CÓDIGO 31

SEGURANÇA CIBERNÉTICA, UMA ANÁLISE DE INFRAESTRUTURA SEGURA PARA UM E-COMMERCE

CYBER SECURITY, AN ANALYSIS OF SECURE INFRASTRUCTURE FOR AN E-COMMERCE

Presleyson Plínio de Lima[1]
presleyson.lima@academico.domhelder.edu.br

Samuel Alves Da Mata Sá[2]
e00812@academico.domhelder.edu.br

Claudio Roberto Magalhães Pessoa[3]
claudio.pessoa@academico.domhelder.edu.br

DOI: 10.70493/cod31.v2i2.9617

Data de Submissão: 03/07/2023
Data de Aprovação: 20/12/2023

RESUMO

Introdução: Os avanços tecnológicos viabilizaram a competitividade e a necessidade de informações mais assertivas o mais rápido possível para que decisões sejam tomadas para diminuir o estrago causado. Um mundo diretamente conectado tem suas vantagens, ainda mais nos negócios, mais sem as devidas precauções no ambiente virtual pode se tornar um pesadelo para empresas e usuários, podendo ter problemas financeiros e um impacto negativo na imagem da empresa. Há uma grande discussão a respeito da globalização e da alta competitividade dos mercados, em que as empresas disputam a atenção do consumidor, e nesse sentido o espaço que a internet vem conquistando é algo que dificilmente retrocederá. O *e-commerce* trouxe novas perspectivas de trabalho, acesso à informação, desenvolvendo a comunicação entre empresas e profissionais, facilitando a distribuição de produtos e a disponibilização de bens e serviços, além do próprio processo comercial. Para o mercado de trabalho, essa dinâmica proporcionou novas oportunidades de crescimento e uma recolocação em um mercado que tende a se expandir devido sua atual evolução. Acredita-se que este trabalho contribuirá para os estudantes e jovens profissionais que estão ingressando no mercado e buscam uma oportunidade para iniciar suas carreiras. **Objetivos:** O objetivo geral deste estudo é analisar o crescimento do *e-commerce* nos últimos anos juntamente com a segurança cibernética. Já os objetivos específicos são: apresentar o contexto histórico do *e-commerce*; elencar os tipos de *e-commerce* e a sua relação com os *startups*; analisar o crescimento do *e-commerce* e o impacto com o mercado de trabalho; demonstrar os perigos dos ataques virtuais; descrever os tipos de ameaças virtuais; compreender o impacto dos crimes cibernéticos. **Metodologia:** O presente trabalho se baseia em uma revisão bibliográfica, de metodologia qualitativa, com foco no caráter subjetivo da bibliografia analisada, por uma pesquisa literária. **Resultados:** Assim os resultados da pesquisa evidenciam que, os perigos que se encontra no ambiente virtual e as ameaças virtuais, causam um o impacto no ambiente virtual, entre diversas reações no capital e nas receitas de empresas e até mesmo afeta o usuário comum, verifica-se que o *e-commerce* já vinha crescendo, mas espera-se que as pessoas entendam que mesmo com o fim da pandemia e a retomada das atividades de forma presencial ele não deve desacelerar. **Conclusão:** O medo de exposição ao vírus pode ter forçado alguns a aderirem às compras online, mas uma vez que se conhece essa facilidade, a tendência é que ela passe a ser cada vez mais utilizada.

Palavras-chave: segurança cibernética; tecnologia; *e-commerce*.

1 Escola Superior Dom Helder, Belo Horizonte, Brasil
https://orcid.org/0000-0002-6850-3638
Doutor em Sistemas de Informação e Comunicação e Gestão do Conhecimento

2 Dom Helder Escola Superior, Belo Horizonte, Brasil
https://orcid.org/0009-0001-8830-509X
Bacharel em Ciência da Computação

