 3 - Princípios levados em consideração no desenvolvimento dos formulários e na comparação dos resultados.

Foram desenvolvidos 2(dois) formulários para a pesquisa, um para os colaboradores(funcionários que têm acesso a informações sigilosas na escola) e outro para os respectivos diretores. Os princípios destacados a cima foram utilizados como base para a formulação de perguntas para os formulários e posteriormente para a comparação com os resultados obtidos, afim de obter um panorama sobre a segurança da informação nas escolas. A seguir, detalhamos a metodologia empregada no estudo.

Tabela 3 – Princípios levados em consideração no desenvolvimento dos formulários e na compa- ração dos resultados.

Princípios	**Definições**
Conhecimento e Capacitação em Segurança da Informação	Observar o nível de importância que o entrevistados atribuem à segurança da informação e como ela é priorizada.
Políticas e Procedimentos de Segurança	Entender as práticas de proteção de dados, desde o armazenamento até o compartilhamento.
Acesso e Controle de Informações	Identificar como o acesso às informações é controlado e quem tem responsabilidade sobre isso.

Uso e Compartilhamento de Dispositivos e Senhas	Compreender se a escola possui políticas formais de segurança e como elas são implementadas.
Práticas de Segurança no Dia a Dia	Identificar os desafios e as dificuldades percebidas pelos diretores na implementação de medidas de segurança.
Incidentes de Segurança e Conscientização	Obter informações sobre incidentes e a resposta da escola a eles.
Sugestões de Melhorias	Explorar quais recursos e treinamentos são oferecidos para segurança da informação.

Fonte: Elaborado pelo autor.

3.1 DELIMITAÇÃO DO ESTUDO

O estudo foi realizado em escolas estaduais de ensino médio e escolas municipais de ensino fundamental. A escolha de escolas que ficam na zona urbana visa uma maior concentração de recursos e infraestrutura tecnológica, o que pode impactar e influenciar significativamente as práticas de segurança da informação. A pesquisa buscou envolver o máximo de escolas possíveis, visando conseguirmos uma amostra com mais relevância, para possuirmos resultados mais precisos.

Inicialmente conseguiu-se contato com 9 escolas, que acenaram positivamente para colaborar com a pesquisa, porém foram diretores de 6 escolas e colaboradores de 3 escolas que participaram de fato da pesquisa.

3.2 TIPO DE PESQUISA

Conforme Nunes *et al.* (2016), a pesquisa descritiva tem como propósito observar, registrar e analisar características ou variáveis de um fenômeno sem intervir diretamente. Esse tipo de estudo busca descrever situações ou processos de forma detalhada, geralmente utilizando ferramentas como questionários. A presente pesquisa apresenta caráter descritivo oferecendo *insights* sobre o contexto abordado, combinando abordagens quantitativas e qualitativas para enriquecer a análise, descrever características, práticas e percepções relacionadas à segurança da informação nas escolas que aceitaram participar da pesquisa, fazendo também uma comparação dos pontos citados com os princípios da segurança da

informação.

Foram introduzidas perguntas objetivas e subjetivas, buscando coletar dados numéricos e também informações mais interpretativas e contextuais. De acordo com Santos *et al.* (2017), a combinação desses tipos de dados traz uma visão abrangente e detalhada sobre o conteúdo abordado, contribuindo para compreender as práticas e percepções dos diretores e colaboradores das escolas em relação à segurança da informação.

3.3 ETAPAS DA PESQUISA

A pesquisa foi feita em 3 etapas, se tratando da aplicação de questionários, da análise dos resultados e da comparação dos resultados, como mostrado na tabela a seguir:

Tabela 4 – Etapas da pesquisa

Etapas da pesquisa	**Definições**	**Período das etapas**
Aplicação de questionários	Coletar dados dos participantes afim de se obter uma linha de base, para assim ter um panorama de como está a segurança da informação nas escolas	Ocorreu em 14(quatorze) dias
Análise dos resultados	Fazer um estudo em cima das respostas obtidas através dos formulários aplicados a os participantes	Ocorreu em 12(doze) dias
Comparação dos resultados	Comparar os resultados obtidos com os formulário com os princípios da segurança da informação	Ocorreu em 13(treze) dias

Fonte: Elaborado pelo autor.

3.4 COLETA DE DADOS

A coleta de dados se deu através de formulários online, sendo utilizada a ferramenta *Google Forms* (Google, 2025) para a criar e gerenciar todo o processo, eles foram aplicados junto aos participantes da pesquisa, um para diretores e outro para os colaboradores das escolas em questão.

3.4.1 Amostragem

A pesquisa utilizou a amostragem intencional, que como observado por Sargi *et al.* (2024), o pesquisador escolhe os participantes de forma deliberada, levando em consideração características específicas que são fundamentais para o objetivo do estudo. A técnica foi usada para selecionar os participantes, sendo aplicada para incluir diretores e colaboradores que possuem acesso direto e contínuo às informações sensíveis das escolas, como secretários e coordenadores pedagógicos(se houverem), por serem diretamente relevantes para os objetivos do estudo.

Também foi utilizada a amostragem por conveniência, que, com base no estudo de Etikan *et al.* (2016), os participantes são escolhidos com base em fatores práticos, como estarem facilmente acessíveis ou disponíveis no momento da pesquisa. A técnica foi usada para selecionar as escolas que estavam disponíveis e dispostas a participar da pesquisa. Essa abordagem mista permitiu uma maior flexibilidade na coleta de dados, mantendo o foco nos objetivos centrais do estudo.

3.4.2 Questionários

O formulário dos diretores continha 30 questões, 6 delas sendo objetivas, abordando questionamentos mais diretos em relação a o entrevistado como conhecimento do mesmo a cerca da segurança da informação, treinamento ou capacitação do entrevistado sobre segurança da informação, consentimento em participar da pesquisa, mecanismos utilizados pela escola para limitação do acesso a informações sensíveis a os funcionários. 24 das 30 eram subjetivas, contendo questões que tratavam de temas como questões pessoais sobre o entrevistado, relação dos funcionários com a segurança da informação dentro da escola, procedimentos que a escola possui para garantir a segurança da informação, definição do acesso a informações sensíveis, gerenciamento do uso dos dispositivos das escolas, orientação da escola aos funcionários, com- prometimento dos funcionários com a segurança da informação, protocolos para lidar com incidentes, conscientização dos funcionários sobre a segurança da informação, dificuldades en- frentadas, projetos futuros para fortalecer as práticas de segurança da informação, consentimento sobre está pesquisa e outros pontos relevantes sobre a segurança da informação nas escolas.

O formulário dos colaboradores continha 26 questões, 5 delas sendo subjetivas,

abor- dando assuntos como questões pessoais e sugestões de melhorias. 20 das 26 questões eram objetivas, abordando assuntos como o conhecimento do entrevistado a cerca da segurança da informação, se ele já recebeu alguma capacitação sobre segurança da informação, identificação de dados sensíveis, tipo de informações acessadas, compartilhamento do dispositivo de trabalho, compartilhamento de senhas, verificação de links e e-mails suspeitos, práticas recomendadas, procedência no caso de um problema na segurança da informação da escola, nível de conscien- tização na escola, consentimento em participar da pesquisa e outros pontos relevantes sobre a segurança da informação em instituições de ensino. A seguir se encontram os apêndices dos respectivos formulários.

1. **Apêndice A - Formulário utilizado com os diretores**

2. **Apêndice B - Formulário utilizado com os colaboradores**

3.5 ANÁLISE DE DADOS

A análise dos dados foi realizada utilizando técnicas quantitativas e qualitativas de avaliação:

- **Análise Quantitativa:** Os questionamentos dos formulários que utilizavam perguntas objetivas foram analisados estatisticamente para identificar padrões na segurança da infor- mação por parte dos entrevistados e correlacionar práticas de segurança com a ocorrência de incidentes de segurança.
- **Análise Qualitativa:** Os questionamentos dos formulários que utilizavam perguntas subjetivas foram analisadas por meio de uma análise de textual. Buscou-se encontrar padrões nas respostas com o objetivo de identificar temas recorrentes a serem tratados e padrões nas procedimentos práticas de segurança.

