UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I – CAMPINA GRANDE
CENTRO DE CIÊNCIAS E TECNOLOGIA
DEPARTAMENTO DE ANÁLISE E DESENVOLVIMENTO DE SISTEMAS
CURSO DE GRADUAÇÃO EM TECNÓLOGO EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

JANYELLE OLIVEIRA PINTO DE CASTRO

A SEGURANÇA DE DADOS NA GESTÃO EMPREENDEDORA EM PLATAFORMAS DIGITAIS

JOÃO PESSOA - PB
2025

JANYELLE OLIVEIRA PINTO DE CASTRO

A SEGURANÇA DE DADOS NA GESTÃO EMPREENDORA EM PLATAFORMAS DIGITAIS

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Tecnologia em Análise e Desenvolvimento de Sistemas da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Tecnóloga em Tecnologia em Análise e Desenvolvimento de Sistemas.

Orientadora: Profa. Dra. Janayna Souto Leal.

JOÃO PESSOA - PB
2025

C355s Castro, Janyelle Oliveira Pinto de.
A segurança de dados na gestão empreendedora em plataformas digitais [manuscrito] / Janyelle Oliveira Pinto de Castro. - 2025.
33 f. : il. color.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Tecnologia em análise e desenvolvimento de sistemas) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia, 2025.

"Orientação : Prof. Dra. Janayna Souto Leal, Departamento de Administração e Economia - CCSA".

1. Segurança de dados. 2. Gestão empreendedora. 3. Plataformas digitais. 4. Riscos cibernéticos. I. Título

21. ed. CDD 005.8

Elaborada por Bruno Rafael Freitas de Lima - CRB - 15/1021 BC

JANYELLE OLIVEIRA PINTO DE CASTRO

A SEGURANÇA DE DADOS NA GESTÃO EMPREENDEDORA EM PLATAFORMAS DIGITAIS

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Tecnologia em Análise e Desenvolvimento de Sistemas da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Tecnóloga em Tecnologia em Análise e Desenvolvimento de Sistemas

Aprovada em: 23/05/2025.

BANCA EXAMINADORA

Documento assinado eletronicamente por:

- **Ana Caroline Salviano Ramos** (***.235.994-**), em **31/05/2025 10:26:25** com chave **d9c06cba3e2211f09a3e1a1c3150b54b**.
- **José Wilker de Lima Silva** (***.435.933-**), em **30/05/2025 11:06:06** com chave **3a95d3143d5f11f089ff2618257239a1**.
- **Janayna Souto Leal** (***.548.164-**), em **30/05/2025 11:05:35** com chave **2880393a3d5f11f0b8dc1a7cc27eb1f9**.

Documento emitido pelo SUAP. Para comprovar sua autenticidade, faça a leitura do QrCode ao lado ou acesse https://suap.uepb.edu.br/comum/autenticar_documento/ e informe os dados a seguir.
Tipo de Documento: Folha de Aprovação do Projeto Final
Data da Emissão: 03/06/2025
Código de Autenticação: ccbf7c

Aos meus pais, por acreditarem em mim; à minha irmã, por seu apoio e incentivo constante; e a todos que contribuíram de alguma forma na minha jornada, dedico.

"A segurança não é um produto, mas um processo."

Bruce Schneier

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

SUMÁRIO

A SEGURANÇA DE DADOS NA GESTÃO EMPREENDEDORA EM PLATAFORMAS DIGITAIS

Janyelle Oliveira Pinto de Castro[1]
Janayna Souto Leal[2]

RESUMO

A segurança de dados tem se tornado um pilar essencial para a gestão empreendedora em plataformas digitais, diante do avanço da transformação digital e dos crescentes riscos cibernéticos. Dessa forma, este estudo teve como objetivo geral analisar a percepção dos profissionais de tecnologia acerca da segurança de dados na gestão empreendedora em plataformas digitais. Metodologicamente, adotou-se uma abordagem qualitativa, com coleta de dados por meio de entrevistas estruturadas aplicadas a 12 profissionais, utilizando análise de conteúdo nas seguintes categorias: ações de segurança de dados, práticas empreendedoras e uso de plataformas digitais. Os resultados destacaram a importância da integração da segurança de dados à gestão empreendedora, evidenciando que essa prática não apenas mitiga riscos como ataques cibernéticos, mas também incentiva a inovação e fortalece ações proativas no ambiente digital, exigindo maior maturidade organizacional e comprometimento estratégico.

Palavras-Chave: segurança de dados; gestão empreendedora; plataformas digitais; riscos cibernéticos.

ABSTRACT

Data security has become an essential pillar of entrepreneurial management on digital platforms, given the advancement of digital transformation and the increasing cyber risks. Therefore, this study aimed to analyze technology professionals' perceptions of data security in entrepreneurial management on digital platforms. Methodologically, a qualitative approach was adopted, with data collected through structured interviews conducted with 12 professionals, and content analysis carried out in the following categories: data security actions, entrepreneurial practices, and use of digital platforms. The results underscored the importance of integrating data security into entrepreneurial management, showing that this practice not only mitigates risks such as cyberattacks but also fosters innovation and strengthens proactive measures in the digital environment, demanding greater organizational maturity and strategic commitment.

Keywords: data security; entrepreneurial management; digital platforms; cyber risks.

1 INTRODUÇÃO

Com o avanço da transformação digital, tornou-se mais comum a produção e o armazenamento de dados *on-line*, e, consequentemente, a necessidade de protegê-los. No âmbito empresarial, esses dados são considerados ativos, pois são elementos que representam grande importância. Nesse sentido, mesmo com os benefícios que a internet proporciona diariamente para as pessoas e, principalmente, para muitas empresas, o cuidado com a segurança desses dados se tornou um pilar fundamental, pois quando alguém fornece suas informações, ela confia que sua privacidade será garantida pela organização.

[1] Discente da Universidade Estadual da Paraíba. E-mail: janyelleoliveira30@gmail.com
[2] Docente da Universidade Estadual da Paraíba. E-mail: janaynaleal@servidor.uepb.edu.br

Diante disso, algumas empresas estão investindo para tornar suas plataformas de negócios mais seguras e, também, no cumprimento das normas de proteção de dados. De acordo com dados apresentados pela Cybersecurity Ventures, os prejuízos com cibercrimes devem atingir US$ 10,5 trilhões por ano em todo o mundo até 2025 (Exame Solutions, 2023). Desse modo, nota-se o quão necessário tem sido a adoção de medidas preventivas para as corporações, pois os casos de vazamento de dados ainda são um grande motivo de preocupação, especialmente com o aumento da digitalização e dos serviços prestados no contexto tecnológico.

Assim, evidencia-se a segurança de dados como um tema cuja relevância tem crescido no ambiente organizacional, devido ao seu papel na proteção de ataques em plataformas digitais e na diminuição de vulnerabilidades em sistemas computacionais das organizações. Em relação a esse tema, há várias definições. De acordo com Sêmola (2003), a segurança da informação é definida como a área responsável por proteger os ativos de informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Por conseguinte, ela engloba não apenas a proteção dos dados digitais, mas também de todo o processo que envolve a coleta, armazenamento e transmissão de dados e informações físicas e *on-line*. Com o crescente uso da tecnologia e automação no mundo corporativo, a segurança da informação tem se tornado indispensável, necessitando de um alinhamento estratégico com as metas empresariais e com a gestão de negócios (Fernandes, 2007).

Seguindo essa linha de pensamento, a segurança da informação depende da implementação de controles que abrangem programas, políticas e práticas organizacionais, sendo fundamental para a proteção de informações sensíveis da empresa (Tomaz, 2023). Nesse contexto, a adoção de uma gestão empreendedora voltada para a proteção de dados e o controle de acesso é essencial, especialmente para empresas que utilizam a digitalização de tarefas e serviços em suas operações diárias. Neste sentido, a gestão empreendedora refere-se à aplicação de práticas inovadoras e transformadoras dentro da empresa, com o objetivo de motivar equipes e reduzir incertezas em um mercado competitivo (Oliveira, 2021). Assim, torna-se evidente que a inovação está intrinsecamente ligada à adoção de tecnologias que facilitam os serviços no ambiente de trabalho e, consequentemente, a discussão sobre segurança de dados na gestão empresarial é crucial para evitar prejuízos financeiros, não conformidade com legislações como a Lei Geral de Proteção de Dados (LGPD), e danos à reputação, que podem resultar das consequências mencionadas.

Como parte essencial do processo de adaptação das empresas à era da transformação digital, destaca-se o crescimento das plataformas digitais como facilitadoras da comunicação e do compartilhamento de informações entre indivíduos, instituições e empresas. Segundo Rogers (2017), as plataformas digitais constituem um modelo de negócios em rede que facilita a interação entre empresas e clientes, permitindo a troca de valor e o crescimento exponencial do ecossistema à medida que mais usuários as utilizam. Hoje em dia, a depender do seu tamanho/porte, é difícil imaginar uma empresa sem um *site* próprio que ofereça informações e serviços aos seus clientes. Partindo desse princípio, embora a tecnologia traga benefícios e facilidades para os negócios, para que uma empresa mantenha seu desempenho no ambiente digital, é crucial que ela esteja atenta às constantes mudanças tecnológicas e aos novos riscos que surgem, garantindo assim um gerenciamento seguro dos processos empresariais e a entrega confiável de serviços aos seus clientes.

Tendo em vista o conteúdo exposto, este artigo apresenta a seguinte problemática de pesquisa: **Qual a percepção dos profissionais da área de tecnologia acerca da segurança de dados na gestão empreendedora em plataformas digitais?** Para responder a este questionamento, o trabalho tem como objetivo geral analisar a percepção dos profissionais acerca da segurança de dados na gestão empreendedora em plataformas digitais.

Como justificativa para este estudo, os dados apresentados por uma pesquisa realizada pela Netscout, empresa especializada em soluções de cibersegurança, revelam que o Brasil

tem sido o principal alvo de ciberataques na América Latina, uma realidade que persiste na região há quase uma década (O Globo, 2023). O relatório intitulado "*Global DDoS Threat Intelligence*" mostra que houve um aumento de 19% no número de tentativas de ataques cibernéticos no segundo semestre de 2022, em comparação ao primeiro semestre.

Além disso, outro dado preocupante aponta que o número de organizações que adotam práticas gerenciais eficazes de segurança digital ainda é muito baixo, conforme aponta o relatório TIC Empresas, divulgado pelo Comitê Gestor da Internet no Brasil (CGI.br) (2023). Nesse relatório destaca-se que apenas 50% das empresas entrevistadas possuem alguma política de segurança digital, o que representa uma situação alarmante, uma vez que demonstra que somente metade das empresas no Brasil têm diretrizes claras sobre o manuseio de dados, sistemas e informações no ambiente de trabalho. Ademais, apenas 27% das empresas promovem treinamentos sobre a gestão de riscos de segurança digital para engajar seus colaboradores na causa. Logo, tais números apontam que os aspectos gerenciais da segurança digital ainda estão longe de serem uma realidade na maioria das organizações do mercado brasileiro, o que se estende ao uso de plataformas digitais, haja visto que muitas empresas atuam neste âmbito.