3 Dom Helder Escola Superior, Belo Horizonte, Brasil
https://orcid.org/0000-0002-9439-0382

ABSTRACT

Introduction: Technological advances have enabled competitiveness and the need for more assertive information as quickly as possible so that decisions can be made to reduce the damage caused. A directly connected world has its advantages, especially in business, but without proper precautions in the virtual environment it can become a nightmare for companies and users, leading to financial problems and a negative impact on the company's image. There is a great discussion about globalization and the high competitiveness of markets, in which companies compete for consumer attention, and in this sense the space that the internet has been conquering is something that is unlikely to recede. E-commerce has brought new perspectives of work, access to information, developing communication between companies and professionals, facilitating the distribution of products and the availability of goods and services, in addition to the commercial process itself. For the job market, this dynamic provided new opportunities for growth and a replacement in a market that tends to expand due to its current evolution. It is believed that this work will contribute to students and young professionals who are entering the market and looking for an opportunity to start their careers. Objectives: The general objective of this study is to analyze the growth of e-commerce in recent years together with cybersecurity. The specific objectives are: to present the historical context of e-commerce; list the types of e-commerce and their relationship with startups; analyze the growth of e-commerce and its impact on the job market; demonstrate the dangers of cyberattacks; describe the types of virtual threats; understand the impact of cybercrime. Methodology: This work is based on a bibliographic review, using qualitative methodology, focusing on the subjective character of the bibliography analyzed, through literary research. Results: Thus, the results of the research show that the dangers found in the virtual environment and virtual threats cause an impact on the virtual environment, among different reactions on the capital and revenues of companies and even affect the common user, verify It is believed that e-commerce was already growing, but it is expected that people understand that even with the end of the pandemic and the resumption of in-person activities, it should not slow down. Conclusion: The fear of exposure to the virus may have forced some to adopt online shopping, but once this facility is known, the tendency is for it to be used more and more.

Keywords: *cybersecurity; technology; e-commerce.*

1 INTRODUÇÃO

Contextualização da Segurança Cibernética tem uma grande importância na civilização moderna, já que vivemos onde praticamente tudo está on-line, com isso a proteção virtual e indispensável já que armazenamos atualmente dado potencialmente prejudicial para terceiros, a Segurança Cibernética visa proteger pessoas e empresas contra ataques, com o surgimento da indústria 4.0 e a internet das coisas, é fundamental garantir confidencialidade, integridade e disponibilidade dos dados, o objetivo da Segurança Cibernética e prevenir detectar possíveis ataques, que visam invadir, roubar, manipular e tornar indisponível os dados.

Se no passado as pessoas sentiam-se um pouco incomodadas e até desconfiadas em comprar produtos pela internet, hoje a realidade é completamente diferente. Ainda existem pessoas que preferem se deslocar até as lojas físicas, principalmente pessoas de mais idade, mas a verdade é que o *e-commerce* tem conquistado cada vez mais espaço na vida dos consumidores (Siqueira, 2008).

É fato também que a pandemia de Covid-19 acelerou essa realidade, pois as questões de saúde e medo do contágio, bem como a orientação de isolamento, fez com que a população passasse a utilizar o digital em peso. Estudiosos como Novaes *et al.* (2021) são categóricos ao afirmar que as mudanças trazidas pela pandemia irão continuar e mesmo com a retomada das atividades normais,

muita gente permanecerá comprando por meio de *marketplace*.

Sendo assim, as empresas devem estar atentas às necessidades e desejos dos clientes e se eles preferem efetuar suas compras online, é obrigação delas contar com uma plataforma de *e-commerce* bem estruturada que permita que a compra ocorra sem problemas, bem como com um sistema de logística ágil na entrega das mercadorias.

Cada vez mais a presença online é importante, e vem tomando o lugar do espaço físico. Desse modo, trabalhadores que temem por seus empregos, passam a empreender por necessidade[1], com poucos recursos e, muitas vezes, prestar serviços como o tão necessário *delivery* atualmente. Além disso, o meio digital surge com novas profissões e novas possibilidades de negócios, permitindo até empreender sem sair de casa.

Há um debate recorrente acerca da globalização e da alta competitividade dos mercados, em que as empresas disputam a atenção do consumidor e nesse sentido o espaço que a internet vem conquistando é algo que dificilmente retrocederá. Diversas pessoas que não acreditavam ser possível abrir um negócio com pouco dinheiro, ou mesmo trabalhar sem sair de casa aprenderam a utilizar a tecnologia para isso (Limeira, 2007). E o que vem acontecendo nos últimos anos tem desencadeado uma onda de empreendedores individuais e *startups* no mercado, além da geração de novos empregos no mercado de trabalho.