3.6 COMPARAÇÃO DOS RESULTADOS

Buscou-se compreender as percepções dos participantes em relação aos princípios definidos previamente, conforme apresentado na Tabela 3 - Princípios levados em consideração no desenvolvimento dos formulários e na comparação dos resultados

No que se refere a **Conhecimento e Capacitação**, investigou-se a presença de

políticas de segurança e a existência de treinamentos voltados para a segurança da informação. Em **Políticas e Procedimentos**, analisou-se o nível de controle e a responsabilidade atribuída ao acesso às informações dentro das escolas. Já em **Acesso e Controle**, a pesquisa examinou as práticas adotadas para o armazenamento e o compartilhamento de dados.

Quanto ao **Uso e Compartilhamento de Dispositivos e Senhas**, avaliou-se a disponibilidade de recursos, a segurança no uso de dispositivos institucionais e pessoais, além da existência de treinamentos sobre boas práticas. No aspecto **Práticas no Dia a Dia**, verificou-se como as escolas lidam com incidentes de segurança e quais medidas são adotadas para minimizar riscos. No tópico **Incidentes e Conscientização**, identificaram-se os desafios percebidos pelos diretores em relação à implementação de uma cultura de segurança da informação.

Por fim, em **Sugestões de Melhorias**, analisou-se a importância dada à segurança da informação pelas escolas e a priorização de medidas para aprimorar a proteção dos dados. Essa comparação permitiu identificar pontos de convergência e divergência dos grupos com os princí- pios abordados, fornecendo uma visão mais ampla sobre as práticas, desafios e oportunidades na gestão da segurança da informação nas instituições analisadas.

3.7 ÉTICA

Conforme discutido por Del-Masso *et al.* (2011), o compromisso ético vai além do cumprimento de normas, envolvendo o rigor metodológico e a responsabilidade social do pesquisador. Essa abordagem reforça a importância de garantir a confidencialidade dos dados e o consentimento esclarecido como práticas fundamentais durante a realização de pesquisas científicas.

Neste trabalho, os princípios éticos foram seguidos, garantindo o anonimato e a confi- dencialidade dos dados, tanto das escolas quanto dos participantes. Questões como localização exata das escolas, dados pessoais dos participantes e entre outros pontos que envolvam informa- ções dos participantes serão mantidos em sigilo. O consentimento de participação informado foi obtido de todos os participantes desta pesquisa, sendo necessária confirmação do termo de aceite imposto nos formulários respondidos pelos mesmos.

3.8 LIMITAÇÕES DO ESTUDO

A presente pesquisa apresenta algumas limitações que devem ser consideradas. A utilização de uma amostragem intencional e conveniência pode restringir a representatividade dos participantes, refletindo as percepções de um grupo específico e dificultando a generalização das conclusões para todas as escolas. Além disso, o foco geográfico nas escolas municipais de Pedro II, PI, limita a aplicabilidade dos resultados a outras localidades com diferentes contextos sociais, econômicos e tecnológicos.

Outro aspecto relevante é a sensibilidade do tema, que pode gerar resistência ou relutân- cia por parte dos participantes em fornecer informações completas ou precisas, resultando em possíveis vieses nas respostas. As restrições de tempo, que são comuns em trabalhos acadêmicos, também podem impactar o escopo do estudo, dificultando a ampliação da coleta de dados.

Os formulários usados como instrumento de coleta podem não capturar todos os detalhes do problema, especialmente se houver dificuldades de compreensão por parte dos participantes, o que pode comprometer a profundidade e a qualidade das informações coletadas. Além disso, o nível de conhecimento dos participantes sobre segurança da informação pode variar significativamente, dificultando a identificação de tendências claras. Por fim, a pesquisa depende da participação voluntária, o que pode excluir percepções importantes de pessoas que, por falta de interesse ou disponibilidade, não participam.

Para tentar mitigar as limitações, a pesquisa incluiu participantes de diferentes perfis dentro do ambiente escolar, buscando maior representatividade. Para incentivar respostas hones- tas sobre um tema sensível, garantiu-se o anonimato e aplicou-se um tom ético na abordagem. Os formulários foram elaborados com linguagem acessível e exemplos práticos para facilitar a compreensão. Além disso, foram feitas ações de conscientização para engajar mais participantes, reduzindo o risco de viés na amostra.

É importante enaltecer que a metodologia da pesquisa seria realizada em 3 etapas, consistindo nos seguintes passos: Coleta de dados, Aplicação de um pequeno minicurso (formato de vídeo-aula) e posteriormente um novo formulário com perguntas equiparadas ao aplicado na primeira etapa. Infelizmente não houve adesão por parte dos participantes para as etapas posteriores à tempo da execução conforme o cronograma estabelecido. Tendo sido necessário outra metodologia para a pesquisa, como descrito nos tópicos anteriores.

Contudo, ainda mantemos a hipótese de que a adoção dessa proposta metodológica inicial teria proporcionado resultados importantes. Dessa forma, os conteúdos que seriam

abordados no curso introdutório sobre segurança da informação estão disponíveis no **Apêndice C**, se tratando da ementa elaborada para o minicurso.

4 RESULTADOS

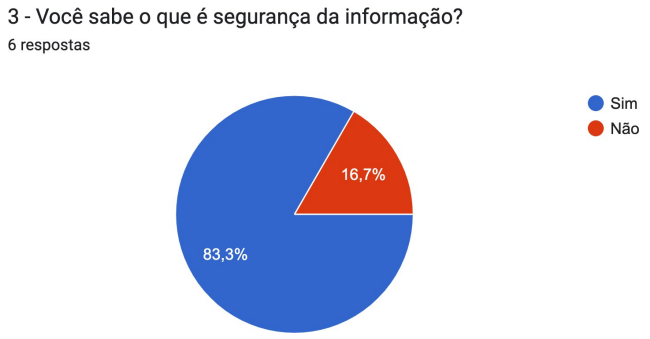
Para uma melhor compreensão dos resultados, quando houver uma referência a uma questão dos formulários ela será abreviada, como no exemplo a seguir: "Questão 01"passará a ser "Q1"e assim por diante.

As escolas da zona urbana do município de Pedro II têm em média 3 a 5 funcionários que possuem acesso informações tratadas como sigilosas ou comprometedoras e 1 diretor em cada escola. Obtivemos 6 respostas de diretores, das respectivas 6 escolas e 5 respostas de colaboradores das respectivas 3 escolas. Com base nas respostas obtidas conseguimos os seguintes resultados dispostos de forma separada a seguir.

4.1 DIRETORES

Os diretores, em sua maioria, afirmam saber o que é a segurança da informação, de acordo com as repostas da Q3, apresentadas na Figura 1 - ***Q03 - Formulário dos Diretores***. Tam- bém demonstram ter uma compreensão básica sobre o tema, mencionando em suas respostas há Q4, onde dissertaram algumas palavras-chave relacionadas ao tema de segurança da informação.

Figura 1 – ***Q03 - Formulário dos Diretores***



Fonte: Elaborado pelo autor.

No entanto, nenhum dos diretores recebeu treinamento ou algum tipo de

capacitação sobre o assunto, e não há nenhum programa de atualização contínua para os funcionários em relação à segurança da informação nas escolas, como mostrado nas receptivas respostas da Q5, dispostas na Figura 2 - ***Q05 - Formulário dos Diretores*** e Q10.

