INSTITUTO FEDERAL GOIANO – CAMPUS CERES
BACHAREL EM SISTEMAS DE INFORMAÇÃO
KALITA STEPHANE ALVES DE ALMEIDA

VULNERABILIDADES NA SEGURANÇA DIGITAL DE MARKETPLACES: um estudo de caso nos marketplaces Mercado Livre, Americanas, OLX e Facebook

CERES – GO
2025

KALITA STEPHANE ALVES DE ALMEIDA

VULNERABILIDADES NA SEGURANÇA DIGITAL DE MARKETPLACES: um estudo de caso nos marketplaces Mercado Livre, Americanas, OLX e Facebook

Trabalho de curso apresentado ao curso de Sistemas de Informação do Instituto Federal Goiano – Campus Ceres, como requisito parcial para a obtenção do título de Bacharel em Sistemas de Informação, sob orientação do Prof. Ms. Roitier Campos Gonçalves.

CERES – GO
2025

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema Integrado de Bibliotecas do IF Goiano - SIBi

Almeida, Kalita Stephane Alves
A447 VULNERABILIDADES NA SEGURANÇA DIGITAL DE MARKETPLACES: um estudo de caso nos marketplaces Mercado Livre, Americanas, OLX e Facebook / Kalita Stephane Alves Almeida. Ceres 2025.

71f. il.

Orientador: Prof. Me. Roitier Campos Gonçalves.
Tcc (Bacharel) - Instituto Federal Goiano, curso de 0320203 - Bacharelado em Sistemas de Informação - Ceres (Campus

I. Título.

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO

PARA DISPONIBILIZAR PRODUÇÕES TÉCNICO-CIENTÍFICAS NO REPOSITÓRIO INSTITUCIONAL DO IF GOIANO

Com base no disposto na Lei Federal nº 9.610, de 19 de fevereiro de 1998, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia Goiano a disponibilizar gratuitamente o documento em formato digital no Repositório Institucional do IF Goiano (RIIF Goiano), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IF Goiano.

IDENTIFICAÇÃO DA PRODUÇÃO TÉCNICO-CIENTÍFICA

- ☐ Tese (doutorado)
- ☐ Dissertação (mestrado)
- ☐ Monografia (especialização)
- ☒ TCC (graduação)
- ☐ Artigo científico
- ☐ Capítulo de livro
- ☐ Livro
- ☐ Trabalho apresentado em evento
- ☐ Produto técnico e educacional - Tipo:

Nome completo do autor: Kalita Stephane Alves de Almeida

Matrícula: 2021103202030084

Título do trabalho: VULNERABILIDADES NA SEGURANÇA DIGITAL DE MARKETPLACES: um estudo de caso nos marketplaces Mercado Livre, Americanas, OLX e Facebook

RESTRIÇÕES DE ACESSO AO DOCUMENTO

Documento confidencial: ☒ Não ☐ Sim, justifique:

Informe a data que poderá ser disponibilizado no RIIF Goiano: 20 / 06 / 2025

O documento está sujeito a registro de patente? ☐ Sim ☒ Não

O documento pode vir a ser publicado como livro? ☐ Sim ☒ Não

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O(a) referido(a) autor(a) declara:

• Que o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;

• Que obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autoria, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia Goiano os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;

• Que cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia Goiano.

Itapuranga - Goias (Local) 17 / 06 / 2025 (Data)

gov.br Documento assinado digitalmente
KALITA STEPHANE ALVES DE ALMEIDA
Data: 17/06/2025 19:23:47-0300
Verifique em https://validar.iti.gov.br

Assinatura do autor e/ou detentor dos direitos autorais

gov.br Documento assinado digitalmente
ROITIER CAMPOS GONCALVES
Data: 17/06/2025 19:31:14-0300
Verifique em https://validar.iti.gov.br

Ciente e de acordo:

Assinatura do(a) orientador(a)

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO

ATA DE DEFESA DE TRABALHO DE CURSO

Aos seis dias do mês de junho do ano de dois mil e vinte e cinco , reuniu-se a banca examinadora de defesa de Trabalho de Curso da acadêmica Kalita Stephane Alves de Almeida, do Curso de BACHARELADO EM SISTEMAS DE INFORMAÇÃO, matrícula 2021103202030084, cujo título é "**VULNERABILIDADES NA SEGURANÇA DIGITAL DE MARKETPLACES: um estudo de caso nos marketplaces Mercado Livre, Americanas, OLX e Facebook**" . A defesa iniciou-se às 19 horas e 39 minutos, finalizando-se às 20 horas e 15 minutos. A banca examinadora considerou o trabalho APROVADO com média 8,5 no trabalho escrito, média 8,0 no trabalho oral, apresentando assim média aritmética final de 8,25 pontos, estando a estudante APTA para fins de conclusão do Trabalho de Curso. Após atender às considerações da banca e respeitando o prazo disposto em calendário acadêmico, a estudante deverá fazer a submissão da versão corrigida em formato digital (.pdf) no Repositório Institucional do IF Goiano – RIIF, acompanhado do Termo Ciência e Autorização Eletrônico (TCAE), devidamente assinado pelo autor e orientador.

Os integrantes da banca examinadora assinam a presente.

.

(Assinado Eletronicamente)
Roitier Campos Gonçalves
Professor Orientador

(Assinado Eletronicamente)
Paulo Henrique Rodrigues Araujo
Membro Interno

(Assinado Eletronicamente)
Isaac Mendes Melo
Membro Externo

gov.br
Documento assinado digitalmente
ISAAC MENDES DE MELO
Data: 17/06/2025 21:04:31-0300
Verifique em https://validar.iti.gov.br

Documento assinado eletronicamente por:

- **Roitier Campos Goncalves**, **PROFESSOR ENS BASICO TECN TECNOLOGICO** , em 06/06/2025 20:17:16.
- **Paulo Henrique Rodrigues Araujo**, **PROF ENS BAS TEC TECNOLOGICO-SUBSTITUTO**, em 06/06/2025 20:19:44.

Este documento foi emitido pelo SUAP em 06/06/2025. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifgoiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 714619
Código de Autenticação: b4afa26aa7

INSTITUTO FEDERAL GOIANO
Campus Ceres
Rodovia GO-154, Km 03, SN, Zona Rural, CERES / GO, CEP 76300-000
(62) 3307-7100

Dedico este trabalho ao meu pai, que me ensinou a contar nos dedos. À minha mãe, que me ensinou a contar com Deus. Ao meu marido, que é meu porto seguro. À Daianny, que é com quem posso contar.

AGRADECIMENTOS

Gostaria de expressar minha mais profunda gratidão ao Prof. Me. Roitier Campos Gonçalves pela orientação dedicada, valiosos ensinamentos e apoio incondicional ao longo de toda a realização deste trabalho de conclusão de curso. Sua expertise e paciência foram essenciais para o desenvolvimento deste estudo.

Agradeço de coração aos meus pais, cujo apoio constante, incentivo e amor foram pilares fundamentais durante toda a minha trajetória acadêmica. Ao meu marido, Daniel Siqueira, sou imensamente grata pela compreensão, motivação e por estar sempre ao meu lado nos momentos desafiadores.

Também registro meus sinceros agradecimentos à Daianny, cuja colaboração e suporte contribuíram significativamente para a concretização deste trabalho.

A todos vocês, meu muito obrigada por fazerem parte desta caminhada e por tornarem essa jornada ainda mais especial e significativa.

“Em um mundo onde a tecnologia avança rapidamente, a segurança cibernética torna-se a linha de frente na proteção da nossa privacidade e integridade digital.”

Bruce Schneier

RESUMO

O presente estudo investiga os principais desafios e riscos associados à segurança digital nessas plataformas de e-commerce. Diante da problemática central, como a falta de regulamentação padronizada nos marketplaces pode impactar a segurança digital dessas plataformas e quais seriam as medidas mais eficazes para mitigar essas vulnerabilidades, considerando tanto a atualização dos sistemas de segurança quanto a conscientização dos usuários? O estudo visa analisar como a ausência de normas padronizadas contribui para a exposição dos usuários a fraudes, phishing e roubo de identidade, entre outras ameaças. O objetivo geral é identificar as principais vulnerabilidades nesses marketplaces, oferecendo uma compreensão aprofundada dos riscos envolvidos e sugerindo estratégias de mitigação que possam proteger os dados dos consumidores e aumentar a confiança nas transações online. Por meio de uma abordagem exploratória qualitativa fundamentada em pesquisa bibliográfica, o estudo destaca a importância de um conjunto de medidas, como a autenticação multifatorial, o monitoramento em tempo real e a implementação de políticas educacionais que promovam a conscientização dos usuários sobre práticas seguras. Essas ações visam fortalecer a segurança e criar um ambiente mais confiável para todos os envolvidos nas transações digitais.

Palavras-chave: Segurança Digital. Marketplaces. Vulnerabilidades. Regulamentação. Conscientização do Usuário.

ABSTRACT

This study investigates the main challenges and risks associated with digital security on these e-commerce platforms. Given the central problem, how can the lack of standardized regulations on marketplaces impact the digital security of these platforms and what would be the most effective measures to mitigate these vulnerabilities, considering both the update of security systems and user awareness? The study aims to analyze how the lack of standardized regulations contributes to the exposure of users to fraud, phishing and identity theft, among other threats. The overall objective is to identify the main vulnerabilities on these marketplaces, offering an in-depth understanding of the risks involved and suggesting mitigation strategies that can protect consumer data and increase trust in online transactions. Through a qualitative exploratory approach based on bibliographic research, the study highlights the importance of a set of measures, such as multi-factor authentication, real-time monitoring and the implementation of educational policies that promote user awareness of safe practices. These actions aim to strengthen security and create a more trustworthy environment for all those involved in digital transactions.

Keywords: Digital Security. Marketplaces. Vulnerabilities. Regulation. User Awareness.

LISTA DE SIGLAS E ABREVIATURAS

B2B	Business to Business
B2C	Business to Consumer
DDoS	Ataques de Negação de Serviço
GDPR	Regulamento Geral de Proteção de Dados
LGPD	Lei Geral de Proteção de Dados
MFA	Autenticação Multifatorial
P2P	Peer-to-Peer

LISTA DE FIGURAS

Figura 1 - Cadeia de consequências da falta de conscientização digital..... 39
Figura 2 - Comparação entre os modelos de negócio e recursos de segurança em marketplaces selecionados.....45
Figura 3 - Mapa-múndi com destaque às regiões de legislação rigorosa de proteção de dados (GDPR e LGPD).....46
Figura 4 - Fluxo de informações entre marketplaces, autoridades regulatórias e usuários.....48

LISTA DE GRÁFICOS

Gráfico 1 - Crescimento do uso de certificados SSL e percepção de segurança no e-commerce brasileiro (2019–2023)..... 1
Gráfico 2 - Faturamento dos marketplaces no Brasil (2020–2024).....4
Gráfico 3 - Indicadores de segurança em sites de e-commerce (2023)..... 5
Gráfico 4 - Impacto das fraudes em e-commerce no Brasil e América Latina (2023)..... 6
Gráfico 5 - Indicadores de Segurança e Vulnerabilidade em Marketplaces Digitais.....13
Gráfico 6 - Comparação de Segurança entre Plataformas..... 14
Gráfico 7 - Comparação entre legislações de proteção de dados (LGPD, GDPR e CCPA) quanto aos critérios de segurança digital aplicados a marketplaces..16
Gráfico 8 - Vulnerabilidades de segurança por marketplaces..... 20
Gráfico 9 - Evolução da taxa de tentativas de fraude no e-commerce brasileiro (2022–2023)..... 27
Gráfico 10 - Tentativas de fraude e valor total em 2023.....28
Gráfico 11 - Tipos de ataques cibernéticos mais comuns em marketplaces..... 34

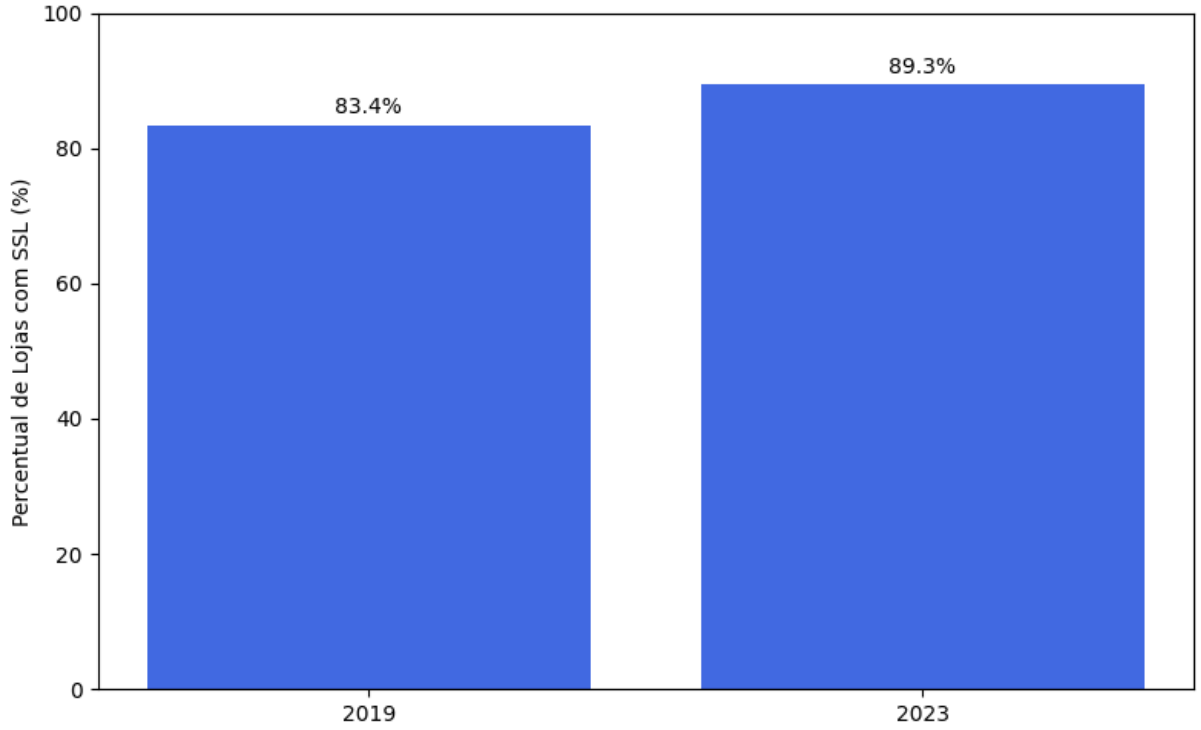
SUMÁRIO

1. INTRODUÇÃO..... 1
2. JUSTIFICATIVA..... 3
3. OBJETIVO GERAL..... 7
3.1. OBJETIVOS ESPECÍFICOS..... 7
4. METODOLOGIA..... 8
5. ANÁLISE DAS PRÁTICAS DE SEGURANÇA E REGULAMENTAÇÃO NOS MARKETPLACES..... 9
5.1. Estrutura e funcionamento dos marketplaces: Mercado Livre, Americanas, OLX e Facebook..... 10
5.2. Regulamentação de segurança digital: políticas e diretrizes vigentes para marketplaces..... 13
5.3. Lacunas nas práticas de segurança adotadas por cada plataforma..... 18
5.4. Impacto das regulamentações (ou da ausência delas) na segurança dos dados dos usuários..... 22
6. PRINCIPAIS FORMAS DE FRAUDE E ATAQUES CIBERNÉTICOS NOS MARKETPLACES..... 25
6.1. Tipos de fraudes mais recorrentes em transações online..... 26
6.2. Fraudes financeiras: golpes de pagamento e não entrega de produtos..... 31
6.3. Impacto dos ataques cibernéticos na confiabilidade e no funcionamento das plataformas..... 33
7. CONSCIENTIZAÇÃO DO USUÁRIO E A IMPORTÂNCIA DA REGULAMENTAÇÃO PADRONIZADA..... 37
7.1. Importância da conscientização do usuário para a segurança digital..... 38
7.2. Estratégias de comunicação e educação para práticas seguras..... 41
7.3. Desafios e benefícios de uma regulamentação padronizada para marketplaces..... 44
7.4. Propostas de melhoria para aumentar a segurança e a confiança nas transações online..... 49
8. CONSIDERAÇÕES FINAIS..... 52
9. REFERÊNCIAS..... 54

1. INTRODUÇÃO

A proteção digital passou a ser um elemento estratégico para garantir o bom desempenho e a expansão contínua das plataformas de marketplace. Isso ocorre porque, com o crescimento acelerado do comércio eletrônico, torna-se essencial adotar medidas que assegurem a integridade das transações virtuais e reforcem a confiança dos usuários. Dados da BigDataCorp mostram que o uso de certificados de segurança SSL por lojas virtuais no Brasil cresceu significativamente nos últimos anos, passando de 83,36% em 2019 para 89,35% em 2023, o que evidencia o aumento das iniciativas voltadas à segurança digital (ComputerWeekly, 2023). Essa evolução pode ser visualizada no Gráfico 1, que apresenta o crescimento percentual do uso de SSL no comércio eletrônico brasileiro entre 2019 e 2023.

Gráfico 1 - Crescimento do uso de certificados SSL e percepção de segurança no e-commerce brasileiro (2019–2023)



Fonte: Elaborado pela autora e adaptado de ComputerWeekly (2023) e Security Leaders (2023).

Além disso, uma pesquisa da Sociedade Brasileira de Varejo e Consumo (SBVC) revelou que 87% dos consumidores afirmam se sentir seguros ao comprar

em lojas virtuais, demonstrando que a segurança é um fator determinante para a fidelização e crescimento das plataformas online (Security Leaders, 2023). Com o aumento do uso de plataformas como Mercado Livre, Americanas, OLX e Facebook para compra e venda de produtos e serviços, cresce também o número de ataques cibernéticos e fraudes, levando a uma preocupação maior com as vulnerabilidades nesses ambientes virtuais. Esses marketplaces, cada um com suas particularidades e públicos específicos, enfrentam desafios significativos na proteção de dados e na segurança das transações, envolvendo tanto a proteção de informações dos usuários quanto a prevenção de práticas fraudulentas.

As vulnerabilidades em marketplaces podem se manifestar de diversas formas, indo desde fraudes de identidade e pagamento até invasões de sistemas e ataques de phishing (Instituto Propague, 2024). A proteção contra essas ameaças envolve a implementação de medidas rigorosas de segurança, como autenticação multifatorial, criptografia de dados e análise constante das atividades suspeitas nas plataformas (Twilio, s.d.; TI INSIDE, 2024). Entretanto, esses recursos nem sempre são suficientes para garantir a total segurança do usuário, uma vez que os cibercriminosos estão em constante evolução, desenvolvendo novas técnicas para burlar as camadas de segurança existentes (ClearSale, s.d.).

Este estudo tem como objetivo compreender as vulnerabilidades na segurança digital de marketplaces. A análise dessas fragilidades em plataformas digitais aponta para um denominador comum: a necessidade de sistemas de segurança mais robustos, que ultrapassem as medidas tradicionais de proteção. Um dos principais desafios enfrentados por essas plataformas é manter o equilíbrio entre proporcionar uma experiência de compra ágil e prática, sem comprometer a integridade dos dados e das transações dos usuários.

Com o avanço das ameaças cibernéticas, torna-se cada vez mais urgente a adoção de estratégias proativas, como o uso de tecnologias baseadas em inteligência artificial (IA) e aprendizado de máquina (machine learning), capazes de identificar comportamentos suspeitos e reagir rapidamente a possíveis tentativas de fraude. Estudos demonstram que a aplicação dessas tecnologias em sistemas de detecção de fraudes aumenta significativamente a precisão na identificação de ameaças e reduz falsos positivos, o que melhora a segurança e a eficiência operacional no ambiente digital (Science Times, 2024).

Além disso, a ausência de regulamentações padronizadas nos marketplaces representa um risco substancial. A falta de normas consistentes pode comprometer não apenas a segurança dos dados, mas também a concorrência e a inovação nesses ambientes. Regulamentações eficazes são essenciais para mitigar vulnerabilidades e proteger os direitos dos usuários e das empresas (ScienceDirect, 2024).

Dessa forma, levanta-se a seguinte questão como problematização central: como a ausência de regulamentação padronizada nos marketplaces pode impactar a segurança digital dessas plataformas, e quais medidas seriam mais eficazes para mitigar essas vulnerabilidades, considerando tanto a atualização tecnológica quanto a conscientização dos usuários?

Como hipótese e em resposta a problematização; a falta de uma regulamentação padronizada para marketplaces também é um ponto crítico que afeta diretamente a segurança digital dessas plataformas. Muitas vezes, as regras e normas de segurança ficam a critério de cada empresa, o que leva a disparidades nas práticas adotadas e deixa brechas para cibercriminosos explorarem. É essencial que os marketplaces invistam em programas contínuos de monitoramento e atualização de seus sistemas de segurança, e que adotem uma política de transparência com seus usuários sobre as práticas e cuidados necessários para evitar fraudes.