Diante esse contexto, é possível compreender o motivo pelo qual o *e-commerce* só cresce e diversas empresas estão optando pelo *marketplace*. Para sobreviver em um mundo globalizado e competitivo é preciso se adaptar e se adequar, caso contrário corre-se o risco de perder espaço e desaparecer por completo.

Assim, a justificativa da presente pesquisa é demonstrar o porquê precisamos nos preocupar com a Segurança Cibernética, quais os cuidados que devemos tomar em relação a ela e qual a preocupação que ela traz atualmente e destacar os motivos do crescimento do *e-commerce* no Brasil nos últimos anos, e como isso tem afetado a economia, essencialmente no que tange ao desenvolvimento do empreendedorismo, dos *startups*, e do crescimento do mercado de trabalho pelas novas tecnologias.

A importância dessa pesquisa é demonstrar o quão perigoso são os ataques cibernéticos, e o quanto é prejudicial atualmente, facilitará para que o leitor compreenda como é importante a segurança no ambiente virtual, sendo empresas ou usuários comuns. Essa pesquisa poderá contribuir para a comunidade acadêmica por meio de um levantamento de dados e questionamentos sobre o ambiente virtual atualmente, será capaz de ser fonte para futuras pesquisas, para sociedade, o estudo pretende mostrar de forma fácil os perigos virtuais e como minimizar possíveis ameaças.

Assim, importa destacar os motivos do crescimento do *e-commerce* no Brasil nos últimos anos, e como isso tem afetado a economia, essencialmente no que tange ao desenvolvimento do empreendedorismo, dos *startups*, e do crescimento do mercado de trabalho pelas novas tecnologias.

Como hipóteses, tem-se que: a tecnologia presente nos *smartphones* e a internet móvel facilita a busca por informações, referências e fornecedores de todo o tipo de produto e serviço; trabalhar com *e-commerce* é bastante vantajoso para empresas de todos os tamanhos, mas para empresas menores e em especial para o pequeno empreendedor as plataformas de *e-commerce* são soluções altamente viáveis em termos financeiros; e a pandemia do coronavírus a partir de

1 Empreender por necessidade se refere a um indivíduo que, diante da situação de desempregado, ou de incapacidade de exercer atividades que antes exercia, inicia um processo de empreendimento autônomo, como necessidade, a fim de gerar renda para si e sua família.

2019 causou mudanças drásticas na economia e na forma de consumir. De um lado está o consumidor, que evita ao máximo sair de casa com medo de ser contaminado pelo vírus. De outro, está a empresa, que precisa vender online ou não terá faturamento.

O problema da pesquisa foi baseado aonde ou qualquer lugar que você vá, qualquer coisa que você faça a internet está em torno de tudo, atualmente são mais de 4.3 bilhões de pessoas com acesso à internet, ainda que esse número seja impactante ele só tende a aumentar ao longo dos anos, com isso muitas pessoas e empresas estão expostos aos perigos da internet.

A presente pesquisa é construída sobre as seguintes questões: "De que forma o crescimento do *e-commerce* impacta no mercado de trabalho?"; "Por que a Segurança Cibernética é fundamental para a sociedade?"

O objetivo geral deste estudo é analisar o crescimento do *e-commerce* nos últimos anos juntamente com a segurança cibernética. Já os objetivos específicos são: apresentar o contexto histórico do *e-commerce*; elencar os tipos de *e-commerce* e a sua relação com os *startups*; analisar o crescimento do *e-commerce* e o impacto com o mercado de trabalho;

A tecnologia não para de evoluir, e hoje o mundo conta com modernos aparelhos celulares, os *smartphones*, computadores completos que cabem na palma da mão e permitem o acesso à internet em qualquer lugar. Já se tornou hábito abrir um site de busca para responder a uma dúvida do cotidiano, localizar um endereço ou encontrar o estabelecimento mais próximo para atender alguma necessidade. Hoje é algo perfeitamente corriqueiro recorrer à internet e às redes sociais no auxílio da tomada de decisão antes de comprar qualquer coisa, pois as pessoas buscam informações sobre a empresa, bem como a opinião de outros clientes.

Seguindo esse raciocínio, as empresas vêm se dando conta de que precisam se posicionar no meio digital, conquistar uma boa reputação e oferecer a possibilidade do *e-commerce* para os consumidores. A pandemia que o mundo vem enfrentando desde o final de 2019 só reforçou essa necessidade, pois mais do que nunca o consumidor deseja ser atendido do conforto de sua casa, em segurança.