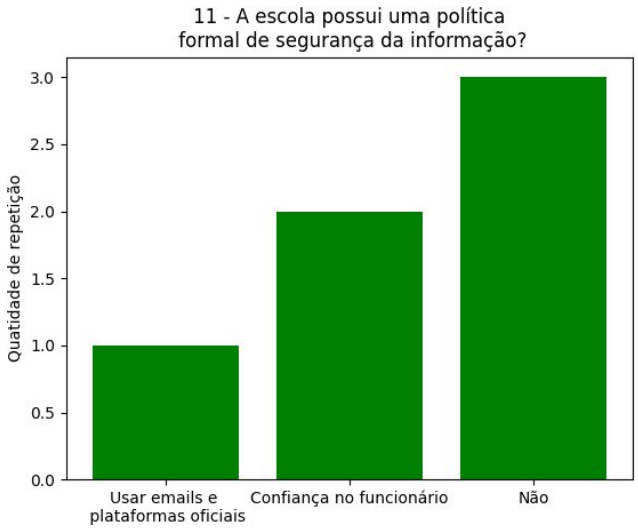
A pesquisa identificou que não existe um regimento específico a ser seguido pelos colaboradores, o que reflete um excesso de confiança por parte de alguns diretores na capacidade

Figura 2 – ***Q05 - Formulário dos Diretores***

Fonte: Elaborado pelo autor.

dos funcionários para lidar com questões de segurança, como visto pelos resultados da Q11, mostrados na Figura 3 – ***Q11 - Formulário dos Diretores***

Figura 3 – ***Q11 - Formulário dos Diretores***



Fonte: Elaborado pelo autor.

Os procedimentos de segurança adotados nas escolas limitam-se principalmente ao uso de senhas, sem políticas ou práticas mais robustas, de acordo com a respostas da Q12. A percepção geral entre os entre os diretores que participaram da pesquisa é de que as políticas e procedimentos de segurança não estão sendo adequadamente seguidos, como apontado pela respostas da Q13. De acordo com as repostas da Q14, a definição de quem tem acesso a quais informações é determinada diretamente pelos cargos dos funcionários, com a gestão da escola decidindo quem pode acessar dados sensíveis. Na Q16, houve apenas um relato de acesso não autorizado aos dados, no qual alguns professores tiveram acesso ao e-mail da escola, o que aumentou o risco de vazamento de informações.

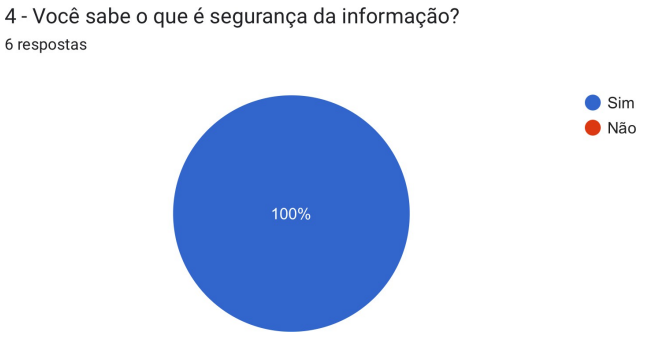
De acordo com a repostas Q17, não há uma política bem definida, o que reflete a falta de um protocolo claro sobre como os dispositivos devem ser utilizados e gerenciados. O compartilhamento de senhas é um ponto crítico, com a confiança nos funcionários se destacando como uma das principais vulnerabilidades encontradas nas escolas, sendo notado nas respostas da Q18. O uso de dispositivos pessoais pelos funcionários dentro da instituição foi pouco constatado.

A segurança da informação no dia a dia das escolas é garantida de forma limitada, principalmente através do uso de senhas e algumas orientações informais, como analisado nas respostas da Q20. No entanto, não há orientações sobre o armazenamento seguro de dados, o que evidência o despreparo tanto dos funcionários quanto das coordenações das escolas para lidar com essas questões, ao ser constatado nas respostas da Q21. Além disso, não existem protocolos estabelecidos para tratar incidentes de segurança, deixando as escolas sem um rumo claro a seguir em caso de ataques.

4.2 COLABORADORES

Os colaboradores afirmaram saber o que é segurança da informação, mas relataram não ter recebido capacitação ou treinamento específico sobre o tema, o que da entender uma certa contradição ou um conhecimento bastante superficial sobre a segurança da informação, por conta de não terem um referencial a ser seguido, como apontado pelas repostas da Q4 e Q5, e que podem ser vistas nas Figuras 4 - ***Q04 - Formulário dos Colaboradores*** e 5 - ***Q05 - Formulário dos Colaboradores***.

Figura 4 – ***Q04 - Formulário dos Colaboradores***



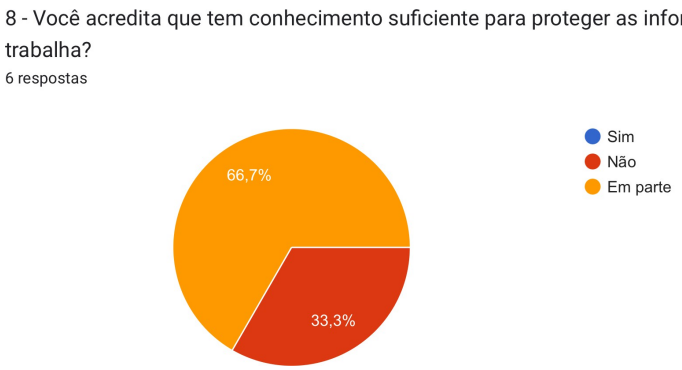
Fonte: Elaborado pelo autor.

Figura 5 – ***Q05 - Formulário dos Colaboradores***

Fonte: Elaborado pelo autor.

Embora possuam um conhecimento parcial sobre segurança da informação, eles não demonstraram ter plena compreensão sobre dados sensíveis ou confidenciais e sobre a neces- sidade de protegê-los adequadamente, sendo bastante prejudicial a segurança dos dados das escolas, como apresentado pelas respostas da Q8, podendo ser visualizadas na Figura 6 - ***Q08 - Formulário dos Colaboradores***. A maioria apresentou um conhecimento intermediário sobre os riscos digitais, como vazamento de dados e ataques cibernéticos, mas não recebeu orientações ou protocolos claros para seguir em relação à segurança da informação, como apontado pelas respostas em Q9, Q10 e Q11.

Figura 6 – ***Q08 - Formulário dos Colaboradores***



Fonte: Elaborado pelo autor.

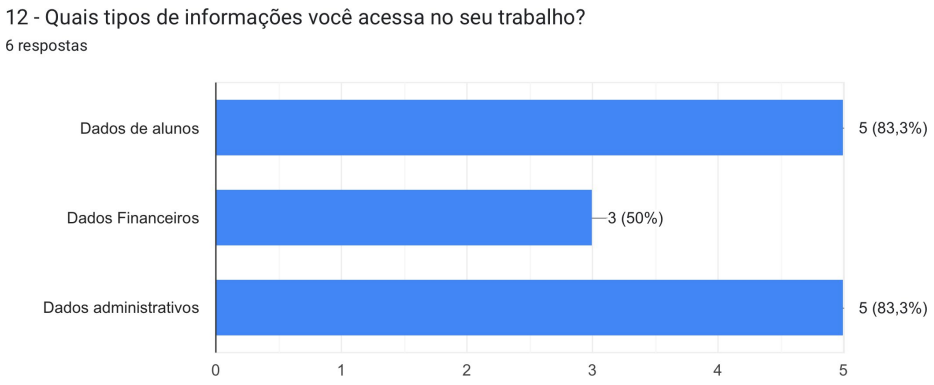
Todos os colaboradores têm acesso a pelo menos um tipo de dado considerado sensível, como informações de alunos, dados financeiros e administrativos, como assegurado pelas respostas da Q12, tendo sua visualização garantida por meio da Figura 7 - ***Q12 - Formulário dos Colaboradores***. Apesar disso, a maioria indicou que o acesso a essas informações é restrito a um grupo específico de pessoas. O uso de dispositivos escolares é compartilhado entre colegas, sendo que, em média, até três pessoas compartilham os dispositivos, de acordo com as respostas da Q15, apresentadas pela Figura 8 - ***Q15 - Formulário dos Colaboradores***, incluindo diretores e colegas do mesmo setor, e as senhas desses dispositivos também são compartilhadas.

