Revista Científica Sistemática
ISSN: 2675-521

A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO NO COMÉRCIO DIGITAL: RISCOS CIBERNÉTICOS E GOVERNANÇA DA CADEIA DE SUPRIMENTOS NO MODELO DROPSHIPPING

THE IMPORTANCE OF INFORMATION SECURITY IN DIGITAL COMMERCE: CYBER RISKS AND SUPPLY CHAIN GOVERNANCE IN THE DROPSHIPPING MODEL

LA IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN EL COMERCIO DIGITAL: RIESGOS CIBERNÉTICOS Y GOBERNANZA DE LA CADENA DE SUMINISTRO EN EL MODELO DROPSHIPPING

https://doi.org/10.56238/rcsv16n1-009

Data de submissão: 30/12/2025 **Data de aprovação**: 30/01/2026

George Coelho Kleinau Vasconcelos
Mestrando em História das Ciências e das Técnicas e Epistemologia
Instituição: Universidade Federal do Rio de Janeiro
E-mail: gcvasconcelos@firjan.com.br

Alfredo Nazareno Pereira Boente
Doutor em Ciências da Engenharia de Produção
Instituição: Universidade Federal do Rio de Janeiro
E-mail: boente@nce.ufrj.br

Juan Gabriel Pires Boente
Graduando em Administração e Marketing Digital
Instituição: Universidade Veiga de Almeida
E-mail: juangabrielpires@gmail.com
E-mail: boente@nce.ufrj.br

Juan Gabriel Pires Boente
Graduando em Administração e Marketing Digital
Instituição: Universidade Veiga de Almeida
Endereço: Rio de Janeiro – RJ, Brasil
E-mail: juangabrielpires@gmail.com

RESUMO

O crescimento do comércio eletrônico tem impulsionado modelos de negócios baseados em plataformas digitais e na terceirização intensiva de processos, entre os quais se destaca o *dropshipping*. Embora esse modelo reduza custos operacionais, ele intensifica a fragmentação da cadeia de suprimentos digital e amplia a exposição a riscos cibernéticos. Considerando esse cenário, este artigo objetiva analisar, sob a perspectiva da Segurança da Informação, os riscos associados ao modelo de *dropshipping*, com ênfase na responsabilidade do controlador de dados e na necessidade de uma governança estruturada de segurança. Para tanto, procede-se a uma pesquisa qualitativa, exploratória e descritiva, fundamentada em estudo de caso único da loja virtual Pawzzi, utilizando análise documental, mapeamento de fluxos de dados, modelagem teórica de ameaças e análise comparativa com referenciais normativos consolidados, como o NIST *Cybersecurity Framework*, o NIST *Cybersecurity Supply Chain Risk Management* (C-SCRM), a ISO/IEC 27001:2022 e a Lei Geral de Proteção de Dados (LGPD). Desse modo, observa-se que o *dropshipping* amplia significativamente a superfície de ataque ao dispersar dados sensíveis entre múltiplos operadores, expondo o controlador a riscos sistêmicos, especialmente ataques à cadeia de suprimentos, falhas de integração e

Revista Científica Sistemática
ISSN: 2675-521

vulnerabilidades associadas ao fator humano. Conclui-se que a sustentabilidade desse modelo de comércio eletrônico depende da adoção de uma governança de segurança da informação baseada em gestão contínua de riscos e controles distribuídos ao longo de toda a cadeia de suprimentos digital.

Palavras-chave: Segurança da Informação. Dropshipping. Cadeia de Suprimentos Digital. Gestão de Riscos. Governança da Informação.

ABSTRACT

The growth of electronic commerce has fostered business models strongly based on digital platforms and the intensive outsourcing of processes, among which dropshipping stands out. Although this model reduces operational costs, it intensifies the fragmentation of the digital supply chain and increases exposure to cyber risks. Considering this context, this article aims to analyze, from an Information Security perspective, the risks associated with the dropshipping model, emphasizing the responsibility of data controllers and the need for structured security governance. To this end, a qualitative, exploratory, and descriptive study was conducted, based on a single case study of the Pawzzi online store, using documentary analysis, data flow mapping, theoretical threat modeling, and comparative analysis with consolidated normative references such as the NIST Cybersecurity Framework, the NIST Cybersecurity Supply Chain Risk Management (C-SCRM), ISO/IEC 27001:2022, and Brazil's General Data Protection Law (LGPD). The findings indicate that dropshipping significantly expands the attack surface by dispersing sensitive data across multiple operators, exposing controllers to systemic risks, particularly supply chain attacks, integration failures, and human-related vulnerabilities. This study concludes that the sustainability of dropshipping depends on the adoption of information security governance grounded in continuous risk management and distributed controls throughout the digital supply chain.

Keywords: Information Security. Dropshipping. Digital Supply Chain. Risk Management. Information Governance.

RESUMEN

El crecimiento del comercio electrónico ha impulsado modelos de negocio basados en plataformas digitales y en la externalización intensiva de procesos, entre los cuales destaca el dropshipping. Aunque este modelo reduce los costos operativos, intensifica la fragmentación de la cadena de suministro digital y amplía la exposición a riesgos cibernéticos. Considerando este escenario, este artículo tiene como objetivo analizar, desde la perspectiva de la Seguridad de la Información, los riesgos asociados al modelo de dropshipping, con énfasis en la responsabilidad del controlador de datos y en la necesidad de una gobernanza estructurada de la seguridad. Para ello, se realiza una investigación cualitativa, exploratoria y descriptiva, basada en un estudio de caso único de la tienda virtual Pawzzi, utilizando análisis documental, mapeo de flujos de datos, modelado teórico de amenazas y análisis comparativo con marcos normativos consolidados, como el NIST Cybersecurity Framework, el NIST Cybersecurity Supply Chain Risk Management (C-SCRM), la norma ISO/IEC 27001:2022 y la Ley General de Protección de Datos de Brasil (LGPD). De este modo, se observa que el dropshipping amplía significativamente la superficie de ataque al dispersar datos sensibles entre múltiples operadores, exponiendo al controlador a riesgos sistémicos, especialmente ataques a la cadena de suministro, fallas de integración y vulnerabilidades asociadas al factor humano. Se concluye que la sostenibilidad de este modelo de comercio electrónico depende de la adopción de una gobernanza de la seguridad de la información basada en la gestión continua de riesgos y controles distribuidos a lo largo de toda la cadena de suministro digital.

Palabras clave: Seguridad de la Información. Dropshipping. Cadena de Suministro Digital. Gestión de Riesgos. Gobernanza de La Información.

Revista Científica Sistemática
ISSN: 2675-521

1 INTRODUÇÃO

A consolidação da economia digital tem ampliado a adoção de modelos de negócios baseados na desmaterialização de ativos físicos e na terceirização intensiva de processos. Nesse contexto, o *dropshipping* destaca-se como um modelo de comércio eletrônico que elimina a necessidade de estoque próprio, transferindo a execução logística para fornecedores externos. Apesar de suas vantagens econômicas, essa configuração organizacional impõe desafios relevantes à Segurança da Informação, uma vez que o tratamento de dados pessoais e transacionais ocorre em um ecossistema altamente fragmentado.

No contexto regulatório brasileiro, a Lei Geral de Proteção de Dados (LGPD) estabelece que o controlador permanece responsável pelo tratamento adequado dos dados pessoais, mesmo quando há terceirização de operações. Dessa forma, o *dropshipping* cria um paradoxo estrutural: enquanto a cadeia operacional é descentralizada, a responsabilidade legal e informacional permanece centralizada no lojista digital.

Diante desse cenário, este estudo parte do seguinte problema de pesquisa: como garantir a segurança da informação em um ecossistema de comércio eletrônico caracterizado pela fragmentação da cadeia de suprimentos digital? O objetivo geral do trabalho é analisar os riscos cibernéticos associados ao modelo de *dropshipping* e discutir a importância de uma governança estruturada de segurança da informação, alinhada a padrões e *frameworks* internacionalmente reconhecidos.