Assim, o *e-commerce* tende a ter grande impacto sobre o mercado de trabalho, mudando a forma de atuação de algumas empresas. É provável que alguns postos de trabalho sejam fechados e algumas profissões deixem de existir, dando espaço a novas oportunidades e gerando um novo perfil de profissionais. Diante disso, o presente projeto busca compreender a extensão desse impacto no mercado de trabalho, abordando o crescimento do *e-commerce* nos últimos anos.

2 REFERENCIAL TEÓRICO

2.1 Os perigos dos ataques virtuais

Um mundo diretamente conectado tem suas vantagens, ainda mais nos negócios, mais sem as devidas precauções no ambiente virtual pode se tornar um pesadelo para empresas e usuários, podendo ter problemas financeiros e um impacto negativo na imagem da empresa, sem um monitoramento a infraestrutura de uma empresa poderá ser comprometida, se não houver uma checagem periódica, fica impossível saber as brechas de segurança das aplicações e quais são elas, conhecer os riscos que sua empresa pode estar correndo e fundamental para a manutenção e correção das brechas (Rocha, 2021).

Os perigos que se tem no século XXI vem aumentando drasticamente, os criminosos virtuais roubam e vendem informações de usuários no mercado negro, isso se torna um caminho fácil para roubo de identidade, que tem como princípio se passar pela pessoa para obter informações e ter acesso à alguma área específica, podendo até mesmo usar essas informações para abrir contas de empréstimo é cartão de crédito (Kaspersky, 2022).

No século XXI, o roubo a bancos passou a ser digital, um exemplo é o malware chamado "Carbanak", segundo a Kaspersky (2022) ele durou cerca de 2 anos, atingindo diversas instituições financeiras em todo o mundo, os criminosos enviaram e-mails para funcionários e gerentes dos bancos com o malware "Carbanak", após conseguir infectar os dispositivos os criminosos simularam o comportamento dos funcionários de transferir dinheiro, porém para si, instruíam caixas eletrônicos para liberar dinheiro em horários específicos e usar de sistemas de pagamento eletrônico para receber o dinheiro:

> Muitas empresas caem na armadilha de pensar que elas não possuem informações que poderiam ser de qualquer valor a um cibercriminoso. Além disso, o fundador pode acreditar que um incidente de perda de informações não causaria qualquer grande prejuízo para sua empresa (Gilmore, 2014, p. 23).

A legislação de alguns países pode punir severamente empresas que não protegem dados sigilosos de seus clientes, levando multa e até mesmo prisão aos diretores e proprietário, por isso e importante a proteção de dados sensíveis para que eles não sejam vazados ou vendidos no mercado negro, que podem causar danos a terceiros caso os dados sejam expostos (Gilmore, 2014).

Com a chegada das criptomoedas aumentou-se o potencial de retorno de um cibercriminoso, aumentando significativamente a capacidade de ganhar dinheiro e se esconder em meio a internet, antes das criptomoedas os criminosos estavam sujeitos a serem pegos já que era um desafio retirar o dinheiro de atos ilegais, já que a conta do qual era retirada poderia estar ligada diretamente a eles facilitando a busca e apreensão dos criminosos, a criptomoeda praticamente eliminou esses riscos (Steinberg, 2020).

A maioria das pessoas sabe quais os tipos de vírus que podem infectá-los, dos quais um ficou bem famoso nos anos 2000, o famoso cavalo de Troia, quem nunca foi infectado ou não conheça alguém que foi, e praticamente impossível mensurar a quantidade de vírus atualmente, conhecer as possíveis ameaças e benéfico para não ter dor de cabeça ao navegar na web (Barro, 2022):

> Malware e ameaças de segurança de TI podem ter um efeito prejudicial sobre qualquer negócio. Para as empresas menores, os resultados podem ser fatais. Ao mesmo tempo, em que a lista a seguir não é uma lista exaustiva de todos os tipos de ameaças, esta seção dá uma indicação de alguns dos riscos de segurança que as empresas têm de enfrentar... (Gilmore, 2014, p. 40).