O uso de dispositivos pessoais no ambiente de trabalho é comum, com uma boa parte dos entrevistados utilizando seus próprios dispositivos para desempenhar as funções profissionais, segundo as respostas a Q17. Quanto ao processo de encerramento dos dispositivos, alguns entrevistados afirmaram nunca ter realizado esse procedimento, enquanto outros garantiram que o fazem sempre, sendo apontado pelas respostas da Q19. Como apontado nas respostas da Q20, a verificação de links e e-mails suspeitos antes de clicar é uma prática adotada na maioria dos casos, o que indica um certo cuidado com a segurança.

No entanto, a maioria dos colaboradores afirmou não saber como proceder caso identifi- quem algum problema relacionado à segurança da informação, como apontado pelas respostas da Q22. O nível de conscientização sobre o tema dentro da escola é, em grande parte, consi- derado insatisfatório pelos entrevistados, sendo observado nas respostas a Q23. Por fim, todos concordam que treinamentos e capacitações adicionais

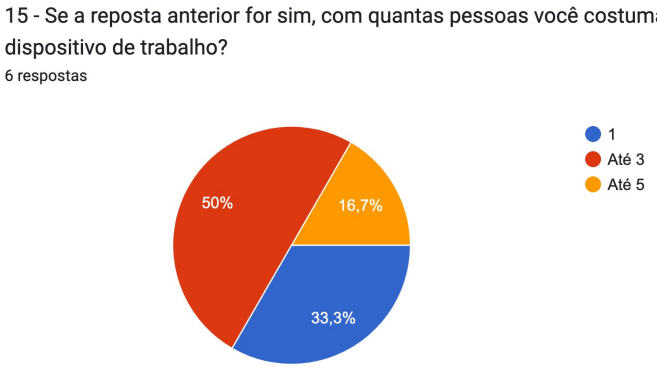
seriam fundamentais para melhorar a segurança da informação na instituição.

Figura 7 – ***Q12 - Formulário dos Colaboradores***



Fonte: Elaborado pelo autor.

Figura 8 – ***Q15 - Formulário dos Colaboradores***



Fonte: Elaborado pelo autor

Para mais detalhes sobre os dados obtidos, o **Apêndice D** está disposto no final deste documento, mostrando um conjunto de gráficos referentes aos resultados de questões fechadas e de múltipla alternativa que foram aplicadas no formulário em questão.

4.3 DISCUSSÕES DOS RESULTADOS

A conscientização sobre segurança da informação é praticamente inexistente, não há estratégias ou protocolos claros fornecidos nem pela coordenação das escolas, nem pelos órgãos municipais ou estaduais responsáveis. O excesso de confiança dos gestores

escolares nos funcionários é notório, podendo resultar na ausência de medidas preventivas, como a falta de treinamento adequado, o não monitoramento do acesso a informações sensíveis e a negligência na implementação de protocolos de segurança.

As principais dificuldades apontadas em relação à segurança da informação incluem a falta de capacitação dos funcionários, a insegurança nas práticas adotadas e o acesso informal a informações sensíveis por parte de muitos colaboradores. Para melhorar a situação, foi sugerido que cursos e capacitações sejam oferecidos para aumentar o conhecimento e a conscientização dos funcionários. Além disso, as escolas não apresentam planos ou projetos futuros voltados para fortalecer as práticas de segurança da informação.

4.4 COMPARAÇÃO DOS RESULTADOS

Ao comparar os resultados obtidos com colaboradores e diretores com os princípios da segurança da informação em âmbitos escolares, surgem pontos que mostram tanto alinhamentos quanto diferenças nas percepções sobre a segurança da informação nas escolas, evidenciando desafios que precisam ser enfrentados. Logo abaixo os resultados estão comparados divididos pelos princípios:

- **1. Conhecimento e Capacitação:** Tanto os colaboradores quanto os diretores demons- traram ter noções básicas sobre segurança da informação, mas nenhum deles teve acesso a treinamentos ou capacitações específicas. Ambos destacaram a ausência de qualquer programa que atualize os funcionários sobre o tema, o que acaba gerando insegurança e limitações no entendimento mais aprofundado sobre práticas adequadas. Essa necessidade de aprendizado aparece como um pedido claro vindo de ambos os lados.

- **2. Políticas e Procedimentos:** De forma unânime, foi apontada a falta de políticas e regimentos claros nas escolas. Os colaboradores mencionaram que não há orientações con- cretas para guiar suas ações e que muitas vezes tudo é feito de forma intuitiva, enquanto os diretores admitiram confiar excessivamente nos funcionários, sem estabelecer mecanismos formais de controle. Essa ausência de estrutura abre margem para inconsistências e riscos desnecessários.

- **3. Acesso e Controle:** O acesso às informações nas escolas é determinado pelos cargos, algo que, em teoria, traz organização, mas que na prática ainda apresenta

falhas. Um exemplo disso foi o relato de um caso em que professores tiveram acesso indevido ao e-mail da escola, evidenciando fragilidades no controle. Além disso, ambos os grupos apontaram que não há qualquer orientação sobre o armazenamento seguro dos dados, o que aumenta a exposição a possíveis incidentes.

- **4. Uso e Compartilhamento de Dispositivos e Senhas:** O uso de dispositivos e senhas foi identificado como um ponto crítico. É comum que os funcionários compartilhem dispositivos e até senhas entre si, confiando uns nos outros sem qualquer regulamentação ou controle. Para os colaboradores, essa prática se tornou parte da rotina, enquanto os diretores enxergam nela uma vulnerabilidade evidente. O uso de dispositivos pessoais no trabalho foi considerado pouco frequente, mas também sem qualquer política que o regule.

5. Práticas no Dia a Dia: Na prática, o que se vê é que a segurança da informação depende muito do uso de senhas e de orientações informais. Quando questionados sobre o que fariam diante de um problema de segurança, a maioria dos colaboradores revelou não saber como agir, o que reforça a ausência de protocolos claros ou orientações que preparem a equipe para lidar com situações críticas. Isso deixa evidente a falta de preparo tanto dos funcionários quanto da gestão para enfrentar esses desafios.

- **6. Incidentes e Conscientização:** Ambos os grupos apontaram a falta de conscientização como um dos principais problemas. Nem os colaboradores nem os diretores se sentem suficientemente preparados, e essa lacuna reflete a ausência de estratégias organizadas por parte da coordenação ou mesmo dos órgãos municipais e estaduais. É um problema que não apenas dificulta o trabalho diário, mas também deixa as escolas vulneráveis a ameaças.

- **7. Sugestões de Melhorias:** Quando se trata de melhorias, há consenso: a capacitação dos funcionários é vista como essencial. Tanto os colaboradores quanto os diretores acreditam que treinamentos e orientações mais claras poderiam transformar a forma como a segurança da informação é tratada nas escolas. No entanto, nenhum dos grupos relatou a existência de planos ou projetos para implementar essas melhorias, o que mostra que o tema ainda não é tratado como prioridade.

De maneira geral, colaboradores e diretores estão alinhados em identificar os

principais problemas: falta de políticas claras, ausência de capacitação e práticas inadequadas no uso de dispositivos e senhas. No entanto, enquanto os colaboradores sentem mais de perto os impactos dessas falhas no dia a dia, os diretores tendem a enfatizar questões de gestão, como controle de acesso. Ambos, porém, reconhecem a importância de mudanças urgentes, especialmente no que diz respeito à capacitação e à implementação de políticas mais estruturadas.

5 CONCLUSÕES E TRABALHOS FUTUROS

Com base nos dados apresentados e nas análises feitas, conclui-se que a há evidências de que as escolas enfrentam desafios significativos em relação à segurança da informação, desde o excesso de confiança por parte dos diretores em seus funcionários, passando pela ausência de políticas bem definidas e treinamentos até a falta de conscientização e práticas consistentes. Embora tanto colaboradores quanto diretores reconheçam a importância do tema, a ausência de iniciativas concretas indicam que as instituições estão vulneráveis a riscos que poderiam ser minimizados com ações simples e acessíveis. Essa realidade reforça a necessidade de um esforço conjunto para promover mudanças estruturais e culturais no tratamento da segurança da informação nesses espaços.