2 REFERENCIAL TEÓRICO

2.1 SEGURANÇA DA INFORMAÇÃO COMO CAMPO CIENTÍFICO E ORGANIZACIONAL

A Segurança da Informação consolidou-se, ao longo das últimas décadas, como um campo científico interdisciplinar, articulando dimensões técnicas, organizacionais, jurídicas e estratégicas. Inicialmente associada quase exclusivamente à proteção de sistemas computacionais, essa área ampliou seu escopo diante da crescente dependência das organizações em relação à informação como ativo estratégico (ENISA, 2025). De acordo com Whitman e Mattord (2018), a proteção da informação ultrapassa a aplicação de controles tecnológicos, exigindo a formulação de políticas institucionais, a definição de processos estruturados e o desenvolvimento de uma cultura organizacional orientada à segurança.

Nesse sentido, a Segurança da Informação passa a ser compreendida como um componente essencial da gestão organizacional, diretamente relacionada à continuidade dos negócios, à reputação institucional e à conformidade legal. Von Solms e Van Niekerk (2013) reforçam essa perspectiva ao afirmarem que a segurança da informação deve ser tratada como um problema de governança e gestão, e não apenas como uma questão tecnológica. Tal abordagem destaca a responsabilidade da alta

Revista Científica Sistemática
ISSN: 2675-521

administração na definição de diretrizes, na alocação de recursos e no monitoramento dos riscos informacionais.

Além disso, normas e *frameworks* internacionais, como a ISO/IEC 27001, contribuem para a consolidação da Segurança da Informação como campo organizacional estruturado, ao estabelecer requisitos para sistemas de gestão voltados à proteção da confidencialidade, integridade e disponibilidade da informação. Dessa forma, a Segurança da Informação assume um papel estratégico, integrando-se aos processos decisórios e à governança corporativa das organizações contemporâneas.

2.2 CADEIAS DE SUPRIMENTOS DIGITAIS E RISCO CIBERNÉTICO

A transformação digital intensificou de forma significativa a dependência das organizações em relação a cadeias de suprimentos fundamentadas em software, serviços em nuvem e múltiplas integrações sistêmicas. Esse novo cenário ampliou a complexidade operacional e os riscos associados à interconectividade entre fornecedores, plataformas tecnológicas e parceiros estratégicos. Segundo Boyson (2014), as cadeias de suprimentos digitais configuram-se como ecossistemas altamente interdependentes, nos quais a vulnerabilidade ou falha de um único componente pode desencadear efeitos em cascata capazes de comprometer todo o sistema organizacional.

Nessa perspectiva, a gestão de riscos torna-se um elemento central para a resiliência das cadeias digitais. Chopra e Sodhi (2014) ressaltam que a falta de visibilidade e controle sobre fornecedores tecnológicos aumenta a exposição das organizações a interrupções operacionais e perdas estratégicas. Assim, a segurança e a confiabilidade das cadeias de suprimentos digitais passam a exigir abordagens integradas, envolvendo governança, monitoramento contínuo e políticas de segurança alinhadas aos objetivos organizacionais.

2.3 O MODELO DE *DROPSHIPPING* SOB A ÓTICA DA SEGURANÇA DA INFORMAÇÃO

O *dropshipping* pode ser compreendido como uma expressão avançada das cadeias de suprimentos digitais, caracterizando-se pela centralidade da informação em detrimento do controle direto de ativos físicos. Nesse arranjo, o lojista assume o papel de coordenador dos fluxos informacionais, comerciais e financeiros, operando a partir de plataformas digitais e integrações sistêmicas com fornecedores e operadores logísticos. Conforme observa Boyson (2014), esse tipo de estrutura amplia a dependência de ecossistemas tecnológicos interconectados, nos quais vulnerabilidades em um único elo podem comprometer toda a cadeia.

Sob a perspectiva da Segurança da Informação, o *dropshipping* apresenta desafios relevantes, especialmente no que se refere à confidencialidade, integridade e disponibilidade dos dados compartilhados entre múltiplos atores. Laudon e Laudon (2020) destacam que ambientes digitais

Revista Científica Sistemática
ISSN: 2675-521

altamente terceirizados tendem a ampliar a superfície de ataque e a complexidade da gestão de riscos informacionais. Ademais, Whitman e Mattord (2018) enfatizam a necessidade de políticas de segurança e mecanismos de governança capazes de mitigar riscos decorrentes da dependência tecnológica de parceiros externos. Dessa forma, o *dropshipping* demanda uma abordagem estratégica de segurança da informação, integrada à gestão e à governança organizacional.

2.4 GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO E MARCOS NORMATIVOS

A governança da segurança da informação tem sido operacionalizada por meio de *frameworks* e normas internacionais amplamente aceitos, os quais visam alinhar práticas técnicas às estratégias organizacionais e às exigências regulatórias. Nesse contexto, a governança ultrapassa a dimensão operacional da segurança, assumindo um papel estratégico na gestão de riscos, na conformidade legal e na sustentabilidade organizacional. Segundo Von Solms e Van Niekerk (2013), a governança da segurança da informação deve ser integrada à governança corporativa, com participação ativa da alta administração.

O NIST *Cybersecurity Framework* destaca-se por propor uma abordagem sistemática baseada nas funções identificar, proteger, detectar, responder e recuperar, permitindo às organizações avaliarem sua maturidade em segurança e aprimorar continuamente seus controles. Complementarmente, o NIST *Cyber Supply Chain Risk Management* (C-SCRM) amplia essa perspectiva ao tratar especificamente dos riscos distribuídos ao longo da cadeia de suprimentos, reconhecendo a interdependência entre organizações e fornecedores tecnológicos (NIST, 2022). Boyson (2014) ressalta que a ausência de governança adequada nesse contexto pode gerar efeitos sistêmicos e impactos significativos sobre a continuidade dos negócios.

No âmbito normativo, a ISO/IEC 27001:2022 estabelece os requisitos para a implementação e manutenção de um Sistema de Gestão da Segurança da Informação (SGSI), fundamentado no ciclo de melhoria contínua e na gestão baseada em riscos. Whitman e Mattord (2018) afirmam que essa norma contribui para a padronização de práticas e para o fortalecimento da cultura organizacional de segurança. Paralelamente, no contexto brasileiro, a Lei Geral de Proteção de Dados Pessoais (LGPD) impõe obrigações legais explícitas aos controladores e operadores de dados, inclusive em cenários de terceirização e compartilhamento de informações. Conforme Doneda et al. (2019), a LGPD reforça a necessidade de mecanismos de governança capazes de assegurar responsabilidade, transparência e prestação de contas no tratamento de dados pessoais, consolidando a segurança da informação como elemento central da governança organizacional.

Revista Científica Sistemática
ISSN: 2675-521

3 METODOLOGIA

A pesquisa adota uma abordagem qualitativa, exploratória e descritiva, utilizando o método de estudo de caso único. A unidade de análise é a loja virtual Pawzzi, operante no modelo de *dropshipping*. Os procedimentos metodológicos compreenderam análise documental do modelo de negócios e da arquitetura técnica, mapeamento dos fluxos de dados pessoais e transacionais, modelagem teórica de ameaças relevantes ao contexto do dropshipping e análise comparativa (*gap analysis*) entre as práticas observadas e os requisitos estabelecidos pelos *frameworks* NIST, NIST C-SCRM, ISO/IEC 27001 e LGPD.

4 ESTUDO DE CASO

4.1 EMPRESA ESTUDADA: LOJA VIRTUAL PAWZZI

A Loja Virtual Pawzzi foi a empresa escolhida para estudo de vulnerabilidades no meio digital (online). A Pawzzi baseou-se numa estratégia de Empreendedorismo Digital e Marketing Digital, operando sob o modelo de negócio *dropshipping*, posicionando-se, basicamente, como intermediária de vendas, cujo foco de atuação está na comercialização de produtos para animais de estimação, cães e gatos, não havendo, portanto, a necessidade de estoque físico próprio, e com isso, a empresa teve uma redução nos custos operacionais, buscando maximizar a escalabilidade dos negócios.