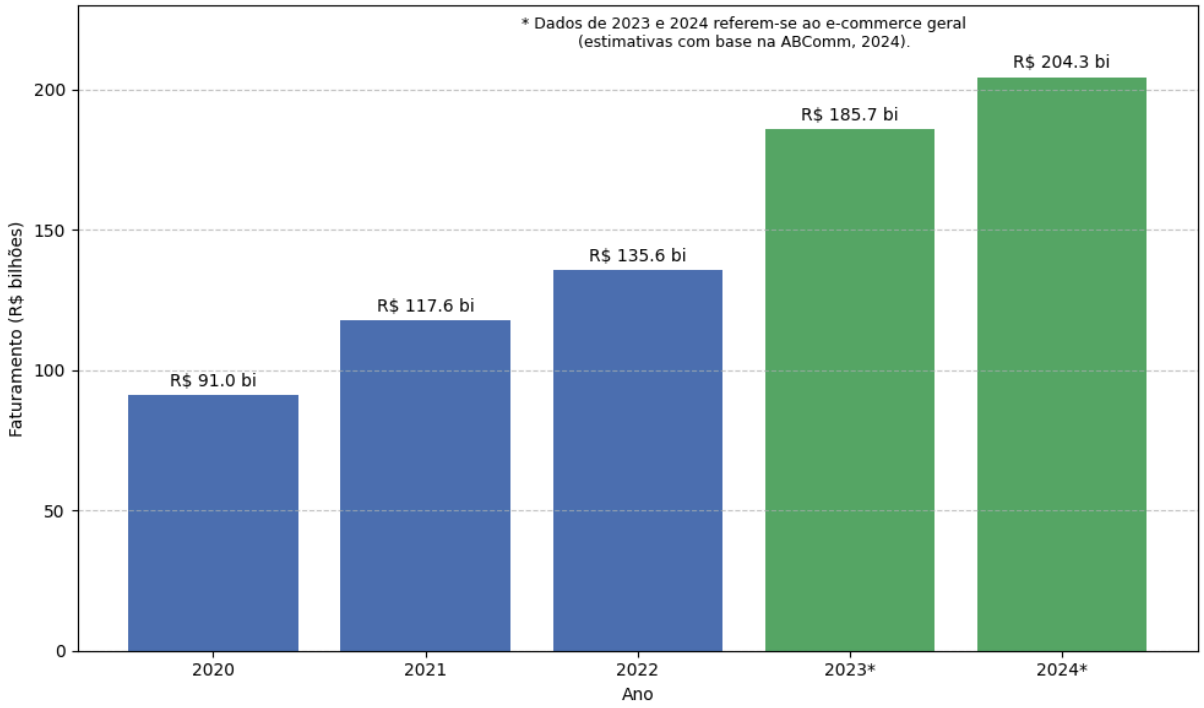
2. JUSTIFICATIVA

Este estudo se justifica pela crescente utilização dos marketplaces como principais plataformas de comércio eletrônico, o que os torna alvos preferenciais de ameaças cibernéticas. Estima-se que as vendas globais por e-commerce tenham atingido cerca de US$ 6,3 trilhões em 2024, com mais de 2,64 bilhões de compradores online (SELLERSCOMMERCE, 2024). Essa expansão exponencial evidencia a importância dos marketplaces para a economia digital, mas também revela o aumento da exposição de dados e transações a riscos de segurança.

No Brasil, o faturamento dos marketplaces apresentou crescimento expressivo nos últimos anos. De acordo com dados da Associação Brasileira de Comércio Eletrônico (ABComm), o setor movimentou R$ 91,0 bilhões em 2020, R$

117,6 bilhões em 2021 e R$ 135,6 bilhões em 2022. Em 2023, o faturamento do e-commerce brasileiro totalizou R$ 185,7 bilhões, e a projeção para 2024 é de R$ 204,3 bilhões. Considerando que os marketplaces representam aproximadamente 80% do e-commerce nacional, esses valores indicam a contínua relevância dessas plataformas para o comércio eletrônico e, consequentemente, a urgência em fortalecer medidas de segurança digital. Esses dados podem ser visualizados no Gráfico 2, que apresenta a evolução do faturamento dos marketplaces no Brasil entre 2020 e 2024.

Gráfico 2 - Faturamento dos marketplaces no Brasil (2020–2024)



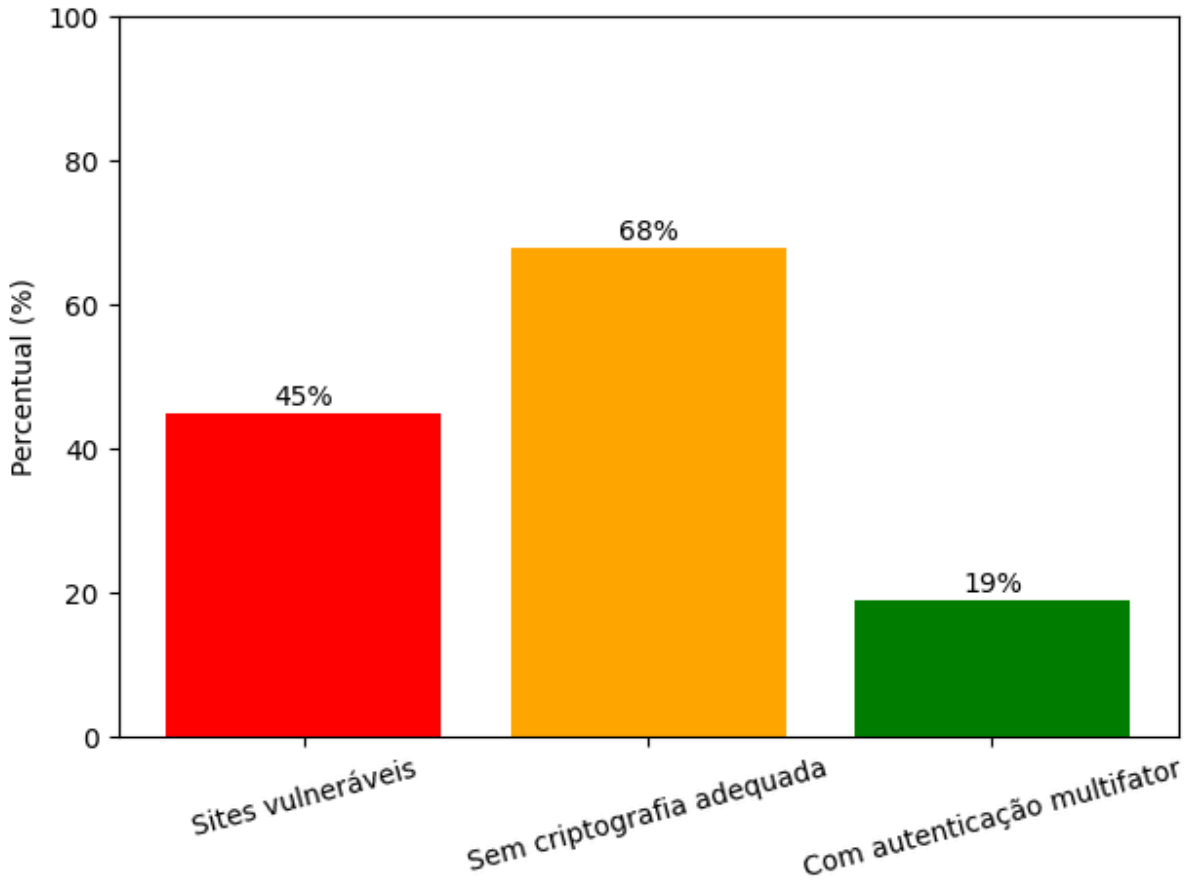
Fonte: Elaborado pela autora com dados da ABComm (2024).

Nota:Os dados de 2023 e 2024 referem-se ao e-commerce como um todo. Estimativas indicam que marketplaces representam cerca de 80% desse volume.

Dados recentes evidenciam sérias fragilidades na segurança dos sites de e-commerce. Conforme ilustrado no Gráfico 3, 45% dessas plataformas apresentam algum tipo de vulnerabilidade digital, enquanto 68% não utilizam protocolos de criptografia adequados, expondo dados sensíveis dos usuários. Outro dado preocupante é que apenas 19% dos sites analisados adotam autenticação multifator, um mecanismo essencial para reforçar a proteção contra acessos não autorizados (THALES GROUP, 2023). Esses números revelam um cenário alarmante de

insegurança digital que contribui diretamente para os prejuízos financeiros do setor. Em escala global, as perdas com fraudes em plataformas de e-commerce ultrapassaram US$ 48 bilhões em 2023, com projeções indicando um aumento para mais de US$ 200 bilhões até 2025 (JAVELIN STRATEGY & RESEARCH, 2023).

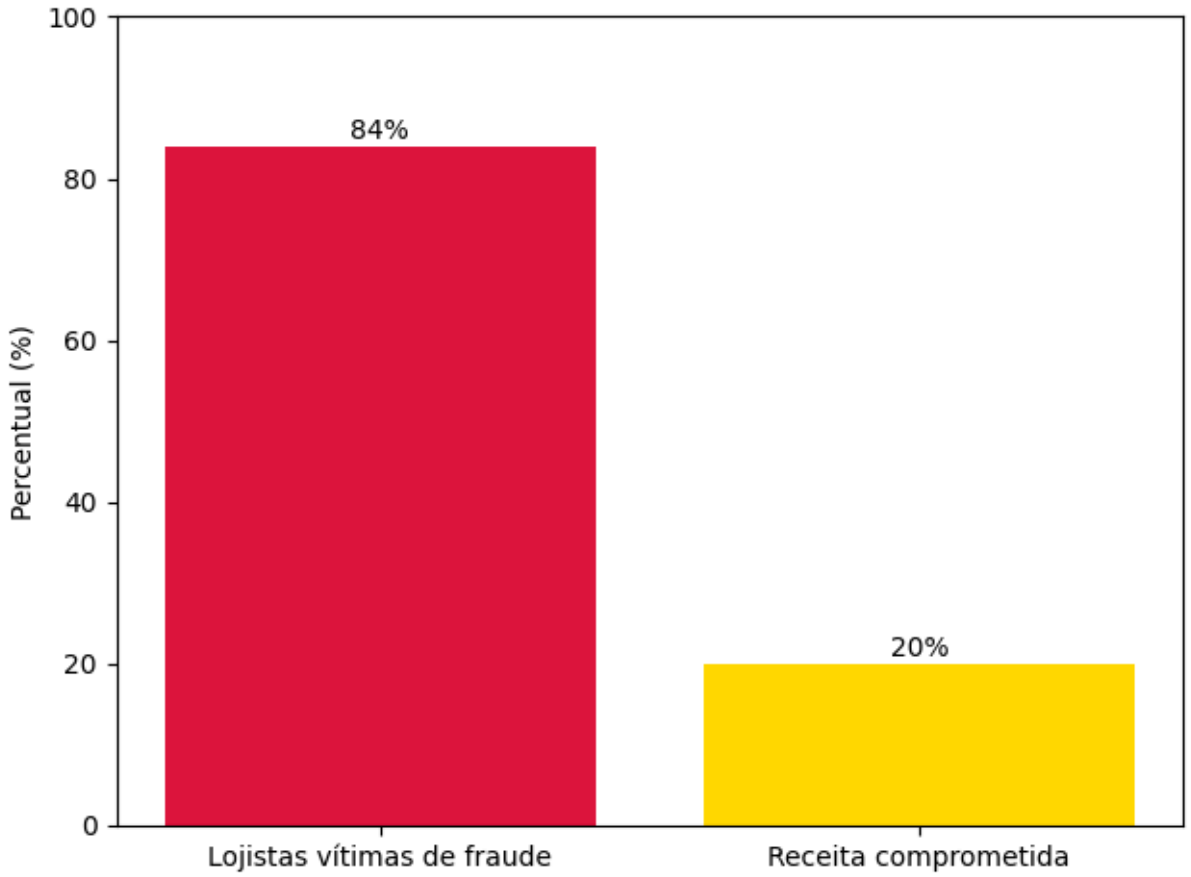
Gráfico 3 - Indicadores de segurança em sites de e-commerce (2023)



Fonte: Elaborado pela autora com base em dados de THALES GROUP (2023) e JAVELIN STRATEGY & RESEARCH (2023).

No Brasil e na América Latina, a situação também é alarmante: 84% dos lojistas online afirmam ter sido vítimas de fraudes no último ano, e cerca de 20% da receita do setor foi comprometida por práticas fraudulentas, como ilustra o Gráfico 4. Esses números demonstram falhas graves nas práticas de segurança adotadas pelas plataformas e indicam a necessidade de estratégias mais eficazes de proteção de dados (CLEARSALE, 2023).

Gráfico 4 - Impacto das fraudes em e-commerce no Brasil e América Latina (2023).



Fonte: Elaborado pela autora, adaptado de CLEARSALE, 2023.

Além disso, a ausência de regulamentação padronizada contribui para o agravamento do cenário. Segundo pesquisa da SecurityScorecard, mais da metade dos sites auditados não atendem plenamente aos padrões PCI DSS, e muitos deles continuam operando com brechas críticas (SECURITYSCORECARD, 2023). Casos de grandes marketplaces operando com políticas frágeis de privacidade e segurança reforçam a urgência de medidas normativas e boas práticas de governança digital.

Diante desse contexto, este trabalho busca investigar e contribuir com propostas de práticas mais seguras, que possam fortalecer a proteção dos dados dos usuários e a confiança nas plataformas digitais, elementos essenciais para a sustentabilidade e credibilidade do comércio eletrônico.

3. OBJETIVO GERAL

O objetivo geral deste estudo é investigar as vulnerabilidades na segurança digital dos principais marketplaces, como Mercado Livre, Americanas, OLX e Facebook, visando identificar falhas de segurança e propor soluções tecnológicas para mitigar essas vulnerabilidades. Portanto, fazendo-se necessários os seguintes objetivos específicos.

3.1. Objetivos Específicos

- Estudar as regulamentações e práticas de segurança adotadas por cada uma das plataformas, evidenciando as diferenças e lacunas que podem ser exploradas por cibercriminosos;
- Identificar as principais vulnerabilidades de segurança nos marketplaces selecionados, analisando tanto as ameaças externas quanto internas que possam comprometer a integridade dos dados e das transações;
- Analisar as causas e origens das vulnerabilidades identificadas, investigando os processos de desenvolvimento, as práticas de segurança adotadas e os pontos fracos na infraestrutura tecnológica dos marketplaces.

4. METODOLOGIA

Este trabalho foi desenvolvido com base em uma abordagem qualitativa e exploratória, tendo como foco a investigação das vulnerabilidades na segurança digital presentes nos marketplaces Mercado Livre, Americanas, OLX e Facebook. A pesquisa qualitativa se mostra apropriada por possibilitar uma compreensão aprofundada dos fenômenos envolvidos, especialmente em contextos onde os aspectos humanos, técnicos e regulatórios se inter-relacionam de forma complexa. O caráter exploratório, por sua vez, justifica-se pela necessidade de ampliar o conhecimento sobre um tema ainda pouco delimitado na literatura científica, sobretudo no que diz respeito à comparação entre práticas de segurança adotadas por diferentes plataformas digitais no Brasil.

A metodologia adotada foi estruturada em três etapas principais. A primeira consistiu em uma pesquisa bibliográfica, com o levantamento e análise de artigos científicos, livros, legislações, relatórios de mercado e documentos técnicos publicados por empresas especializadas em segurança digital. As fontes utilizadas incluíram bases de dados como Scielo, Google Scholar e ScienceDirect, além de organizações como ClearSale, Thales Group, SecurityScorecard, Javelin Strategy & Research, entre outras. Essa etapa foi essencial para embasar teoricamente o estudo e compreender o estado atual da segurança digital em ambientes de e-commerce.

A segunda etapa corresponde ao estudo de caso múltiplo, no qual foram analisadas quatro plataformas distintas: Mercado Livre, Americanas, OLX e Facebook Marketplace. Para cada uma delas, foi realizada uma análise de seu modelo operacional, práticas de segurança digital, mecanismos de prevenção a fraudes e histórico de incidentes de segurança reportados. Essa análise comparativa permitiu identificar padrões e lacunas nas estratégias adotadas por diferentes modelos de marketplace, incluindo os de intermediação direta (B2C) e os peer-to-peer (P2P).

A terceira etapa da metodologia envolveu a análise documental e normativa, focada na verificação das legislações e diretrizes aplicáveis à segurança digital em marketplaces. Foram consideradas, principalmente, a Lei Geral de Proteção de Dados (LGPD) no Brasil, o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e os padrões técnicos do PCI DSS. A partir disso, avaliou-se o nível de conformidade das plataformas com tais normas e o impacto da regulamentação (ou da ausência dela) sobre a proteção dos dados dos usuários.

A análise dos dados foi feita de forma descritiva e interpretativa, com foco na identificação das principais ameaças enfrentadas pelos usuários, como fraudes de pagamento, roubo de identidade, phishing e não entrega de produtos. Também foram observadas as tecnologias utilizadas para mitigar essas ameaças, como a autenticação multifatorial, criptografia e inteligência artificial. Além disso, foram avaliadas as estratégias de comunicação e conscientização dos usuários em relação à segurança digital.

5. ANÁLISE DAS PRÁTICAS DE SEGURANÇA E REGULAMENTAÇÃO NOS MARKETPLACES

O estudo analisa o funcionamento de marketplaces digitais como Mercado Livre, Americanas, OLX e Facebook Marketplace, destacando suas diferentes estruturas e modelos operacionais. Enquanto Mercado Livre e Americanas atuam com maior intermediação, oferecendo sistemas próprios de pagamento e logística (SOUZA, 2020), OLX e Facebook adotam o modelo peer-to-peer, priorizando a negociação direta entre usuários (MARTINS, 2021). Apesar dessas diferenças, todas enfrentam desafios em segurança digital, como fraudes, golpes e vazamento de dados (COSTA; ALMEIDA, 2019).

A ausência de regulamentações específicas para marketplaces agrava esses riscos. Embora leis como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na Europa contribuam para a proteção de dados (BRASIL, 2018; EUROPEAN UNION, 2016), ainda existem lacunas quanto à segurança transacional. A falta de padronização faz com que cada plataforma implemente suas próprias políticas de segurança, resultando em inconsistências e vulnerabilidades exploradas por cibercriminosos (FERREIRA; MENDES, 2022).

O trabalho enfatiza a necessidade de regulamentações mais específicas, cooperação internacional e conscientização dos usuários para que o ambiente de comércio eletrônico seja mais seguro, transparente e confiável.

5.1. Estrutura e funcionamento dos marketplaces: Mercado Livre, Americanas, OLX e Facebook

A estrutura e o funcionamento dos marketplaces digitais, como Mercado Livre, Americanas, OLX e Facebook, revelam uma grande variedade de abordagens e modelos de operação que visam facilitar o comércio eletrônico entre vendedores e compradores. Cada uma dessas plataformas tem sua própria arquitetura tecnológica e estratégias operacionais, mas todas compartilham o objetivo de criar um ambiente dinâmico e seguro para transações online (De Mello, 2006).

O Mercado Livre, por exemplo, é uma das plataformas de e-commerce mais populares da América Latina, oferecendo uma infraestrutura robusta que integra diversas funcionalidades, como métodos de pagamento por meio do Mercado Pago, sistema de entrega rápida com o Mercado. Envios e uma interface de fácil navegação. A plataforma utiliza um modelo de marketplace aberto, onde tanto pessoas físicas quanto empresas podem anunciar seus produtos. Segundo a ClearSale (2019), o Mercado Livre é um dos líderes em volume de transações e, ao mesmo tempo, uma das plataformas que mais enfrenta desafios relacionados a fraudes. Esse aspecto evidenciado pelo Mapa da Fraude 2019, destaca a necessidade de segurança contínua e inovação para combater ameaças cibernéticas. A plataforma também adota mecanismos de feedback e avaliação, nos quais os usuários podem classificar suas experiências de compra e venda, criando um sistema de reputação que ajuda a aumentar a confiança entre as partes.

No caso das Americanas, a estrutura é ligeiramente distinta, pois essa plataforma tem como base uma parceria com lojistas terceiros, além de vender diretamente seus próprios produtos. A integração entre lojistas externos e a própria Americanas permite à plataforma diversificar seu catálogo e alcançar uma audiência ainda maior, uma prática comum em marketplaces *Business to Consumer* (B2C) e *Business to Business* (B2B) (Durbano, 2019). A Americanas investe em um sistema de logística próprio e trabalha em colaboração com parceiros de entrega para garantir a entrega rápida dos produtos. Conforme apontado por Gabriel (2020), essa estrutura híbrida, que envolve a comercialização direta e indireta de produtos, gera um ambiente de complexidade para o gerenciamento de segurança, pois o fluxo de dados entre vendedores, consumidores e a própria empresa necessita de proteção constante para evitar fraudes e vazamentos de informações.