2 REFERENCIAL TEÓRICO

2.1 Segurança de dados

A preocupação com a proteção de dados, abrangendo os pilares de confidencialidade, integridade e disponibilidade, não é um tema novo, embora esteja em evidência atualmente. Ao longo da história, diversos acontecimentos evidenciam a importância da informação e a preocupação em protegê-la. Um dos episódios mais significativos foi a criação da máquina Enigma, usada pelos exércitos alemães na Segunda Guerra Mundial para criptografar e decifrar as mensagens enviadas às suas tropas. A Enigma surgiu da necessidade dos alemães de assegurar o sigilo de suas comunicações (Mascarenhas Neto; Araújo, 2019). Em vista disso, Alexandria (2009) afirma que sempre que surge uma nova tecnologia para gravação, armazenamento ou transmissão de informações, geralmente, logo aparecem métodos que buscam explorar possíveis vulnerabilidades dessa inovação. Em resposta, são desenvolvidos também mecanismos para proteger as informações processadas por essa nova tecnologia.

De acordo com Silva (2021), a segurança de dados envolve as medidas adotadas por uma organização para proteger suas informações e impedir o acesso não autorizado. Nesse contexto, o gerenciamento e a proteção de dados vêm sendo cada vez mais discutidos e aplicados no ambiente organizacional, especialmente porque as políticas de segurança da informação exigem que tanto instituições públicas quanto privadas assegurem a proteção de seus dados. Além disso, a privacidade de dados está diretamente relacionada aos direitos individuais dos usuários, com foco na coleta e processamento adequado de suas informações.

Diante dessa necessidade crescente por proteção, legislações e diretrizes, têm sido fundamentais para garantir os pilares da segurança da informação — confidencialidade, integridade e disponibilidade. A Lei Geral de Proteção de Dados (LGPD), promulgada em 2018, surgiu como um marco regulatório no Brasil, com o objetivo de assegurar a privacidade e os direitos dos indivíduos frente ao tratamento de dados pessoais, especialmente em um cenário fortemente influenciado pelas tecnologias digitais (Ramos et al., 2024).

Essa legislação estabelece fundamentos e princípios essenciais que orientam o uso e tratamento dos dados, como o respeito à privacidade, a autodeterminação informativa e a segurança, a qual exige das organizações medidas técnicas e administrativas para garantir o uso responsável dessas informações (Araújo Neto; Aguiar, 2024). Além disso, a LGPD determina

que incidentes de segurança que comprometam os dados devem ser comunicados às autoridades competentes e aos titulares, reforçando a transparência e a responsabilidade.

Somado a isso, normas internacionais como a ISO/IEC 27001 e a NBR ISO/IEC 27002 fornecem diretrizes práticas para a implementação de sistemas de gestão de segurança da informação, que estabelecem controles para proteger os ativos informacionais e fortalecer a confiança entre as partes envolvidas (Araújo Neto; Aguiar, 2024). Essas regulamentações e normas demonstram como a segurança de dados é essencial para a gestão empreendedora em plataformas digitais, que exigem adaptações contínuas para lidar com os riscos e garantir a conformidade legal.

Assim, empresas que utilizam sistemas de informação para gerenciar dados pessoais devem tratá-los de acordo com as exigências legais, conforme reforça Silva (2021). Dessa forma, Souza et al. (2021) destacam que à medida que a sociedade e as organizações crescem, a informação se torna um recurso estratégico de valor crescente, capaz de melhorar os serviços corporativos e servir como um instrumento multifuncional.

Levando isso em consideração, no passado, as informações eram armazenadas em papel e guardadas em caixas ou pastas. Com o crescimento das empresas e o aumento da complexidade das atividades, tornou-se necessário automatizar e simplificar o processo de gestão e armazenamento de dados (Oliveira et al., 2022). Com o avanço da era digital, não é mais necessário um espaço físico com prateleiras ou gavetas para arquivar documentos, visto que a internet facilita o armazenamento digital, aumentando a eficiência e a capacidade de gerenciamento de dados. Entretanto, o grande volume de dados que circula pela rede, incluindo informações confidenciais e estratégicas, exige uma estratégia de segurança robusta, garantindo que apenas pessoas autorizadas possam acessar, modificar ou atualizar essas informações (Galvão; Costa, 2023).

Logo, para assegurar essa gestão estratégica da segurança de dados no ambiente empresarial, é fundamental considerar os pilares essenciais da segurança da informação: integridade, confidencialidade e disponibilidade. Segundo Silva (2022), a **confidencialidade** visa restringir o acesso não autorizado por meio de senhas e controles, garantindo que apenas pessoas autorizadas possam acessar informações e preservando a privacidade dos dados. Para reforçar essa confidencialidade, é importante contar com profissionais especializados em cada área da empresa, capacitados para gerenciar esses dados e reduzir riscos de vazamentos. Já a **integridade**, conforme explana Leal (2023), assegura que as informações permaneçam inalteradas desde sua origem, protegendo-as contra modificações não autorizadas, acidentais ou intencionais. E, por fim, a **disponibilidade** refere-se à garantia de que os sistemas e as informações estejam acessíveis de forma contínua sempre que forem requisitados, garantindo o funcionamento adequado das operações e o acesso oportuno por usuários autorizados (Costa; Galvão, 2023).

Nesse sentido, a proteção de dados é uma prioridade para empresas e indivíduos, pois falhas podem comprometer os pilares da segurança da informação (Galvão; Costa, 2023). A adoção de tecnologias oferece um diferencial competitivo, especialmente na era da transformação digital, onde a internet facilita muitos processos organizacionais. No entanto, o avanço tecnológico também aumenta o número de ataques e ameaças frequentemente, em um ritmo superior ao das inovações em segurança. Consequentemente, mesmo as empresas que adotam tecnologias avançadas de proteção podem, simultaneamente, se expor a novas vulnerabilidades (Pereira et al., 2022).

À vista disso, pode-se definir ameaças como fatores que podem comprometer informações ao explorar vulnerabilidades, resultando na perda de confidencialidade, integridade e disponibilidade, com impactos negativos nos negócios (Leal, 2023). Essas ameaças podem ser intencionais, quando há a intenção deliberada de causar prejuízos à organização, como em casos de sabotagem ou vazamento proposital de dados; ou acidentais, que ocorrem sem a in-

tenção de dano, geralmente causadas por erros humanos, falta de capacitação ou descuidos operacionais. Também se classificam em passivas, quando não geram consequências perceptíveis de imediato para o funcionamento da empresa, como a simples observação ou interceptação de dados sem alteração; e ativas, que envolvem ações diretas de alteração ou corrupção das informações, comprometendo sua veracidade e confiabilidade.

Além disso, podem ser internas, quando originadas de dentro da própria organização, por colaboradores ou prestadores de serviço; ou externas, quando partem de agentes fora do ambiente corporativo, como cibercriminosos ou concorrentes (Pereira et al., 2022). A análise dessas ameaças permite identificar vulnerabilidades e corrigi-las de forma mais eficaz.

Logo, é essencial que as empresas adotem políticas e técnicas de segurança para proteger os ativos dos usuários e da organização. Segundo Costa (2023), manter sistemas atualizados e utilizar antivírus eficazes é crucial, já que *hackers* exploram falhas em *softwares* desatualizados. Para mais, Teixeira, Fracarolli Junior e Reggiolli (2023) destacam a autenticação multifatorial, biométrica e a criptografia de dados como principais medidas de proteção. Ademais, limitar o acesso a dados a profissionais autorizados e garantir a criptografia e *backups* previnem acessos indevidos e perda de informações.

Mediante o atual contexto de transformação digital, as tendências de segurança de dados refletem a crescente sofisticação das ameaças cibernéticas e a adaptação das empresas para proteger informações sensíveis. De acordo com Braz (2023), o avanço tecnológico confere aos sistemas de Inteligência Artificial (IA) uma vantagem singular na luta contra ameaças cibernéticas de maneira eficiente. A capacidade da IA de analisar grandes quantidades de dados rapidamente possibilita a identificação, prevenção e reação em tempo real a possíveis ataques. Com a análise de padrões e irregularidades, a IA proporciona uma segurança robusta e altamente sofisticada.

Perante o exposto, Martinelli e Lahr (2021) argumentam, também, que com o aumento constante das ameaças, tornou-se imprescindível adotar medidas corporativas, como capacitar e conscientizar os funcionários sobre a importância de estarem alertas a ataques de *phishing*, engenharia social e possíveis fraudes. Além disso, é fundamental reforçar os protocolos de segurança vigentes e incentivar os funcionários a reportarem qualquer irregularidade sem hesitação.

Para tanto, Santana (2022) defende que as organizações precisam considerar que mudanças são indispensáveis e devem ocorrer gradualmente ao longo do tempo. Assim, as expectativas futuras na área de segurança de dados apontam para um avanço no desenvolvimento de tecnologias, com esforços globais crescentes voltados à criação de novas ferramentas que possam aprimorar o gerenciamento da segurança em redes de internet (Oliveira, 2020), inclusive no tocante à gestão empreendedora.

2.2 Gestão empreendedora

A competitividade é impulsionada pela entrada de novos negócios no mercado. Com isso, a maneira de competir força o empreendedor a se adaptar, não apenas em termos de conceitos e valores, mas também através da inovação tecnológica, estrutural e comportamental. Em outras palavras, o mercado necessita de novas posturas e ferramentas estratégicas, uma vez que as inovações tecnológicas e as mudanças econômicas exigem que os empreendedores adotem novos paradigmas (Gonçalves; Correia; Albertins, 2023).

Diante disso, atualmente, o empreendedorismo se destaca como um dos temas mais debatidos e amplamente disseminados em diversas áreas do conhecimento, com significativos avanços tanto na teoria quanto na prática no campo da gestão (Backes et al., 2021). Nesse sentido, segundo Borges (2020), a gestão empreendedora introduziu recentes práticas gerenciais, sendo o empreendedorismo uma delas.

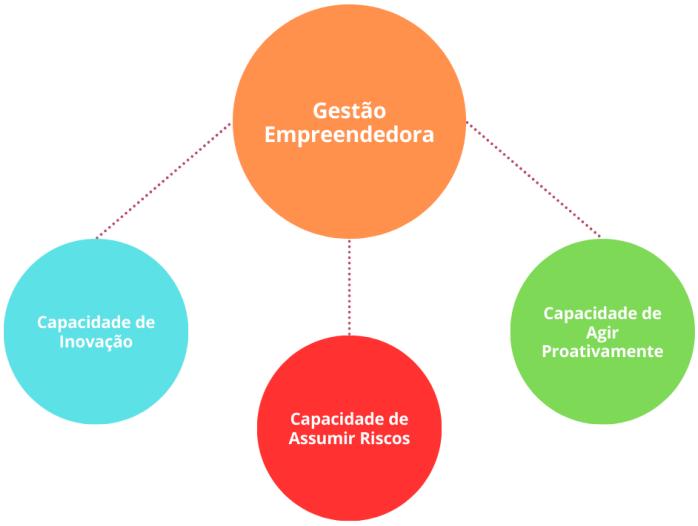
O termo empreendedorismo, de acordo com a literatura, é utilizado para descrever o trabalho autônomo ou o início de um novo empreendimento. Outras definições associam o conceito à inovação e ao processo de (re)criar, avaliar e aproveitar oportunidades, bens e serviços (Backes et al., 2021). Embora o empreendedorismo já fosse uma prática comum na maioria dos países desenvolvidos, seu crescimento global acelerou na década de 1900 e ganhou ainda mais força nos anos 2000. No Brasil, o movimento empreendedor seguiu essa linha temporal, consolidando-se com a criação do Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE) na década de 1990 (Borges, 2020).