Apresentando uma plataforma de *e-commerce* robusta, intuitiva e totalmente responsiva, garantindo ao cliente uma experiência de usuário (UX) otimizada tanto para acesso em *desktop*s quanto em dispositivos móveis, permitindo que vendas pudessem ser realizadas em qualquer lugar, a qualquer momento. As Figuras 1 e 2, ilustram a interface projetada, transmitindo, aos clientes, confiança, credibilidade e facilidade de navegação, características consideradas pilares essenciais para o sucesso de qualquer comércio digital.

Revista Científica Sistemática
ISSN: 2675-521

Figura 1. Loja Virtual Pawzzi - Tela inicial (DESKTOP).

Fonte: Boente et al., 2025.

Consegue-se observar que na Figura 1 existe a presença de depoimentos de clientes que aparecem logo abaixo do *banner* rotativo que demonstra claramente uma estratégia de negócio com foco na "Gestão de Relacionamento com o Cliente" (CRM), construindo, portanto, prova social de engajamento com a loja virtual Pawzzi.

Figura 2. Loja Virtual Pawzzi - Tela inicial (MOBILE).

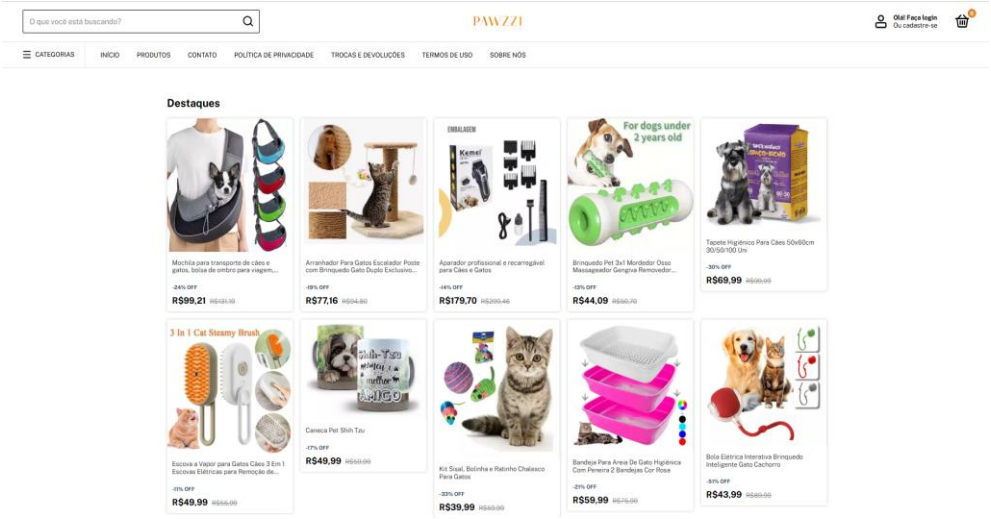
Fonte: Boente et al., 2025.

A Figura 3 e 4 ilustram a “vitrine virtual de produtos”, essencial para a jornada de compra

Revista Científica Sistemática
ISSN: 2675-521

(BOENTE et al., 2025, p. 63). Pode-se observar que a seção "Destaques" apresenta uma ampla variedade de itens para cães e gatos de diversos fornecedores parceiros, ilustrando a vasta oferta de produtos disponíveis por meio do modelo *dropshipping*.

Figura 3. Loja Virtual Pawzzi - Produtos em destaque (DESKTOP).



Fonte: Boente et al., 2025.

A apresentação de cada produto na loja virtual Pawzzi é composta por uma imagem nítida, nome, preço original e preço promocional, utilizando “gatilhos” de escassez e oportunidades para incentivar a compra imediata.

Revista Científica Sistemática
ISSN: 2675-521

Figura 4. Loja Virtual Pawzzi - Produtos em destaque (MOBILE).

Fonte: Boente et al., 2025.

As Figuras 5 e 6 ilustram a página de detalhes do produto, considerado tecnicamente como o ponto mais importante para a conclusão efetiva de uma venda online. A figura ilustrada como exemplo, mostra um produto específico, "Brinquedo para Mordedor", exibindo uma variedade de imagens, variações de cores, preço com um desconto destacado e opções de pagamento, incluindo a estratégia do cliente ter concedido um desconto de 5% acumulativo, via Pix, incentivando o pagamento em dinheiro como estratégia de marketing. O campo de cálculo do frete por CEP informa ao cliente o prazo de entrega (gerenciado pelo fornecedor dropshipping parceiro), garantindo transparência no processo de distribuição logística, mesmo tendo apresentado a estratégia de parceria de "Frete Grátis em todo território nacional".

Revista Científica Sistemática
ISSN: 2675-521

Figura 5. Loja Virtual Pawzzi - Detalhes do produto para venda (DESKTOP).

Fonte: Boente et al., 2025.

Como um bom estrategista de marketing digital, a loja virtual Pawzzi, reconhecendo que a maior parte do tráfego de comércio eletrônico atualmente é *mobile*, conforme afirma Boente et al. (2025, p. 64), muitos usuários de lojas online usam aplicativos móveis.

Figura 6. Loja Virtual Pawzzi - Detalhes do produto para venda (MOBILE).

Fonte: Boente et al., 2025.

A loja virtual Pawzzi foi projetada com o princípio *Mobile-First*, garantindo uma experiência do usuário completa e integrada em smartphones. Tecnicamente, *Mobile-First* é um conceito aplicado

Revista Científica Sistemática
ISSN: 2675-521

a projetos web onde o foco inicial da arquitetura e do desenvolvimento é direcionado para dispositivos móveis e, posteriormente, para desktops (LOPES, 2014).

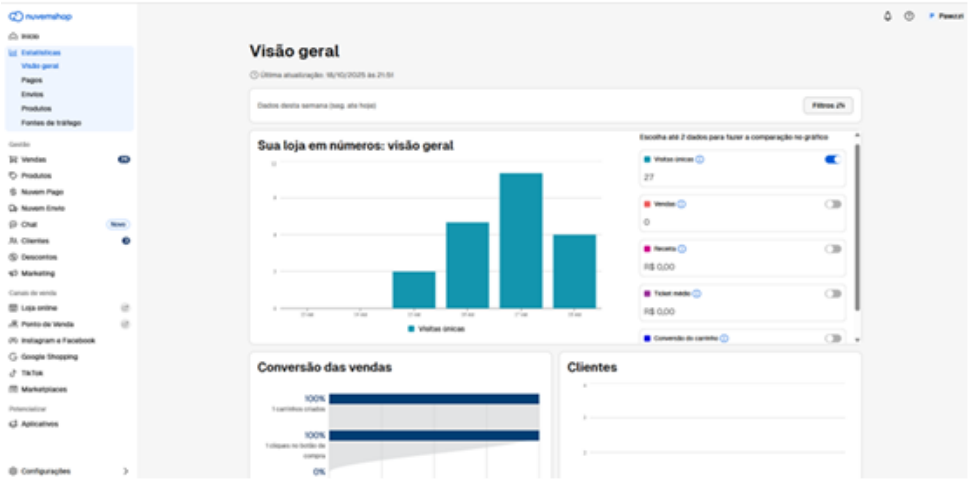
Dessa forma, a loja virtual Pawzzi pautada pela estratégia de marketing digital, apoiada pelo modelo *dropshipping*, obteve vantagens significativas como redução de custos operacionais, flexibilidade logística e escalabilidade da estrutura do negócio digital.

Um ponto crucial para qualquer *e-commerce*, mesmo aquela loja virtual que utiliza o modelo *dropshipping*, sem estoque próprio, é realizar um gerenciamento efetivo e de qualidade sobre seus produtos, seus clientes e suas vendas (ALLEN, 2021).