A OLX, por outro lado, adota uma abordagem mais simplificada, focando na venda entre indivíduos, permitindo que compradores e vendedores negociem diretamente entre si. Isso caracteriza a plataforma como um marketplace *Peer-to-Peer* (P2P), onde não há intermediação de pagamento ou entrega por parte da OLX. Esse modelo descentralizado atrai uma grande quantidade de usuários interessados em adquirir e vender produtos de segunda mão ou itens locais, sendo especialmente popular para transações de produtos usados e serviços, como imóveis e automóveis. A ausência de uma intermediação direta, no entanto, faz com que a OLX enfrente desafios relacionados à segurança das transações e ao controle

de qualidade dos produtos anunciados. Monteverde (2014) ressalta que marketplaces como a OLX precisam investir continuamente em sistemas de detecção de fraudes e educar os usuários sobre boas práticas para evitar golpes, uma vez que a responsabilidade de verificação dos produtos e segurança nas transações recai, em grande parte, sobre os próprios usuários.

O Facebook Marketplace, por sua vez, é uma extensão da rede social, permitindo que os usuários do Facebook comprem e vendam produtos dentro da própria plataforma de mídia social. Esse marketplace é amplamente utilizado para vendas locais e, assim como a OLX, não oferece um sistema de pagamento ou entrega integrado, sendo a negociação entre compradores e vendedores feita diretamente. Segundo o relatório de ameaças globais da NTT (2021), as plataformas sociais, quando se expandem para o e-commerce, enfrentam um número crescente de vulnerabilidades digitais, visto que a grande base de usuários atrai cibercriminosos interessados em explorar a falta de regulamentação específica para o comércio local e o baixo controle sobre a origem dos produtos. Assim, o Facebook enfrenta o desafio de manter a segurança do marketplace sem limitar a flexibilidade e a conveniência que a plataforma oferece aos seus usuários.

Essas plataformas, apesar de suas diferenças em estrutura e modelo de funcionamento, têm em comum a necessidade de implementar estratégias robustas para garantir a segurança das transações e a proteção dos dados dos usuários.

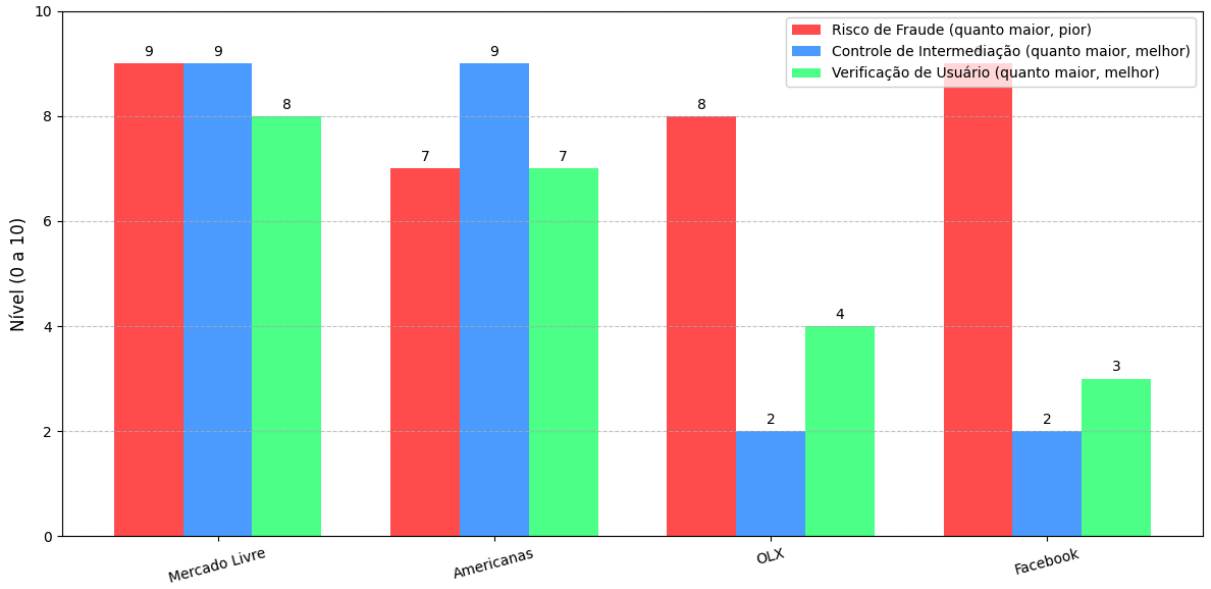
Lopes (2016) enfatiza a importância de mecanismos de cooperação internacional e de regulamentações para ajudar a combater crimes cibernéticos que afetam esses marketplaces, sugerindo que, além das práticas de segurança individuais de cada empresa, a colaboração entre plataformas e a regulamentação podem ser soluções eficazes para reduzir fraudes. Além disso, a estrutura de cada plataforma reflete diferentes estratégias de operação no comércio eletrônico: enquanto o Mercado Livre e a Americanas oferecem suporte e intermediação, a OLX e o Facebook Marketplace focam na conexão direta entre os usuários, proporcionando maior liberdade e menor custo operacional, porém com menos controle sobre a segurança das transações (Araújo, 2022).

Portanto, o Mercado Livre, Americanas, OLX e Facebook Marketplace representam diferentes abordagens no ecossistema de marketplaces digitais, cada um com suas vantagens e desafios específicos. O sucesso e a eficácia desses marketplaces dependem de um equilíbrio entre segurança, conveniência e

diversidade de opções para os usuários. Em um cenário de crescentes ameaças digitais e novas demandas dos consumidores, investir em segurança e regulamentação é essencial para que essas plataformas continuem sendo confiáveis e relevantes no mercado digital.

Para ilustrar essas diferenças, o Gráfico 5 apresenta uma comparação entre os principais indicadores de segurança dos marketplaces analisados, considerando três dimensões: risco de fraude, controle de intermediação e verificação de usuários. Esses dados foram sintetizados com base em estudos recentes e análises de especialistas do setor.

Gráfico 5 - Indicadores de Segurança e Vulnerabilidade em Marketplaces Digitais



Fonte: Elaborado pelo autor com base em De Mello (2006), ClearSale (2019), Durbano (2019), Gabriel (2020), Monteverde (2014), NTT (2021), Lopes (2016) e Araújo (2022).

5.2. Regulamentação de segurança digital: políticas e diretrizes vigentes para marketplaces

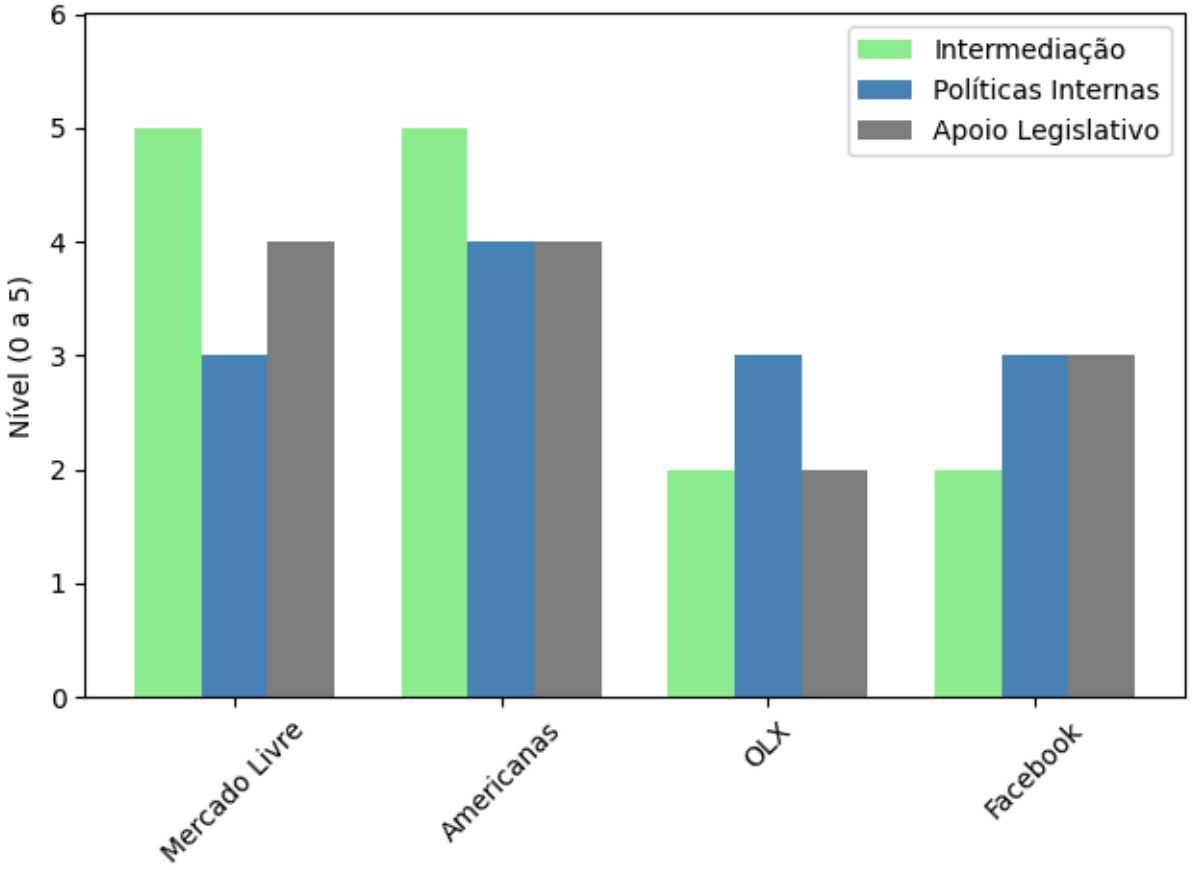
A regulamentação de segurança digital para marketplaces tem se tornado uma questão central em face do crescimento exponencial do comércio eletrônico e das frequentes ameaças cibernéticas (BRASIL, 2020). Plataformas como Mercado Livre, Americanas, OLX e Facebook, que facilitam transações entre milhões de

usuários, enfrentam desafios complexos para proteger dados e garantir transações seguras (BRASIL, 2013; BRASIL, 2018).

A ausência de uma regulamentação específica voltada exclusivamente para marketplaces também gera discussões sobre a responsabilidade dessas plataformas em casos de incidentes de segurança e fraudes (CAPITAL ABERTO, 2023).Contudo, as políticas e diretrizes de segurança para marketplaces ainda estão em desenvolvimento em muitas regiões, o que deixa brechas para fraudes e atividades maliciosas. A regulamentação desses ambientes digitais é uma área de interesse global, e estudos destacam que a falta de padrões normativos pode expor consumidores e vendedores a riscos significativos (Kreidich, 2016). Em muitos casos, a responsabilidade pela segurança digital recai sobre as próprias plataformas, que adotam políticas de segurança interna para proteger os dados dos usuários e evitar fraudes, mas o alcance dessas políticas varia conforme as diretrizes locais e o modelo de negócio de cada empresa.

O Gráfico 6 ilustra comparativamente o nível de intermediação das plataformas, o grau de políticas internas adotadas e o apoio legislativo percebido. É possível observar que plataformas como Mercado Livre e Americanas apresentam níveis mais altos de estruturação interna e apoio institucional, enquanto OLX e Facebook operam com menor grau de intermediação e respaldo normativo, o que pode aumentar a exposição a riscos.

Gráfico 6 - Comparação de Segurança entre Plataformas



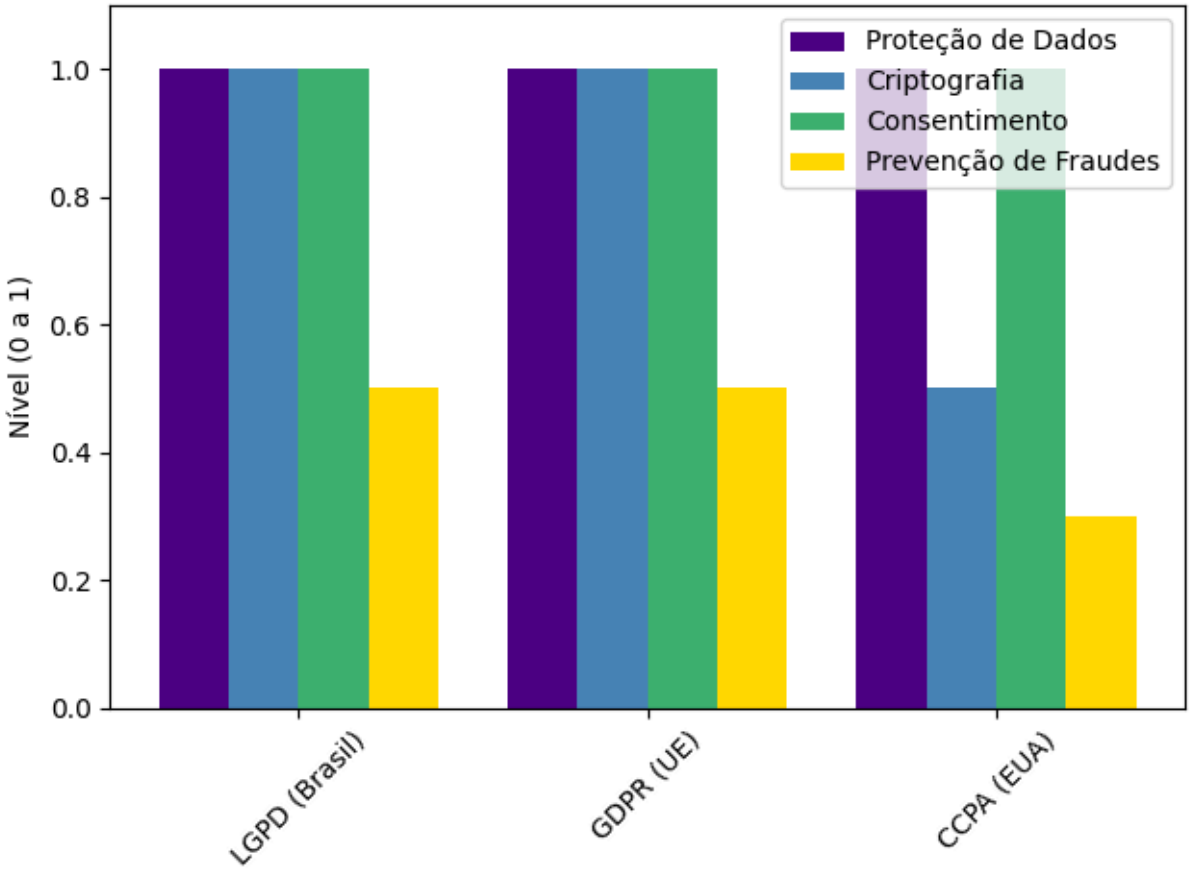
Fonte: Elaborado pela autora com base em BRASIL (2013, 2018, 2020), Kreidich (2016), Capital Aberto (2023).

Em muitos países, incluindo o Brasil, a regulamentação de segurança digital para marketplaces é orientada pela Lei Geral de Proteção de Dados (LGPD), que estabelece diretrizes rigorosas para o tratamento de dados pessoais, exigindo que as empresas tomem medidas de segurança proporcionais para proteger as informações dos usuários. A LGPD obriga as plataformas a adotar práticas de segurança robustas e transparentes, com mecanismos de consentimento e uma política clara de uso de dados, o que é essencial para marketplaces que coletam grandes quantidades de informações sensíveis (Marcondes, 2015). Para empresas como o Mercado Livre, por exemplo, a implementação de práticas de segurança em conformidade com a LGPD é crucial para o relacionamento de confiança com os usuários e para o cumprimento das exigências legais.

Nos Estados Unidos e na União Europeia, a regulamentação de segurança digital é pautada por legislações específicas de proteção de dados, como o

Regulamento Geral de Proteção de Dados (GDPR) europeu. Essa regulamentação exige que marketplaces e plataformas digitais de e-commerce sigam um conjunto de diretrizes rígidas para garantir a proteção dos dados dos usuários e a segurança das transações. Segundo Gabriel (2020), o GDPR é considerado um dos padrões de segurança digital mais completos, com regras sobre a coleta, armazenamento e processamento de dados pessoais, e tem servido como um modelo para legislações de outros países.

Gráfico 7 - Comparação entre legislações de proteção de dados (LGPD, GDPR e CCPA) quanto aos critérios de segurança digital aplicados a marketplaces.



Fonte: Elaborado pela autora com base na LGPD (Lei nº 13.709/2018), GDPR (Regulamento (UE) 2016/679) e CCPA (California Consumer Privacy Act, 2018).

O Gráfico acima mostra como as três principais legislações de proteção de dados — LGPD, GDPR e CCPA — se comparam em quatro critérios fundamentais: proteção de dados, criptografia, consentimento e prevenção de fraudes. Tanto a LGPD quanto o GDPR apresentam pontuações altas nos três primeiros quesitos,

refletindo uma abordagem robusta à segurança dos dados pessoais. No entanto, observa-se que a prevenção de fraudes, que é especialmente relevante para marketplaces, ainda não é contemplada com a mesma ênfase, o que demonstra a necessidade de regulamentações complementares voltadas especificamente para os riscos do comércio eletrônico.

No entanto, essas regulamentações focadas na proteção de dados pessoais muitas vezes não abordam de forma abrangente as práticas de segurança necessárias para marketplaces, como a prevenção de fraudes financeiras e de *phishing*, que são frequentes em plataformas de e-commerce.

Conforme destaca a ClearSale (2019) em seu Mapa da Fraude, as fraudes financeiras são uma das maiores ameaças em marketplaces, e a falta de regulamentações específicas para prevenção de fraudes digitais dificulta o combate a esses crimes. As políticas de segurança de marketplaces, portanto, precisam ir além das exigências legais de proteção de dados, abrangendo mecanismos preventivos e de resposta rápida contra atividades fraudulentas, mas, em muitos casos, essas práticas variam de uma plataforma para outra, criando inconsistências e vulnerabilidades.

A ausência de um padrão regulamentar específico para marketplaces permite que cada empresa desenvolva suas próprias políticas de segurança, o que resulta em abordagens variadas e, em alguns casos, insuficientes para lidar com as complexidades do ambiente digital.

Marcondes (2015) observa que as empresas de comércio eletrônico precisam equilibrar o investimento em segurança com a usabilidade e a conveniência dos usuários, e essa flexibilidade sem regulamentação padrão pode ser um fator de risco. A OLX, por exemplo, que permite transações diretas entre usuários, depende fortemente da conscientização do próprio usuário e de recursos de segurança internos para prevenir golpes e garantir a confiabilidade das transações. Já marketplaces como a Americanas, que atuam também como intermediários em algumas transações, têm mais controle sobre o processo e implementam políticas mais rígidas, mas ainda enfrentam desafios para padronizar a segurança em parcerias com terceiros (Kuniyoshi, 2009).

Estudos sugerem que a regulamentação de segurança digital para marketplaces poderia se beneficiar de um modelo de colaboração entre as plataformas e autoridades reguladoras, promovendo a criação de diretrizes mais

específicas e abrangentes. Segundo Lopes (2016), mecanismos de cooperação internacional são fundamentais para combater o cibercrime, e a regulamentação de segurança digital para marketplaces deveria considerar essa dimensão. Plataformas de alcance global, como o Mercado Livre e o Facebook, poderiam se beneficiar de uma regulamentação mais uniforme, que facilite o monitoramento e a resposta a ameaças em diferentes regiões, além de promover uma experiência de uso mais segura para os usuários.

A regulamentação de segurança digital, portanto, é uma questão complexa e multifacetada, que abrange não apenas a proteção de dados, mas também a criação de um ambiente seguro e confiável para transações. Os marketplaces precisam não só atender às legislações vigentes, como a LGPD no Brasil e o GDPR na Europa, mas também desenvolver políticas internas que acompanhem a evolução das ameaças digitais e promovam a segurança de seus usuários. Em última análise, as diretrizes e políticas vigentes para a segurança digital de marketplaces devem considerar tanto as exigências legais quanto as melhores práticas de mercado, criando uma infraestrutura de segurança capaz de responder de forma eficaz e ágil aos desafios da era digital.

5.3. Lacunas nas práticas de segurança adotadas por cada plataforma

As plataformas de marketplace como Mercado Livre, Americanas, OLX e Facebook enfrentam desafios significativos para garantir a segurança digital de suas operações. No entanto, cada uma adota práticas de segurança distintas que, embora direcionadas para proteger dados e prevenir fraudes, possuem lacunas que podem ser exploradas por cibercriminosos.