Mesmo com desafios, há uma grande oportunidade de mudança. Promover treinamentos contínuos, estabelecer diretrizes claras e incentivar a responsabilidade coletiva pode fazer toda a diferença no dia a dia das escolas. Quando a segurança da informação é tratada como uma prioridade, não só os dados são protegidos, mas também se constrói um ambiente de confiança entre gestores, professores e demais colaboradores.

5.1 TRABALHOS FUTUROS

Partindo das lacunas identificadas, nota-se que futuras pesquisas podem aprofundar a análise sobre segurança da informação em ambientes educacionais, ampliando o escopo, para incluir mais escolas e diferentes níveis de ensino. Também seria relevante adicionar a influência de políticas públicas na conscientização e treinamento de gestores e colaboradores das instituições escolares. Outro ponto relevante seria a investigação da atuação dos órgãos superiores, como as Secretarias de Educação, sobre a questão da segurança da informação nas escolas e como a influência desses órgãos sobre as escolas impacta nas atitudes e comportamentos do gestores escolares.

Outra linha de pesquisa interessante seria avaliar o impacto da implementação de

programas de capacitação contínua para os trabalhadores, analisando mudanças na percepção e nas práticas de segurança ao longo do tempo. Por fim, estudos futuros podem explorar a viabilidade de ferramentas tecnológicas para reforçar o controle de acesso, o gerenciamento de dados sensíveis e a proteção contra incidentes de segurança no contexto escolar.

REFERÊNCIAS

ALKHUDHAYR, F. et al. Information security: a review of information security issues and techniques. In: INTERNATIONAL CONFERENCE ON COMPUTER APPLICATIONS & INFORMATION SECURITY (ICCAIS), 2., 2019. **Anais [...].** [S.l.: s.n.], 2019. Disponível em: https://ieeexplore.ieee.org/document/8769504. Acesso em: 20 ago. 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001: tecnologia da informação — técnicas de segurança — sistemas de gestão da segurança da informação — requisitos. Rio de Janeiro: ABNT, 2013.

BEZERRA, E. d. S**. Desafios na proteção de dados e segurança da informação em ambientes acadêmicos: um estudo de caso na UFERSA Campus Pau dos Ferros**. 2023. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Universidade Federal Rural do Semi-Árido, Campus Pau dos Ferros, Pau dos Ferros, 2023. Disponível em: https://repositorio.ufersa.edu.br/items/51cc6952-b982-4e6f-9e06-29cafb8c7617. Acesso em: 24 ago. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 05 Jan. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 5 ago. 2024.

BRASIL. **Secretaria de Governo Digital**. Modelo de Política de Segurança da Informação (PPSI). Brasília, DF: Secretaria de Governo Digital, 2024. Versão 1.0. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf. Acesso em: 23 ago. 2024.

CASTANHO, R. Principais ameaças à segurança da informação nas empresas e como se proteger. **Gestão Pro**, 1 jun. 2023. Disponível em: https://gestaopro.com.br/blog/seguranca/principais-ameacas-a-seguranca-da-informacao-nas-empresas-e-como-se-proteger. Acessado em: 22 Ago 2024.

COADIC, Y.-F. L. **A ciência da informação**. Brasília: Briquet de Lemos, 2004. Book (124 p.). Disponível em: http://bds.unb.br/handle/123456789/738. Acessado em: 27 Ago 2024.

CONCEIÇÃO, B. T. L. **Confidencialidade e segurança da informação**. 2019. Dissertação

(Mestrado Integrado em Engenharia Eletrotécnica e de Computadores) - Faculdade de Engenharia, Universidade do Porto, 2019, Disponível em: https://repositorio-aberto.up.pt/bitstream/10216/119203/2/318583.pdf. Acessado em: 15 Ago 2024.

COUTINHO, M. M. *et al.* Estudo de caso: Principais pilares da segurança da informação nas organizações. **Revista Gestão em Foco**, v. 9, p. 489–500, 2017. Disponível em: https://portal.unisepe.com.br/unifia/wp-content/uploads/sites/10001/2018/06/052_estudo5.pdf Acessado em: 27 Ago 2024.

DEL-MASSO, M. C. S.; COTTA, M. A. de C.; SANTOS, M. A. P. **Ética em pesquisa científica: conceitos e finalidades**. 2014. Dissertação (Especialização) – UNESP, Faculdade de Filosofia e Ciências, 2014. Disponível em: https://acervodigital.unesp.br/handle/unesp/155306. Acessado em: 22 Ago 2024.

ESPÍRITO SANTO. Secretaria de Estado da Educação. **Guia orientativo de boas práticas de segurança da informação e proteção dos dados pessoais na educação**. Vitória: Secretaria de Estado da Educação, 2024. Disponível em: https://sedu.es.gov.br/Media/sedu/pdf%20e%20Arquivos/[Guia]%20Guia%20Orientativo%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o%20e%20PDPP.pdf. Acesso em: 22 ago. 2024.

ESTADOS UNIDOS. Cybersecurity and Infrastructure Security Agency. **What is cybersecurity?** Washington, DC: CISA, 2021. Disponível em: https://www.cisa.gov/news-events/news/what-cybersecurity. Acesso em: 20 ago. 2024.

ETIKAN, I.; MUSA, S. A.; ALKASSIM, R. S. Comparison of convenience sampling and purposive sampling. **American Journal of Theoretical and Applied Statistics**, New York, v. 5, n. 1, p. 1–4, 2016. Disponível em: https://www.sciencepublishinggroup.com/article/10.11648/j.ajtas.20160501.11. Acesso em: 25 ago. 2024.

FORNASIER, M. de O.; SPINATO, T. P.; RIBEIRO, F. L. Ransomware e cibersegurança: a informação ameaçada por ataques a dados. **Revista Thesis Juris**, São Paulo, v. 9, n. 1, p. 208–236, 2020. Disponível em: https://periodicos.uninove.br/thesisjuris/article/view/16739. Acesso em: 25 ago. 2024.

GOOGLE. **Google Forms**. Versão 8.9.58.7. [S. I.]: Google, 2025. Disponível em: https://forms.google.com. Acessado em: 28 Jan. 2025.

GUPTA, S. S.; THAKRAL, A.; CHOUDHURY, T. Social media security analysis of threats and security measures. In: INTERNATIONAL CONFERENCE ON ADVANCES IN COMPUTING AND COMMUNICATION ENGINEERING (ICACCE), 2018. **Anais [...]**. [S.l.: s.n.], 2018. p. 115–120. Disponível em: https://ieeexplore.ieee.org/document/8441710. Acesso em: 30 jan. 2025.

KANAGUSKU, A. R. A.; GASETA, E. Fator humano na segurança da informação: desmistificando o elo mais fraco. In: FATECSEG – CONGRESSO DE SEGURANÇA DA INFORMAÇÃO, 3., 2023, Americana, SP. **Anais do FATECSEG [...]**. Americana: Faculdade de Tecnologia de Americana Ministro Ralph Biasi, 2023. Disponível em: https://fatecseg.fatecourinhos.edu.br/index.php/fatecseg/article/view/114. Acesso em: 2 fev. 2025.

LATTO, N. O que é o WannaCry?. **Avast**, 27 fev 2020 . Disponível em: https://www.avast.com/c-wannacry. Acessado em: 19 Ago 2024.

MACKIEVICZ, A. C. L. Segurança da informação e LGPD: tudo que sua escola precisa saber. **Sponte**. 16 set. 2022.Disponível em: https://www.sponte.com.br/blog/seguranca-da-informacao-para-escolas. Acesso em: 05 Ago 2024.

MARINHO, R. A.; BODÊ, J. Gamificação aplicada a programas e campanhas de conscientização de segurança da informação. In: FATECSEG – CONGRESSO DE SEGURANÇA DA INFORMAÇÃO, 2., 2022, Americana, SP. **Anais do FATECSEG [...]**. Americana: Faculdade de Tecnologia de Americana, 2022. Disponível em: https://fatecseg.fatecourinhos.edu.br/index.php/fatecseg/article/view/50. Acesso em: 12 set. 2024.