Neste contexto, é importante a escolha de uma plataforma robusta para a criação e gestão de sua loja *online*. Para tanto, a gestão operacional da loja virtual Pawzzi é realizada pela plataforma Nuvemshop, ferramenta especializada em comércio eletrônico que possibilita ao empreendedor administrar produtos, vendas e relacionamento com clientes em um único ambiente digital (NUVEMSHOP, 2025).

Mesmo adotando o modelo *dropshipping*, que dispensa estoque próprio, a empresa mantém um sistema de gestão integrada para monitorar indicadores de desempenho, fluxo financeiro e controle logístico (BOENTE, et al., 2025, p. 22).

Figura 7. Gestão da Loja Virtual Pawzzi - Plataforma Nuvemshop - Estatística Geral.



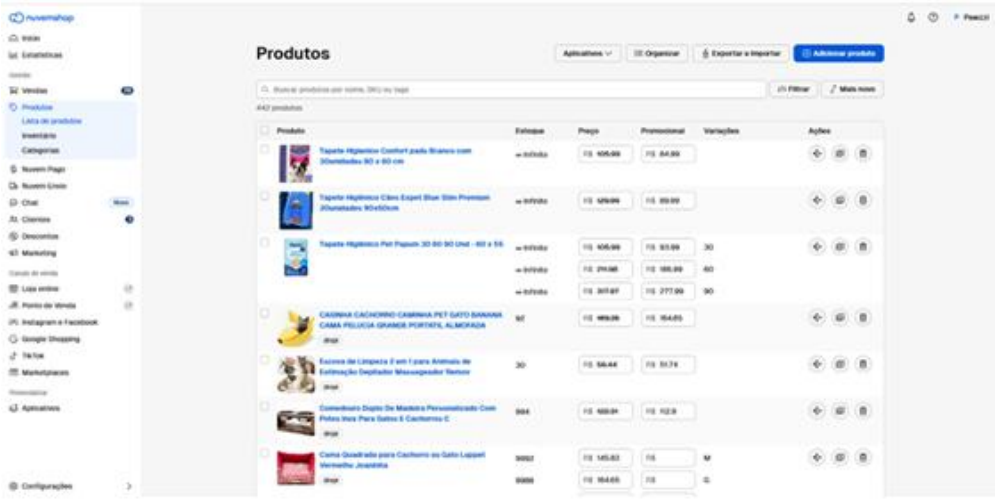
Fonte: Boente et al., 2025.

A Figura 7 ilustra o painel de estatísticas gerais da Nuvemshop, evidenciando métricas essenciais como número de vendas, ticket médio e receita acumulada, indicadores utilizados para tomada de decisão e avaliação de performance.

Em seguida, a Figura 8 ilustra o cadastro de produtos, interface que permite atualizar descrições, valores, imagens e disponibilidade de estoque de maneira automatizada.

Revista Científica Sistemática
ISSN: 2675-521

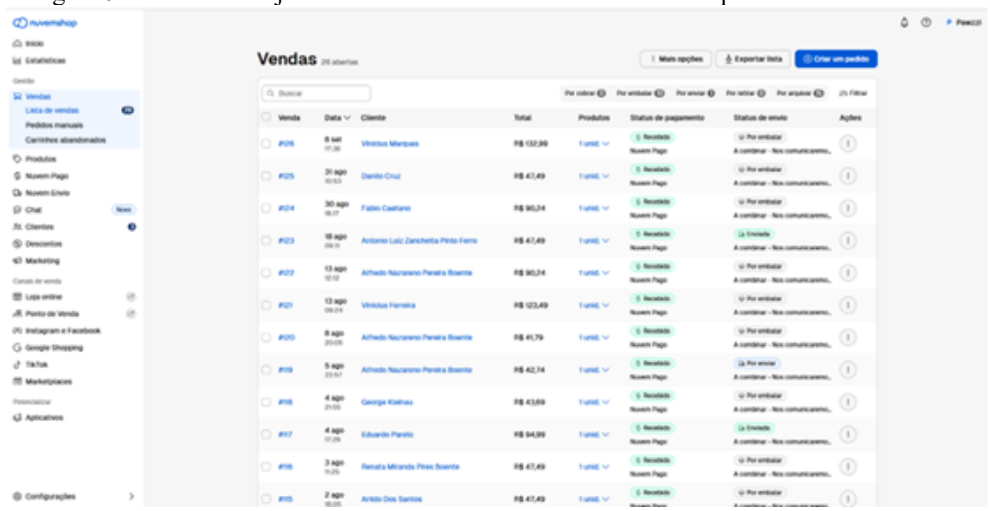
Figura 8. Gestão da Loja Virtual Pawzzi - Plataforma Nuvemshop - Produtos Cadastrados.



Fonte: Boente et al., 2025.

A Figura 9 ilustra o módulo de vendas realizadas, no qual é possível acompanhar o status dos pedidos, desde o processamento até a entrega final.

Figura 9. Gestão da Loja Virtual Pawzzi - Plataforma Nuvemshop - Vendas Realizadas.

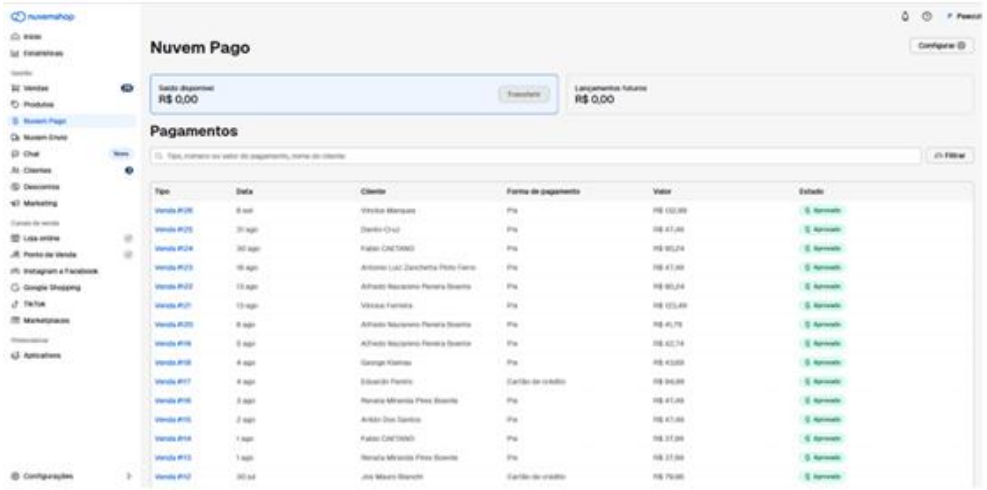


Fonte: Boente et al., 2025.

A Figura 10 ilustra o painel de pagamentos recebidos, assegurando transparência e controle financeiro sobre todas as transações comerciais online concluídas.

Revista Científica Sistemática
ISSN: 2675-521

Figura 10. Gestão da Loja Virtual Pawzzi - Plataforma Nuvemshop - Pagamentos Recebidos.



Fonte: Boente et al., 2025.

Esse conjunto de recursos reflete a importância da segurança em tecnologia da informação aplicada à gestão de *e-commerce*, que permite a integração entre os processos administrativos e a experiência do cliente. Assim, a utilização da Nuvemshop demonstra como plataformas digitais robustas podem otimizar a operação de lojas online, especialmente no modelo *dropshipping*, como é o caso da loja virtual Pawzzi, promovendo eficiência, segurança e escalabilidade.

No entanto, a gerência técnico-operacional da loja virtual Pawzzi, observou alguns problemas de vulnerabilidades da plataforma digital, no que diz respeito aos riscos cibernéticos, que poderiam interferir diretamente na segurança da informação que, até então, não era vista como um problema.