De acordo com Pereira, Oliveira Junior e Baptista (2018), a gestão empreendedora pode ser definida como um processo contínuo de aprimoramento e busca por novas oportunidades de negócio. Diferente da gestão tradicional, que se concentra em adaptar-se às mudanças do ambiente, a gestão empreendedora promove essas mudanças de forma a beneficiar tanto a organização quanto a sociedade em geral.

Borges (2020) destaca que o modelo de gestão empreendedora surgiu nos Estados Unidos, no final dos anos 70, quando grandes empresas americanas começaram a perder mercado e competitividade para empresas japonesas. Essas organizações perceberam que, para manter suas posições no mercado, precisariam reestruturar suas formas de gestão. A partir daí, as empresas americanas passaram a focar mais em seus processos internos, promovendo inovações em produtos, serviços e tecnologias, além de melhorar o relacionamento com funcionários, fornecedores e clientes. Esse esforço de adaptação levou ao desenvolvimento do modelo de gestão empreendedora.

A partir disso, Backes et al. (2021) defendem que o modo de gestão empreendedora é caracterizado em três dimensões, conforme apresentados na figura a seguir:

Figura 1 - Dimensões da gestão empreendora



Fonte: Elaborada pela autora, 2025.

Conforme Silva e Nobrega (2018), as dimensões se caracterizam da seguinte forma:

- **Capacidade de inovação** - É caracterizada por indivíduos que continuamente geram novas ideias e se destacam por oferecer soluções únicas, abordando problemas de maneira diferenciada. Essa habilidade está associada à aptidão para pensar de forma al-

ternativa, utilizando a criatividade não apenas para enfrentar desafios, mas também para impulsionar os resultados e aumentar a lucratividade da empresa;

- **Capacidade de assumir riscos** - Está relacionada à habilidade do empreendedor de enfrentar desafios de forma cautelosa, optando por riscos moderados e bem calculados. O empreendedor deve buscar esses riscos de maneira estratégica, onde as recompensas obtidas estejam diretamente ligadas à sua disposição em assumir tais riscos;
- **Capacidade de agir proativamente** - Refere-se à habilidade do empreendedor de identificar e aproveitar oportunidades de forma antecipada, tomando iniciativas antes de ser solicitado. Ademais, o empreendedor é aquele que age de forma rápida e utiliza diversas estratégias alternativas para lidar com desafios, assumindo a responsabilidade pelo cumprimento dos objetivos e metas estabelecidos.

Diante do exposto, a gestão empreendedora desempenha um papel essencial na sobrevivência e no sucesso das empresas atuais. Ela é uma via importante para promover inovação, a qual gera benefícios tanto para a organização quanto para seus colaboradores e para a sociedade (Dourado; Schmidt; Daga Cielo, 2023). Ademais, para Backes et al. (2021), a gestão empreendedora, além de aumentar as oportunidades de emprego tanto em países desenvolvidos quanto em desenvolvimento, contribui para o crescimento econômico e melhora os padrões de vida social e individual ao aproveitar oportunidades.

Nesse sentido, Ribeiro (2021) entende que as transformações nas empresas são impulsionadas pela rápida evolução do mercado. Tanto em nível global quanto nacional, as organizações precisam se reinventar continuamente. Em tal cenário, criar uma cultura empreendedora dentro das empresas envolve aprimorar a gestão, de modo a incentivar os funcionários a adotarem um comportamento empreendedor, capaz de converter desafios em oportunidades.

Por conseguinte, nos últimos anos, as organizações têm se reestruturado para melhorar seus processos, produtos e serviços, pois, sem essas adaptações, enfrentarão dificuldades em um mercado altamente competitivo. A principal força impulsionando essas mudanças é a tecnologia (Ribeiro, 2021). Conforme Sanchez e Araújo (2019) afirmam, diante de tantas mudanças, as empresas precisam focar na transformação digital, que é um dos passos iniciais para a modernização dos negócios.

Em síntese, neste cenário de constante mudança, com clientes mais exigentes e concorrentes mais capacitados, as empresas precisam não apenas se reinventar, mas também aprimorar suas tecnologias e métodos de gestão. Dessa forma, é essencial não só desenvolver novas soluções para problemas conhecidos, mas também aplicar conceitos inovadores em seus produtos e serviços (Ribeiro, 2021).

2.3 Plataformas digitais

A partir dos anos 2000, as plataformas digitais se consolidaram como gestoras de negócios, com o objetivo de intermediar e simplificar as conexões entre consumidores e fornecedores de serviços utilizando a Internet. Por conseguinte, segundo Oliveira (2019), o conceito de plataforma digital tem evoluído ao longo do tempo, resultando em diversas definições devido à sua natureza multidisciplinar. No entanto, não há uma definição única que se aplique a todos os casos, tornando impossível generalizar o termo "plataforma digital" de forma universal.

As plataformas digitais também podem ser vistas como redes coordenadas por um agente central, que pode ser uma empresa ou uma instituição, tendo a possibilidade de ser pública ou privada (Chiarini et al., 2023). Diante das transformações digitais e tecnológicas dos últimos anos, esses ambientes virtuais têm influenciado cada vez mais a organização das atividades econômicas e sociais, tanto no cenário *on-line* quanto *off-line*.

À vista disso, uma plataforma digital funciona como um intermediário digital que oferece serviços destinados a simplificar processos e formas tradicionais de transação. Além disso, atua como uma rede que conecta diferentes participantes (Oliveira, 2019). As lojas físicas, antes essenciais, agora perdem relevância, já que o cenário global está passando por uma transformação na organização do trabalho. As relações se tornam mais flexíveis, e as transações entre consumidores e fornecedores são simplificadas por meio de aplicativos digitais automatizados (Paz, 2023).

De acordo com Cezar et al. (2018), à medida que a Internet se expande, observa-se um aumento significativo de diferentes tipos de plataformas digitais, que oferecem uma variedade de funcionalidades. Esses sistemas promovem a troca de informações e influências entre os usuários, permitindo que discutam interesses pessoais, marcas e produtos. Diversos *sites*, plataformas de redes sociais e comunidades *on-line* surgiram com esse propósito, não apenas em nível local, mas também atravessando fronteiras entre cidades e países.

Por conseguinte, Oliveira (2019) ressalta que, ao tratar do conceito de plataforma digital, é importante reconhecer a diversidade de tipos de plataformas disponíveis atualmente. Entre elas, Marques (2024) sugere as seguintes tipologias: (i) **plataformas de comércio/venda**, focadas na intermediação de transações de produtos de terceiros, sem serem proprietárias desses itens. Exemplos incluem Amazon e Mercado Livre; (ii) **plataformas de redes sociais digitais**, que facilitam a interação entre indivíduos e grupos, permitindo a criação de perfis, troca de mensagens e publicações. Exemplos são Snapchat e WeChat; (iii) **plataformas de sistemas de aplicações**, que organizam o acesso a um conjunto de aplicativos para dispositivos pessoais, como sistemas operacionais e lojas de *apps*. Exemplos: Windows, Linux, Android/Play Store, iOS/Apple Store; (iv) **plataformas de compartilhamento de bens, serviços e atividades**, que possibilitam a troca e compartilhamento de serviços, bens, tempo e trabalho, seja físico ou intelectual. Exemplos: Uber, Airbnb, Craigslist, TaskRabbit; (v) **plataformas de circulação de conteúdo**, que promovem a disseminação de conteúdos culturais, informativos e científicos. Exemplos incluem YouTube, Google, Spotify, Vimeo, ResearchGate e Academia.edu.

Embora existam diferentes tipos de plataformas digitais, todas compartilham o objetivo de criar modelos de negócios que possibilitem uma maior diversificação de funcionalidades a custos relativamente baixos. Ou seja, independentemente do setor em que atuam ou de seus objetivos principais, essas plataformas buscam atender ou gerar novas demandas entre os usuários (Marques, 2024).

Para Sena e Araújo (2018), apesar da Internet oferecer inúmeros recursos, como conectividade em tempo real e uma significativa expansão no volume de informações transacionadas, ela também intensificou as preocupações relacionadas à segurança do tráfego de dados eletrônicos. A segurança da informação tornou-se crucial para evitar a perda de recursos, o uso não autorizado ou inadequado, a divulgação ou modificação de informações confidenciais, além de prevenir interrupções nas operações organizacionais. As vulnerabilidades presentes em plataformas digitais, como *websites*, representam falhas no *design* de processos ou programas, criando um ambiente suscetível a ameaças e ataques.

Nesse contexto, os recursos mais vulneráveis em plataformas digitais geralmente envolvem componentes que lidam com dados sensíveis e interações dos usuários. Conforme Ferreira (2017), as principais vulnerabilidades exploradas por ataques cibernéticos nos ambientes digitais incluem: o ***SQL Injection***, em que o criminoso explora uma falha no sistema inserindo comandos maliciosos em campos de entrada, como em *sites* ou bancos de dados SQL; o ***Cross-Site Scripting*** (XSS), que também explora a falta de tratamento adequado das informações fornecidas pelos usuários, permitindo que o *hacker* envie comandos para obter ou apagar dados no banco de dados; e o ***Session Hijacking***, em que o invasor rouba o *cookie* de autenticação de um usuário para acessar a plataforma como se fosse ele.

Deste modo, na contemporaneidade, as plataformas digitais estão crescendo em um ritmo muito rápido, já que não há fatores que limitem esse desenvolvimento. Essencialmente, essas plataformas oferecem novas maneiras de atender os mercados, uma vez que as demandas dos usuários estão em constante expansão (Oliveira, 2019).

As tendências futuras das plataformas digitais acompanham o avanço tecnológico e a evolução das expectativas dos usuários e mercados. Segundo Gonçalves (2024), entre elas, o **uso da Inteligência Artificial (IA)** destaca-se por otimizar tarefas e melhorar a tomada de decisões. A **personalização e segmentação avançada** tornam-se essenciais para empresas se diferenciarem em um mercado saturado, gerando fidelidade do cliente e vantagem competitiva. Ademais, a **realidade aumentada** oferece experiências interativas ao combinar elementos virtuais e reais, enquanto as **mensagens instantâneas** possibilitam uma comunicação mais rápida e personalizada, fortalecendo o relacionamento com os consumidores e facilitando a compreensão de seus comportamentos.

Em resumo, apesar dos avanços da tecnologia, conforme mencionados anteriormente, e o crescente uso da internet, criminosos e oportunistas podem acessar dados confidenciais, comprometendo tanto a privacidade dos usuários quanto a segurança das organizações, o que pode impactar negativamente os negócios. Para mitigar essas ameaças, as empresas tornaram-se cada vez mais dependentes da segurança de dados em suas plataformas digitais, visando proteger conjuntos específicos de informações. Essas medidas de proteção são essenciais para qualquer organização que manipula dados, uma vez que todas geram informações próprias que devem ser preservadas para garantir sua integridade e segurança (Oliveira; Filgueiras, 2022).