Essas lacunas decorrem, em grande parte, da diversidade dos modelos operacionais e da ausência de uma regulamentação padronizada, o que expõe tanto consumidores quanto vendedores a riscos (Westphall, 2013). De acordo com Kreidich (2016), a falta de uniformidade nas políticas de segurança entre marketplaces cria um ambiente vulnerável, onde criminosos cibernéticos podem explorar fragilidades específicas de cada plataforma.

O Mercado Livre, um dos maiores marketplaces da América Latina, investe em segurança digital por meio de práticas como autenticação de dois fatores e a

integração de um sistema de pagamento próprio, o Mercado Pago. Essas medidas são eficazes até certo ponto, mas, como aponta o relatório Mapa da Fraude 2019 da ClearSale, a plataforma ainda enfrenta altos índices de tentativas de fraude e ataques de *phishing*. Esses ataques geralmente ocorrem por meio de mensagens falsas enviadas a usuários, tentando enganá-los para que revelem informações pessoais. Embora o Mercado Livre promova campanhas de conscientização para evitar fraudes, a plataforma ainda encontra dificuldades em educar todos os usuários sobre práticas seguras, o que se torna uma vulnerabilidade crítica para a proteção de seus clientes.

A Americanas, que também atua como um marketplace para diversos lojistas, adota políticas de segurança para proteger o ambiente de compra e venda, incluindo monitoramento de transações e processos de avaliação dos vendedores. Contudo, a integração de diversos vendedores independentes cria um cenário de complexidade onde fraudes e vendas de produtos falsificados podem ocorrer com maior frequência. Lopes (2016) ressalta que a falta de controle direto sobre todos os vendedores em marketplaces como a Americanas representa uma lacuna relevante nas práticas de segurança, uma vez que a plataforma precisa balancear a experiência do usuário com o controle e verificação dos fornecedores. Essa limitação faz com que alguns produtos e anúncios não passem por um controle rigoroso, aumentando os riscos de fraude para os compradores.

A OLX, uma plataforma com foco em transações diretas entre usuários, apresenta um modelo P2P que elimina a necessidade de intermediários, mas aumenta a vulnerabilidade para golpes. Embora a OLX ofereça recomendações de segurança aos seus usuários e disponibilize canais para denúncias de fraudes, a plataforma ainda sofre com uma alta incidência de golpes, principalmente em transações de alto valor, como veículos e imóveis. Marcondes (2015) observa que a falta de uma intermediação formal nas transações P2P aumenta o risco para os consumidores, pois as medidas de segurança ficam quase inteiramente sob a responsabilidade dos próprios usuários. A dependência de práticas autônomas de segurança revela uma lacuna importante: sem a mediação da OLX em pagamentos e entrega, a plataforma não possui meios eficazes de garantir que os usuários cumpram as negociações de forma legítima e segura.

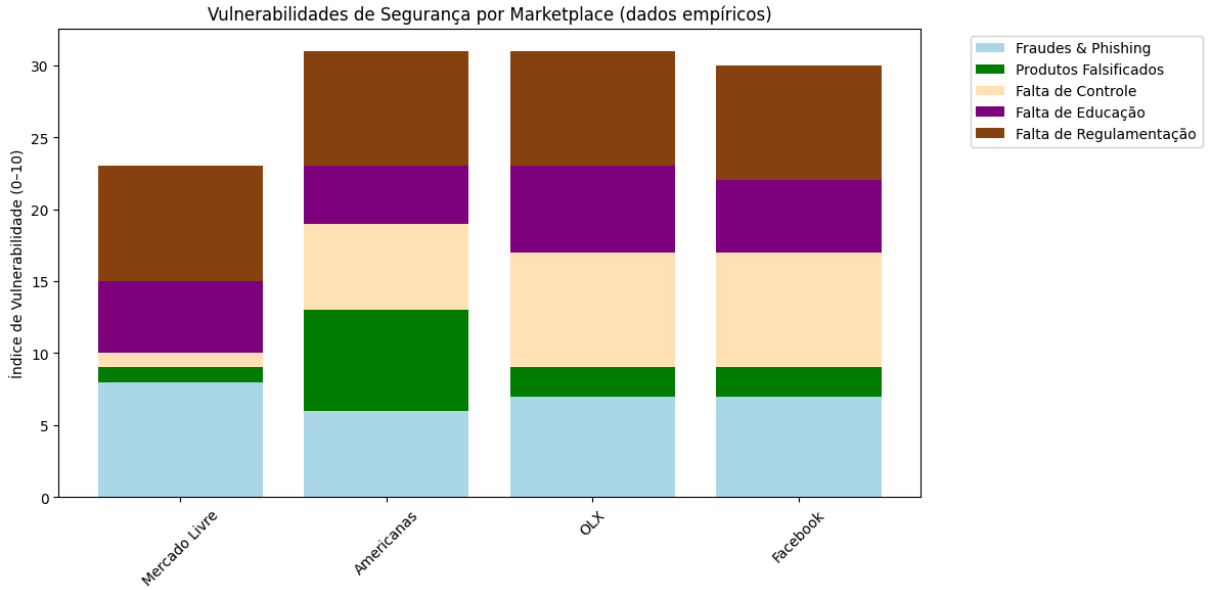
Já o Facebook Marketplace, que permite a compra e venda de produtos dentro da rede social, enfrenta desafios similares em relação ao controle de

segurança, visto que não há um sistema próprio de pagamento ou de entrega. A plataforma permite que usuários negociem livremente, mas essa falta de controle intermediário expõe compradores e vendedores a uma série de golpes e fraudes. O relatório da NTT (2021) sobre ameaças globais destaca que marketplaces em redes sociais, como o Facebook, atraem criminosos digitais pela facilidade de realizar transações com pouca supervisão e pela falta de verificação rigorosa dos vendedores. Embora o Facebook disponibilize orientações gerais sobre práticas seguras, as ferramentas de segurança são limitadas, e o controle sobre as transações é praticamente inexistente, o que permite que fraudadores publiquem anúncios falsos e realizem transações fraudulentas com mais facilidade.

Em todas essas plataformas, uma lacuna comum é a dificuldade em educar os usuários sobre práticas seguras e em criar uma conscientização contínua sobre os riscos digitais. Lopes (2016) enfatiza que a cooperação entre plataformas e a criação de diretrizes padronizadas são essenciais para mitigar as ameaças e reduzir a vulnerabilidade dos usuários.Cada marketplace investe em segurança de maneira independente, mas as práticas variam em efetividade e abrangência, o que gera inconsistências e facilita a ação de cibercriminosos.

O Gráfico 8 exemplifica os principais pontos vulneráveis identificados empiricamente: alta incidência de fraudes e phishing, número expressivo de produtos falsificados, falta de controle administrativo, lacunas na educação dos usuários e a ausência de regulamentação padronizada.

Gráfico 8 - Vulnerabilidades de segurança por marketplaces



Fonte: elaborado pela autora com base em dados da ClearSale (Mapa da Fraude 2024) e análises acadêmicas sobre segurança digital em plataformas.

O Mercado Livre, por exemplo, adota tecnologias de inteligência artificial para monitoramento de fraudes, autenticação em dois fatores e aplicação do modelo de segurança Zero Trust (MERCADO LIVRE, 2023). Ainda assim, a plataforma é frequentemente alvo de golpes, como a divulgação de vídeos falsos com celebridades promovendo produtos inexistentes, com o objetivo de induzir pagamentos ou coleta de dados (REUTERS, 2024).

A Americanas implementou canais de denúncia, como o “Apito”, e orienta lojistas e clientes a adotarem boas práticas de segurança digital, como a atenção a e-mails suspeitos e a verificação do domínio oficial da loja (AMERICANAS, 2023). No entanto, casos de venda de produtos falsificados ou não entregues continuam a ocorrer, explorando brechas na relação de confiança com os consumidores (TECMUNDO, 2024).

A OLX oferece medidas como perfis verificados, chat seguro e histórico de conexões, além da ferramenta “Garantia OLX” para transações controladas (OLX, 2023a). Contudo, mesmo com essas iniciativas, golpes como perfis clonados, falsas confirmações de pagamento e phishing via links externos são comuns na plataforma (OLX, 2023b).

O Facebook Marketplace permite avaliações públicas de vendedores, denúncia de comportamentos suspeitos e sugere encontros em locais públicos (FACEBOOK, 2023). Apesar disso, os usuários continuam vulneráveis a fraudes como envio de comprovantes bancários falsos, produtos que nunca são entregues e ataques de phishing via Messenger (ESET, 2023).

Esses exemplos demonstram que, apesar dos avanços tecnológicos e dos mecanismos de segurança adotados, os marketplaces ainda enfrentam desafios significativos na prevenção de crimes digitais, devido à falta de padronização entre plataformas e à constante reinvenção das táticas dos cibercriminosos.

A implementação de práticas mais uniformes e a promoção de uma regulamentação específica para marketplaces poderiam reduzir essas lacunas e oferecer maior proteção para consumidores e vendedores.

Essas vulnerabilidades nas práticas de segurança adotadas por cada plataforma mostram que, embora os marketplaces tenham avançado em medidas de

proteção, ainda existem pontos fracos explorados frequentemente por criminosos (SOCRADAR, 2024).

Ataques como injeção de SQL e Cross-Site Scripting (XSS) continuam sendo uma ameaça significativa para e-commerces, permitindo o roubo de dados sensíveis e comprometendo a experiência do usuário (SECURITY BOULEVARD, 2021). Essas brechas indicam que é necessário um esforço contínuo de atualização e reforço das práticas de segurança digital, mesmo nas plataformas mais consolidadas (SU SOCIAL, s.d.). A ausência de uma regulamentação padronizada e a variedade de modelos de operação dificultam o estabelecimento de práticas de segurança uniformes, deixando os usuários expostos a uma série de riscos. As lacunas nas práticas de segurança digital refletem, assim, tanto a complexidade dos modelos de negócios de cada marketplace quanto a necessidade de políticas mais abrangentes para garantir um ambiente de transações mais seguro e confiável.

5.4. Impacto das regulamentações (ou da ausência delas) na segurança dos dados dos usuários

A regulamentação de segurança digital tem um papel fundamental na proteção dos dados dos usuários em plataformas de marketplace. Com o aumento do volume de transações online e da coleta de dados pessoais, a falta de regulamentações específicas coloca em risco a segurança dos usuários e amplia as possibilidades de exploração por parte de cibercriminosos. A ausência de normas padronizadas para marketplaces como Mercado Livre, Americanas, OLX e Facebook faz com que cada empresa adote políticas de segurança distintas, que muitas vezes são insuficientes para enfrentar as ameaças digitais emergentes. Lopes (2016) aponta que a falta de regulamentação específica para plataformas de e-commerce permite que cibercriminosos encontrem brechas nas práticas de segurança, colocando em risco informações sensíveis dos usuários, como dados pessoais e financeiros.

No Brasil, a LGPD representa um marco na tentativa de regulamentar o tratamento e a segurança dos dados pessoais. Ela estabelece uma série de diretrizes para que as empresas implementem práticas de proteção e evitem o uso indevido das informações dos usuários. Plataformas como o Mercado Livre e a

Americanas são obrigadas a se adequar à LGPD, o que inclui medidas como o consentimento explícito dos usuários para a coleta de dados e a implementação de protocolos de segurança para proteger essas informações (Kreibich, 2016). Segundo Marcondes (2015), regulamentações como a LGPD são essenciais para garantir que os marketplaces adotem medidas de segurança efetivas e sejam transparentes em relação ao uso dos dados dos consumidores.

Apesar disso, dados recentes indicam que 63% das empresas brasileiras sofreram algum tipo de incidente de segurança em 2023, e entre elas, 41% não estavam totalmente em conformidade com a LGPD, o que evidencia a relação entre ausência de regulamentação adequada e aumento da vulnerabilidade (Jusbrasil, 2023). Por outro lado, empresas que implementaram integralmente a LGPD apresentaram redução de 37% nos incidentes de segurança, demonstrando que a aplicação rigorosa da lei é um fator decisivo para a proteção dos dados dos usuários (Jusbrasil, 2023).

A LGPD, embora abrangente em muitos aspectos, não cobre todas as especificidades do ambiente de marketplace, como a questão das fraudes financeiras e dos ataques de phishing, que exigem regulamentações mais específicas e detalhadas. A lei se concentra principalmente na proteção de dados pessoais, não abordando de forma direta aspectos como segurança transacional e prevenção a crimes cibernéticos (BRASIL, 2018). Assim, questões como ataques de phishing, golpes financeiros e roubo de identidade em plataformas de e-commerce ainda carecem de regulamentações complementares mais direcionadas.

Nos Estados Unidos e na União Europeia, as regulamentações de segurança digital são mais avançadas, com leis específicas que orientam o setor de e-commerce e exigem o cumprimento de práticas de segurança. O GDPR europeu, por exemplo, é uma das regulamentações mais completas no que diz respeito à proteção de dados, impondo sanções severas para o descumprimento das normas. Para marketplaces globais, como o Facebook, o cumprimento do GDPR é obrigatório nas operações dentro da União Europeia, o que leva a empresa a adotar políticas de segurança robustas, incluindo criptografia avançada e auditorias regulares de segurança. Gabriel (2020) observa que o GDPR não apenas estabelece normas para a coleta e o processamento de dados, mas também exige que as empresas notifiquem rapidamente as autoridades em caso de violação de segurança, aumentando a transparência e a confiança dos usuários.

No entanto, para marketplaces que operam em países onde a regulamentação é menos rigorosa, as práticas de segurança podem ser menos desenvolvidas, o que coloca os usuários em situações de vulnerabilidade. Um exemplo claro disso é o aumento de 493% nos vazamentos de dados no Brasil em um período recente, conforme apontado por um estudo do Massachusetts Institute of Technology (MIT), o que reforça a necessidade urgente de regulamentações eficazes e bem aplicadas (Tribuna, 2023).

A ausência de regulamentação específica para marketplaces representa uma lacuna crítica em muitos países, especialmente na América Latina. A falta de normas específicas permite que cada empresa adote políticas de segurança distintas, o que resulta em inconsistências e, muitas vezes, em proteção insuficiente. Monteverde (2014) destaca que, sem uma regulamentação uniforme, as plataformas estão sujeitas a interpretações individuais das boas práticas de segurança, o que cria brechas exploráveis para ataques cibernéticos.

A OLX, por exemplo, adota um modelo de negócio que facilita transações diretas entre usuários, caracterizando-se como uma plataforma de comércio C2C (consumer-to-consumer), em que consumidores negociam produtos entre si (PORTAL INSIGHTS, 2023). Nesse formato, a empresa oferece a plataforma para conexão entre vendedores e compradores, mas não realiza mediação completa ou verificação rigorosa dos dados, o que dificulta o controle sobre a veracidade das informações e a segurança das transações (OLX, 2025a). Apesar de contar com ferramentas como a "Identidade Verificada", destinadas a aumentar a confiabilidade dos perfis na plataforma, a responsabilidade pela verificação e segurança ainda recai majoritariamente sobre o usuário (OLX, 2025b). A própria empresa recomenda cautela durante as negociações, reforçando que a segurança depende, em grande parte, de ações preventivas por parte dos usuários (OLX, 2025c).

A regulamentação também impacta diretamente a confiança dos usuários nas plataformas. Quando não há uma política clara e padronizada de segurança digital, o consumidor pode se sentir inseguro em compartilhar dados sensíveis ou realizar transações de maior valor. De acordo com a ClearSale (2019), marketplaces que não adotam práticas robustas de segurança ou que possuem uma regulamentação fraca acabam sofrendo com altos índices de fraude, o que afeta a reputação da plataforma e reduz a confiança do usuário.

Além disso, Lopes (2016) destaca que a regulamentação internacional desempenha um papel crucial para aumentar a cooperação entre plataformas e governos, criando um ambiente mais seguro para transações online. A ausência de regulamentação impede que as empresas compartilhem informações sobre ameaças cibernéticas e padrões de fraude, dificultando a prevenção e o combate eficaz aos ataques digitais. Em um cenário global, onde as ameaças são transfronteiriças e as redes criminosas operam em múltiplas jurisdições, a falta de regulamentação uniforme e de diretrizes de segurança pode comprometer a proteção dos dados e a segurança das transações, deixando tanto usuários quanto empresas expostos a perdas financeiras e danos à reputação (Malone, 2020).

Portanto, o impacto das regulamentações, ou da ausência delas, na segurança dos dados dos usuários é evidente em cada aspecto do comércio eletrônico. A implementação de leis como a LGPD exige que as empresas adotem medidas rigorosas de proteção e tratamento de dados, promovendo maior confiança nas plataformas. Contudo, quando essas regulamentações são inexistentes ou mal aplicadas, os usuários ficam mais vulneráveis a riscos como vazamentos e fraudes (PAGAR.ME, [s.d.]). A falta de normas padronizadas para marketplaces cria vulnerabilidades que podem ser exploradas por criminosos, e mesmo as regulamentações como a LGPD e o GDPR ainda têm lacunas que precisam ser abordadas para garantir uma proteção mais abrangente (BRASCT, 2023).

6. PRINCIPAIS FORMAS DE FRAUDE E ATAQUES CIBERNÉTICOS NOS MARKETPLACES

Com o crescimento das compras online, aumentaram também os casos de fraudes em marketplaces como Mercado Livre, Americanas, OLX e Facebook. Dados da CNDL e do SPC Brasil (2023) revelam que cerca de 32% dos consumidores já sofreram tentativas de fraude. Entre os principais golpes estão a fraude de pagamento, o roubo de identidade, o phishing, a venda de produtos falsificados, o golpe da não entrega e a fraude de triangulação.

As fraudes financeiras, como o uso de cartões de crédito roubados e o não envio de produtos após o pagamento, afetam diretamente a confiança dos consumidores e causam prejuízos para os lojistas. A falta de intermediação nas

plataformas OLX e Facebook Marketplace, por exemplo, facilita esses crimes. Mesmo marketplaces com sistemas de proteção, como Americanas e Mercado Livre, não estão imunes a fraudes realizadas por vendedores terceiros.

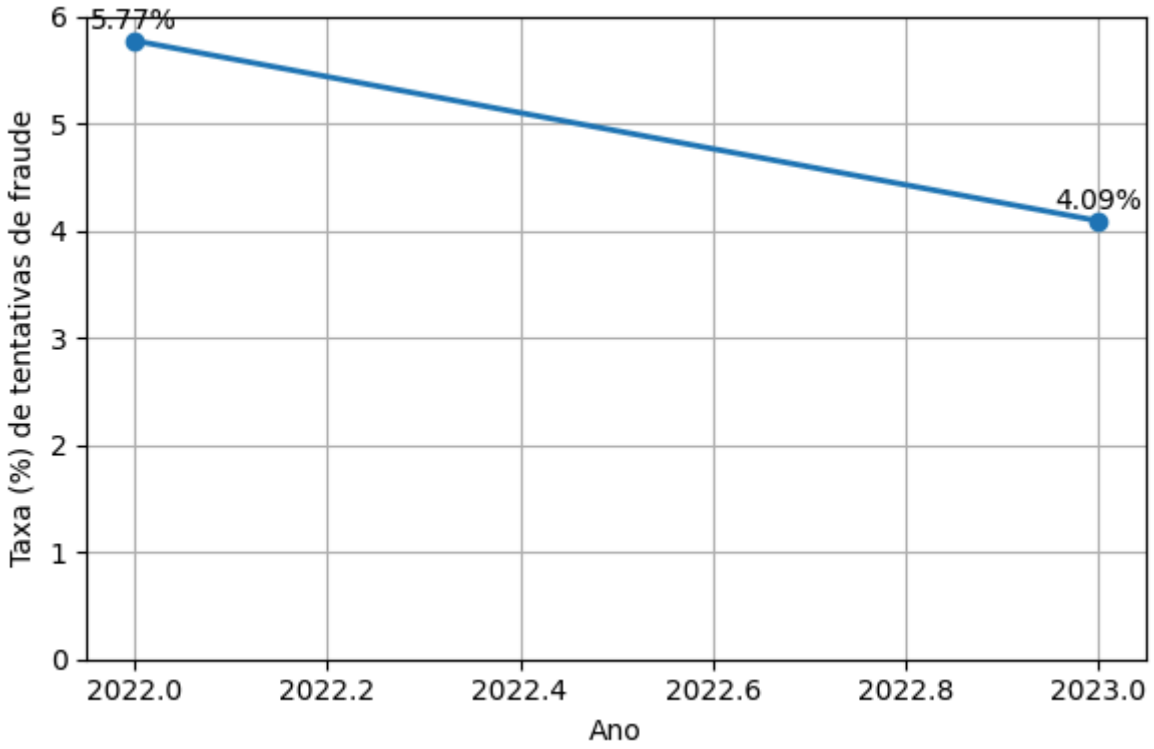
Além das fraudes, os ataques cibernéticos — como roubo de dados, phishing e ataques DDoS — prejudicam o funcionamento das plataformas, comprometem a segurança dos usuários e geram altos custos operacionais. Esses ataques minam a confiança dos consumidores, afetam vendedores e expõem as empresas a penalidades legais por falhas na proteção de dados.