MONTAGNER, A. S.; WESTPHALL, C. M. Uma breve análise sobre phishing. **Revista ComInG-Communications and Innovations Gazette**, Santa Maria, v. 6, n. 1, p. 46–56, 2022. Disponível em: https://periodicos.ufsm.br/coming/article/view/71731. Acesso em: 23 fev. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Data Encryption Standard. **NIST**, 15 jan. 2001. Disponível em: https://csrc.nist.gov/pubs/book-section/2001/01/data-encryption-standard/final. Acessado em: 28 Fev 2025.

NEVES, D. L. F. *et al.* A segurança da informação de encontro às conformidades da LGPD. **Revista Processando o Saber**, Ponta Grossa, v. 13, n. 1, p. 1–15, 2021. Disponível em: https://fatecpg.edu.br/revista/index.php/ps/article/view/171. Acesso em: 31 jan. 2025.

NUNES, G. C.; NASCIMENTO, M. C. D. d.; LUZ, M. A. C. A. Pesquisa científica: conceitos básicos. **Id on Line Revista de Psicologia**, Jaboatão dos Guararapes, v. 10, n. 29, p. 144–151, 2016. Disponível em: https://idonline.emnuvens.com.br/id/article/view/390. Acesso em: 25 ago. 2024.

OLIVEIRA, E. V. d.; FILGUEIRAS, R. A. A importância da segurança da informação para as organizações. **Revista Alomorfia**, Presidente Prudente, v. 6, n. 2, p. 438–447, 2022. Disponível em: https://www.alomorfia.com.br/index.php/alomorfia/article/view/137. Acesso em: 25 ago. 2024.

OTTEN, N. Segurança da Informação: conceito, função e como proteger dados sigilosos. **Docusign**, 8 dez. 2022. Disponível em https://www.docusign.com/pt-br/blog/seguranca-da-informacao. Acesso em: 05 Ago 2024.

PRÜMMER, J.; VAN STEEN, T.; VAN DEN BERG, B. A systematic review of current cybersecurity training methods. **Computers & Security**, Amsterdam, v. 136, p. 103585, 2024. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404823004959. Acesso em: 20 set. 2024.

SANTOS, J. L. G. d. *et al.* **Integração entre dados quantitativos e qualitativos em uma pesquisa de métodos mistos**. 2017. Dissertação (Especialização) – Faculdade de Enfermagem, Universidade Federal de Santa Catarina, 2017. Disponível em: https://www.scielo.br/j/tce/a/cXFB8wSVvTm6zMTx3GQLWcM/?format=html&lang=pt.

Acessado em: 14 Set 2024.

SANTOS, R. C. dos; SANTOS, M. F. dos; CARREIRA, F. S. Campanha de conscientização em segurança da informação: um estudo de caso. In: CONFERÊNCIA SOBRE SEGURANÇA DA INFORMAÇÃO, 2021. **Anais [...]**. Rio de Janeiro: COPPE/UFRJ; UNESA; IBMEC-RJ, 2021. p. 1–10. Disponível em: https://www.aedb.br/seget/arquivos/artigos16/382440.pdf. Acesso em: 20 set. 2024.

SARGI, M. P.; SILVA, J. R. d. M.; CARMO, C. R. S. Amostragem e análise de dados: um estudo de caso sobre pesquisas eleitorais brasileiras de 2022. **GETEC**, v.14, p.1-18, 2024. Disponível em: https://revistas.fucamp.edu.br/index.php/getec/article/view/3302. Acessado em: 22 Set 2024.

SFREDDO, J. A.; FLORES, D. O controle de acesso na percepção dos profissionais de arquivo: uma questão de segurança das informações institucionais**. Perspectivas em Ciência da Informação**, Belo Horizonte, v. 14, n. 2, p. 152–168, 2009. Disponível em: https://www.scielo.br/j/pci/a/sqf4sjKKbcwb8mwn7d4bFRm/. Acesso em: 25 set. 2024.

SILVA, D. B. da; OLIVEIRA, R. N. de; SILVA, E. N. da. Segurança da informação: um estudo em escolas municipais em Girau do Ponciano-AL. In: ESCOLA REGIONAL DE COMPUTAÇÃO BAHIA, ALAGOAS E SERGIPE (ERBASE), 21., 2021. **Anais da XXI Escola Regional de Computação Bahia, Alagoas e Sergipe (ERBASE)**. [S.l.: s.n.], 2021. p. 1–9. Disponível em: https://sol.sbc.org.br/index.php/erbase/article/view/20050. Acesso em: 30 set. 2024.

SILVA, V. L. L. d**. Ataque cibernético ransomware: o que é e como prevenir**. 2023. Trabalho de Conclusão de Curso (Tecnologia em Análise e Desenvolvimento de Sistemas) – Centro Paula Souza, Faculdade de Tecnologia, São Paulo, 2023. Disponível em: https://ric.cps.sp.gov.br/bitstream/123456789/16242/1/analise_e_desenvolvimento_de_sistemas_2023_1_victor_luiz_lopes_da_silva_ataque_cibernetico_ransomware_o_que_e_e_como_previnir.pdf. Acesso em: 1 out. 2024.

SILVEIRA, L. A.; REALAN, M.; AMARAL, É. Engenharia social: uma análise sobre o ataque de phishing. In: SULCOMP – SIMPÓSIO SUL DE COMPUTAÇÃO, 8., 2016. **Anais do SULCOMP [...]**. [S.l.: s.n.], 2016. Disponível em: https://scholar.google.com/scholar?hl=ptBR&as_sdt=0%2C5&q=Engenharia+social. Acesso em: 2 out. 2024.

SOARES, C. C.; SILVA, P. C. d. Uma avaliação sobre o conhecimento em segurança da informação. **Revista Expressão Científica**, Aracaju, v. 3, n. 1, p. 70–79, 2019. Disponível em: https://periodicos.ifs.edu.br/periodicos/REC/article/view/287. Acesso em: 2 out. 2024.

SOUSA, L. S.; BRANDÃO, J. S**. Segurança da informação em instituições públicas municipais: um estudo**. 2023. Trabalho de Conclusão de Curso (Graduação em [curso não informado]) – Universidade Federal Fluminense, Niterói, 22 out. 2023. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=5755894. Acesso em: 28 jan. 2025.

SOUZA, J. G. S.; ARIMA, C. H.; BELDA, F. R. Análise de tratamento da segurança da informação de uma instituição de ensino público federal. **Revista Ibero-Americana de Estudos em Educação**, Araraquara, v. 15, n. 4, p. 1309–1321, 2020. Disponível em: https://periodicos.fclar.unesp.br/iberoamericana/article/view/13584. Acesso em: 7 out. 2024.

STALLINGS, W.; BROWN, L. **Computer Security: Principles and Practice**. Boston

(EUA): Pearson Education, 2014. Book (512 p.). Disponível em: https://books.google.com.br/books? id=NsZEBAAAQBAJ. Acessado em: 15 Out 2024.

Apêndices

APÊNDICE A – FORMULÁRIO DOS DIRETORES

Este apêndice apresenta o questionário aplicado à os diretores para a coleta de informa- ções sobre segurança da informação no ambiente educacional.

1. Identificação

    1. Qual o seu nome? (De preferência o nome completo)

    2. Em qual escola você atua?

2. Conhecimento e Treinamento em Segurança da Informação

    3. Você sabe o que é segurança da informação? ( ) Sim ( ) Não

    4. Se sim, sobre o que se trata a segurança da informação?

    _____

    5. Você já recebeu algum treinamento ou capacitação sobre segurança da informação? ( ) Sim ( ) Não

    6. Caso tenha participado de treinamento/capacitação, há quanto tempo foi realizado? ( ) Há semanas ( ) Há meses ( ) Há anos ( ) Há mais de 5 anos

    7. Caso tenha participado de treinamento/capacitação, qual foi o tema ou conteúdo abordado? ( ) Proteção de dados ( ) Uso seguro de sistemas ( ) Boas práticas digitais ( ) Outro: ____

    8. Os funcionários da escola recebem algum tipo de treinamento ou capacitação sobre segurança da informação? Se sim, sobre qual tema se trata?