3 PROCEDIMENTOS METODOLÓGICOS

O trabalho tem como objetivo geral analisar a percepção dos profissionais de tecnologia em relação à segurança de dados na gestão empreendedora em plataformas digitais, caracterizando-se como uma pesquisa exploratória-descritiva. Conforme Silva et al. (2020), a pesquisa de caráter exploratório busca promover uma familiarização com temas ainda pouco investigados ou conhecidos, a fim de proporcionar um maior entendimento sobre o assunto ao final do estudo, possibilitando a construção de novas hipóteses. Esse tipo de pesquisa permite ao leitor aprofundar seu conhecimento no tema estudado, tornando-o apto a analisar os aspectos abordados e formular hipóteses com base nos resultados obtidos. No que tange às pesquisas descritivas, essas visam levantar informações detalhadas sobre uma população ou fenômeno, utilizando técnicas específicas para entender suas características. Além de descrever o objeto de estudo, permitem a análise de relações entre variáveis (Marzzoni et al., 2021).

Em vista disso, optou-se por utilizar uma abordagem qualitativa que, de acordo com Sousa e Santos (2020), foca na interpretação das relações sociais e na compreensão da dinâmica dessas interações. Ademais, esse método se aplica ao estudo de aspectos como história, crenças, percepções e opiniões, baseando-se nas interpretações humanas sobre suas experiências e construções, permitindo uma investigação mais adequada de grupos específicos, análises de discursos e documentos, e histórias sociais sob a perspectiva dos próprios atores envolvidos.

No que diz respeito aos métodos técnicos de investigação, o estudo caracteriza-se como um estudo de múltiplos casos, já que foram realizadas entrevistas com pessoas de diferentes empresas. Conforme Valle (2023), esse método busca compreender de maneira aprofundada, a realidade de um indivíduo, grupo de pessoas ou organizações, através das relações estabelecidas entre suas variáveis. Ainda de acordo com Valle (2023), o estudo de caso trata-se de uma pesquisa empírica que explora um fenômeno dentro do seu contexto no mundo real.

Para a coleta de dados, foi utilizado um roteiro de entrevistas elaborado por meio do *software* Google Forms, cuja aplicação seguiu um formato estruturado, no período de 17/03/25 a 31/03/25, proporcionando mais conforto e praticidade aos participantes, permitindo que respondessem conforme suas disponibilidades. O roteiro de entrevistas foi composto por 9 perguntas, que estão disponíveis ao final deste trabalho, no apêndice A.

Para a escolha dos sujeitos de pesquisa, foi feita uma seleção por conveniência, considerando que a pesquisadora possui conhecimento e fácil acesso aos possíveis entrevistados dentro da população alvo da pesquisa. Os demais sujeitos foram selecionados posteriormente, utilizando a técnica *snowball sampling*. Segundo Roman Junior et al. (2022), essa técnica de amostragem conhecida também como "bola de neve" é um método não probabilístico, no qual o pesquisador colabora com especialistas da comunidade, reconhecidos por seu conhecimento sobre o tema da pesquisa. Esse método se distingue pelo fato de que os primeiros participantes do estudo indicam novos participantes, e esse ciclo continua até que se atinja o objetivo proposto ou o ponto de saturação (Lima et al., 2021). O total de participantes nesta pesquisa foi de 12 sujeitos e o quadro 1 traz os respectivos perfis de cada um:

Quadro 1 - Perfil dos entrevistados

Entrevistados	**Gênero**	**Idade**	**Grau de Escolaridade**	**Cargo**	**Tempo na Empresa**
Entrevistado 01	Masculino	28 anos	Ensino Superior	Engenheiro de Dados	1 mês
Entrevistado 02	Masculino	36 anos	Ensino Superior	Analista de Suporte Técnico Pleno	13 anos
Entrevistado 03	Masculino	26 anos	Ensino Médio	Analista	1 ano e 2 meses
Entrevistado 04	Masculino	20 anos	Ensino Superior	Estagiário	6 meses
Entrevistado 05	Masculino	26 anos	Ensino Superior	Analista	6 meses
Entrevistado 06	Feminino	27 anos	Pós-graduação	Desenvolvedor *Fullstack*	2 anos
Entrevistado 07	Masculino	29 anos	Ensino Superior	Suporte Técnico n2	3 anos
Entrevistado 08	Masculino	20 anos	Ensino Superior	Desenvolvedor *Web*	1 ano
Entrevistado 09	Masculino	21 anos	Ensino Superior	Desenvolvedor Pleno	3 anos
Entrevistado 10	Masculino	23 anos	Pós-graduação	Engenheiro de software	6 meses
Entrevistado 11	Masculino	29 anos	Ensino Superior	Analista de Sistemas	2 anos
Entrevistado 12	Masculino	23 anos	Ensino Superior	Estatístico	8 meses

Fonte: Elaborada pela autora, 2025.

Dessa forma, é importante destacar, entre as informações fornecidas pelos entrevistados, a relevância de garantir sua segurança. Para preservar suas identidades e privacidade, foram utilizados pseudônimos na coleta dos relatos e informações. Além disso, o recurso do *Ipsis Litteris* foi aplicado para assegurar que as declarações fossem transcritas exatamente como foram ditas.

Por fim, para a análise dos dados, foi adotado o método da análise de conteúdo que, de acordo com Flick (2009), refere-se a uma técnica tradicional utilizada para examinar textos de diferentes fontes, como entrevistas. O processo envolve a utilização de categorias baseadas em modelos teóricos, a fim de organizar o conteúdo dos textos, classificando declarações, frases ou palavras em um sistema de categorias. Em vista do que foi apresentado, o estudo foi dividido em três categorias, *a priori*, organizadas da seguinte maneira: **ações referentes à segurança de dados; práticas empreendedoras; o uso dos recursos das plataformas digi-**

tais. Elas foram fundamentadas na revisão bibliográfica e nos objetivos específicos desenvolvidos neste estudo, sendo discutidas e analisadas a seguir.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

A análise e interpretação dos resultados da pesquisa são organizadas em tópicos, conforme a sequência das perguntas presentes no roteiro da entrevista aplicada. Assim, a análise baseia-se nas seguintes categorias identificadas: Ações Referentes à Segurança de Dados; Práticas Empreendedoras; e O Uso dos Recursos das Plataformas Digitais. Para isso, foram coletadas as declarações dos participantes, tendo as respostas apresentadas no decorrer da análise com a apresentação das declarações que mais ressaltam as perguntas.

4.1 Ações referentes à segurança de dados

De acordo com a pergunta 1, "*Quais são os principais desafios que sua empresa já enfrentou ou enfrenta para garantir a segurança dos dados em plataformas digitais e como esses desafios impactam a confidencialidade, integridade e disponibilidade das informações na gestão empresarial?*", algumas das respostas apresentadas foram:

> **Entrevistado 02:** "No ambiente hospitalar, a segurança dos dados é essencial para proteger **informações sensíveis** de pacientes e garantir a continuidade dos serviços. Os principais desafios incluem: **Ataques cibernéticos** (*ransomware*, *phishing*): Podem comprometer a **confidencialidade** dos prontuários e dados clínicos. Conformidade com regulamentações (LGPD): Exige controle rigoroso sobre o **armazenamento** e **compartilhamento de informações**. Erros humanos e acessos indevidos: **Falta de treinamento** pode levar a **vazamentos** acidentais. **Disponibilidade** dos sistemas: Ataques ou falhas podem impactar a assistência médica."
> **Entrevistado 05:** "Os principais desafios que minha empresa enfrenta para garantir a segurança dos dados em plataformas digitais e seus impactos na confidencialidade, integridade e disponibilidade das informações são **ameaças** Cibernéticas Avançadas, conformidade com Regulamentações e **vulnerabilidades** em sistemas legados."
> **Entrevistado 09:** "O **vazamento** de URL de *endpoints* públicos. Esse tipo de falha afeta a confidencialidade, pois **dados privados** podem ser acessados indevidamente; a **integridade**, pois atacantes podem manipular informações sem **autenticação** adequada; e a disponibilidade, já que serviços podem sofrer ataques como DDoS devido ao acesso não controlado."

Ao analisar as respostas obtidas em relação ao questionamento, é possível observar que os entrevistados reconhecem os crescentes desafios das organizações na proteção de dados, diante do avanço das ameaças cibernéticas e da transformação digital. Destacam-se riscos aos pilares da segurança da informação (confidencialidade, integridade e disponibilidade), causados por ataques como *ransomware*, *phishing* e falhas em sistemas. Exemplos como o ambiente hospitalar mostram o impacto direto na continuidade dos serviços. A LGPD também exige maior controle e preparo técnico. Ademais, erros humanos e falhas estruturais aumentam os riscos, reforçando a importância da capacitação contínua e de investimentos em tecnologia. Assim, a segurança da informação é vista como prioridade estratégica, abrangendo aspectos técnicos e humanos.

Essa percepção evidencia a relevância da segurança da informação para a gestão organizacional na era digital. De acordo com Pereira et al. (2022), o avanço tecnológico, apesar de seus benefícios, intensifica vulnerabilidades e amplia as possibilidades de ataques, exigindo conhecimento técnico e estratégias preventivas. Mesmo com recursos avançados de proteção, o fator humano continua sendo o principal alvo, uma vez que muitas violações partem de dentro das instituições, de forma intencional ou não. Nesse contexto, torna-se essencial investir

em capacitação contínua e em políticas de segurança bem definidas, promovendo a conscientização dos colaboradores e o alinhamento institucional às práticas de proteção da informação.

A segunda questão buscou compreender quais estratégias ou tecnologias são utilizadas pelas empresas, segundo a experiência dos entrevistados, para garantir a proteção de dados. Além disso, procurou identificar quais dessas práticas os entrevistados consideram mais eficazes e os motivos que justificam essa escolha. Abaixo estão algumas das respostas fornecidas:

> **Entrevistado 04:** "Criar contas, logins e sessões temporárias, **autenticação multifator** e disponibilização de **cursos de cibersegurança** como material obrigatório."
> **Entrevistado 06:** "Adotamos **criptografia**, autenticação multifator e **monitoramento contínuo** para proteger os dados. Essas práticas são eficazes porque dificultam acessos indevidos e permitem **detectar ameaças** rapidamente"
> **Entrevistado 07:** "Utiliza sempre uma **cadeia de permissões** para os grupos de usuários internos, adota **políticas de segurança** internas, *firewalls* pagos e uso de vpns para acesso remoto."

A partir das respostas apresentadas pelos entrevistados, é possível compreender que as empresas representadas demonstram um comprometimento crescente com a proteção de dados, no que concerne a adoção de práticas como criptografia, autenticação multifator, controle de acessos e políticas internas de segurança. Tais ações evidenciam uma tentativa de mitigar riscos associados ao acesso indevido e à exposição de informações sensíveis. Adicionalmente, é possível observar uma preocupação com a conscientização e capacitação, o que reforça a importância da atuação preventiva frente às ameaças cibernéticas. Isto posto, compreende-se que essas medidas estão alinhadas aos pilares da segurança da informação e refletem um esforço organizacional em acompanhar as exigências impostas pela transformação digital e pela crescente sofisticação dos ataques virtuais.

Com base nas práticas mencionadas pelos entrevistados, observa-se um alinhamento com os princípios da segurança da informação. Conforme Teixeira, Fracarolli Junior e Reggiolli (2023), mecanismos como a autenticação multifatorial e a criptografia são fundamentais para restringir acessos não autorizados, mesmo diante do comprometimento de credenciais. A criptografia, em especial, visa proteger os dados durante sua transmissão, a fim de dificultar possíveis interceptações. Soma-se a isso a importância de políticas de segurança bem estruturadas e da capacitação contínua dos colaboradores, conforme recomenda a NBR ISO/IEC 27002:2013. Tais medidas evidenciam que a combinação entre tecnologia, conscientização e conformidade normativa é essencial para garantir a integridade, confidencialidade e disponibilidade das informações organizacionais.