Diante disso, torna-se essencial que os marketplaces invistam em medidas robustas de segurança digital, monitoramento contínuo, e na conscientização dos usuários para mitigar riscos e garantir um ambiente de compra mais seguro.

6.1. Tipos de fraudes mais recorrentes em transações online

Com o crescimento das compras online, aumentou também a preocupação de consumidores e empresas com a segurança das transações virtuais. De acordo com uma pesquisa realizada pela Confederação Nacional de Dirigentes Lojistas (CNDL) em parceria com o Serviço de Proteção ao Crédito (SPC Brasil), aproximadamente 32% dos consumidores já enfrentaram ou foram alvo de tentativas de fraude durante compras pela internet (CNDL; SPC Brasil, 2023). Dentre os tipos mais recorrentes, destacam-se fraudes de pagamento, roubo de identidade, *phishing* e fraudes relacionadas a produtos falsificados. A ClearSale (2019), em seu Mapa da Fraude, aponta que o número de ataques em plataformas de e-commerce tem se intensificado, com criminosos desenvolvendo novas técnicas para enganar os consumidores e burlar os sistemas de segurança.Embora os dados mais recentes indiquem uma leve queda percentual nas tentativas de fraude — conforme mostra o Gráfico 9 — o número absoluto de ocorrências ainda é expressivo e representa uma ameaça constante para consumidores e empresas.

Gráfico 9 - Evolução da taxa de tentativas de fraude no e-commerce brasileiro no período 2022 a 2023

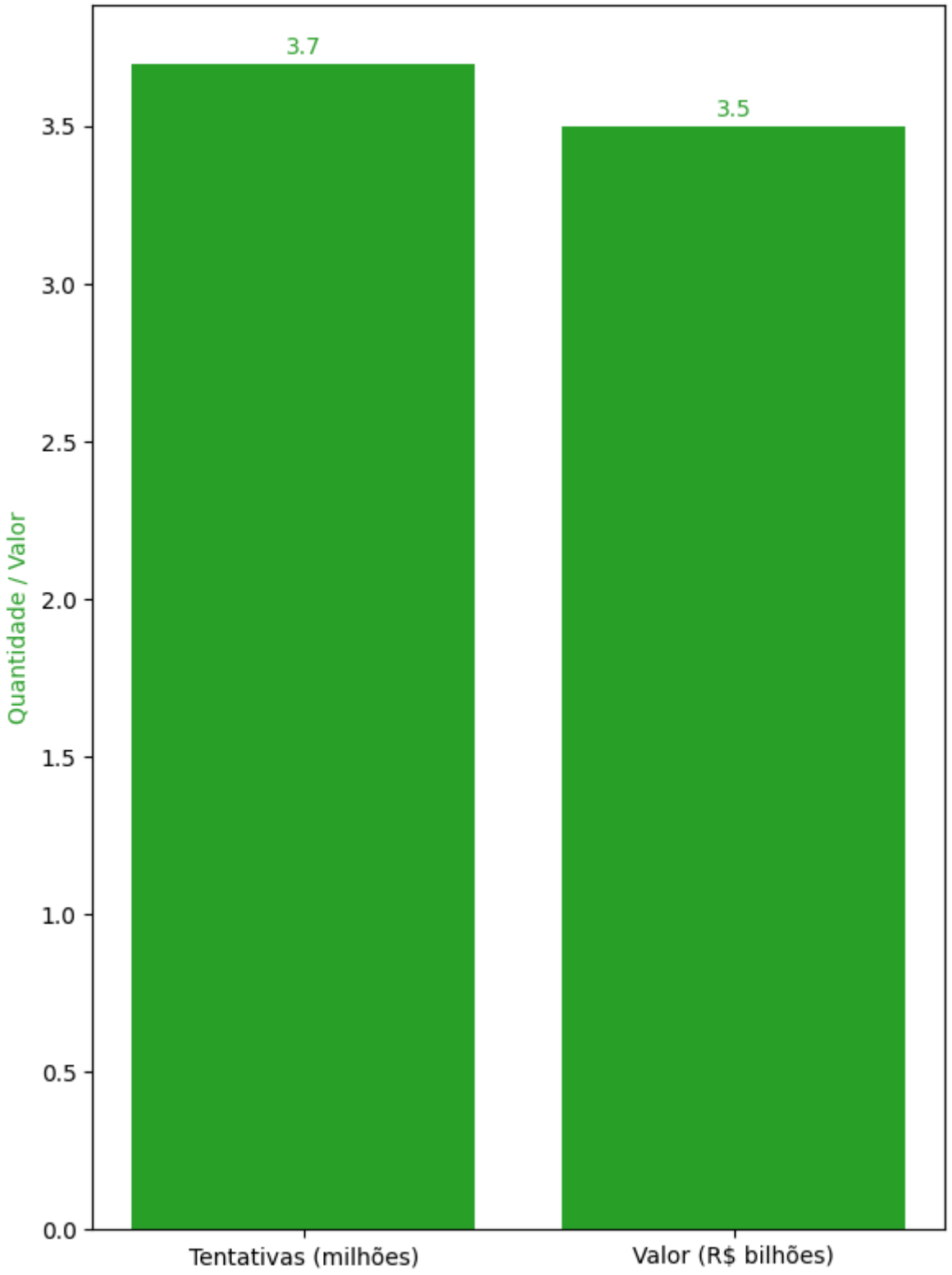


Fonte: Elaborado pela autora com base em dados da Boa Vista – Raio-X da Fraude 2024

Em marketplaces como Mercado Livre, Americanas, OLX e Facebook, as fraudes ocorrem de várias formas e se aproveitam, principalmente, de lacunas nas práticas de segurança e da falta de conscientização dos usuários.

Um dos tipos de fraude mais comuns é a fraude de pagamento, na qual golpistas utilizam métodos como cartões de crédito roubados ou clonados para realizar compras. De acordo com a Serasa Experian, na fraude de cartão de crédito roubado, as informações são adquiridas na chamada dark web, e os produtos são enviados a agentes de frete para evitar a identificação do comprador. Além disso, conforme destacado pela Escola de E-commerce, os fraudadores podem utilizar cartões roubados para efetuar compras fraudulentas, causando prejuízos significativos aos lojistas. Para se ter uma dimensão do impacto financeiro desse tipo de prática, estima-se que as tentativas de fraude no e-commerce brasileiro tenham alcançado, somente em 2023, um valor total de aproximadamente R$ 3,5 bilhões, conforme ilustrado no Gráfico 10.

Gráfico 10 - Tentativas de fraude e valor total em 2023



Fonte: Elaborado pela autora com base em dados da ClearSale – Mapa da Fraude 2023

Essa prática é especialmente frequente em plataformas de marketplace, onde transações são realizadas diariamente e em grande volume. De acordo com Lopes

(2016), a fraude de pagamento é um desafio significativo para o setor de e-commerce, pois envolve não só a proteção dos dados financeiros, mas também o monitoramento constante das transações. Os marketplaces que não possuem medidas robustas de autenticação e monitoramento em tempo real podem ser mais vulneráveis a esse tipo de golpe, gerando prejuízos para vendedores e danos à confiança dos consumidores.

Outra fraude recorrente nas transações online é o roubo de identidade, onde criminosos obtêm informações pessoais dos usuários para se passar por eles e realizar compras ou até solicitar crédito. Esse tipo de fraude tem crescido de forma expressiva e afeta diretamente plataformas como o Mercado Livre e a Americanas, que exigem o cadastro de informações pessoais e financeiras para realizar transações (TECNOBLOG, 2024; SECURITY LEADERS, 2024; TERRA, 2024). Marcondes (2015) destaca que o roubo de identidade é facilitado pela falta de segurança em sistemas de autenticação, como senhas fracas e a ausência de autenticação de dois fatores, o que torna as contas dos usuários mais vulneráveis a invasões. Com os dados pessoais em mãos, os golpistas podem até criar contas falsas em nome dos usuários, comprometendo a integridade das transações e o histórico do consumidor na plataforma.

O *phishing*, uma prática criminosa em que fraudadores enviam mensagens enganosas para coletar dados pessoais, é outra forma de fraude amplamente presente nas transações online. Em marketplaces, os criminosos frequentemente se passam por representantes das plataformas para induzir os usuários a fornecerem informações sensíveis, como senhas, números de cartões de crédito e CPF. A ClearSale (2019) aponta que o *phishing* representa uma das fraudes mais prejudiciais para os consumidores, pois é muitas vezes difícil de identificar, especialmente quando o e-mail ou mensagem parece autêntico. Os ataques de *phishing*, que visam roubar informações e comprometer contas, são especialmente perigosos em plataformas abertas como OLX e Facebook Marketplace, onde a comunicação direta entre usuários facilita o contato dos criminosos com as vítimas, expondo-as a riscos sem que a plataforma intervenha diretamente no processo.

Além disso, a venda de produtos falsificados é uma prática recorrente em marketplaces, onde golpistas anunciam itens que, na realidade, não correspondem ao que é descrito ou simplesmente não existem. Esse tipo de fraude é comum em plataformas como Americanas e OLX, onde diversos vendedores atuam de forma

independente, dificultando o controle e verificação de cada anúncio. Segundo Monteverde (2014), a venda de produtos falsificados prejudica não só o consumidor, que recebe itens de baixa qualidade ou diferentes do esperado, mas também a reputação das plataformas, que ficam associadas à falta de controle sobre a procedência dos produtos. O uso de imagens manipuladas e descrições enganosas são estratégias comuns usadas por esses vendedores fraudulentos para atrair consumidores, que podem acabar adquirindo produtos falsificados ou de origem desconhecida.

Uma outra prática comum em fraudes de marketplace é o golpe de “não entrega”, onde o vendedor recebe o pagamento, mas não envia o produto. Esse golpe é facilitado em plataformas que não possuem um sistema integrado de entrega, como OLX e Facebook Marketplace, onde o comprador e o vendedor geralmente combinam os detalhes da transação diretamente. A falta de intermediação nesses casos permite que golpistas ofereçam produtos a preços atraentes e convençam os compradores a fazer o pagamento antecipado, geralmente por transferências bancárias ou boletos, sem qualquer garantia de recebimento do produto (E-commerce Brasil, 2020). Lopes (2016) destaca que esses golpes são prejudiciais tanto para os consumidores quanto para a imagem da plataforma, pois, além de perderem dinheiro, as vítimas ficam desamparadas por não haver um sistema de suporte ou garantia que assegure a transação.

A fraude de triangulação é mais um tipo de golpe sofisticado presente nas transações online, onde o criminoso age como intermediário entre o comprador e o verdadeiro vendedor, utilizando um cartão de crédito roubado para realizar a compra e enviá-la ao comprador. Esse tipo de fraude afeta tanto os consumidores quanto os próprios marketplaces, uma vez que o verdadeiro titular do cartão acaba identificando a compra não autorizada, o que gera problemas de estorno e pode afetar a segurança financeira da plataforma (CLEARSALE, 2023). De acordo com Lopes (2016), a fraude de triangulação é difícil de detectar e exige que os marketplaces invistam em monitoramento contínuo e análise comportamental para identificar transações suspeitas e impedir que o golpe seja concluído.

Esses tipos de fraude mostram como as transações online estão suscetíveis a práticas criminosas que se adaptam e evoluem conforme surgem novos sistemas de segurança.

As fraudes de pagamento, roubo de identidade, *phishing*, venda de produtos falsificados, golpe de não entrega e fraude de triangulação são alguns dos exemplos de como criminosos aproveitam as vulnerabilidades dos marketplaces para obter ganhos ilícitos (Alves, 2021).

6.2. Fraudes financeiras: golpes de pagamento e não entrega de produtos

As fraudes financeiras em marketplaces representam um dos maiores desafios para a segurança digital, afetando a confiança dos consumidores e a integridade das plataformas. Os golpes de pagamento e a não entrega de produtos são fraudes recorrentes que afetam tanto os compradores quanto os vendedores em marketplaces como Mercado Livre, Americanas, OLX e Facebook. Esses golpes exploram brechas nos sistemas de pagamento, na comunicação entre usuários e na própria logística, criando prejuízos financeiros e colocando em risco a reputação das plataformas (Ebit, 2019). Segundo o Mapa da Fraude da ClearSale (2019), a incidência de fraudes financeiras em transações online é alta, e os cibercriminosos estão cada vez mais sofisticados em suas abordagens, adotando novas estratégias para burlar as medidas de segurança.

Os golpes de pagamento ocorrem principalmente quando o comprador ou vendedor realiza uma transação fora das plataformas oficiais de pagamento. No Mercado Livre, por exemplo, é comum que golpistas induzam o comprador a realizar o pagamento por meios alternativos, como transferências bancárias, ao invés de utilizar o Mercado Pago, que oferece proteção ao consumidor. Quando o pagamento é feito fora do sistema seguro da plataforma, o comprador perde qualquer garantia de reembolso caso a transação não seja completada ou o produto não seja entregue. Lopes (2016) aponta que a fraude financeira através de golpes de pagamento se aproveita da falta de conhecimento dos consumidores sobre as políticas de proteção oferecidas pelos marketplaces, sendo um problema persistente em plataformas onde muitos usuários buscam preços atrativos e negociam diretamente com o vendedor.

A prática de não entrega de produtos é outra fraude financeira que afeta os marketplaces, especialmente em plataformas que facilitam a negociação direta entre usuários, como OLX e Facebook Marketplace. Nesse golpe, o vendedor oferece um

produto e, após receber o pagamento, não realiza o envio, desaparecendo com o dinheiro do comprador. Esse tipo de golpe é mais frequente em plataformas onde não há uma mediação direta dos pagamentos, permitindo que os golpistas atuem com maior liberdade. Segundo Gabriel (2020), a não entrega de produtos é uma das fraudes mais prejudiciais para a confiança dos consumidores, pois muitos usuários preferem realizar pagamentos antecipados sem questionar a veracidade dos vendedores, o que aumenta o risco de perdas financeiras. Em marketplaces sem intermediação, a possibilidade de resolver disputas de forma eficiente é limitada, deixando os consumidores vulneráveis a esse tipo de golpe.

No caso da Americanas, embora a plataforma possua um sistema intermediário que controla pagamentos e entrega, golpes de pagamento ainda podem ocorrer, principalmente em transações realizadas com vendedores terceiros. Nesses casos, vendedores fraudulentos se aproveitam da confiança que a marca Americanas possui e anunciam produtos falsos ou de qualidade inferior, fazendo o comprador acreditar que está adquirindo um item legítimo. Quando a plataforma intermedia o pagamento e a entrega, as chances de fraude são reduzidas, mas em alguns casos, o próprio sistema de logística pode falhar, resultando em produtos que nunca chegam ao destino ou chegam com qualidade inferior ao anunciado (Ebit, 2018). Monteverde (2014) destaca que a intermediação reduz a fraude, mas não elimina completamente os riscos, especialmente quando há uma grande variedade de vendedores independentes com diferentes padrões de qualidade e compromisso.

Os golpes de pagamento e a não entrega de produtos prejudicam tanto os consumidores quanto os marketplaces, pois além das perdas financeiras, esses incidentes afetam a reputação da plataforma. A confiança é um elemento central para o sucesso de marketplaces e, conforme apontado por Marcondes (2015), a recorrência de fraudes e golpes pode levar os consumidores a evitar transações online ou a migrar para plataformas que oferecem maior segurança. No Mercado Livre, a introdução de políticas de proteção ao consumidor e de intermediação de pagamentos foi uma resposta às fraudes frequentes, mas muitos usuários ainda optam por formas de pagamento alternativas, que deixam o processo vulnerável a golpes. Além disso, o sistema de reputação dos vendedores nem sempre é suficiente para evitar fraudes, uma vez que criminosos podem criar perfis falsos ou manipular avaliações para parecerem confiáveis.

A OLX e o Facebook Marketplace, que promovem uma negociação direta entre as partes, enfrentam desafios ainda maiores na prevenção desses golpes. A ausência de um sistema de pagamento próprio torna essas plataformas altamente vulneráveis a fraudes financeiras, pois cabe ao comprador e ao vendedor decidirem como finalizar a transação. Essa falta de intermediação formal faz com que golpes de não entrega sejam frequentes, uma vez que não há um mecanismo claro para garantir que o produto será enviado após o pagamento. Segundo Lopes (2016), marketplaces que dependem de negociação direta devem investir na conscientização dos usuários, informando-os sobre os riscos de realizar pagamentos antecipados e incentivando o uso de métodos mais seguros, como a troca de produtos em mãos ou o pagamento na entrega, quando possível.

Portanto, as fraudes financeiras em marketplaces são um problema complexo que envolve tanto questões tecnológicas quanto a educação dos usuários. As plataformas que possuem intermediação de pagamento e políticas de proteção ao consumidor, como a Americanas e o Mercado Livre, conseguem reduzir o número de golpes de pagamento e não entrega, mas ainda assim enfrentam dificuldades em lidar com a sofisticação das fraudes. Em marketplaces que não têm intermediação de pagamento, como OLX e Facebook Marketplace, a vulnerabilidade é ainda maior, e cabe aos próprios usuários tomarem precauções extras para evitar perdas (Ebit, 2021). A ClearSale (2019) enfatiza que as fraudes financeiras continuarão a evoluir, e a única forma de combater esses golpes de forma efetiva é através de uma combinação de medidas de segurança digital, políticas claras de proteção ao consumidor e um esforço contínuo de conscientização dos usuários sobre os riscos de transações online.

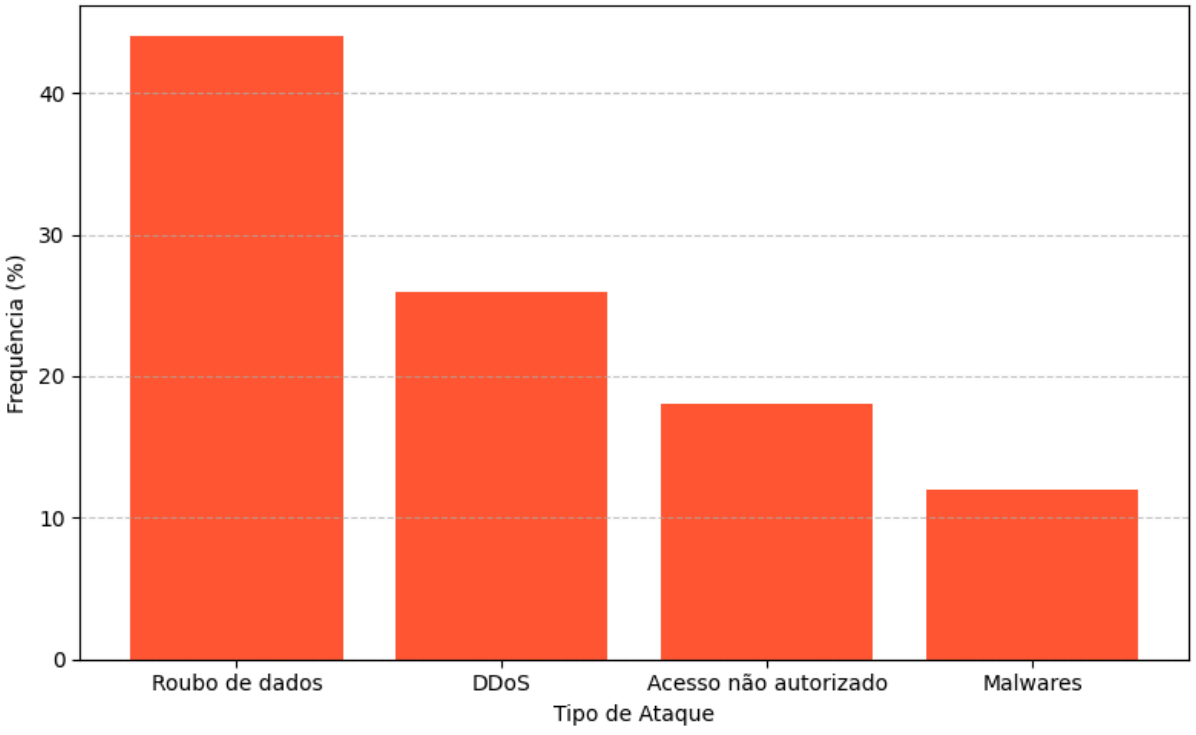
6.3. Impacto dos ataques cibernéticos na confiabilidade e no funcionamento das plataformas

Os ataques cibernéticos têm um impacto profundo na confiabilidade e no funcionamento das plataformas de marketplace, afetando desde a percepção dos usuários até a integridade dos sistemas que sustentam essas operações. Em marketplaces como Mercado Livre, Americanas, OLX e Facebook, esses ataques se tornam cada vez mais comuns e sofisticados, explorando vulnerabilidades nas redes

e sistemas digitais. À medida que as ameaças cibernéticas aumentam, esses marketplaces enfrentam desafios constantes para manter a segurança de seus dados e garantir que os usuários possam realizar transações com confiança. Segundo o relatório da NTT (2021), as plataformas digitais enfrentam riscos variados que vão desde a interrupção dos serviços até a perda de dados confidenciais, o que impacta negativamente a confiança dos usuários e gera custos altos para a recuperação dos sistemas e das informações.