4.2 VULNERABILIDADES NA SEGURANÇA DE INFORMAÇÃO

O crescimento exponencial do comércio eletrônico intensificou a dependência das lojas virtuais em relação às tecnologias da informação e comunicação, tornando-as alvos frequentes de ameaças cibernéticas. As vulnerabilidades digitais presentes nesses ambientes representam riscos cibernéticos significativos à confidencialidade, integridade e disponibilidade das informações, afetando tanto as organizações quanto os consumidores. Segundo Laudon e Laudon (2021), sistemas de e-commerce operam em ecossistemas complexos e interconectados, nos quais falhas de segurança podem comprometer dados financeiros, informações pessoais e a própria continuidade do negócio.

Uma das principais vulnerabilidades das lojas virtuais está relacionada a falhas de desenvolvimento e configuração inadequada de sistemas web. Problemas como injeção de SQL, falhas de autenticação, controle de acesso inadequado, quebra de seções e exposição de dados sensíveis figuram entre as vulnerabilidades mais recorrentes em aplicações web (OWASP, 2023). Essas fragilidades, identificadas na loja virtual Pawzzi, permitem que agentes maliciosos explorem brechas para obter acesso não autorizado a bancos de dados, realizar fraudes ou interromper serviços,

Revista Científica Sistemática
ISSN: 2675-521

prejudicando a reputação e a confiabilidade da loja virtual, além de expor seus clientes.

Além disso, a ausência de políticas robustas de segurança da informação contribui para o aumento da superfície de ataques cibernéticos. Conforme destaca Stallings (2020, p.87), a segurança cibernética não deve ser compreendida apenas como um conjunto de ferramentas tecnológicas, mas como um processo contínuo que envolve governança, gestão de riscos, capacitação de usuários e monitoramento constante. Em muitas lojas virtuais, a negligência quanto à atualização de sistemas, uso de senhas fracas e falta de criptografia adequada facilita a ocorrência de ataques como *phishing*, *malware* e *ransomware*.

Outro aspecto crítico refere-se à proteção dos dados dos consumidores, especialmente em um contexto regulatório mais rigoroso. A Lei Geral de Proteção de Dados Pessoais (LGPD) impõe às organizações a responsabilidade de adotar medidas técnicas e administrativas para proteger dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas (BRASIL, 2018). Nesse sentido, Kurose e Ross (2021) ressaltam que a transmissão insegura de informações em redes públicas pode resultar em interceptação de dados, comprometendo transações financeiras e violando a privacidade dos usuários.

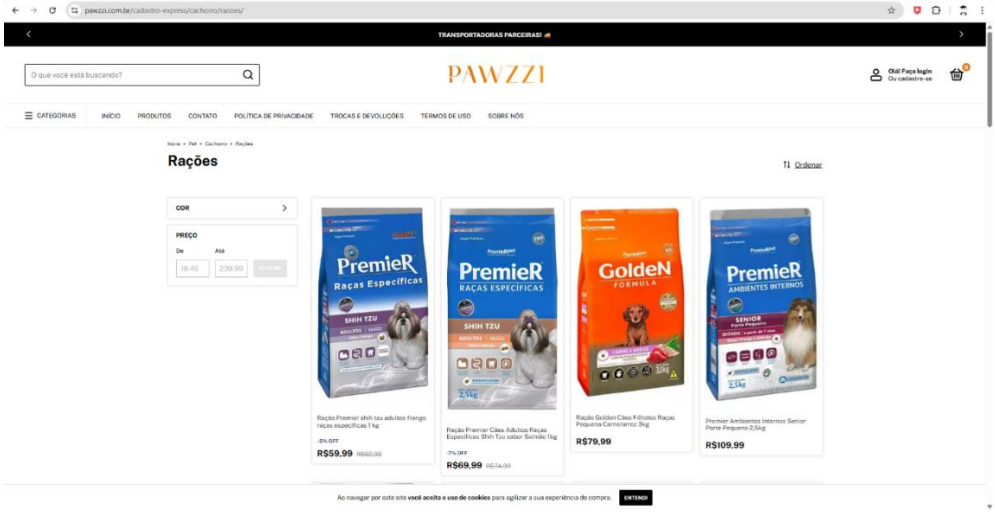
Por fim, os riscos cibernéticos enfrentados pelas lojas virtuais tendem a se intensificar com a sofisticação das ameaças e o uso crescente de tecnologias emergentes. Conforme aponta a ISO/IEC 27001 (2022), a gestão eficaz da segurança da informação exige a identificação sistemática de vulnerabilidades, avaliação de riscos e implementação de controles adequados. Assim, investir em segurança cibernética torna-se não apenas uma exigência técnica e legal, mas um fator estratégico para a sustentabilidade e competitividade das lojas virtuais no ambiente digital.

Neste contexto, são elencados alguns problemas de segurança da informação quanto a riscos cibernéticos, na loja virtual Pawzzi.

A Figura 11 ilustra a página de acesso aos produtos da loja elencados por categoria.

Revista Científica Sistemática
ISSN: 2675-521

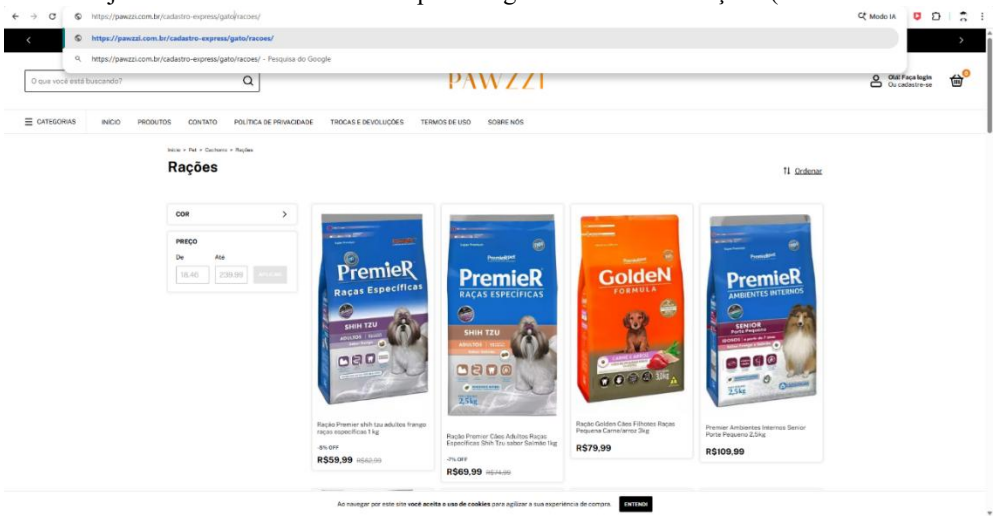
Figura 11. Loja Virtual Pawzzi - Produtos por categoria - Cachorro Rações.



Fonte: Pawzzi, 2026.

Consegue-se observar que na Figura 12, existe a possibilidade do usuário, através da barra de endereço, alterar o status de chamada (endereço de chamada) de uma página da loja virtual Pawzzi.

Figura 12. Loja Virtual Pawzzi - Produtos por categoria - Cachorro Rações (VULNERABILIDADE).

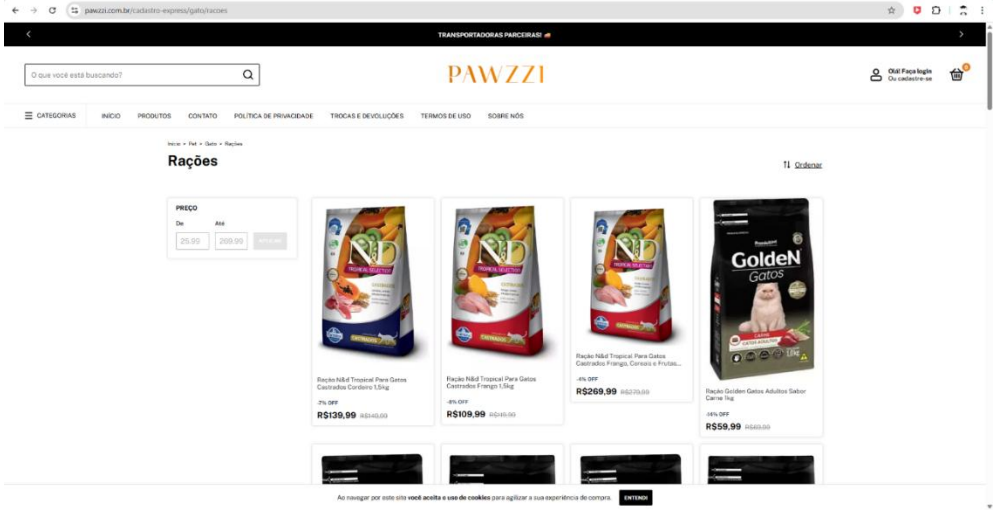


Fonte: Pawzzi, 2026.