No que tange ao questionamento 3, *"Como você percebe o impacto das medidas de proteção de dados adotadas atualmente em sua empresa? Elas influenciam a produtividade, a inovação ou o relacionamento com clientes? Justifique sua resposta.*", seguem algumas respostas listadas dos entrevistados.

> **Entrevistado 06:** "Às vezes, podem tornar alguns processos mais demorados, mas no geral, vale a pena. Quando bem implementadas, elas não atrapalham a **produtividade** nem a **inovação**, só garantem que tudo funcione de forma mais segura."
> **Entrevistado 07:** "Quanto mais **seguro** for o ambiente teremos menor **praticidade**, mais é algo necessário em alguns ambientes."
> **Entrevistado 09:** "É significativo, pois influencia diferentes aspectos da empresa. Do ponto de vista da produtividade, pode haver um aumento inicial no tempo de desenvolvimento para implementar **controles**, mas isso se traduz em menos **incidentes de segurança** e **correções emergenciais**."

Ante o exposto, evidencia-se uma compreensão madura sobre o impacto das medidas de segurança da informação na produtividade organizacional. Ainda que alguns apontem uma possível lentidão inicial nos processos, há um consenso de que a implementação adequada dessas medidas não compromete a inovação, mas sim promove um ambiente mais estável e protegido. Os entrevistados reconhecem que a segurança pode demandar mais tempo em etapas iniciais, porém os benefícios se evidenciam na redução de falhas e incidentes ao longo do tempo. Assim, constata-se que a segurança da informação, quando integrada de forma estratégica, não é um obstáculo à produtividade, mas uma aliada na construção de sistemas mais eficientes e sustentáveis.

A partir da análise realizada, é possível identificar uma consonância com a perspectiva teórica apresentada por Oliveira (2020), ao considerar que a segurança da informação, embora demande esforços iniciais e possa impactar momentaneamente a produtividade, é uma condição indispensável para a sustentabilidade dos processos organizacionais. Segundo o autor, a crescente dependência das tecnologias para armazenar e processar dados exige investimentos contínuos em ferramentas e protocolos capazes de mitigar riscos cibernéticos. Dessa forma, constata-se que a integração estratégica da segurança da informação não apenas assegura a integridade dos dados, como também fortalece a confiança dos usuários, viabilizando decisões mais seguras e assertivas em um cenário digital cada vez mais desafiador.

4.2 Práticas empreendedoras

O questionamento 4 buscou identificar, a partir da opinião dos entrevistados, de que forma a gestão empreendedora pode se tornar mais inovadora na busca por soluções de segurança de dados mais eficazes para plataformas digitais. Abaixo estão algumas das respostas fornecidas:

> **Entrevistado 03:** "Sempre manter seus colaboradores **atualizados** com a tecnologia."
> **Entrevistado 06:** "**Testar soluções** antes dos problemas surgirem faz diferença. Além disso, o uso de **IA** pode ajudar na **detecção de ameaças**."
> **Entrevistado 11:** "Acredito que basta um **maior investimento** no fator de segurança como **treinamentos frequentes**, simulações e **revisões** periódicas do sistema."

As respostas dos entrevistados indicam que a gestão empreendedora se torna mais inovadora na segurança de dados ao adotar uma postura preventiva e estratégica, com foco em atualização tecnológica, capacitação contínua e uso de inteligência artificial. As falas refletem uma compreensão de que a inovação na segurança digital deve ser incorporada à cultura organizacional por meio de ações preventivas e estruturadas, capazes de antecipar riscos e fortalecer a resiliência das plataformas digitais. Logo, fica evidente que a efetividade da gestão empreendedora, em contextos digitais, está diretamente relacionada à sua capacidade de se adaptar às novas demandas tecnológicas e de proteger os ativos informacionais de maneira inteligente e dinâmica.

Destarte, a segurança de dados nas plataformas digitais tornou-se uma exigência estratégica no cenário atual da gestão empreendedora. Conforme Gonçalves, Correia e Albertins (2023), a entrada constante de novos negócios no mercado intensifica a competitividade e obriga os empreendedores a se adaptarem por meio da inovação tecnológica, estrutural e comportamental. Nesse contexto, é imprescindível adotar novas ferramentas e posturas que acompanhem as transformações digitais e econômicas, promovendo uma gestão mais dinâmica, segura e eficiente. Dessa forma, a segurança da informação deixa de ser apenas uma medida técnica e passa a integrar o processo de inovação e adaptação contínua exigido pela nova lógica do mercado.

O questionamento 5 apresentou aos participantes a seguinte pergunta: "*Com relação à gestão empreendedora da sua empresa, como você percebe a abordagem em relação aos riscos de segurança de dados? Há uma tendência a adotar medidas mais conservadoras ou a experimentar novas soluções, mesmo com certo nível de risco? Detalhe sua resposta.*" A seguir, são apresentadas algumas das contribuições oferecidas pelos entrevistados em resposta a essa pergunta.

> **Entrevistado 01:** "Super **conservador** afinal tem **dados sensíveis** de créditos, contas, vendas, dados como CPF e CNPJ então tudo é feito com **cautela**."
> **Entrevistado 07:** "São sempre conservadores, prezam bastante pela **segurança**, optam por **parar processos** e operações se realmente for ter alguma **vulnerabilidade**."
> **Entrevistado 12:** "Pelo menos aqui, estamos sempre experimentando **novas soluções**, mas levando sempre em consideração contestar pela **experiência** de outras empresas."

Diante das respostas dos entrevistados, é possível perceber que a gestão empreendedora voltada à segurança de dados assume, predominantemente, uma postura conservadora. Os depoimentos revelam uma tendência à cautela e à preservação da integridade das informações sensíveis, ao demonstrarem uma priorização da estabilidade e prevenção de riscos. Ainda que haja abertura para o uso de novas soluções tecnológicas, como apontado por um dos participantes, tal inovação ocorre de forma ponderada e baseada em referências externas. Isso sugere uma busca por equilíbrio entre a experimentação e a segurança, o qual indica que a tomada de decisões é cuidadosamente estruturada para minimizar vulnerabilidades.

A maneira como as empresas lidam com os riscos de segurança de dados revela um comportamento estratégico que visa equilibrar prudência e inovação. Nesse contexto, Silva e Nobrega (2018) ressaltam que a capacidade de assumir riscos está diretamente ligada à habilidade do empreendedor de enfrentar desafios de maneira calculada, optando por caminhos que ofereçam recompensas proporcionais aos riscos assumidos. Assim, a gestão empreendedora, ao lidar com dados sensíveis e operações críticas, tende a adotar decisões fundamentadas em estratégias seguras, a qual prioriza a estabilidade e a continuidade dos processos, sem, no entanto, descartar completamente a possibilidade de inovação quando esta se mostra bem embasada.

O questionamento 6 buscou compreender de que maneira os entrevistados percebem a atuação da gestão empreendedora no que se refere ao risco calculado e à proatividade na abordagem da segurança de dados dentro de suas empresas. A seguir, destacam-se algumas das contribuições apresentadas:

> **Entrevistado 04:** "Na **divisão das permissões** entre os cargos, e na obrigatoriedade de terminar o **curso** sobre **cibersegurança**."
> **Entrevistado 08:** "Utilizando ***backups***, **monitoramento** constante das aplicações e serviços e sempre buscar utilizar **versões atualizadas** das bibliotecas externas etc."
> **Entrevistado 09:** "O **risco** é avaliado com base no **potencial impacto** e na **probabilidade** de ocorrência, permitindo decidir quando inovar e quando ser mais **cauteloso**."

Segundo as respostas obtidas, observa-se que as empresas vêm adotando práticas que refletem uma atuação empreendedora voltada à segurança de dados, com destaque para a adoção de medidas organizacionais e tecnológicas com uma maior preocupação estratégica na mitigação de riscos. A divisão criteriosa de permissões, o investimento em capacitação, o uso de backups, o monitoramento contínuo e a atualização constante de ferramentas indicam uma postura voltada à eficiência operacional e à antecipação de possíveis vulnerabilidades. Essas ações evidenciam uma gestão que busca não apenas responder a desafios, mas, principalmen-

te, preveni-los, priorizando decisões alinhadas a um contexto dinâmico, competitivo e cada vez mais dependente de soluções tecnológicas eficazes.

Conforme destacam Dourado, Schmidt e Daga Cielo (2023), a gestão empreendedora é um elemento crucial para o êxito e a continuidade das empresas na atualidade, pois promove a inovação como ferramenta estratégica que beneficia não apenas a organização, mas também seus colaboradores e a sociedade em geral. Nesse sentido, Ribeiro (2021) destaca que, em um cenário de transformações constantes e alta competitividade, é imprescindível que as empresas adotem tecnologias avançadas e métodos de gestão mais eficientes, capazes de oferecer soluções criativas e diferenciadas. Essa perspectiva evidencia a importância de uma atuação proativa e orientada ao risco calculado na segurança de dados, permitindo decisões equilibradas entre inovação e proteção.

4.3 O uso dos recursos das plataformas digitais

O sétimo questionamento investigou a percepção dos entrevistados sobre a aplicação da segurança de dados no contexto da crescente utilização de plataformas digitais para a gestão de negócios. Dessa forma, foram dispostas, a seguir as principais respostas dos entrevistados:

> **Entrevistado 07:** "Desde que devidamente **armazenados** em **servidores** bem **estruturados** e com monitoramento adequado, acredito que é o progresso, estamos evoluindo a uma velocidade em que vai ser bem mais prático **manter dados** em nuvens."
> **Entrevistado 10:** "Nesse ambiente existem diversas postagens ou **publicações** que podem levar a situações em que **conteúdos maliciosos** são expostos."
> **Entrevistado 11:** "A segurança é muito **robusta** e a plataforma ainda fornece **treinamentos** gratuitos para garantir a **segurança** e **integridade dos dados**."

A partir das respostas apresentadas pelos entrevistados, é possível observar que a percepção sobre a segurança de dados em plataformas digitais varia entre a confiança na robustez dos sistemas e a preocupação com potenciais vulnerabilidades. Os colaboradores destacam que a adoção de servidores bem estruturados, monitoramento adequado e treinamentos específicos reforça a segurança, consolidando o ambiente digital como uma solução prática e eficiente para a gestão de negócios. No entanto, também há a consciência de que a exposição a conteúdos maliciosos representa um risco, evidenciando a dualidade entre os benefícios e os desafios inerentes à crescente digitalização. Essa visão reflete a importância contínua de medidas que garantam a integridade dos dados, alinhando-se à necessidade de proteção em um cenário de transformação tecnológica acelerada.

Essa percepção está alinhada com o que afirmam Sena e Araújo (2018), ao destacarem que, embora a internet ofereça vantagens como conectividade e amplo acesso à informação, ela também amplia os riscos relacionados à segurança dos dados eletrônicos. Diante disso, a segurança da informação surge como um elemento crucial para evitar perdas, uso indevido ou exposição de dados sensíveis, além de garantir a continuidade das operações organizacionais. Essa discussão reforça a necessidade de medidas robustas, como servidores bem monitorados e treinamentos especializados, para mitigar as vulnerabilidades inerentes às plataformas digitais, equilibrando os benefícios da transformação tecnológica com a proteção contra ameaças cibernéticas.