    _____

    9. Você considera que os funcionários têm o conhecimento necessário para lidar com infor- mações sensíveis?

_____

3. Políticas e Procedimentos de Segurança

10. Existe algum programa contínuo para atualizar os funcionários sobre práticas de segurança? Se sim, qual o programa e como funciona?

_____

11. A escola possui uma política formal de segurança da informação? Se sim, como ela foi desenvolvida?

_____

12. Quais são os principais procedimentos adotados para proteger informações sensíveis na escola?

_____

13. Você acredita que essas políticas e procedimentos estão sendo seguidos de forma eficaz?

_____

14. Como é definido quem tem acesso às informações sensíveis na escola?

_____

15. Existem mecanismos para limitar o acesso a informações com base no cargo ou na necessidade do funcionário? ( ) Sim ( ) Não

16. Já ocorreram casos de acessos não autorizados às informações escolares? Como foram tratados?

_____

4. Uso de Dispositivos e Senhas

17. Existe uma política sobre o uso de dispositivos de trabalho, como computadores e

tablets, pelos funcionários?

_____

18. Como é gerenciado o uso e o compartilhamento de senhas na escola?

_____

19. Você observa a prática de funcionários utilizarem dispositivos pessoais para fins profissio- nais? Se sim, há algum controle sobre isso?

_____

5. Práticas de Segurança no Dia a Dia

20. Quais práticas a escola adota para proteger as informações no dia a dia?

_____

21. Há orientação sobre o armazenamento seguro de documentos impressos e digitais? Se sim, quais são essas orientações?

_____

22. Como você avalia o comprometimento dos funcionários com a adoção de boas práticas de segurança?

_____

6. Incidentes e Protocolos de Segurança

23. A escola já enfrentou algum incidente relacionado à segurança da informação? Se sim, como foi gerenciado?

_____

24. Existem protocolos claros para lidar com incidentes de segurança? Se sim, quais são esses protocolos?

_____

25. Os funcionários estão suficientemente conscientizados sobre a importância da segurança da informação?

_____

7. Sugestão de Melhorias

26. Quais estratégias são utilizadas para conscientizar a equipe sobre a importância de proteger informações?

_____

27. Quais são as principais dificuldades enfrentadas pela escola em relação à segurança da informação?

_____

28. Quais recursos (financeiros, tecnológicos ou humanos) seriam necessários para melhorar a proteção das informações na escola?

_____

29. Há planos ou projetos futuros para fortalecer as práticas de segurança da informação?

_____

8. Termo de Aceite

30. Termo de Aceite:

    Eu aceito participar da pesquisa respondendo este formulário, sabendo que meus dados e as informações fornecidas serão mantidos em total sigilo e que meu nome não será divulgado.

APÊNDICE B – FORMULÁRIO DOS COLABORADORES

Este apêndice apresenta o questionário aplicado aos colaboradores para a coleta de

informações sobre segurança da informação no ambiente escolar.

1. Identificação

1. Qual o seu nome? (De preferência o nome completo)

2. Em qual escola você atua?

3. Qual a sua função dentro da escola?

2. Conhecimento e Treinamento em Segurança da Informação

4. Você sabe o que é segurança da informação? ( ) Sim ( ) Não

5. Você já recebeu algum treinamento ou capacitação sobre segurança da informação? ( ) Sim ( ) Não

6. Caso tenha participado, há quanto tempo foi realizado o treinamento/capacitação? ( ) Há semanas ( ) Há meses ( ) Há anos ( ) Há mais de 5 anos

7. Caso tenha participado, qual foi o tema ou conteúdo abordado? ( ) Proteção de dados ( ) Uso seguro de sistemas ( ) Boas práticas digitais ( ) Outro: _____

3. Políticas e Procedimentos de Segurança

8. Você acredita que tem conhecimento suficiente para proteger as informações com as quais trabalha? ( ) Sim ( ) Não ( ) Em parte

9. Sabe identificar o que são dados sensíveis ou confidenciais? ( ) Sim ( ) Não ( ) Não sei

10. Tem conhecimento sobre os riscos de segurança digital, como vazamento de dados ou ata- ques cibernéticos? ( ) Não tenho conhecimento ( ) Pouco conhecimento ( ) Conhecimento intermediário ( ) Conhecimento avançado ( ) Total conhecimento

11. Você já recebeu alguma orientação ou documento sobre os procedimentos de segurança da informação? ( ) Sim ( ) Não

4. Acesso e Compartilhamento de Informações

12. Quais tipos de informações você acessa no seu trabalho? ( ) Dados de alunos ( ) Dados financeiros ( ) Dados administrativos ( ) Outro: _____
13. Você possui acesso restrito a informações específicas, dependendo do seu cargo? ( ) Sim ( ) Não ( ) Não sei
14. Você compartilha seu dispositivo de trabalho (computador, tablet, etc) com outros colegas? ( ) Sim ( ) Não
15. Se a resposta anterior for sim, com quantas pessoas você costuma compartilhar o seu dispo- sitivo de trabalho? ( ) 1 ( ) Até 3 ( ) Até 5 ( ) Outro:_____
16. Com quem você costuma compartilhar o seu dispositivo de trabalho? ( ) Diretor ( ) Professores ( ) Colegas do mesmo setor ( ) Outro: _____
17. Você compartilha as senhas dos dispositivos de trabalho com outras pessoas? ( ) Sim ( ) Não
18. Costuma utilizar dispositivos pessoais para trabalhar, como celulares ou notebooks? ( ) Sim ( ) Não

5. Práticas de Segurança no Dia a Dia

19. Você costuma fazer o processo de logoff (encerrar sessão, sair do sistema) ao final do expediente? ( ) Sempre ( ) Às vezes ( ) Não sei ( ) Nunca
20. Você verifica links e e-mails suspeitos antes de clicar ou abrir anexos? ( ) Sempre ( ) Às vezes ( ) Nunca
21. Você segue práticas recomendadas para proteger informações durante o trabalho? ( ) Sim ( ) Não ( ) Não sei
22. Você saberia como proceder caso identifique um problema de segurança da informação? (

) Sim ( ) Não ( ) Não sei

23. Acha que o nível de conscientização sobre segurança da informação na escola é satisfatório? ( ) Ruim ( ) Pouco Satisfatório ( ) Intermediário ( ) Satisfatório ( ) Muito satisfatório

6. Sugestão de Melhorias

24. Você acredita que mais treinamentos ou capacitações ajudariam a melhorar a segurança da informação? ( ) Sim ( ) Não

25. Em sua opinião, o que poderia ser feito para melhorar a segurança da informação na escola?

_____

7. Termo de Aceite

26. Termo de Aceite:

Eu aceito participar da pesquisa respondendo este formulário, sabendo que meus dados e as informações fornecidas serão mantidos em total sigilo e que meu nome não será divulgado.

APÊNDICE C – EMENTA DO MINICURSO SOBRE SEGURANÇA DA INFORMAÇÃO

1. Informações Gerais

- **Duração:** 1 hora
- **Formato:** Vídeo-aula
- **Público-alvo:** Colaboradores (funcionários) que possuem acesso a dados sensíveis e confidenciais, além de diretores das escolas selecionadas que participaram da primeira etapa proposta na metodologia.

2. Objetivo Geral

Capacitar de forma rápida e prática os participantes para compreenderem os princípios básicos de segurança da informação, permitindo que protejam dados sensíveis e adotem boas práticas no uso de dispositivos e na identificação de riscos.

3. Conteúdo Programático Detalhado

3.1 - Introdução à Segurança da Informação (10 minutos)

Objetivo: Introduzir o assunto por meio de exemplos práticos do cotidiano escolar, destacando os tipos de informações que precisam de proteção. Será utilizado um slide com definições claras e imagens ilustrativas para facilitar a compreensão. Além disso, será feita uma breve interação inicial, perguntando quais dados os participantes consideram sensíveis em suas funções, para contextualizar a importância da proteção.