Na Figura 13, após alterar no endereço original da URL https://pawzzi.com.br/cadastro-express/**cachorro**/racoes/, substituindo no endereço o nome cachorro por gato, https://pawzzi.com.br/cadastro-express/**gato**/racoes/, a loja permite que seja alterada a página da loja virtual que o cliente estava navegando.

Revista Científica Sistemática
ISSN: 2675-521

Figura 13. Loja Virtual Pawzzi - Produtos por categoria - Gato Rações (VULNERABILIDADE).



Fonte: Pawzzi, 2026.

Note que as rações, ora disponíveis para cachorro na Figura 12, são substituídas por rações para gato na Figura 13, demonstrando vulnerabilidade e falta de tratamento de seções em páginas internet para que tais problemas não venham ocorrer.

Outra vulnerabilidade mais grave identificada foi identificada na Figura 14 está na página de "Compra Segura" que, em princípio, deveria ocorrer efetivamente de forma segura. Como já foi identificada a não existência do tratamento de seção em páginas virtuais, o endereço de URL podem ser alterados a qualquer tempo, conforme ilustrado na Figura 15.

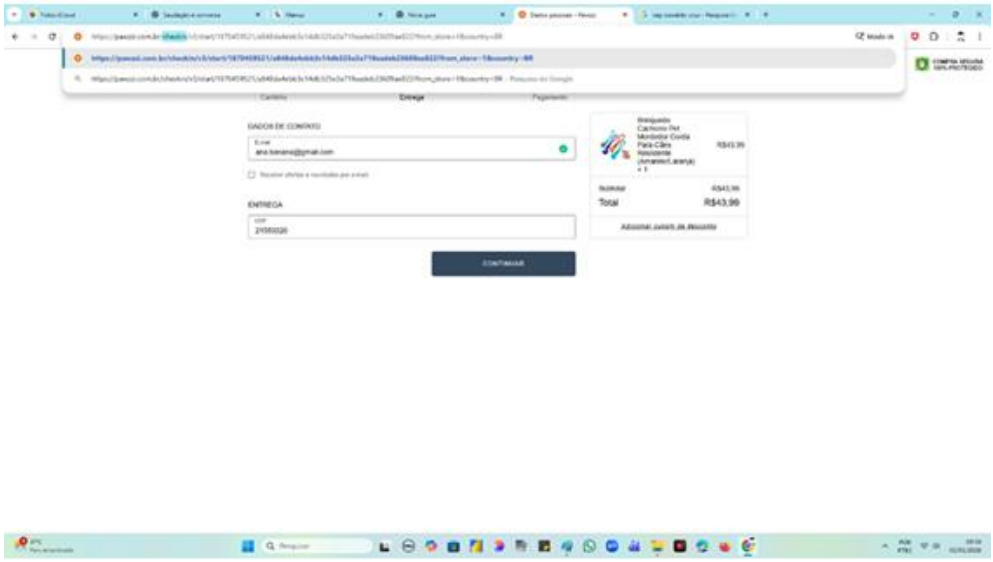
Figura 14. Loja Virtual Pawzzi - Compra e registro de dados de clientes.

Fonte: Pawzzi, 2026.

Com qualquer tipo de alteração, por apresentar seção de URL aberta, dados dos clientes passam a ficar vulneráveis infringindo o aspecto de segurança junto a Lei Geral de Proteção de Dados (LGPD).

Revista Científica Sistemática
ISSN: 2675-521

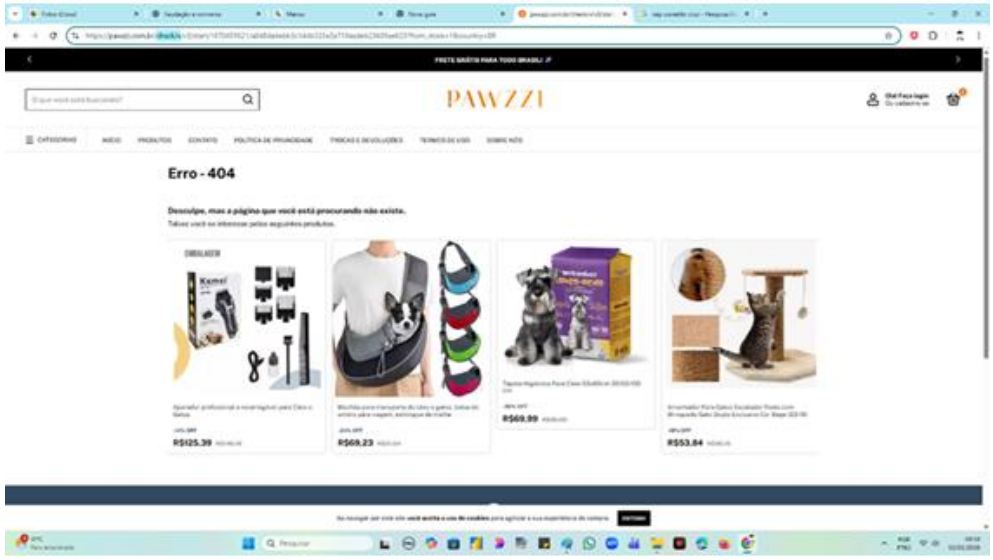
Figura 15. Loja Virtual Pawzzi - Compra e registro de dados de clientes (VULNERABILIDADE).



Fonte: Pawzzi, 2026.

Este não é o único problema vinculado a este tipo de operação em ambiente virtual de compras. Note na Figura 16 que ao alterar o conteúdo de URL numa página de pagamento, em princípio em ambiente seguro, ocorrerá um erro de página, o que certamente, deixaria qualquer eventual cliente totalmente inseguro em continuar sua experiência de compra na loja virtual Pawzzi.

Figura 16. Loja Virtual Pawzzi - Página com erro de processamento (VULNERABILIDADE).



Fonte: Pawzzi, 2026.

Outros erros e vulnerabilidades também foram identificadas ao estudar o caso da loja virtual Pawzzi. No entanto, não foram todos tratados neste artigo.

4.3 DESAFIOS AOS RISCOS CIBERNÉTICOS

Os riscos cibernéticos enfrentados pelas lojas virtuais tendem a se intensificar com a

Revista Científica Sistemática
ISSN: 2675-521

sofisticação das ameaças e o uso crescente de tecnologias emergentes. Conforme aponta a ISO/IEC 27001 (2022), a gestão eficaz da segurança da informação exige a identificação sistemática de vulnerabilidades, avaliação de riscos e implementação de controles adequados.

Esses aspectos foram identificados na loja virtual Pawzzi, que precisaria investir em segurança cibernética tornando-se não apenas uma exigência técnica e legal, mas um fator estratégico para a sustentabilidade e competitividade das lojas virtuais no ambiente digital.

No entanto, esse tipo de investimento não seria apenas necessário à loja virtual Pawzzi, pois tanto os parceiros de negócios, quanto a plataforma de gestão de negócios e pagamentos, Nuvemshop, também precisam investir nesse aspecto para garantir maior segurança às operações comerciais em ambiente virtual.

5 RESULTADOS E DISCUSSÕES

A análise do ambiente estudado evidenciou vulnerabilidades estruturais relevantes, associadas principalmente à fragmentação da cadeia de suprimentos digital adotada pela loja virtual Pawzzi no modelo *dropshipping*.