Os ataques cibernéticos, como o roubo de dados e a disseminação de malwares, afetam diretamente a experiência do usuário, minando a confiança dos consumidores e reduzindo a frequência de transações. Como pode ser observado no Gráfico 11, o roubo de dados representa o tipo mais recorrente de ataque cibernético em marketplaces, seguido pelos ataques DDoS e acessos não autorizados, evidenciando os principais vetores de vulnerabilidade nas plataformas.

Gráfico 11 - Tipos de ataques cibernéticos mais comuns em marketplaces



Fonte: Elaborado pela autora adaptado de MORPHISEC. Morphisec Cybersecurity Threat Report 2024; IBM. X-Force Threat Intelligence Index 2024.

Quando ocorre uma violação de segurança, como a exposição de informações financeiras ou pessoais, os usuários tendem a perceber a plataforma

como insegura, levando-os a evitar novas transações e até a desativar suas contas. Marcondes (2015) observa que a confiança do consumidor é essencial para o sucesso de marketplaces, e qualquer incidente de segurança compromete a percepção de confiabilidade, dificultando a retenção de clientes e o crescimento da base de usuários. Além disso, os consumidores prejudicados por ataques cibernéticos costumam exigir respostas rápidas e compensações, o que pressiona as plataformas a adotarem medidas mais rigorosas de segurança.

Os ataques de negação de serviço (DDoS), por exemplo, são uma ameaça frequente que prejudica o funcionamento das plataformas ao sobrecarregar os servidores, tornando-os indisponíveis para os usuários. Em marketplaces de grande porte como o Mercado Livre e a Americanas, esse tipo de ataque causa interrupções que impactam milhões de transações e prejudicam diretamente as vendas. Durante um ataque DDoS, a plataforma pode ficar instável ou completamente inacessível, frustrando os usuários e causando perdas financeiras significativas. Segundo Lopes (2016), as plataformas de e-commerce dependem de uma operação estável para garantir que as transações ocorram de forma ininterrupta, e as interrupções resultantes de ataques cibernéticos representam um risco significativo para o desempenho e a reputação dessas empresas. Quando uma plataforma sofre uma interrupção desse tipo, não só as vendas são afetadas, mas também a percepção de segurança do usuário, que passa a questionar a capacidade da empresa de proteger seus dados e de oferecer um ambiente seguro para compras.

O roubo de dados e o acesso não autorizado também têm um impacto severo no funcionamento das plataformas, especialmente quando os cibercriminosos conseguem acessar informações sensíveis dos usuários, como dados financeiros e históricos de transações. Em plataformas como OLX e Facebook Marketplace, onde os usuários compartilham dados pessoais e financeiros para concluir as transações, a exposição desses dados pode resultar em fraudes e no uso indevido das informações. Gabriel (2020) aponta que o roubo de dados não apenas gera danos financeiros para os usuários, mas também expõe as plataformas a multas e sanções regulatórias, especialmente em regiões onde legislações de proteção de dados, como o GDPR e a LGPD, impõem penalidades rigorosas para incidentes de segurança. Além das consequências legais, a plataforma que sofre um roubo de dados enfrenta uma crise de confiança, pois os usuários se sentem vulneráveis e

podem optar por migrar para concorrentes que oferecem maior proteção e segurança.

Os ataques cibernéticos não afetam apenas a confiança dos consumidores, mas também a própria infraestrutura das plataformas, exigindo investimentos contínuos em medidas de proteção e atualizações de segurança. Para lidar com essas ameaças, as empresas precisam investir em tecnologias avançadas de monitoramento e defesa, como firewalls, sistemas de detecção de intrusão e criptografia. No entanto, esses recursos demandam um alto custo operacional e exigem uma equipe especializada para garantir a eficácia dos sistemas de segurança. De acordo com Monteverde (2014), a pressão para manter a segurança das plataformas é constante, e as empresas que não conseguem acompanhar a evolução das ameaças acabam deixando brechas que podem ser exploradas por cibercriminosos, comprometendo ainda mais o funcionamento e a confiabilidade das operações.

Além dos danos diretos aos usuários, os ataques cibernéticos também afetam os vendedores que dependem dessas plataformas para realizar negócios. Em marketplaces como o Mercado Livre e a Americanas, que reúnem uma grande variedade de vendedores, os ataques cibernéticos interrompem a comunicação e o processamento de pedidos, resultando em atrasos nas entregas e perda de vendas. Lopes (2016) observa que esses incidentes afetam a relação entre os vendedores e as plataformas, pois os comerciantes esperam que o ambiente de e-commerce ofereça uma experiência segura e estável. Quando a segurança é comprometida, os vendedores podem buscar alternativas que ofereçam maior proteção para suas transações e dados, o que impacta negativamente a competitividade e a participação de mercado das plataformas afetadas.

Os ataques cibernéticos também geram prejuízos financeiros expressivos para as plataformas, pois, além das perdas diretas, as empresas precisam destinar recursos significativos para a recuperação dos sistemas e o fortalecimento das medidas de segurança. Segundo o relatório da NTT (2021), os custos com a resposta a ataques cibernéticos e a restauração de sistemas podem ser extremamente altos, especialmente para plataformas com grande volume de transações. Além disso, os marketplaces que não conseguem responder rapidamente a esses incidentes acabam enfrentando ações judiciais e multas

regulatórias, o que agrava ainda mais os prejuízos financeiros e dificulta a recuperação da imagem da empresa no mercado.

Desta forma, os ataques cibernéticos representam uma ameaça complexa e multifacetada para os marketplaces, afetando tanto a confiança dos consumidores quanto o funcionamento das operações. A recorrência desses ataques prejudica a experiência do usuário, gera perdas financeiras para os vendedores e exige que as plataformas invistam constantemente em medidas de proteção, aumentando os custos operacionais. Para que os marketplaces possam garantir uma experiência segura e confiável, é essencial que adotem uma abordagem de segurança robusta e atualizada, que inclua tanto a tecnologia quanto a conscientização dos usuários sobre os riscos cibernéticos.

7. CONSCIENTIZAÇÃO DO USUÁRIO E A IMPORTÂNCIA DA PADRONIZAÇÃO DA REGULAMENTAÇÃO

A segurança digital e a confiança nas transações em marketplaces como Mercado Livre, Americanas, OLX e Facebook Marketplace são temas centrais diante do crescimento do comércio eletrônico e dos riscos crescentes de fraudes e ataques cibernéticos. Estratégias de comunicação e educação para práticas seguras desempenham papel fundamental na proteção dos usuários, uma vez que a segurança depende não apenas de ferramentas tecnológicas, mas também do comportamento informado dos consumidores. Conforme Gabriel (2020), a comunicação educativa deve ser clara, acessível e constante, utilizando notificações em tempo real, campanhas por e-mail, seções informativas, vídeos educativos e a colaboração ativa dos usuários para criar uma cultura de segurança digital.

A implementação de uma regulamentação padronizada para marketplaces apresenta tanto desafios quanto benefícios. A diversidade dos modelos de negócio — que variam de intermediação formal em plataformas como Mercado Livre até negociações diretas em OLX e Facebook Marketplace — dificulta a criação de normas únicas sem prejudicar a flexibilidade operacional (Lopes, 2016). Além disso, o alcance internacional das plataformas impõe a necessidade de harmonização entre legislações nacionais distintas, como GDPR e LGPD (Marcondes, 2015). Apesar disso, uma regulamentação uniforme aumentaria a proteção ao consumidor

por meio da padronização de práticas de segurança, reduziria riscos legais para as plataformas e facilitaria a cooperação entre marketplaces e autoridades de segurança (Gabriel, 2020; Monteverde, 2014; ClearSale, 2019).

Entre as propostas de melhorias para aumentar a segurança e a confiança nas transações online, destaca-se o investimento em autenticação multifatorial (MFA), que reduz significativamente os riscos de invasões (Gabriel, 2020; Lopes, 2016). Sistemas avançados de monitoramento em tempo real, que empregam inteligência artificial, também são essenciais para detectar e prevenir fraudes (Marcondes, 2015). A comunicação e a educação contínua dos usuários, por meio de campanhas e recursos educativos, contribuem para uma base de consumidores mais preparada (ClearSale, 2019). A adoção de programas de recompensa para identificação de vulnerabilidades (bug bounty) e garantias financeiras que protejam o consumidor — como o uso de sistemas de custódia e pagamento intermediado — fortalecem a segurança das transações (Monteverde, 2014; Lopes, 2016). Além disso, a transparência nas comunicações sobre incidentes de segurança é fundamental para manter a confiança dos usuários (Gabriel, 2020).

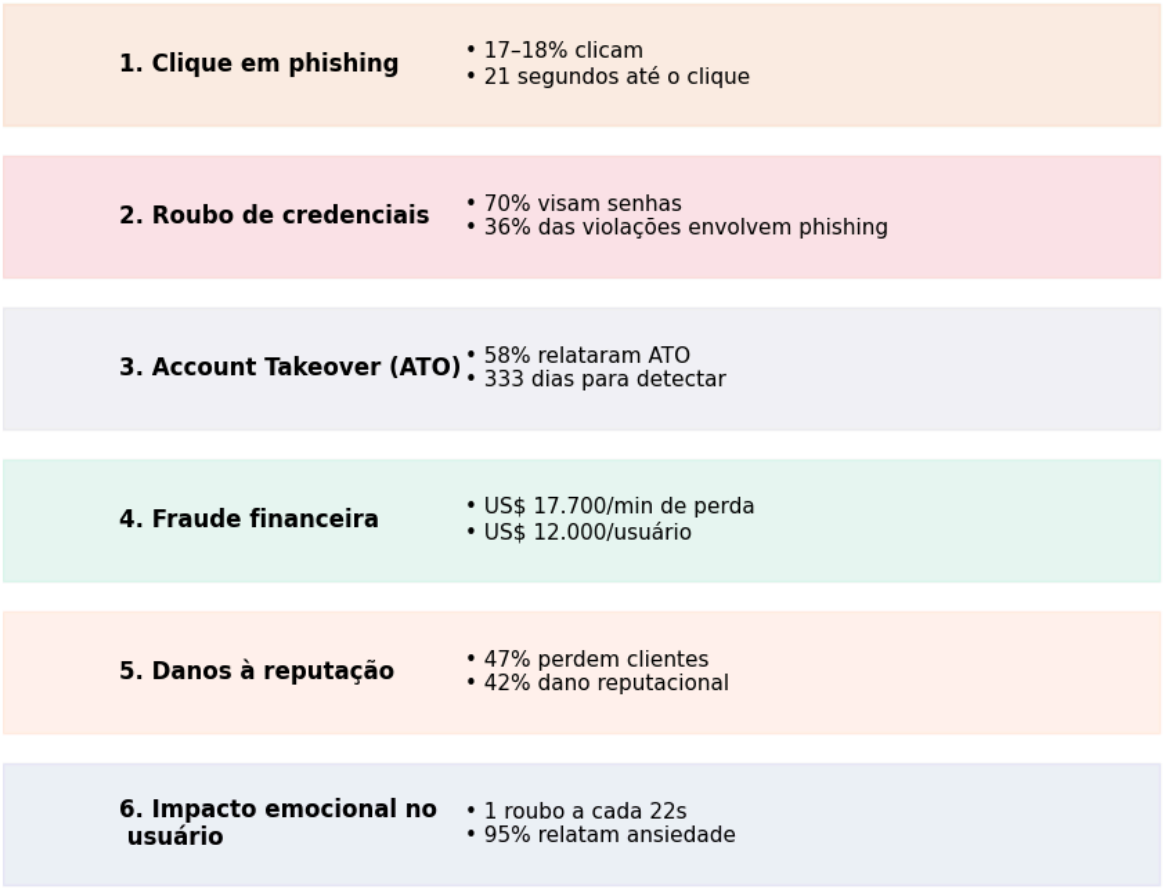
Dessa forma, a segurança em marketplaces exige uma abordagem multifacetada, integrando avanços tecnológicos, educação do usuário, regulamentação adequada e transparência. A cooperação entre plataformas, legisladores, autoridades regulatórias e consumidores é essencial para criar um ambiente digital mais seguro, confiável e eficiente.

7.1. Importância da conscientização do usuário para a segurança digital

A conscientização do usuário é um elemento crucial para a segurança digital em plataformas de marketplace e em qualquer ambiente online onde ocorram transações e trocas de informações sensíveis. Em marketplaces como Mercado Livre, Americanas, OLX e Facebook, a segurança depende não apenas de tecnologias robustas, mas também da colaboração ativa dos usuários em adotar práticas seguras e estar atentos a possíveis ameaças, como fraudes, *phishing* e roubo de identidade. Gabriel (2020) destaca que, mesmo com sistemas de segurança sofisticados, a falta de conscientização dos usuários cria vulnerabilidades significativas, uma vez que os cibercriminosos tendem a explorar o desconhecimento e o comportamento impulsivo dos consumidores para aplicar

golpes e obter acesso a informações pessoais e financeiras. A imagem a seguir resume os principais impactos causados por ataques cibernéticos aos usuários, destacando desde o clique em phishing até o impacto emocional dessas ameaças:

Figura 1 - Cadeia de consequências da falta de conscientização digital



Fonte: Elaborada pela autora, adaptado de dados do Verizon Data Breach Investigations Report (2024), IBM Cost of a Data Breach Report (2024), Proofpoint State of the Phish (2023), ClearSale, Febraban, Serasa Experian, FTC (Federal Trade Commission) e Cybersecurity Ventures.

A educação digital dos usuários é especialmente relevante em plataformas que promovem a interação direta entre compradores e vendedores, como OLX e Facebook Marketplace, onde as negociações ocorrem sem a mediação direta das empresas. Em tais ambientes, a falta de informação sobre segurança pode levar os usuários a realizarem transações fora dos canais oficiais ou a compartilhar dados sensíveis de forma imprudente. Lopes (2016) observa que a falta de conhecimento dos usuários sobre segurança digital facilita a ação de golpistas, pois as vítimas não reconhecem sinais de fraude e frequentemente caem em armadilhas como

mensagens de *phishing* e ofertas fraudulentas. A conscientização dos usuários sobre a importância de utilizar as ferramentas de proteção oferecidas pelas plataformas, como autenticação de dois fatores e canais seguros de pagamento, é essencial para reduzir esses riscos.

Além disso, a conscientização digital dos consumidores auxilia no combate a práticas de engenharia social, um método amplamente usado em fraudes e que se baseia na manipulação psicológica para induzir a vítima a compartilhar informações. Marcondes (2015) ressalta que a engenharia social é uma das técnicas mais eficazes para o roubo de dados, pois explora a confiança e a curiosidade dos usuários. Ao educar os consumidores sobre como identificar mensagens suspeitas e verificar a autenticidade das comunicações, as plataformas podem reduzir significativamente a probabilidade de que os usuários compartilhem informações sensíveis com golpistas. No Mercado Livre, por exemplo, muitos ataques de phishing envolvem mensagens que parecem legítimas, mas contêm links falsos que direcionam para páginas de login fraudulentas. Usuários conscientes são mais propensos a questionar essas mensagens e a tomar precauções antes de inserir seus dados.

Outro benefício da conscientização é a promoção de práticas de segurança no uso de dispositivos e senhas. Muitos consumidores não têm o hábito de atualizar senhas ou de escolher combinações fortes e únicas para cada serviço, o que facilita o acesso não autorizado em caso de uma violação de dados. Monteverde (2014) destaca que o uso de senhas fracas e a repetição de senhas entre diferentes plataformas aumentam a exposição dos usuários a ataques, uma vez que, ao obter acesso a uma conta, os cibercriminosos podem comprometer outras contas associadas. Ao orientar os usuários sobre a importância de criar senhas fortes, atualizá-las periodicamente e usar gerenciadores de senhas, as plataformas de marketplace podem ajudar a minimizar as vulnerabilidades relacionadas ao comportamento do consumidor.

A conscientização também desempenha um papel fundamental na prevenção de fraudes financeiras, como golpes de pagamento e não entrega de produtos. Muitos usuários desconhecem as proteções oferecidas pelas plataformas e optam por métodos de pagamento alternativos, que não contam com garantia de reembolso em caso de fraude. Lopes (2016) aponta que educar os consumidores sobre a importância de realizar transações dentro dos canais oficiais das plataformas ajuda a

reduzir os riscos de golpes, pois os consumidores entendem que métodos seguros, como Mercado Pago no Mercado Livre, oferecem proteção e intermediação. Esse entendimento é essencial para proteger os usuários de fraudes que poderiam ser evitadas com medidas simples, como o uso dos sistemas de pagamento integrados das plataformas.

Os marketplaces também têm a responsabilidade de investir em campanhas de conscientização e na criação de conteúdos educativos que alcancem toda a base de usuários, de forma clara e acessível. A ClearSale (2019) destaca que, em um ambiente digital onde as ameaças evoluem rapidamente, a comunicação constante e efetiva sobre segurança é crucial para manter os usuários informados e preparados para identificar e evitar riscos. Muitas plataformas adotam notificações e alertas para avisar sobre tentativas de login suspeitas ou mensagens de *phishing* identificadas. Essas ações não apenas protegem o usuário, mas também fortalecem a imagem da plataforma como um ambiente seguro e confiável, essencial para a fidelização dos consumidores e para o crescimento saudável do marketplace.

Desta forma, a conscientização do usuário é uma barreira essencial contra as ameaças digitais e complementa as ferramentas tecnológicas de segurança oferecidas pelas plataformas. A combinação entre sistemas de proteção e uma base de usuários informada e cautelosa cria um ambiente de e-commerce mais seguro e confiável. Para alcançar essa conscientização, é fundamental que as plataformas invistam em programas contínuos de educação digital e que incentivem os usuários a adotar práticas de segurança responsáveis, protegendo-se contra fraudes e garantindo a integridade de suas informações.

7.2. Estratégias de comunicação e educação para práticas seguras

As estratégias de comunicação e educação para práticas seguras são fundamentais para reduzir as vulnerabilidades em plataformas digitais e marketplaces, ajudando a proteger usuários contra-ataques cibernéticos e fraudes. Em marketplaces como Mercado Livre, Americanas, OLX e Facebook, essas estratégias têm se tornado essenciais, pois a segurança digital depende não apenas de ferramentas tecnológicas, mas também do comportamento informado dos consumidores. A conscientização é uma das formas mais eficazes de fortalecer a

segurança digital, pois usuários bem-informados são menos propensos a cair em golpes e mais capazes de reconhecer ameaças como *phishing*, roubo de identidade e fraudes de pagamento. Segundo Gabriel (2020), a comunicação educativa sobre segurança digital deve ser clara, acessível e constante, de modo a alcançar uma ampla gama de usuários e promover uma cultura de segurança digital em toda a plataforma.

Uma das estratégias mais comuns para educar os usuários sobre práticas seguras é a utilização de notificações e alertas sobre atividades suspeitas, que informam o consumidor imediatamente em caso de tentativas de login de locais incomuns ou de transações suspeitas. Esse tipo de comunicação em tempo real é eficaz, pois alerta o usuário no momento exato em que algo fora do comum ocorre, permitindo que ele tome medidas rápidas para proteger sua conta. Plataformas como Mercado Livre e Americanas utilizam esses recursos para notificar os usuários sobre alterações em suas contas ou transações não reconhecidas, reforçando a segurança e incentivando práticas preventivas. Lopes (2016) observa que a comunicação imediata é essencial para mitigar ameaças em tempo real e que, quando aliada a orientações educativas, ajuda o usuário a compreender a importância da verificação de atividades e da manutenção de senhas seguras.

Além das notificações em tempo real, muitas plataformas adotam campanhas de e-mails educativos que orientam os usuários sobre segurança digital, incluindo dicas sobre como reconhecer tentativas de *phishing* e fraudes de pagamento. Essas campanhas visam educar os usuários sobre comportamentos específicos que podem protegê-los, como evitar clicar em links desconhecidos e não compartilhar informações pessoais em mensagens não solicitadas. Marcondes (2015) destaca que o e-mail é um canal poderoso para campanhas de conscientização, pois permite que as plataformas forneçam informações detalhadas e exemplos práticos de situações de risco, ajudando o usuário a identificar fraudes. O Mercado Livre, por exemplo, utiliza e-mails para alertar sobre os tipos mais comuns de golpes e para encorajar a utilização do Mercado Pago, sua ferramenta segura de pagamento, a fim de evitar fraudes durante as transações.