Em relação ao questionamento 8, que apresenta a seguinte pergunta: "*Na sua opinião, quais são os principais riscos de segurança que as empresas enfrentam ao utilizar plataformas digitais para a gestão de negócios?*", foram listadas a seguir algumas respostas dos entrevistados:

> **Entrevistado 01:** "A principal é cair em **golpe**, ***fishing***, cair em reuniões usando ***deep fake***, se não me engano algum grande gestor de banco caiu em um golpe desses em 2024 então todo **cuidado** é pouco."
> **Entrevistado 03:** "**Risco** de **vazamento de informação,** mas quando **confiamos** na empresa isso se torna mais fácil de lidar."
> **Entrevistado 09:** "Vazamento de Dados Sensíveis, Ataques Cibernéticos (*Ransomware*, *Phishing*, DDoS), **Falhas** em APIs e Integrações, **Fraudes** e **Engenharia Social**."

As respostas dos entrevistados indicam uma percepção clara sobre os principais riscos de segurança enfrentados pelas empresas no uso de plataformas digitais. Entre os mais citados estão o vazamento de dados sensíveis, ataques cibernéticos — como *phishing*, *ransomware* e DDoS —, além de fraudes envolvendo engenharia social e o uso de tecnologias como *deep fake*. Tais riscos evidenciam a complexidade crescente das ameaças digitais e reforçam a necessidade de adoção de práticas preventivas, tanto técnicas quanto educativas, para garantir a integridade das informações e a continuidade das operações empresariais.

Essa percepção está em consonância com Ferreira (2017), que aponta falhas como *SQL Injection*, *Cross-Site Scripting* e *Session Hijacking* como formas recorrentes de exploração maliciosa em ambientes digitais. Oliveira (2019) complementa essa perspectiva ao ressaltar que o crescimento acelerado das soluções digitais amplia a superfície de ataque das organizações, exigindo medidas contínuas de proteção. Tais riscos não se limitam a aspectos técnicos, mas envolvem também fatores humanos, como a suscetibilidade a fraudes e manipulações baseadas em engenharia social, que têm se sofisticado com o uso de tecnologias emergentes. Assim, torna-se evidente a necessidade de uma abordagem integrada de segurança da informação, que envolva tanto infraestrutura tecnológica robusta quanto políticas de conscientização e prevenção dentro das empresas.

Por fim, o questionamento 9 buscou identificar, por meio das respostas dos entrevistados, como avaliam o nível de conscientização dos profissionais de tecnologia em relação aos riscos de segurança de dados em plataformas digitais. Assim, foram apresentadas as principais opiniões relatadas por alguns dos entrevistados:

> **Entrevistado 02:** "**Conscientização** é **alta**, o problema é convencer as **gestões** para que **invistam** nesta segurança."
> **Entrevistado 08:** "Penso que boa parte dos **profissionais** não tratam a **segurança dos dados** com a **importância** que ela tem em qualquer tipo de **sistema digital**."
> **Entrevistado 10:** "**Baixo**, a maioria não se **atenta** aos riscos."

De acordo com as respostas obtidas, observa-se uma percepção divergente entre os entrevistados no que diz respeito ao nível de conscientização dos profissionais de tecnologia quanto aos riscos associados à segurança de dados em plataformas digitais. Enquanto alguns participantes reconhecem um grau razoável de conhecimento técnico por parte desses profissionais, há um consenso de que tal conscientização nem sempre se traduz em práticas efetivas ou em investimentos concretos por parte das empresas. Além disso, foi mencionada uma postura de negligência por parte de certos profissionais, que tendem a subestimar os riscos envolvidos. Esse cenário revela um desafio persistente: embora as plataformas digitais estejam cada vez mais presentes nas organizações, o comprometimento com a proteção de dados ainda é desigual entre os envolvidos.

A conscientização sobre segurança de dados é um desafio crítico na transformação digital. Oliveira e Filgueiras (2022) apontam que, embora os avanços tecnológicos ampliem as capacidades das plataformas digitais, também aumentam a exposição a ameaças, exigindo medidas de proteção robustas. Contudo, muitos profissionais, apesar de compreenderem os riscos, subestimam sua gravidade ou enfrentam barreiras para implementar soluções. Essa dis-

tância entre teoria e prática revela uma lacuna preocupante, já que a segurança da informação é um pilar estratégico dos negócios. Em suma, além da capacitação, é necessária uma mudança cultural que priorize a proteção de dados em todos os níveis organizacionais.

4.4 Quadro-resumo com os principais achados

O quadro 2 procura resumir os principais resultados da pesquisa, dividido em três categorias distintas: "Ações Referentes à Segurança de Dados", que contempla os desafios enfrentados pelas empresas, as estratégias adotadas para proteção das informações e os respectivos impactos na gestão e no relacionamento com os clientes; "Práticas Empreendedoras", que discute a abordagem da gestão inovadora diante dos riscos digitais, com ênfase na proatividade e na adoção de soluções eficazes; e "O Uso dos Recursos das Plataformas Digitais", que explora percepções sobre a aplicação da segurança de dados, os principais riscos identificados e o nível de conscientização dos profissionais de tecnologia frente a essas questões.

Quadro 2 - Principais Achados

Categorias	Subcategorias	Códigos	Principais Resultados
Ações Referentes à Segurança de Dados	Desafios na garantia da segurança de dados	informações sensíveis; Ataques cibernéticos; confidencialidade; armazenamento; compartilhamento de informações; Falta de treinamento; vazamentos; Disponibilidade; ameaças; vulnerabilidades; vazamento; dados privados; integridade; autenticação.	Pode-se concluir que os desafios enfrentados pelas empresas para garantir a segurança dos dados em plataformas digitais não comprometem apenas aspectos técnicos da gestão, mas também colocam em risco pilares fundamentais como a confidencialidade, integridade e disponibilidade das informações, que exige preparo estratégico diante de ameaças cibernéticas, erros humanos e exigências legais.
	Estratégias e tecnologias de proteção adotadas	autenticação multifator; cursos de cibersegurança; criptografia; monitoramento contínuo; detectar ameaças; cadeia de permissões; políticas de segurança.	Os entrevistados reconhecem a importância da adoção de estratégias preventivas, como criptografia, autenticação multifator, controle de acessos e capacitação contínua, os quais destacam tais práticas como eficazes para mitigar riscos e fortalecer a proteção de dados frente às crescentes ameaças digitais.
	Efeitos das medidas de segurança na operação empresarial	produtividade; inovação; seguro; praticidade; controles; incidentes de segurança; correções emergenciais.	É perceptível que, embora as medidas de proteção de dados possam, inicialmente, tornar alguns processos mais demorados, os entrevistados destacam sua relevância na construção de um ambiente mais seguro, reconhecendo que, a longo prazo, tais ações fortalecem a produtividade, reduzem incidentes e promovem maior estabilidade organizacional.

Práticas Empreendedoras	Inovação na gestão de segurança de dados	atualizados; Testar soluções; IA; detecção de ameaças; maior investimento; treinamentos frequentes; revisões.	As respostas apontam que a gestão empreendedora se torna mais inovadora ao investir em atualização tecnológica, capacitação contínua e uso de inteligência artificial, por meio da adoção de práticas preventivas e estratégicas que antecipam riscos e fortalecem a segurança das plataformas digitais.
	Postura da gestão frente a riscos	conservador; dados sensíveis; cautela; segurança; parar processos; vulnerabilidade; novas soluções; experiência.	Os participantes indicam que a gestão empreendedora tende a adotar, predominantemente, uma abordagem conservadora frente aos riscos de segurança de dados, a qual prioriza a integridade das informações e a estabilidade dos processos, ainda que haja espaço para inovação de forma cautelosa e baseada em experiências anteriores.
	Proatividade na tomada de decisões	divisão das permissões; curso; cibersegurança; backups; monitoramento; versões atualizadas; riscos; potencial impacto; probabilidade; cauteloso.	A adoção de riscos calculados na segurança de dados envolve uma postura estratégica e preventiva, com destaque para o controle de permissões, capacitações obrigatórias, uso de backups e atualizações constantes. Tais medidas demonstram como a proatividade pode fortalecer a eficiência operacional e antecipar riscos em ambientes digitais.
O Uso dos Recursos das Plataformas Digitais	Aplicabilidade da segurança de dados em ambientes digitais	armazenados; servidores; estruturados; manter dados; publicações; conteúdos maliciosos; robusta; treinamentos; segurança; integridade dos dados.	Diante das respostas dos entrevistados, identificou-se uma percepção dividida quanto à segurança de dados em plataformas digitais. Enquanto alguns confiam na robustez dos sistemas e valorizam práticas como monitoramento e treinamentos, outros demonstram preocupação com possíveis vulnerabilidades e exposição a conteúdos maliciosos.
	Principais riscos associados às plataformas digitais	golpe; fishing; deep fake; cuidado; Risco; vazamento de informação; confiamos; Falhas; Fraudes; Engenharia Social.	Os principais riscos de segurança citados pelos entrevistados foram: vazamento de dados sensíveis; ataques cibernéticos (phishing, ransomware e DDoS); fraudes com deep fake e engenharia social; falhas em APIs e integrações. Tais ameaças demonstram a sofisticação crescente dos riscos digitais e a necessidade contínua de medidas preventivas para proteção dos negócios.
	Conscientização dos profissionais de TI sobre riscos	Conscientização; alta; gestões; invistam; profissionais; segurança dos dados; importância; sistema digital; Baixo; atenta.	A análise das respostas revela que a percepção dos entrevistados sobre a conscientização dos profissionais de tecnologia em relação aos riscos de segurança de dados é divergente. Alguns consideram o nível satisfatório, mas destacam a falta de investimento e apoio das gestões, enquanto outros

			apontam desatenção e negligência, o que revela um comprometimento ainda desigual com a proteção de dados.

Fonte: Elaborada pela autora, 2025.

Ao sintetizar os principais achados da pesquisa em categorias específicas, o quadro oferece uma visão consolidada das percepções dos entrevistados acerca da segurança de dados no ambiente digital. Essa organização permite compreender de forma mais clara como práticas empreendedoras, estratégias de proteção da informação e o uso das plataformas digitais se articulam no contexto da gestão de negócios. Assim, a análise evidencia tanto os avanços quanto as fragilidades percebidas, o que contribui para a construção de uma compreensão crítica e atualizada sobre os desafios enfrentados pelas organizações no cenário digital contemporâneo.

5 CONSIDERAÇÕES FINAIS

O presente estudo buscou analisar a percepção dos profissionais da área de tecnologia acerca da segurança de dados no contexto da gestão empreendedora em plataformas digitais. Para tal, elaborou-se a seguinte problemática: **qual a percepção dos profissionais da área de tecnologia acerca da segurança de dados na gestão empreendedora em plataformas digitais?**

No que concerne ao objetivo geral da pesquisa, analisar a percepção dos profissionais da área de tecnologia acerca da segurança de dados na gestão empreendedora em plataformas digitais, percebe-se que os entrevistados reconhecem a importância da segurança da informação como um pilar estratégico para as organizações, especialmente diante do avanço das ameaças cibernéticas e da transformação digital. Ataques como *ransomware*, *phishing* e falhas em sistemas legados, nota-se como um dos principais impasses enfrentados pelas empresas, que impactam diretamente os pilares da confidencialidade, integridade e disponibilidade das informações, os quais exigem medidas preventivas e investimentos em tecnologias robustas. Por outro lado, os profissionais destacam a necessidade de alinhar práticas de segurança à gestão empreendedora, com foco em inovação, capacitação contínua e adoção de soluções como autenticação multifator e criptografia. No entanto, observa-se uma lacuna entre a conscientização dos riscos e a implementação efetiva de políticas de segurança, muitas vezes limitada pela falta de apoio das gestões. Nesse sentido, a pesquisa revela que, embora haja avanços na proteção de dados, a integração entre segurança e gestão empreendedora ainda requer maior maturidade e comprometimento organizacional para enfrentar os desafios do ambiente digital hodierno.