- O que é segurança da informação e por que ela é importante;
- Exemplos de dados sensíveis no contexto escolar;
- Impactos de falhas na segurança, como vazamento de informações e perda de confiança institucional.

3.2 - Principais Riscos e Boas Práticas (30 minutos)

Cada risco será apresentado com exemplos simples, como simulações de e-mails de phishing ou histórias curtas sobre vazamentos de dados no ambiente escolar. Em seguida, será apresentado um checklist visual com boas práticas que os participantes podem aplicar imediatamente.

- Riscos comuns;
- Boas práticas essenciais.

3.3 - Ações em Caso de Problemas de Segurança (10 minutos)

Objetivo: Este tópico será abordado com exemplos de incidentes fictícios (como um e-mail suspeito recebido por um funcionário). Será explicado o passo a passo de como reagir diante de cada situação, utilizando um fluxograma simples exibido nos slides.

- Como identificar sinais de problemas de segurança;
- Passos básicos ao identificar um problema;
- Importância de criar uma cultura de reporte de incidentes.

3.4 - Conclusão e Reforço da Conscientização (10 minutos)

Objetivo: A vídeo-aula será encerrada com um resumo visual, utilizando um slide que lista as cinco práticas mais importantes apresentadas. Em seguida, será feito um breve reforço da ideia de que a segurança da informação depende de todos. Para finalizar, os participantes serão incentivados a refletir sobre como podem contribuir com a segurança na escola e a importância de manter-se atualizados sobre o tema.

- Resumo das principais práticas;

Importância de uma cultura coletiva de segurança e da capacitação contínua

APÊNDICE D – GRÁFICOS OBTIDOS ATRAVÉS DAS RESPOSTAS DO FORMULÁRIO DOS COLABORADORES

Este apêndice apresenta os resultados gráficos da pesquisa. Os gráficos trazem as respec- tivas respostas dos colaboradores e servem como referência para a análise dos resultados obtidos nesta pesquisa. Foram incluídos apenas os gráficos cujas respostas apresentaram variabilidade significativa e que não foram totalmente abordados na seção de resultados, excluindo aqueles com respostas totalitárias ou de pouca expressão na análise.

Gráficos por Questão

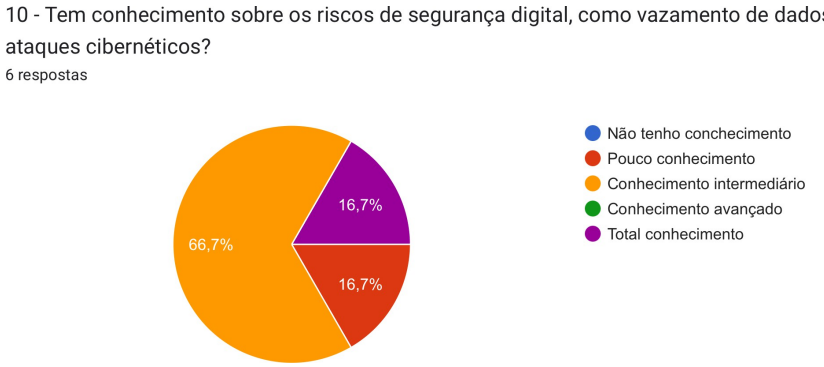
- **Questão 09**

4. Figura 9 – ***Q09 - Formulário dos Colaboradores***

Fonte: Elaborado pelo autor.

- **Questão 10**

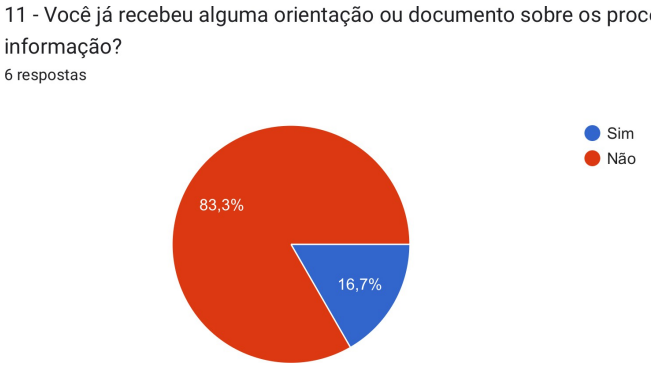
5. Figura 10 – ***Q10 - Formulário dos Colaboradores***



Fonte: Elaborado pelo autor.

- **Questão 11**

Figura 11 – *Q11 - Formulário dos Colaboradores*



Fonte: Elaborado pelo autor.

- **Questão 17**

6. Figura 12 – ***Q17 - Formulário dos Colaboradores***

Fonte: Elaborado pelo autor.

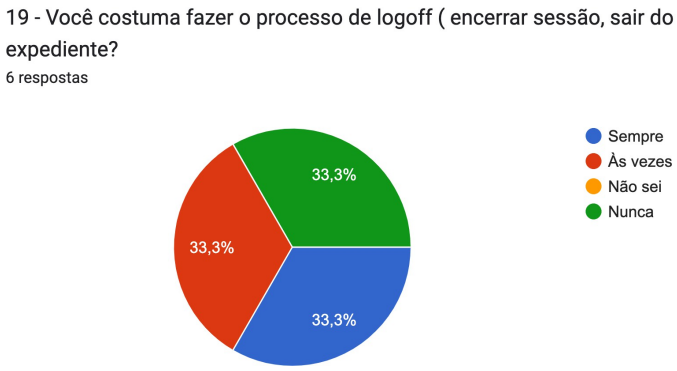
- **Questão 18**

7. Figura 13 – ***Q18 - Formulário dos Colaboradores***

Fonte: Elaborado pelo autor.

- **Questão 19**

8. Figura 14 – ***Q19 - Formulário dos Colaboradores***



Fonte: Elaborado pelo autor.

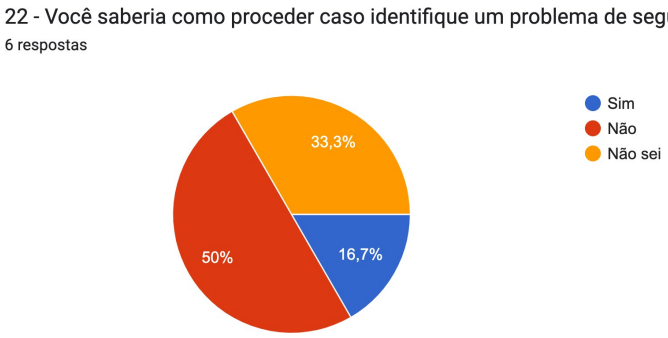
- **Questão 21**

Figura 15 – ***Q21 - Formulário dos Colaboradores***

Fonte: Elaborado pelo autor.

- **Questão 22**

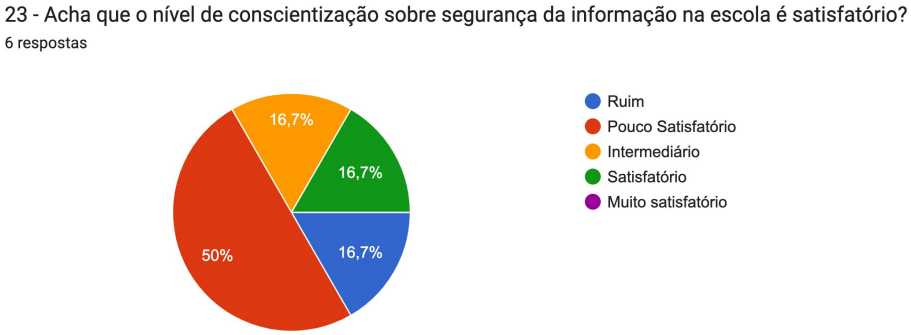
9. Figura 16 – ***Q22 - Formulário dos Colaboradores***



Fonte: Elaborado pelo autor.

- **Questão 23**

Figura 17 – *Q23 - Formulário dos Colaboradores*



Fonte: Elaborado pelo autor.