Outra estratégia eficaz são as seções dedicadas à segurança nos sites e aplicativos das plataformas, onde os usuários podem acessar conteúdos sobre práticas seguras e consultar respostas para dúvidas frequentes sobre proteção digital. Essas seções funcionam como um guia, ensinando os consumidores a evitar

fraudes e a utilizar recursos de segurança, como autenticação de dois fatores. No Facebook Marketplace, por exemplo, há uma área de segurança onde são explicadas as práticas recomendadas para comprar e vender com segurança, incluindo a importância de realizar transações em locais públicos e de verificar a identidade do vendedor ou comprador. Monteverde (2014) aponta que essas seções educativas são essenciais para que os usuários tenham um recurso confiável ao qual possam recorrer em caso de dúvidas, promovendo um ambiente de transação mais seguro e consciente.

Além do conteúdo textual, muitos marketplaces têm explorado o uso de vídeos e tutoriais interativos para facilitar a compreensão de práticas de segurança. Vídeos educativos são uma forma visualmente atraente e de fácil assimilação que permite ao usuário entender rapidamente como identificar e evitar ameaças. Plataformas como Americanas e OLX já utilizam vídeos explicativos para orientar sobre como evitar fraudes e como configurar recursos de segurança, como verificação em duas etapas. Esses vídeos são especialmente úteis para usuários que podem ter dificuldades em interpretar longos textos ou que preferem aprender por meio de demonstrações visuais. Lopes (2016) observa que, com o aumento do uso de dispositivos móveis, vídeos curtos e interativos são eficazes para alcançar um público mais amplo, incluindo aqueles menos familiarizados com o ambiente digital.

A comunicação sobre segurança também envolve a colaboração com os próprios usuários para fortalecer as práticas de segurança. Muitas plataformas permitem que os usuários denunciem atividades suspeitas ou perfis fraudulentos, o que ajuda a identificar padrões de comportamento malicioso e a prevenir que outros usuários sejam vítimas de golpes semelhantes. Gabriel (2020) destaca que a participação dos usuários no monitoramento de segurança é fundamental para criar uma rede de proteção colaborativa e para incentivar um ambiente de confiança. No OLX, por exemplo, a possibilidade de denunciar vendedores e compradores suspeitos é uma ferramenta importante que auxilia a equipe de segurança da plataforma a investigar possíveis fraudes e a manter a comunidade informada sobre os riscos.

As plataformas de marketplace podem também realizar campanhas de conscientização em redes sociais e blogs para alcançar usuários de forma mais informal e envolvente. Conteúdos como posts e artigos educativos permitem que as

plataformas compartilhem informações sobre práticas seguras e alertem sobre novas ameaças em tempo real. Essa abordagem mais descontraída nas redes sociais é eficaz para chamar a atenção de usuários que talvez não tenham o hábito de consultar as seções de segurança nos sites, tornando a educação sobre segurança digital mais acessível. A ClearSale (2019) ressalta que as redes sociais são uma ferramenta poderosa para campanhas de conscientização, especialmente em ambientes onde os cibercriminosos também utilizam essas plataformas para aplicar golpes. Ao utilizar as redes sociais para educar sobre segurança, os marketplaces ampliam o alcance de suas campanhas e promovem a conscientização de uma forma que ressoa com a cultura digital.

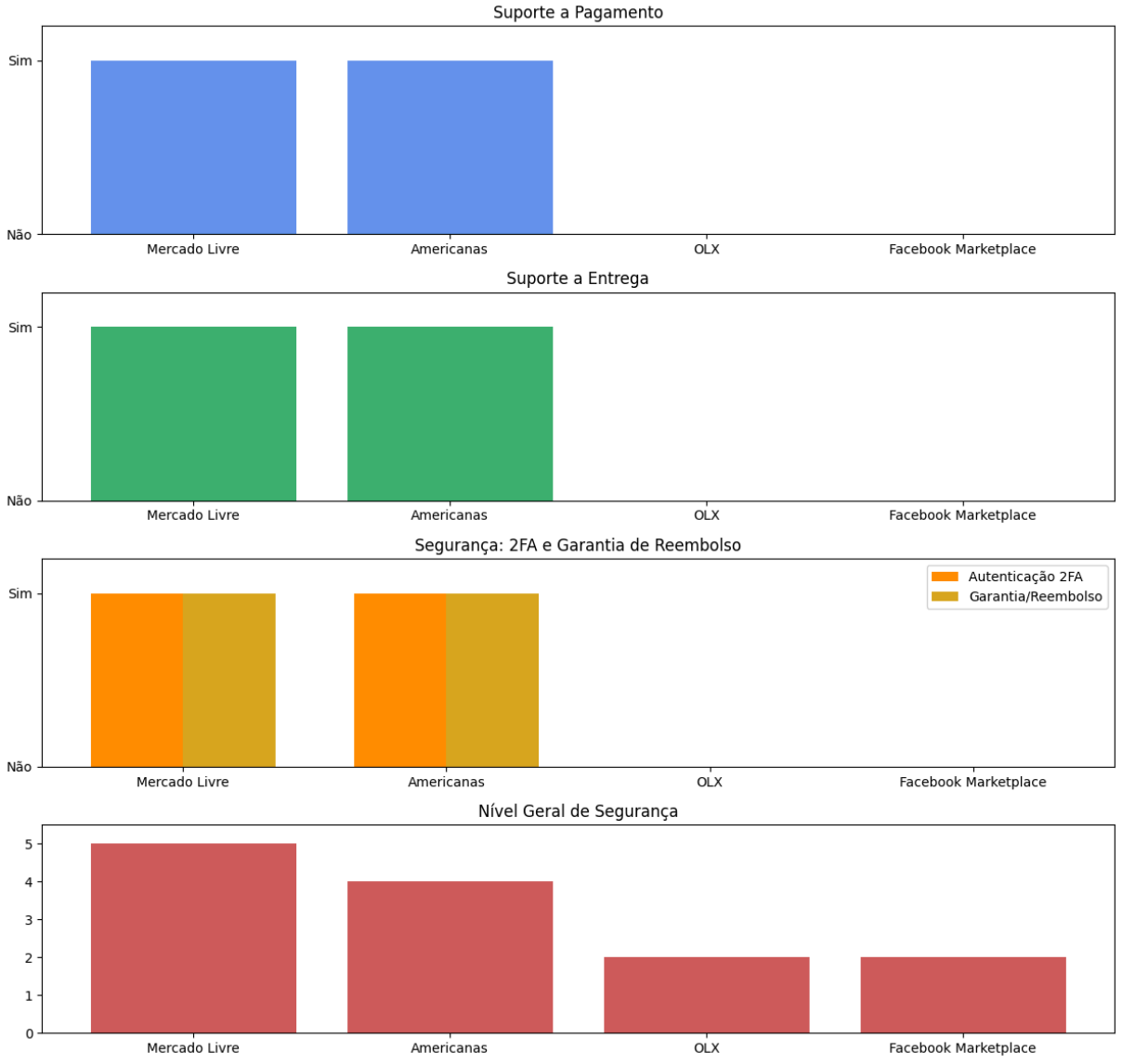
As estratégias de comunicação e educação para práticas seguras em marketplaces combinam notificações em tempo real, campanhas por e-mail, seções informativas, vídeos educativos, colaboração com os usuários e campanhas em redes sociais. Essas ações, integradas, ajudam a construir uma base de consumidores informados e preparados para lidar com ameaças digitais, protegendo-se de fraudes e garantindo uma experiência de compra mais segura.

7.3. Desafios e benefícios de uma regulamentação padronizada para marketplaces

A implementação de uma regulamentação padronizada para marketplaces apresenta uma série de desafios e benefícios, especialmente em um ambiente digital onde as transações online se multiplicam e os riscos de fraudes e violações de segurança são constantes. Marketplaces como Mercado Livre, Americanas, OLX e Facebook operam com modelos variados, cada um com suas próprias práticas e políticas de segurança, o que cria inconsistências e limita a proteção dos consumidores e das próprias plataformas. Uma regulamentação padronizada busca estabelecer normas comuns que poderiam elevar o nível de segurança e transparência em todas as plataformas, garantindo práticas de proteção uniformes e direitos claros para os usuários. Contudo, os desafios para implementar uma regulamentação abrangente e uniforme são significativos, dada a diversidade de serviços e modelos operacionais envolvidos.

Um dos principais desafios para a regulamentação padronizada está na complexidade dos modelos de negócio dos marketplaces, que variam desde vendas diretas e intermediadas até trocas de produtos entre indivíduos. Por exemplo, o Mercado Livre atua como um intermediário em transações, oferecendo suporte para pagamento e entrega, enquanto o OLX e o Facebook Marketplace permitem que os usuários negociem diretamente entre si, sem uma estrutura de intermediação formal. A Figura 2, a seguir, apresenta um infográfico comparativo entre as principais características operacionais dessas plataformas:

Figura 2 - Comparação entre os modelos de negócio e recursos de segurança em marketplaces selecionados.

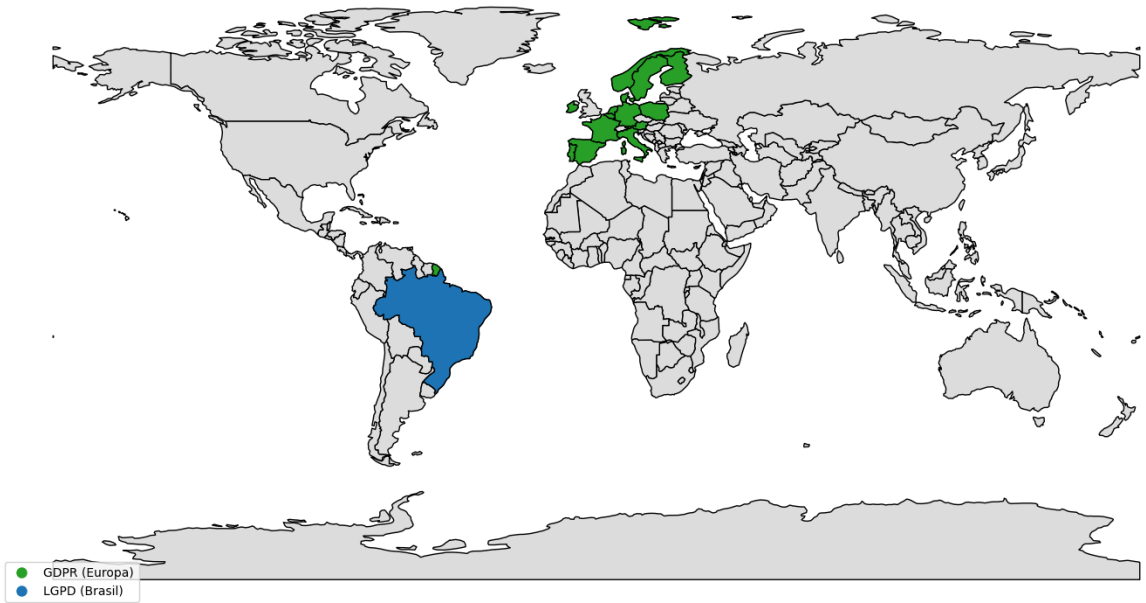


Fonte: Elaborado pela autora com base em dados de Mercado Livre, Americanas, OLX e Facebook (2024).

Lopes (2016) destaca que essa diversidade de modelos torna difícil a criação de uma regulamentação única que contemple todas as especificidades de cada plataforma, sem comprometer a flexibilidade e a conveniência que esses ambientes oferecem aos usuários. Regulamentações padronizadas precisariam encontrar um equilíbrio entre a proteção dos consumidores e a manutenção da eficiência operacional das plataformas, evitando regras que inviabilizem certos modelos de negócio.

Outro desafio significativo na padronização de regulamentações é o alcance internacional dos marketplaces, que operam em diferentes países, cada um com legislações próprias sobre segurança digital, privacidade e transações financeiras. Uma regulamentação que seja aplicável globalmente enfrentaria conflitos de jurisdição, especialmente em regiões onde as leis de proteção de dados são mais rigorosas, como a União Europeia (com o GDPR) e o Brasil (com a LGPD). A Figura 3 ilustra essas regiões e destaca os desafios de harmonização das normas internacionais entre diferentes países e blocos econômicos.

Figura 3 - Mapa-múndi com destaque às regiões de legislação rigorosa de proteção de dados (GDPR e LGPD).



Elaborado pela autora com base em GDPR (2018) e LGPD (2018).

Marcondes (2015) observa que a harmonização de regulamentações internacionais é complexa, pois envolve a cooperação entre diversas autoridades regulatórias e requer que as plataformas adaptem suas políticas para cumprir exigências múltiplas. Marketplaces globais, como o Facebook, estão sujeitos a leis variadas que muitas vezes entram em conflito, exigindo grandes investimentos para cumprir cada requisito regulatório. A criação de uma regulamentação padronizada que respeite as diferenças culturais e legais de cada país é um desafio que exige consenso e diálogo entre legisladores, plataformas e organizações internacionais.

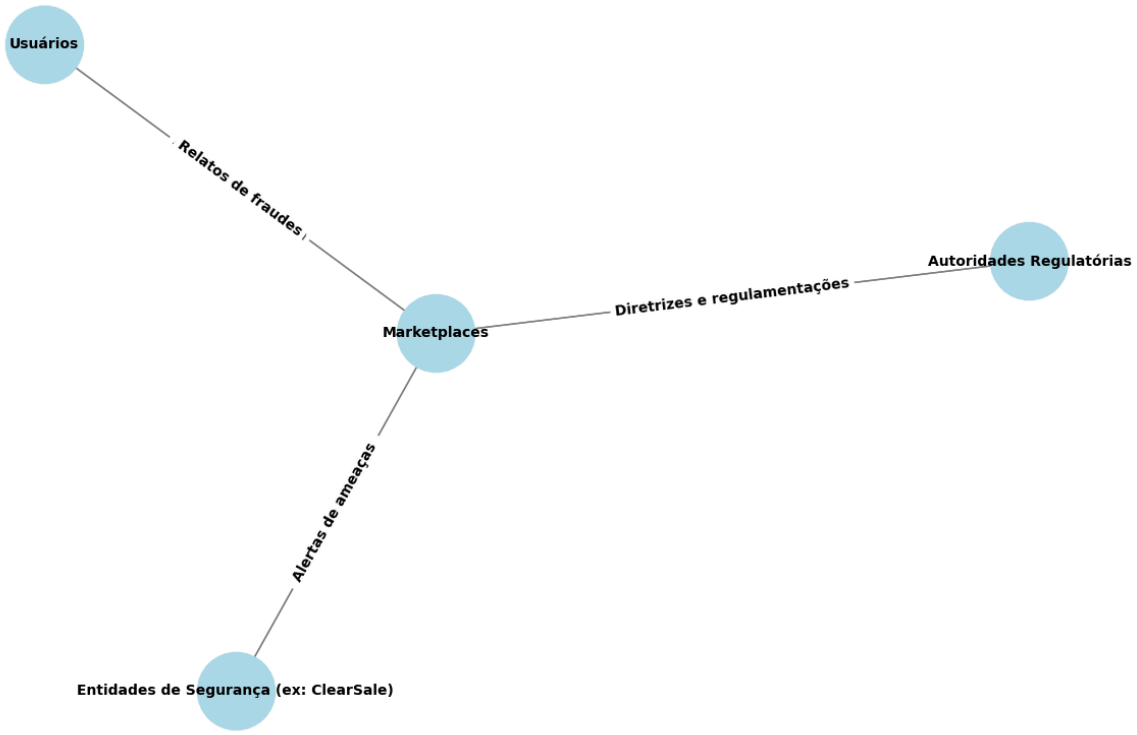
Apesar dos desafios, a padronização regulatória também traz benefícios importantes para a segurança e confiabilidade dos marketplaces. Um dos principais benefícios é o aumento da proteção ao consumidor, uma vez que uma regulamentação padronizada estabelece direitos claros e obrigações para todas as partes envolvidas nas transações. Gabriel (2020) aponta que a falta de uniformidade nas práticas de segurança deixa os consumidores vulneráveis a fraudes e abusos, e que regulamentações padronizadas poderiam estabelecer normas mínimas de segurança, como autenticação de dois fatores e garantias de reembolso, que se aplicariam a todas as plataformas. Esses padrões aumentariam a confiança do consumidor nas transações online, incentivando o uso dos marketplaces de forma mais segura e reduzindo a incidência de fraudes.

A regulamentação padronizada também pode beneficiar os próprios marketplaces, ao criar um ambiente mais previsível e menos vulnerável a penalidades e ações judiciais. Monteverde (2014) sugere que, ao seguir normas claras, as plataformas conseguem operar com mais segurança jurídica e reduzir o risco de multas e sanções relacionadas a falhas de segurança ou vazamentos de dados. Regulamentações como a LGPD no Brasil e o GDPR na Europa têm demonstrado a importância de normas que incentivem as plataformas a adotar medidas rigorosas de proteção de dados. Ao padronizar essas exigências, os marketplaces poderiam reduzir o custo de conformidade e simplificar os processos de segurança, uma vez que não precisariam adaptar-se a diferentes regras em cada região. Essa padronização também facilitaria o monitoramento e a aplicação de leis, criando uma base comum para que as autoridades regulatórias possam fiscalizar as plataformas de forma mais eficaz.

Outro benefício importante é a possibilidade de melhorar a cooperação entre marketplaces e autoridades de segurança cibernética, facilitando a troca de

informações sobre ameaças e fraudes emergentes. Uma regulamentação padronizada pode estabelecer protocolos para o compartilhamento de dados e a comunicação entre plataformas e autoridades, fortalecendo a capacidade de resposta contra-ataques cibernéticos e melhorando a prevenção de fraudes. A Figura 4, a seguir, ilustra o fluxo de informações entre os principais atores envolvidos nesse processo regulatório:

Figura 4 - Fluxo de informações entre marketplaces, autoridades regulatórias e usuários.



Fonte: Elaborado pela autora com base em dados do relatório da ClearSale (2019).

Segundo o relatório da ClearSale (2019), o compartilhamento de informações entre plataformas e entidades reguladoras é essencial para combater fraudes que se propagam rapidamente em redes digitais e impactam milhares de usuários. Quando as plataformas seguem uma regulamentação padronizada, a resposta a incidentes de segurança se torna mais ágil e coordenada, beneficiando tanto os consumidores quanto as empresas.

No entanto, o processo de padronização exige uma abordagem flexível e que considere as particularidades de cada marketplace. Regulamentações rígidas

podem dificultar a inovação e limitar a competitividade, especialmente para marketplaces menores ou que oferecem serviços mais especializados. Lopes (2016) destaca que, para que uma regulamentação padronizada seja eficaz, é necessário que as normas sejam flexíveis o suficiente para permitir a adaptação aos diferentes modelos operacionais, mais rigorosas para garantir um nível mínimo de segurança e proteção aos consumidores. Uma regulamentação bem-sucedida seria aquela que oferece diretrizes claras e exigências práticas de segurança digital, sem restringir a capacidade das plataformas de inovar e expandir seus serviços.

Portanto, a regulamentação padronizada para marketplaces representa uma ferramenta poderosa para aumentar a segurança e a confiança dos consumidores, mas traz desafios consideráveis em termos de implementação e harmonização entre diferentes modelos de negócio e jurisdições. Os benefícios de uma regulamentação uniforme são claros, incluindo maior proteção ao consumidor, redução de riscos legais e maior cooperação na prevenção de fraudes. Entretanto, o sucesso dessa padronização depende de uma abordagem colaborativa que envolva autoridades regulatórias, plataformas e usuários, de forma a criar normas que fortaleçam a segurança digital sem comprometer a flexibilidade e a eficiência operacional dos marketplaces.

7.4. Propostas de melhoria para aumentar a segurança e a confiança nas transações online

A segurança e a confiança nas transações online são aspectos cruciais para o sucesso das plataformas de marketplace, especialmente à medida que o comércio eletrônico continua a crescer e atrair consumidores. As propostas de melhoria para aumentar essa segurança envolvem desde o fortalecimento das práticas de autenticação e proteção de dados até o desenvolvimento de estratégias de conscientização para educar os usuários sobre práticas seguras. Em marketplaces como Mercado Livre, Americanas, OLX e Facebook, onde transações de diversos tipos ocorrem diariamente, implementar melhorias que protejam os usuários e garantam a integridade das transações é essencial para combater ameaças como fraudes financeiras, *phishing* e roubo de identidade. Gabriel (2020) destaca que, embora a tecnologia de segurança digital tenha avançado, o uso de sistemas de

autenticação mais rigorosos, como a autenticação multifatorial, continua sendo uma medida eficaz é fundamental para a proteção dos usuários.