5.1 MAPEAMENTO SIMPLIFICADO DOS FLUXOS DE DADOS

O mapeamento dos fluxos de dados evidenciou a circulação de informações pessoais e transacionais por múltiplos atores do ecossistema de *dropshipping*, ampliando a superfície de ataque e reduzindo a visibilidade do controlador sobre o tratamento integral das informações.

5.2 MATRIZ DE RISCOS IDENTIFICADOS

O Quadro 1 apresenta o posicionamento qualitativo dos principais riscos identificados no modelo de *dropshipping*, considerando impacto e probabilidade.

Quadro 1. Matriz de riscos no modelo de *dropshipping*.

Risco identificado	Impacto potencial	Probabilidade	Classificação	Controles recomendados
Comprometimento de fornecedor	Vazamento de dados pessoais	Média	Alto	Due diligence de terceiros e cláusulas contratuais
Falhas de integração sistêmica	Interrupção do serviço	Média	Médio	Testes de segurança e monitoramento contínuo

Revista Científica Sistemática
ISSN: 2675-521

Uso inadequado de credenciais	Acesso não autorizado	Alta	Alto	Autenticação multifator e segregação de funções
Dependência excessiva de plataformas	Perda de controle operacional	Média	Médio	Estratégias de contingência e avaliação periódica

Fonte: Elaborada pelos autores.

Ao interpretar o Quadro 1, tem-se uma visão estruturada e analítica dos principais riscos associados a esse modelo de negócio sob a ótica da segurança da informação, evidenciando a relação entre tipo de risco, impacto potencial, probabilidade de ocorrência, nível de criticidade e controles recomendados.

Em primeiro lugar, o risco de comprometimento de fornecedor destaca-se como um dos mais críticos, sendo classificado como alto. O impacto potencial associado a esse risco é o vazamento de dados pessoais, o que demonstra a forte dependência do dropshipping em relação a terceiros que, muitas vezes, detêm acesso direto a dados sensíveis de clientes. Embora a probabilidade seja considerada média, a severidade do impacto justifica a classificação elevada. Os controles recomendados, como *due diligence* de terceiros e cláusulas contratuais, evidenciam a necessidade de uma governança preventiva e jurídica, alinhada à LGPD e às boas práticas de gestão de riscos na cadeia de suprimentos.

O segundo risco identificado refere-se às falhas de integração sistêmica, comuns em ambientes altamente dependentes de APIs, plataformas e sistemas externos. O impacto principal é a interrupção do serviço, o que afeta diretamente a disponibilidade, um dos pilares da segurança da informação (VON SOLMS e VAN NIEKERK, 2013). A probabilidade média e a classificação média indicam um risco operacional recorrente, mas controlável. Os controles sugeridos, como testes de segurança e monitoramento contínuo, reforçam a importância de práticas técnicas associadas à resiliência e à confiabilidade dos sistemas.

O uso inadequado de credenciais aparece como um dos riscos mais sensíveis do quadro, apresentando alta probabilidade e classificação alta. O impacto potencial, caracterizado pelo acesso não autorizado, evidencia vulnerabilidades relacionadas ao fator humano e à gestão de identidades e acessos. A recomendação de autenticação multifator e segregação de funções demonstra a necessidade de controles técnicos e administrativos integrados, voltados à mitigação de ameaças internas e externas.

Por fim, a dependência excessiva de plataformas reflete um risco estratégico típico do dropshipping, no qual o lojista perde parte do controle operacional ao depender fortemente de provedores de tecnologia e *marketplaces*. Embora a probabilidade seja média e a classificação também

Revista Científica Sistemática
ISSN: 2675-521

média, o impacto é relevante, pois compromete a autonomia organizacional. Os controles propostos, estratégias de contingência e avaliação periódica, indicam a importância do planejamento estratégico e da diversificação tecnológica.

De forma geral, o quadro evidencia que os riscos no modelo *dropshipping* não são exclusivamente técnicos, mas envolvem dimensões organizacionais, contratuais, humanas e estratégicas, reforçando a necessidade de uma abordagem integrada de governança da segurança da informação. A matriz cumpre, assim, o papel de instrumento decisório, auxiliando gestores na priorização de controles e na mitigação de riscos críticos ao negócio.

5.3 INDICADORES ESTIMADOS DE MATURIDADE EM SEGURANÇA

Com base no NIST *Cybersecurity Framework*, estimou-se qualitativamente o nível de maturidade observado:

Identify: Médio – existência de conhecimento parcial dos ativos e riscos.

Protect: Médio – controles básicos presentes, porém dependentes de terceiros.

Detect: Baixo – ausência de monitoramento ativo próprio.

Respond: Baixo – inexistência de plano formal de resposta a incidentes.

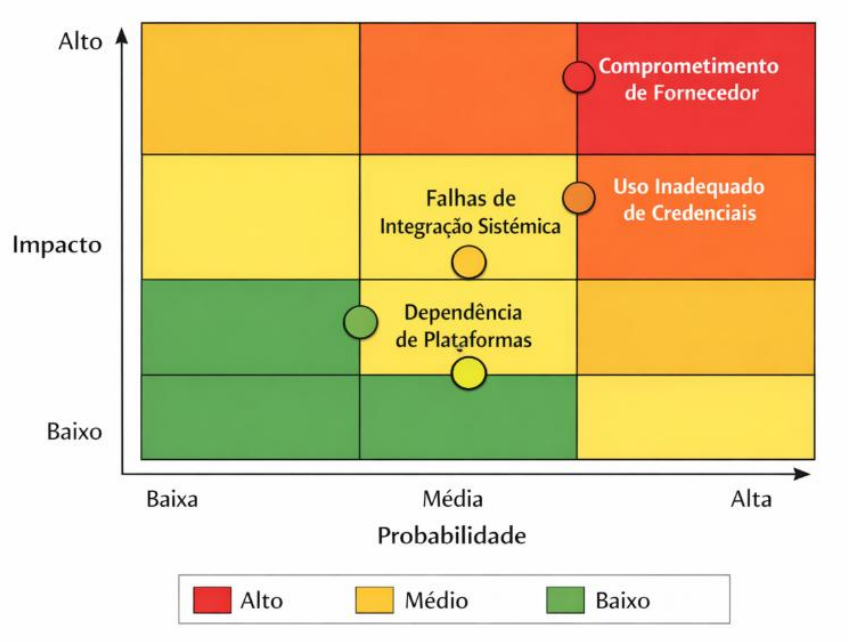
Recover: Médio – dependência de mecanismos das plataformas utilizadas.

Esses indicadores reforçam a necessidade de evolução da governança de segurança ao longo da cadeia de suprimentos digital.

A Figura 17 ilustra o Mapa de Calor dos riscos identificados na adoção do modelo *dropshipping* pela loja virtual Pawzzi.

Revista Científica Sistemática
ISSN: 2675-521

Figura 17. Mapa de calor de risco no modelo *dropshipping*.



Fonte: Elaborada pelos autores.

O mapa de calor de risco no modelo *dropshipping*, ilustrado na Figura 17, representa graficamente a distribuição e a criticidade dos principais riscos associados a esse modelo de negócio, a partir da combinação entre probabilidade de ocorrência (eixo horizontal) e impacto potencial (eixo vertical). O uso de cores, verde, amarelo e vermelho, permite uma visualização imediata do nível de severidade dos riscos, classificando-os, respectivamente, como baixos, médios e altos, o que facilita o processo de tomada de decisão gerencial.

No quadrante superior direito, caracterizado por alta probabilidade e alto impacto, encontra-se o risco de comprometimento de fornecedor, evidenciado em vermelho. Essa posição indica um risco crítico, capaz de gerar danos significativos à organização, como vazamento de dados, interrupções operacionais e impactos legais, especialmente em ambientes que envolvem tratamento de dados pessoais. A localização desse risco no mapa reforça a necessidade de controles prioritários, tais como governança de terceiros, auditorias periódicas e cláusulas contratuais de segurança.