No tocante às contribuições deste trabalho, para o meio acadêmico, a pesquisa enriquece os estudos sobre segurança da informação ao abordar sua integração com a gestão empreendedora em plataformas digitais, tema ainda em expansão na literatura. O estudo oferece uma análise empírica das percepções de profissionais de tecnologia, fornecendo dados relevantes para futuras pesquisas sobre estratégias de proteção de dados e inovação gerencial no contexto digital. Para o mercado, a pesquisa apresenta *insights* valiosos sobre os desafios práticos enfrentados pelas empresas, como ataques cibernéticos e falhas em sistemas legados, além de destacar soluções eficazes, como autenticação multifator e criptografia. Esses resultados podem orientar organizações a adotarem políticas de segurança mais robustas e alinhadas às práticas de gestão empreendedora. Para a sociedade, a pesquisa ressalta a segurança de dados como um direito coletivo e destaca o papel das empresas na preservação da privacidade e no uso ético das informações. Além disso, contribui para a formação de profissionais mais conscientes para lidar com as exigências do âmbito digital, promovendo uma atuação ética, estratégica e alinhada às transformações tecnológicas.

Dentre as limitações deste estudo, destaca-se a dificuldade em localizar participantes que se enquadrassem com precisão no perfil buscado, ou seja, profissionais da área de tecnologia com experiência e conhecimento específico sobre segurança da informação em ambientes digitais. Em diversos casos, alguns dos profissionais entrevistados estavam em início de carreira ou não atuavam diretamente com segurança, o que restringiu a profundidade das contribuições. Outro ponto foi a superficialidade de algumas respostas, que, mesmo partindo de um roteiro estruturado, não possibilitaram uma análise mais consistente das percepções dos participantes. Essa limitação afetou, sobretudo, a compreensão mais detalhada de como as práticas de segurança da informação são percebidas e aplicadas no cotidiano profissional. Ainda assim, os dados coletados permitiram traçar um panorama relevante e coerente com os objetivos da pesquisa.

Como sugestões para estudos futuros, propõe-se a realização de análises comparativas entre diferentes tipos de plataformas digitais, como *e-commerce*, *marketplaces* e redes sociais, no que se refere à adoção de práticas de segurança da informação por empreendedores de diferentes portes. Além disso, seria relevante investigar, por meio de uma abordagem quantitativa, o nível de conhecimento e preparo dos gestores quanto às legislações de proteção de dados, como a LGPD, bem como os impactos dessas práticas na fidelização de clientes. E, por fim, outra sugestão seria explorar modelos de capacitação contínua voltados para profissionais de TI, com o objetivo de reduzir a lacuna entre conscientização e a aplicação efetiva de políticas de segurança.

REFERÊNCIAS

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

ALEXANDRIA, J. C. S. **Gestão de segurança da informação - uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica**. 2009. 229 f. Tese (Doutorado em Tecnologia Nuclear - Aplicações) – Instituto de Pesquisas Energéticas e Nucleares, Universidade de São Paulo, São Paulo, 2009.

BACKES, D. S.; TOSON, M. J.; HAEFFNER, L. S. B.; MARCHIORI, M. T. C.; COSTENARO, R. G. S. Tecnologia de gestão empreendedora para a enfermagem. **Revista Brasileira de Enfermagem**, v. 74, supl. 6, e20190527, 2021. Disponível em: https://doi.org/10.1590/0034-7167-2019-0527.

BRAZ, R. S. **O papel da inteligência artificial na segurança de dados nas empresas**. 2023. 57 f., il. Trabalho de Conclusão de Curso (Bacharelado em Administração) — Universidade de Brasília, Brasília, 2023.

BORGES, B. H. P. Vantagens e desvantagens de uma empresa familiar – estudo de caso da empresa P e Borges Representações e Comércio LTDA. **Revista do COMINE (Congresso Mineiro de Empreendedorismo)**, v. 4, n. 1, p. 1-15, jan./abr. 2020. Disponível em: https://doi.org/10.1590/0034-7167-2019-0527. Acesso em: 19 set. 2024.

CEZAR, B.; VALIM BANDEIRA, M.; DORNELES, F.; BARCELOS, M.; BENEDETTI CORSO, K. Panorama das plataformas digitais de consumo colaborativo no Brasil: uma análise descritiva. **International Journal of Business & Marketing (IJBMKT)**, Porto Alegre, v. 3, n. 1, p. 40–54, 2018.

CHIARINI, T.; SILVA NETO, V. J.; PEREIRA, L. S.; SZIGETHY, L. **Plataformas digitais: mapeamento semissistemático e interdisciplinar do conhecimento produzido nas universidades brasileiras**. Brasília: Instituto de Pesquisa Econômica Aplicada, 2023. (Texto para Discussão, TD 2829). Disponível em: https://repositorio.ipea.gov.br/handle/11058/11677. Acesso em: 29 de set. 2024.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.BR). **Relatório TIC Empresas 2023**. 2023. Disponível em: https://cetic.br/pt/pesquisa/empresas/indicadores/. Acesso em: 04 set. 2024.

COSTA, K. J. S. **A Segurança de dados nas empresas do centro comercial de Valença: uma análise das práticas e desafios**. 2023. 43f. Trabalho de Conclusão de Curso (Tecnólogo em Tecnologia em Análise e Desenvolvimento e Sistemas), Campus Valença, Instituto Federal de Educação, Ciência e Tecnologia da Bahia, Valença, 2023. Disponível em: https://repositorio.ifba.edu.br/jspui/handle/123456789/608. Acesso em: 09 set. 2024.

COSTA, E. S.; GALVÃO, W. C. Segurança da Informação e Proteção dos Dados: Aplicação Web. **Journal of Technology & Information**, [S. l.], v. 3, n. 1, 2023.

DOURADO, L.; SCHMIDT, C. M.; DAGA CIELO, I. Presença de atitude empreendedora em gestores de ambientes de coworking: um estudo no estado do Paraná. **Revista de Empreendedorismo e Gestão de Micro e Pequenas Empresas**, [S. l.], v. 8, n. 02, p. 18–40, 2023.

EXAME SOLUTIONS. **"O número de ciberataques tem crescido 20% ao ano", diz a Huawei**. 2023. Disponível em: https://exame.com/negocios/ciberataques-crescido-20/. Acesso em: 31 ago. 2024.

FERNANDES, M. L. A importância da tecnologia da informação nas organizações. In: OLIVEIRA, F. B. **Tecnologia da informação e da comunicação**: a busca de uma visão ampla e estruturada. 1. ed. São Paulo, SP: Pearson, 2007. p. 184. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 01 set. 2024.

FERREIRA, Rodrigo. **Segurança: em aplicações web.** São Paulo, SP: Casa do Código, 2017. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 30 set. 2024.

FLICK, Uwe. **Introdução à metodologia de pesquisa: um guia para iniciantes**. 1. Ed. Porto Alegre: Penso, 2013.

GALVÃO, W. C.; COSTA, E S. **SEGURANÇA DE DADOS EM APLICAÇÃO WEB.** FatecSeg - Congresso de Segurança da Informação, [S. l.], 2023. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/167. Acesso em: 9 set. 2024.

GONÇALVES, H. S.; CORREIA, A. M. M.; ALBERTINS, P. A. R. Gestão empreendedora dos MEI's: uso da previsão de vendas. In: **VI Simpósio Sul-Mato-Grossense de Administração**, 22-26 maio 2023, Paranaíba - MS. ESG: Demandas Emergentes. Curso de Administração, UFMS.

GONÇALVES, J. O futuro do marketing digital: tendências e inovações emergentes. **The Trends Hub**, Porto, n. 4, 2024. DOI: 10.34630/tth.vi4.5668. Disponível em: https://parc.ipp.pt/index.php/trendshub/article/view/5668. Acesso em: 1 out. 2024.

LEAL, J. P. C. **O fator humano como elemento da segurança da informação**. 2023. Dissertação (Mestrado em Gestão de Sistemas de Informação) – Universidade de Lisboa, Instituto Superior de Economia e Gestão, Lisboa, 2023. Disponível em: http://hdl.handle.net/10400.5/30122. Acesso em: 09 set. 2024.

LIMA, L. L.; AGUIAR, R. B.; LUI, L. Conectando problemas, soluções e expectativas: mapeando a literatura sobre análise do desenho de políticas públicas. **Revista Brasileira de Ciência Política,** n. 36, p. e246779, 2021.

MARTINELLI, W.; LAHR, M. **Impactos da Pandemia de COVID-19 na Segurança da Informação para as empresas e pessoas**. FatecSeg - Congresso de Segurança da Informação, [S. l.], v. 1, 2021.

MARQUES, R. M. PLATAFORMAS DIGITAIS: UMA ANÁLISE SOB AS LENTES DA CRÍTICA DA ECONOMIA POLÍTICA. **Trabalho & Educação**, Belo Horizonte, v. 32, n. 3, p. 127–150, 2024.

MARZZONI, D. N. S.; FREITAS, R. U. C.; OLIVEIRA, L. A.; SILVA, A. W. F.; NERES, J. N. L. Análise bibliométrica: pesquisa científica acerca dos stakeholders / Bibliometric analysis: scientific research about stakeholders. **Brazilian Journal of Development**, [S. l.], v. 7, n. 3, p. 29919–29936, 2021. DOI: 10.34117/bjdv7n3-623. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/26945. Acesso em: 5 out. 2024.

MASCARENHAS NETO, P. T.; ARAUJO, W. J. **Segurança da Informação:** uma visão sistêmica para implantação em organizações. 1. ed. João Pessoa: Editora UFPB, 2019.

O GLOBO. **Brasil é o maior alvo de ataques cibernéticos na América Latina; veja ranking**. 2023. Disponível em: https://oglobo.globo.com/economia/tecnologia/noticia/2023/06/brasil-e-o-maior-alvo-de-ataques-ciberneticos-na-america-latina-veja-ranking.ghtml. Acesso em: 02 set. 2024.

OLIVEIRA, G. S. **O empreendedorismo como estratégia de negócio na Jadlog**. 2021. Monografia (Bacharelado em Comunicação Social) – Pontifícia Universidade Católica de Goiás, Departamento de Comunicação Social, Goiânia, 2021.

OLIVEIRA, J. S. **Avaliação e validação de plataformas digitais orientadas para a indústria como serviço**. 2019. Dissertação (Mestrado em Ciência da Informação) — Faculdade de Engenharia e Faculdade de Letras, Universidade do Porto, Porto, 2019. Disponível em: https://hdl.handle.net/10216/122082. Acesso em: 30 de set. 2019.