Uma das propostas mais importantes para aumentar a segurança das transações online é o investimento em autenticação multifatorial (MFA), que requer que os usuários forneçam uma segunda forma de verificação, como um código enviado ao celular, além da senha. Essa medida ajuda a impedir acessos não autorizados, mesmo que as senhas sejam comprometidas, pois os cibercriminosos precisam de um segundo fator de autenticação para completar o login. Lopes (2016) observa que o uso de MFA reduz significativamente as chances de invasões, uma vez que o acesso a uma conta fica condicionado a uma verificação adicional que apenas o usuário legítimo possui. Em plataformas como Mercado Livre e Americanas, onde muitos usuários salvam informações de pagamento para facilitar compras futuras, essa medida é particularmente relevante para proteger dados financeiros e evitar fraudes.

Outra proposta importante para aumentar a segurança é a implementação de sistemas avançados de monitoramento em tempo real que detectem atividades suspeitas e alertem os usuários e as equipes de segurança imediatamente. Essas ferramentas utilizam inteligência artificial e machine learning para identificar padrões de comportamento incomuns e, assim, sinalizar possíveis fraudes antes que causem danos. Marcondes (2015) aponta que o monitoramento em tempo real é um aliado poderoso contra fraudes, pois permite que as plataformas ajam proativamente para bloquear contas ou transações suspeitas, protegendo tanto os consumidores quanto a integridade da plataforma. No OLX e no Facebook Marketplace, onde transações entre usuários individuais ocorrem frequentemente sem supervisão direta da plataforma, o uso de sistemas de monitoramento pode ser uma maneira eficaz de interceptar atividades fraudulentas e impedir golpes.

Além do uso de tecnologias, a comunicação e a educação dos usuários sobre práticas de segurança são essenciais para garantir a proteção nas transações. A conscientização sobre os riscos, como golpes de pagamento e não entrega de produtos, permite que os usuários identifiquem e evitem fraudes mais facilmente. Campanhas educativas em e-mails, redes sociais e seções de segurança nos sites das plataformas ajudam a manter os consumidores informados sobre ameaças e orientam sobre como se proteger. A ClearSale (2019) ressalta que a educação contínua dos usuários é fundamental para criar uma base de consumidores mais

informada e preparada, especialmente em marketplaces que operam com grande diversidade de produtos e serviços. O Mercado Livre, por exemplo, utiliza e-mails e notificações para alertar os usuários sobre tentativas de *phishing* e para incentivar o uso de sua ferramenta de pagamento, o Mercado Pago, que oferece garantias de proteção ao consumidor.

A criação de programas de recompensa para identificar vulnerabilidades também pode ser uma estratégia eficaz para melhorar a segurança. Programas de bug bounty, onde especialistas em segurança são recompensados por identificar falhas e brechas no sistema, ajudam a fortalecer a proteção digital das plataformas ao corrigir problemas antes que sejam explorados por criminosos. Monteverde (2014) sugere que a colaboração com especialistas externos é uma forma prática e econômica de identificar pontos fracos que poderiam comprometer a segurança dos dados e das transações. Ao adotar essa prática, marketplaces como Americanas e OLX poderiam aumentar a robustez de seus sistemas de segurança, promovendo uma proteção mais abrangente para seus usuários.

A implementação de garantias financeiras para os consumidores é outra proposta que aumenta a confiança nas transações. No Mercado Livre e na Americanas, por exemplo, a presença de um sistema de pagamento intermediado, que retém o valor até que o comprador confirme o recebimento do produto, oferece uma camada adicional de segurança que minimiza o risco de fraudes. Lopes (2016) observa que garantias como essa aumentam a confiança dos consumidores ao oferecer proteção contra golpes, especialmente em transações de alto valor. Para marketplaces que não possuem uma intermediação formal de pagamento, como OLX e Facebook Marketplace, a criação de parcerias com serviços de custódia financeira poderia proporcionar um nível similar de segurança, garantindo que o pagamento seja liberado somente após a confirmação da entrega.

Além dessas medidas, a transparência e a comunicação direta entre a plataforma e os usuários sobre incidentes de segurança são fundamentais para fortalecer a confiança. Informar rapidamente sobre possíveis violações de dados e tomar medidas imediatas para mitigar o impacto desses incidentes mostra aos usuários que a plataforma está comprometida com a segurança. Gabriel (2020) enfatiza que a transparência é uma prática essencial para aumentar a confiabilidade, pois permite que os consumidores confiem na capacidade da plataforma de proteger suas informações e agir de maneira proativa para resolver problemas de segurança.

As propostas de melhoria para aumentar a segurança e a confiança nas transações online exigem uma abordagem multifacetada que combine tecnologia avançada, comunicação eficaz e políticas de proteção robustas. As plataformas de marketplace devem investir em autenticação forte, monitoramento contínuo, educação dos usuários e garantias financeiras, criando um ambiente mais seguro e confiável para todos os envolvidos.

8. CONSIDERAÇÕES FINAIS

A segurança e a confiança nas transações online são pilares fundamentais para o sucesso e a sustentabilidade dos marketplaces, especialmente em um cenário onde o comércio digital cresce rapidamente e as ameaças cibernéticas se tornam cada vez mais sofisticadas. Ao longo da análise, fica evidente que a combinação entre tecnologia avançada, práticas de conscientização dos usuários e regulamentações padronizadas pode fortalecer significativamente a segurança nessas plataformas. A implementação de medidas como autenticação multifatorial, monitoramento em tempo real e sistemas de pagamento intermediados contribui para minimizar fraudes e proteger dados, enquanto campanhas educativas e canais de comunicação transparentes aumentam a capacidade dos usuários de identificar e evitar ameaças.

Os desafios para estabelecer uma regulamentação padronizada, que leve em consideração as especificidades de cada modelo de negócio e as diferentes jurisdições, revelam-se complexos, mas necessários para oferecer proteção uniforme aos consumidores. A colaboração entre plataformas e autoridades regulatórias, juntamente com o desenvolvimento de políticas internas consistentes, é essencial para criar um ambiente digital seguro e confiável. Programas de recompensa por vulnerabilidades e parcerias com serviços de custódia financeira emergem como estratégias complementares que reforçam a robustez dos sistemas de segurança.

Portanto, a segurança digital em marketplaces depende de uma abordagem integrada que una tecnologia, educação e políticas regulatórias. Ao investir em práticas de proteção mais rigorosas e em estratégias de conscientização, os marketplaces podem proporcionar um ambiente mais seguro, fortalecer a confiança

dos usuários e assegurar a continuidade do crescimento no comércio eletrônico, respondendo às necessidades e desafios de um mercado digital em constante evolução.

REFERÊNCIAS

ALVES, Germano Fabrício; MELO, Lucas Rodrigo de. **Responsabilidade civil por danos morais coletivos causados pela veiculação de publicidade enganosa nas plataformas de Marketplace. 2021**. Revista Vianna Sapiens. Disponível em: https://www.viannasapiens.com.br/revista/article/view/799. Acesso em: 11 mai. 2024.

AMERICANAS. **Guia de segurança para clientes e lojistas. 2023**. Disponível em: https://venda.americanas.com.br/guia-de-seguranca-americanas. Acesso em: 15 abr. 2025.

ARAÚJO, Thayana; RESENDE, Isabelle. **E-commerce registra alta de 20,56% nas vendas em janeiro de 2022. CNN Brasil**. Disponível em: https://www.cnnbrasil.com.br/business/e-commerce-registra-alta-de-2056-nas-vendas-em-janeiro-de-2022/. Acesso em: 13 jun. 2024.

BRASCT. **O impacto da LGPD no e-commerce e as medidas de segurança necessárias**. 2023. Disponível em: https://brasct.com.br/o-impacto-da-lgpd-lei-geral-de-protecao-de-dados-no-e-commerce-e-as-medidas-de-seguranca-necessarias. Acesso em: 10 abr. 2025.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/legislacao-federal. Acesso em: 7 abr. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.ecommercebrasil.com.br/artigos/lgpd-e-seguranca-de-dados-dentro-do-e-commerce. Acesso em: 7 abr. 2025.

BRASIL. **Lei nº 7.962, de 15 de março de 2013**. Altera o Decreto nº 7.962/2013 para dispor sobre a contratação no comércio eletrônico. Disponível em: https://www.jusbrasil.com.br/artigos/regulamentacoes-do-e-commerce-no-brasil-principais-aspectos/2025301495. Acesso em: 7 abr. 2025.

CAPITAL ABERTO. **Precauções para uma possível regulamentação dos marketplaces no Brasil. 2023**. Disponível em: https://legislacaoemercados.capitalaberto.com.br/precaucoes-para-uma-possivel-regulamentacao-dos-marketplaces-no-brasil/. Acesso em: 7 abr. 2025.

CLEARSALE. **Fraude no e-commerce:** entenda este fenômeno e saiba quais são os principais tipos. ClearSale, 13 jan. 2023. Disponível em: https://br.clear.sale/blog/fraude-no-ecommerce-entenda-este-fenomeno-e-saiba-quais-sao-os-principais-tipos. Acesso em: 5 abr. 2025.

CLEARSALE. **Mapa da Fraude 2019**. Disponível em: https://br.clear.sale/mapa-da-fraude. Acesso em: 20 jun. 2024.

CLEARSALE. **Tendências em prevenção de fraudes no e-commerce em 2025**. [S. l.]: ClearSale, [s.d.]. Disponível em: https://br.clear.sale/blog/tendencias-prevencao-de-fraudes. Acesso em: 7 abr. 2025.

CNDL; **SPC Brasil. 32% dos consumidores sofreram ou passaram por alguma tentativa de golpe nas compras pela internet, aponta pesquisa CNDL/SPC Brasil. 2023.** Disponível em: https://cndl.org.br/varejosa/32-dos-consumidores-sofreram-ou-passaram-por-alguma-tentativa-de-golpe-nas-compras-pela-internet-aponta-pesquisa-cndl-spc-brasil. Acesso em: 05 abr. 2025.

COMPUTER WEEKLY. **Segurança digital atinge mais de 95% dos e-commerces no Brasil. 2023**. Disponível em: https://www.computerweekly.com/br/reportagen/Seguranca-digital-atinge-mais-de-95-dos-e-Commerces-no-Brasil. Acesso em: 05 abr. 2025.

DE MELLO, Emerson Ribeiro. **Segurança em serviços web**. Livro de Minicursos do VI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. Santos: SBC, p. 1-48, 2006.

DURBANO, V. **Entenda o que é CVE (Common Vulnerabilities and Exposures**). 2019. Disponível em: https://blog.ecotrust.io/o-que-e-cve/. Acesso em: 19 jun. 2024.

E-Commerce Brasil. **Os desafios das tecnologias para tratar os riscos das compras online. 2020.** Disponível em: https://www.ecommercebrasil.com.br/artigos/os-desafios-das-tecnologias-para-tratar-os-riscos-das-compras-online. Acesso em: 10 mar. 2024.

EBIT. **Web hoppers. 2018**. Disponível em: https://www.ebit.com.br/webshoppers. Acesso em: 18 fev. 2024.

EBIT. **Web Shoppers. 39ª edição. 2019**. Disponível em: http://www.medsobral.ufc.br/pdf/Webshoppers_39.pdf. Acesso em: 09 mai. 2024.

EBIT. **Web Shoppers. 44ª edição. 2021**. Disponível em: https://eyagencia.com.br/wp-content/uploads/2021/09/Webshoppers_44-relatorio-2021-resultados-ecommerce-ebit.pdf. Acesso em: 09 mai. 2024.

ESCOLA DE E-COMMERCE. **Fraude no e-commerce:** entenda o que é e como evitar prejuízos. [S. l.]: Tray, 2023. Disponível em: https://tray.com.br/escola/fraude-no-e-commerce/. Acesso em: 8 abr. 2025.

ESET. **Os golpes mais comuns no Facebook Marketplace. 2023**. Disponível em: https://www.welivesecurity.com/pt/golpes-fraudes/os-golpes-mais-comuns-no-facebook-marketplace. Acesso em: 15 abr. 2025.

FACEBOOK. **Trust and Safety – Marketplace. 2023**. Disponível em: https://pt-br.facebook.com/marketplace/learn-more/trust-and-safety. Acesso em: 15 abr. 2025.

GABRIEL, Martha. **Marketing na Era Digital. Conceitos, Plataformas e Estratégias. Grupo GEN, 2020**. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788597025859/. Acesso em: 14 mai. 2024.

INSTITUTO PROPAGUE. **Fraudes nos marketplaces:** entenda os principais desafios e como combater. 9 ago. 2024. Disponível em:

https://institutopropague.org/pagamentos/fraudes-nos-marketplaces-entenda-os-principais-desafios-e-como-combater/. Acesso em: 7 abr. 2025.

JUSBRASIL**. Plataformas digitais de e-commerce e os problemas com a proteção de dados - LGPD**. 2023. Disponível em: https://www.jusbrasil.com.br/artigos/artigo-juridico-plataformas-digitais-de-e-commerce-e-os-problemas-com-a-protecao-de-dados-lgpd/2552696159. Acesso em: 10 abr. 2025.

JAVELIN STRATEGY & RESEARCH. **Identity Fraud Study**: The Virtual Battleground. Califórnia: Javelin, 2023. Disponível em: https://www.javelinstrategy.com/coverage-area/identity-fraud. Acesso em: 09 jun. 2025.

KREIBICH, Eduardo. **Ciberespaço brasileiro:** caracterização, organização e políticas. Universidade Federal do Rio Grande do Sul, Porto Alegre, 2016.

KUNIYOSHI, Márcio Shoiti. **Comércio Eletrônico:** A revolução em tempos digitais. Revista Administração em Diálogo. v. 2, n. 1, 2009. Disponível em: https://revistas.pucsp.br/index.php/rad/article/view/1689. Acesso em: 9 mai. 2024.

LOPES, Jéssica Rodrigues. **Crimes Virtuais**: Uma sucinta abordagem sobre o cibercrime. JusBrasil, 2016. Disponível em: https://www.jusbrasil.com.br/artigos/crimes-virtuais-uma-sucinta-abordagem-sobre-o-cibercrime/716212605. Acesso em: 4 jun. 2025.

MALONE, T. W.; YALES, J.; BENJAMIN, R. I. **Electronic markets and electronic hierarchies**. Communications of ACM, v.30, n.8, p.484-97, June.

MARCONDES, J. S. **Conceito de segurança da informação organizacional**. Gestão de segurança privada. 2015. Disponível em: https://gestaodesegurancaprivada.com.br. Acesso em: 03 Jun. 2019.

MERCADO LIVRE. **Segurança no Mercado Livre. 2023**. Disponível em: https://www.mercadolivre.com.br/institucional/nos-inovamos/seguranca. Acesso em: 15 abr. 2025.

MONTEVERDE, Wagner Aparecido. **Estudo e análise de vulnerabilidades web. 2014**. Trabalho de Conclusão de Curso. Universidade Tecnológica Federal do Paraná.

Nippon Telegraph and Telephone Corporation (NTT). **Relatório de Inteligência de Ameaças Globais 2021** (GTIR). 2021. Disponível em: https://www.accenture.com/br-pt/insights/security/cyber-threat-intelligence#:~:text=Quais%20s%C3%A3o%20as%20principais%20amea%C3%A7as,redes%20de%20TI%20e%20OT. Acesso em: 20 fev. 2024.

OLX. **Golpe na internet:** conheça 10 tipos de fraude e saiba como evitar. 2023b. Disponível em: https://dicas.olx.com.br/seguranca/golpes-conhecidos. Acesso em: 15 abr. 2025.

OLX. **Identidade verificada na OLX**: como funciona. 2025b. Disponível em: https://dicas.olx.com.br/seguranca/seguranca-na-olx/identidade-verificada-na-olx/. Acesso em: 8 abr. 2025.

OLX. **OLX Termos e Condições de Uso. 2025a**. Disponível em: https://ajuda.olx.com.br/public/OLX_Termos_e_Condicoes_de_Uso_01_01_25_eaa6ed1826.pdf. Acesso em: 8 abr. 2025.

OLX. **É seguro vender na OLX?** Veja nossas dicas de segurança. 2025c. Disponível em: https://dicas.olx.com.br/seguranca/e-seguro-vender-na-olx/. Acesso em: 8 abr. 2025.

OLX. **É seguro vender na OLX?. 2023a**. Disponível em: https://dicas.olx.com.br/seguranca/e-seguro-vender-na-olx. Acesso em: 15 abr. 2025.

PORTAL INSIGHTS. **Qual o modelo de negócio da OLX?** [S. l.], 2023. Disponível em: https://www.portalinsights.com.br/perguntas-frequentes/qual-o-modelo-de-negocio-da-olx. Acesso em: 8 abr. 2025.

REUTERS. **Falso vídeo de celebridade com promoção no Mercado Livre circula nas redes. 2024**. Disponível em: https://www.reuters.com/fact-check. Acesso em: 15 abr. 2025.

SECURITY BOULEVARD. **5 high-risk vulnerabilities in e-commerce applications. 11 nov. 2021**. Disponível em: https://securityboulevard.com/2021/11/5-high-risk-vulnerabilities-in-e-commerce-applications/. Acesso em: 8 abr. 2025.

SECURITY LEADERS. **87% dos consumidores sentem-se seguros ao fazer uma compra no e-commerce brasileiro. 2023**. Disponível em: https://securityleaders.com.br/87-dos-consumidores-sentem-se-seguros-ao-fazer-uma-compra-no-e-commerce-brasileiro. Acesso em: 05 abr. 2025.

SECURITYSCORECARD. **E-commerce Security Trends 2023**. New York: SecurityScorecard, 2023. Disponível em: https://securityscorecard.com. Acesso em: 09 jun. 2025.

SECURITY LEADERS. **Modalidades de phishing miram usuários do Mercado Livre. 2024**. Disponível em: https://securityleaders.com.br/modalidades-de-phishing-miram-usuarios-do-mercado-livre/. Acesso em: 4 jun. 2025.

SELLERSCOMMERCE. **Global E-commerce Statistics 2024**. Illinois: SellersCommerce, 2024. Disponível em: https://sellerscommerce.com. Acesso em: 09 jun. 2025.

SERASA EXPERIAN. **Fraude em e-commerce**: como evitá-la e proteger sua loja virtual. [S. l.]: Serasa Experian, 2023. Disponível em: https://www.serasaexperian.com.br/blog-pme/fraude-em-e-commerce/. Acesso em: 8 abr. 2025.

SU SOCIAL. **Typical security weaknesses in e-commerce platforms. [S. l.]**: SU Social, [s.d.]. Disponível em: https://susocial.com/typical-security-weaknesses-in-e-commerce-platforms/. Acesso em: 8 abr. 2025.

THALES GROUP. **2023 Thales Consumer Digital Trust Index. Paris**: Thales, 2023. Disponível em: https://www.thalesgroup.com. Acesso em: 09 jun. 2025.

TECMUNDO. **10 golpes comuns no Facebook Marketplace. 2024**. Disponível em: https://www.tecmundo.com.br/redes-sociais/243770-facebook-marketplace-conheca-10-golpes-comuns.htm. Acesso em: 15 abr. 2025.

TECNOBLOG. **Mercado Livre:** clientes denunciam fraude em contas criadas usando seus CPFs. 2024. Disponível em: https://tecnoblog.net/noticias/mercado-livre-clientes-denunciam-fraude-em-contas-criadas-usando-seus-cpfs/. Acesso em: 4 jun. 2025.

TERRA. **Site falso usa nome das Lojas Americanas para roubar dados de clientes. 2024.** Disponível em: https://www.terra.com.br/byte/site-falso-usa-nome-das-lojas-americanas-para-roubar-dados-de-clientes%2C74619a873fc5881de95dd637bf402385zyvawqxw.html. Acesso em: 4 jun. 2025.

TI INSIDE. **Autenticação é a chave para combater fraudes, afirma especialista. 29 dez. 2024**. Disponível em: https://tiinside.com.br/29/12/2024/autenticacao-e-a-chave-para-combater-fraudes-afirma-especialista/. Acesso em: 7 abr. 2025.

TRIBUNA. **A importância da LGPD**: aumento de 493% nos vazamentos de dados no Brasil. 2023. Disponível em: https://jornaltribuna.com.br/2023/09/a-importancia-da-lgpd-aumento-de-493-nos-vazamentos-de-dados-no-brasil. Acesso em: 10 abr. 2025.

TWILIO. **Prevenção de fraudes no e-commerce**: dicas, estratégias e práticas recomendadas. [S. l.]: Twilio, [s.d.]. Disponível em: https://www.twilio.com/pt-br/blog/ecommerce-fraud. Acesso em: 7 abr. 2025.

WESTPHALL, C. M.; RIGON, E. A. **Modelo de avaliação da maturidade da segurança da informação.** Revista eletrônica de sistemas de informação, v. 12, n. 1, 2013.