Ainda na zona de maior criticidade, observa-se o risco de uso inadequado de credenciais, posicionado em uma região de impacto elevado e probabilidade média a alta. Esse risco reflete fragilidades na gestão de identidades e acessos, frequentemente associadas a falhas humanas ou à ausência de controles robustos de autenticação. Sua representação em área vermelha indica que, mesmo quando a probabilidade não é máxima, o potencial de dano justifica atenção imediata e investimentos em controles preventivos.

No centro do mapa, classificado como zona de risco médio (amarela), encontra-se o risco de falhas de integração sistêmica, com impacto e probabilidade considerados médios. Essa posição evidencia um risco operacional relevante, típico de ambientes altamente integrados por meio de APIs

Revista Científica Sistemática
ISSN: 2675-521

e plataformas externas. Embora não represente uma ameaça crítica imediata, sua recorrência pode afetar a disponibilidade dos serviços e a experiência do usuário, exigindo monitoramento contínuo e estratégias de mitigação.

Na região inferior do mapa, predominantemente verde, está o risco de dependência de plataformas, associado abaixo impacto e probabilidade média. Apesar de classificado como risco baixo a médio, sua presença no mapa indica um risco de natureza estratégica, relacionado à perda gradual de autonomia organizacional. Embora não demande ações emergenciais, esse risco exige acompanhamento periódico e planejamento de contingência para evitar dependência excessiva de fornecedores tecnológicos.

De modo geral, a figura evidencia que os riscos mais críticos no modelo *dropshipping* concentram-se nas áreas relacionadas à terceirização, gestão de acessos e dependência de fornecedores, confirmando a necessidade de uma abordagem integrada de governança da segurança da informação. O mapa de calor cumpre, assim, um papel fundamental como instrumento de priorização, permitindo que gestores visualizem rapidamente quais riscos exigem ações imediatas e quais podem ser tratados de forma planejada e progressiva.

6 CONCLUSÃO

O presente estudo evidenciou que o modelo *dropshipping* amplia de maneira significativa a superfície de ataque das organizações ao promover a dispersão de dados sensíveis entre múltiplos atores da cadeia de suprimentos digital. Essa característica estrutural do modelo reforça a complexidade dos riscos informacionais, uma vez que o controle sobre dados, processos e infraestruturas tecnológicas encontra-se distribuído entre fornecedores, plataformas e operadores externos. Os resultados obtidos indicam que, nesse contexto, a segurança da informação não pode ser compreendida apenas como um conjunto de mecanismos técnicos ou operacionais, mas deve ser abordada como um problema de governança e de gestão integrada de riscos.

Verificou-se que a adoção de práticas estruturadas de segurança da informação, alinhadas a *frameworks* internacionais consolidados, como os propostos pelo NIST e pela ISO/IEC 27001, constitui condição essencial para a sustentabilidade e a resiliência do comércio eletrônico baseado em dropshipping. Tal alinhamento torna-se ainda mais relevante no contexto regulatório brasileiro, especialmente diante das exigências impostas pela Lei Geral de Proteção de Dados Pessoais (LGPD), que atribui responsabilidades claras aos controladores de dados, inclusive em cenários de terceirização e compartilhamento de informações.

Do ponto de vista metodológico, a pesquisa limitou-se à análise de um único estudo de caso, a loja virtual Pawzzi sob o modelo *dropshipping*, o que impede a generalização estatística dos resultados

Revista Científica Sistemática
ISSN: 2675-521

alcançados. Contudo, essa limitação não compromete a relevância do estudo, uma vez que a abordagem qualitativa e exploratória se mostrou adequada para aprofundar a compreensão dos riscos, vulnerabilidades e desafios associados à segurança da informação no modelo *dropshipping*.

Por fim, as evidências levantadas oferecem subsídios analíticos relevantes para o desenvolvimento de pesquisas futuras, especialmente aquelas que adotem abordagens comparativas, multicasos ou quantitativas, capazes de ampliar o entendimento sobre a governança da segurança da informação em cadeias de suprimentos digitais. Espera-se que este estudo contribua tanto para o avanço acadêmico quanto para a prática organizacional, ao reforçar a importância de estratégias integradas de segurança e governança no comércio eletrônico contemporâneo.

REFERÊNCIAS

ALLEN, J**. Tudo sobre Dropshipping**: Como fazer dropshipping na prática no Brasil, começar a importar e como funciona o processo para te dar liberdade financeira. Ebook Kindle, 2021.

BOENTE, J. G. P.; BIANCHI, J. M. B.; BOENTE, A. M. P.; BOENTE, R. M. P. Empreendedorismo Digital: Uma estratégia de marketing digital com e-commerce e dropshipping. **ERR01**, [S. l.], v. 10, n. 5, p. e9365 , 2025. DOI: 10.56238/ERR01v10n5-047. Disponível em: https://periodicos.newsciencepubl.com/err01/article/view/9365. Acesso em: 12 dez. 2025.

BOENTE , J. G. P.; BIANCHI , J. M. B.; BOENTE , A. N. P.; BOENTE , R. M. P.; SANTOS , R. M. dos; FERREIRA , V. M. da S. Comércio Eletrônico e Dropshipping: Um estudo de caso em Marketing Digital. **Revista de Gestão e Secretariado**, [S. l.], v. 16, n. 11, p. e5400, 2025. DOI: 10.7769/gesec.v16i11.5400. Disponível em: https://ojs.revistagesec.org.br/secretariado/article/view/5400. Acesso em: 12 dez. 2025.

BOYSON, S. **Cyber supply chain risk management**: revolutionizing the strategic control of critical IT systems. Technovation, Amsterdam, v. 34, n. 7, p. 342–353, 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União, Brasília, DF, 2018.

CHOPRA, S.; SODHI, M. S. Managing risk to avoid supply-chain breakdown. ***MIT Sloan Management Review*****,** v. 46, n. 1, p. 53–61, 2014.

DONEDA, Danilo et al. **Lei Geral de Proteção de Dados Pessoais***: Comentários à Lei nº 13.709/2018*. São Paulo: Revista dos Tribunais, 2019.

ENISA. **Threat Landscape Report. European Union Agency for Cybersecurity**, edições recentes, 2025.

ISACA. **COBIT 2019 Framework**: Governance and Management Objectives. Rolling Meadows, IL, 2019.

ISO/IEC. **ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements**. Geneva, 2022.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet**: uma abordagem top-down. 8. ed. São Paulo: Pearson, 2021.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de informação gerenciais**. 16. ed. São Paulo: Pearson, 2021.

LOPES, S. A Web Mobile: Design responsivo e além para uma web adaptada ao mundo mobile. São Paulo: Editora Casa do Código, 2014.

NIST. **Framework for improving critical infrastructure cybersecurity**. Version 1.1. Gaithersburg, 2018.

NIST. **Cybersecurity supply chain risk management practices for systems and organizations**. NIST SP 800-161 Rev. 1. Gaithersburg, 2022.

OECD. **Digital Security Risk Management for Economic and Social Prosperity**. Paris, 2015.

OWASP. OWASP Top 10: **The Ten Most Critical Web Application Security Risks**. 2023.

PAWZZI. **E-Commerce da Loja Pawzzi**. Disponível em: https://www.pawzzi.com.br. Acesso em: 08/01/2026.

STALLINGS, W. **Criptografia e segurança de redes**: princípios e práticas. 7. ed. São Paulo: Pearson, 2020.

VERIZON. **Data Breach Investigations Report** (DBIR). Edições recentes, 2025.

VON SOLMS, R.; VAN NIEKERK, J. **From information security to cyber security**. Computers & Security, Oxford, v. 38, p. 97–102, 2013.

WHITMAN, M. E.; MATTORD, H. J. **Principles of information security**. 6. ed. Boston: Cengage Learning, 2018.