OLIVEIRA, R. C. **Adequadas técnicas à gestão de segurança da informação na internet**. 2020. Trabalho de Conclusão de Curso (Graduação em Sistema de Informação) – Anhanguera, Brasília, DF, 2020. Disponível em: https://repositorio.pgsscogna.com.br/bitstream/123456789/64648/1/ROBERT_CERQUEIRA.pdf. Acesso em: 10 set. 2024.

OLIVEIRA, A. E.; AIO, C. E.; PINHEIRO, G. G.; MORAIS, G. **Segurança da informação empresarial.** 2022. Disponível em: https://www.fef.br/upload_arquivos/geral/arq_63fdcfed7ce48.pdf. Acesso em: 8 set. 2024.

OLIVEIRA, E. V.; FILGUEIRAS, R. A importância da segurança da informação para as organizações. **Revista Alomorfia**, [S. l.], v. 6, n. 1, p. 438–447, 2022.

OLIVEIRA, M. C. S.; CARELLI, R. DE L.; GRILLO, S. Conceito e crítica das plataformas digitais de trabalho. **Revista Direito e Práxis**, v. 11, n. 4, p. 2609–2634, out. 2020.

PAZ, E. G. N. **O novo modelo do trabalho nas plataformas digitais: uma análise do perfil dos trabalhadores nos setores de serviços de entregas e transporte de passageiros no Brasil**. 2023. Trabalho de Conclusão de Curso (Graduação em Administração) – Universidade Federal da Paraíba, João Pessoa, 2023. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/26719. Acesso em: 30 set. 2024.

PEREIRA, L. A. S.; VICENTINE, A. L.; RIZO, A. C. **Impactos da Engenharia Social na Segurança da Informação.** Revista Brasileira em Tecnologia da Informação, [S. l.], v. 4, n. 1, p. 48-58, 2022. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/75. Acesso em: 29 set. 2024.

PEREIRA, V. O.; OLIVEIRA JUNIOR, A. H.; BAPTISTA, W. S. A falta de canais de comunicação, base da pirâmide - alta cúpula, como fator inibidor da inovação. In: **Tópicos em Administração**. 1. ed. Belo Horizonte: Editora Poisson, 2018. v. 14, cap. 11, p. 156-157.

RAMOS, R. G. G.; CARVALHO, I. F.; PIANTINO, L. F. M.; DE SOUZA, A. F. Aplicação da segurança da informação e LGPD para a experiência e usabilidade dos usuários em aplicativos móveis. **Revista Sociedade Científica**, [S. l.], v. 7, n. 1, p. 1717–1738, 2024. DOI: 10.61411/rsc202437717.

RIBEIRO, M. B. **Tendências do empreendedorismo corporativo: um estudo bibliométrico**. 2021. 29 f. Trabalho de Conclusão de Curso (Graduação em Administração) - Universidade Federal de Uberlândia, Uberlândia, 2021.

ROGERS, D. L. **Transformação digital**: repensando o seu negócio para a era digital. São Paulo: Grupo Autêntica, 2017. E-book. ISBN 9788551302736. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788551302736/. Acesso em: 02 set. 2024.

ROMAN JUNIOR, W.; SGANZERLA; C. M.; VELOSO; J.; PREDEBON, A.; ROMAN, F. S.; CORÁ, L. M.; SOLIGO, M.; FONSECA, C. H. Conhecimento etnobotânico de plantas medicinais utilizadas por agentes populares de cura em Guatambu, Santa Catarina, Brasil. **Conjecturas**, v. 22, n. 7, p. 102-123, 2022.

SANCHEZ, C. R.; ARAÚJO, L. S. FUTURISMO: tendências da tecnologia no empreendedorismo. **Revista Interface Tecnológica**, [S. l.], v. 16, n. 1, p. 171–183, 2019. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/586. Acesso em: 19 set. 2024.

SANTANA, V. T. **A insegurança no fluxo de dados das redes das empresas**. 2022. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) – União Metropolitana de Educação e Cultura (UNIME), 2022. Disponível em: https://repositorio.pgsscogna.com.br//handle/123456789/58071. Acesso em: 10 set. de 2024.

SÊMOLA, M. **Gestão da segurança da informação**: uma visão executiva. Rio de Janeiro: Campus, 2003.

SENA, A. S. de; ARAÚJO, W. J. de. Sites dos municípios da Paraíba: análise de vulnerabilidades computacionais. **Informação & Tecnologia**, [S. l.], v. 4, n. 2, p. 145–162, 2018. DOI: 10.22478/ufpb.2358-3908.2017v4n2.40418.

SILVA, B. T.; CAMPOS, D. F. A.; CANO, M. G.; GOMES, M. P. **Gestão de documentos: segurança de dados.** 2022.Trabalho de Conclusão de Curso (Técnico em Administração) – Etec Profa. Anna de Oliveira Ferraz, Araraquara, 2022.

SILVA, E. M. **Segurança de dados: a coleta de informação acerca da LGPD.** 2021. Trabalho de Conclusão de Curso (Bacharelado em Sistema da Informação) – Anhanguera, Brasília, 2021. Disponível em: https://repositorio.pgsscogna.com.br/bitstream/123456789/64685/1/ERIVAN_MENDES_DA_SILVA.pdf. Acesso em: 07 set. 2024.

SILVA, E. G.; DOMINGUES, D. A. S. D.; BIAZON, V. V. Comportamento do consumidor: fatores que influenciam o poder de compra. **Scientific Electronic Archives**, [S. l.], v. 14, n. 4, 2020. DOI: 10.36560/14420211252. Disponível em: https://sea.ufr.edu.br/index.php/SEA/article/view/1252. Acesso em: 5 out. 2024.

SILVA, S. L. S.; NOBREGA, C. V. **Gestão no ensino universitário: um estudo de caso no curso de Administração da Universidade Federal do Piauí Campus Senador Helvídio Nunes de Barros com tendência na TEG**. 2018. Trabalho de Conclusão de Curso (Graduação em Administração) – Universidade Federal do Piauí, Picos, 2018.

SOUZA, F. R.; GONÇALO, M. J. S.; MESQUITA, P. H. A. **Gerenciamento de projetos & Segurança da Informação: os impactos da gestão de projetos na segurança da informação.** 2021. 17f. Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação) - Centro Universitário do Planalto Central Apparecido dos Santos, 2021. Disponível em: https://dspace.uniceplac.edu.br/handle/123456789/1612. Acesso em: 07 set. de 2024.

SOUSA, J. R.; SANTOS, S. C. M. Análise de conteúdo em pesquisa qualitativa: modo de pensar e de fazer. **Pesquisa e Debate em Educação**, Juiz de Fora: UFJF, v. 10, n. 2, p. 1396 - 1416, jul. - dez. 2020. ISSN 2237-9444. DOI: https://doi.org/10.34019/2237-9444.2020.v10.31559.

TEIXEIRA, A. A.; FRACAROLLI JUNIOR, M. A.; REGGIOLLI, M. R. Políticas de segurança da informação no ambiente empresarial. **Prospectus**, Itapira, v. 5, n. 2, 12 dez. 2023.

TOMAZ, R. **Gestão estratégica e inteligência na segurança privada.** 1. ed. Curitiba: InterSaberes, 2023.

VALLE, R. S. **Propriedade intelectual: um estudo de múltiplos casos nas cafeterias espe-**

ciais da cidade do Recife/PE. 2023. Dissertação (Mestrado) — Universidade Federal de Pernambuco, Recife, 2023. Disponível em: https://repositorio.ufpe.br/handle/123456789/52153. Acesso em: 07 out. 2024.

APÊNDICE A – ROTEIRO DE ENTREVISTA

Parte I - Perfil dos Entrevistados

Gênero: ( ) Feminino ( ) Masculino ( ) Outro
Idade: _____
Grau de Escolaridade: ( ) Ensino Médio ( ) Ensino Superior ( ) Pós-Graduação
Qual seu cargo atualmente? _____
Quantos tempo trabalha na organização? _____

Parte II - Ações Referentes à Segurança de Dados

1. Quais são os principais desafios que sua empresa já enfrentou ou enfrenta para garantir a segurança dos dados em plataformas digitais e como esses desafios impactam a confidencialidade, integridade e disponibilidade das informações na gestão empresarial?
2. Com base na sua experiência, quais estratégias ou tecnologias sua empresa adota para proteger dados e quais dessas práticas você considera mais eficazes e por quê?
3. Como você percebe o impacto das medidas de proteção de dados adotadas atualmente em sua empresa? Elas influenciam a produtividade, a inovação ou o relacionamento com clientes? Justifique sua resposta.

Parte III - Práticas Empreendedoras

4. Na sua opinião, como a gestão empreendedora pode ser mais inovadora na busca por soluções de segurança de dados mais eficazes para plataformas digitais?
5. Com relação à gestão empreendedora da sua empresa, como você percebe a abordagem em relação aos riscos de segurança de dados? Há uma tendência a adotar medidas mais conservadoras ou a experimentar novas soluções, mesmo com certo nível de risco? Detalhe sua resposta.
6. De que forma você percebe o risco calculado e a proatividade na gestão empreendedora na abordagem da segurança de dados na sua empresa? Detalhe e dê exemplos na sua resposta.

Parte IV - O Uso dos Recursos das Plataformas Digitais

7. Considerando a crescente utilização de plataformas digitais para a gestão de negócios, detalhe a sua percepção sobre a aplicação da segurança de dados nesse ambiente.
8. Na sua opinião, quais são os principais riscos de segurança que as empresas enfrentam ao utilizar plataformas digitais para a gestão de negócios?
9. Como você avalia o nível de conscientização dos profissionais de tecnologia em relação aos riscos de segurança de dados em plataformas digitais? Justifique sua avaliação.

AGRADECIMENTOS

À Deus, por me permitir vivenciar tantas oportunidades e por ter me sustentado com força, fé e sabedoria durante todos os momentos desta caminhada.

Aos meus pais, Maria das Graças e Arnaldo, por todo amor, apoio e incentivo incondicional para a realização deste sonho. À minha irmã Júlia, por ser constante fonte de motivação e companheirismo, mesmo nos dias mais difíceis.

À minha orientadora, professora Dra. Janayna Souto Leal, pela orientação dedicada e comprometida, pela generosidade em compartilhar seus conhecimentos em cada etapa deste processo. Sua contribuição foi essencial para o amadurecimento acadêmico e científico desta pesquisa, refletindo diretamente na qualidade e consistência do trabalho desenvolvido.

Às minhas amigas, Angélica e Luzivânia, que tornaram o percurso mais leve, repleto de apoio mútuo, experiências enriquecedoras e momentos de verdadeira parceria.

À Universidade Estadual da Paraíba (UEPB), pelo ambiente acadêmico acolhedor e compromisso com o ensino.

À Secretaria de Estado da Ciência, Tecnologia, Inovação e Ensino Superior (SECTIES), pelo suporte institucional e incentivo contínuo à pesquisa científica.

À Fundação de Apoio à Pesquisa do Estado da Paraíba (FAPESQ), pelo importante apoio financeiro e pelo fomento à produção acadêmica que possibilitaram não apenas a execução deste trabalho, mas também a permanência e o fortalecimento da minha trajetória acadêmica durante toda a graduação.

Ao Projeto Limite do Visível, pelo suporte ofertado e pelas oportunidades proporcionadas, que ampliaram minha visão sobre o papel transformador da ciência e da tecnologia na sociedade.

Por fim, a todos aqueles que, de alguma forma, contribuíram direta ou indiretamente para a concretização deste trabalho, deixo minha mais profunda gratidão.