Atualmente os criminosos criam sites que imitam sites de bancos e lojas, com o quase infinito nomes de domínios podem induzir pessoas a acreditar que se trata de um site legítimo, esse tipo de cibercrime é caracterizado como Phishing que se trata de coletar os dados de uma pessoa, de modo a fazer transferências bancárias ou até mesmo obter o número de cartão e dados da identidade da vítima (Gilmore, 2014).

Com isso em mente deve-se prevenir e conhecer possíveis vulnerabilidades tanto pessoal como empresarial, pois um dispositivo pessoal infectado, pode também infectar a empresa do

qual trabalha, até mesmo o uso de WI-FI público pode ter riscos, com crescimento da internet é indispensável que hotéis, aeroportos e shoppings oferecem WI-FI público, com o acesso gratuito e fácil verificar e-mails e acessar informações de negócios quando está fora do ambiente de trabalho, de acordo com Gilmore (2014), também é fácil para cibercriminosos invadem redes públicas para capturar informações que você acessa ou envia, isso significa que podem ter acesso a senhas e números de cartão de crédito.

Em um mundo onde as Ameaças Virtuais evoluem continuamente, o que se deve fazer para se proteger? Para a Kaspersky (2022), deve se ter a consciência que a primeira linha de defesa são ferramentas de segurança, mas é necessário usar o bom senso, pois o usuário e a principal defesa, não se deve proteger só o dispositivo, mas as principais etapas de precaução contra vulnerabilidades são: usar senhas fortes para suas contas, incluindo números, letras maiúsculas e minúsculas, e que sejam difíceis de adivinhar, não abrir e-mails suspeitos, principalmente que pede para inserção de dados sigilosos, deve apagar ou destruir arquivos que contém informações potencialmente sigilosas, usar VPN para proteger sua conexão com a internet, caso precise de utilizar um WI-FI pública, sempre manter os aplicativos e dispositivos atualizados.

Conforme as Forças Armadas (Brasil, 2007), Segurança Cibernética é o conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente, uma perspectiva humana existem diversos riscos que a Segurança Cibernética aborda, um dos riscos e o da privacidade ocorre quando há perda indevida e sem controle dos dados sigilosos, podendo trazer prejuízos pessoais comerciais ou profissional.

Dos prejuízos mencionados deve se saber dos riscos, para profissionais e para sua carreira, para Steinberg (2020), executivos podem ser processados ou demitidos de seus cargos, se o hacker liberar informações ou dados sigilosos pode ter prejuízos pessoais também, os riscos comerciais são semelhantes aos profissionais para um indivíduo, documentos internos da Sony Pictures foram vazados em relação a algumas de suas práticas de compensação, foi visto de maneira negativa pelos seus consumidores, muitas pessoas armazenam informações privadas em seus dispositivos eletrônicos, como fotos explícitas ou registros de participação em atividades que podem ser vistas negativamente as pessoas da família ou respectivos círculos sociais, às vezes esses dados podem causar danos significativos em seu relacionamento pessoal, podem também ajudar a fraudar a identidade das pessoas, o que resulta em todos os tipos de problemas pessoais.

Existem medidas a serem tomadas em um ambiente empresarial em relação à Segurança Cibernética, de acordo com Marcondes (2021), as principais medidas para combater ataques cibernéticos são:

- Obter determinado desenvolvimento quanto a implementação de uma Política de Segurança da Informação adequada às necessidades da organização;
- Inserir um Investimento em pessoal especializado e recursos relacionados à Segurança Cibernética;
- Elaborar de um Plano de Gestão da Segurança Cibernética adequado às necessidades da empresa;
- Investir em um programa de educação e conscientização dos colaboradores sobre boas práticas de Segurança Cibernética;
- Estabelecer boas práticas na gestão dos ativos de informações da empresa.
- Prever ações orçamentárias adequadas às necessidades de segurança da organização,

que deve ser dimensionada mediante análise de riscos adequadas.

Assim como tem a Segurança Cibernética existe a segurança da informação e o que é ela afinal, de acordo com Marcondes (2021), a segurança da informação trata de proteger os dados e informações considerados sensíveis pela organização, sejam eles físicos ou digitais, a segurança da informação tem conotação mais ampla, ela envolve proteção de dados e suas formações possíveis, que podem estar contidas em meios eletrônicos ou até mesmo físicos como papel, a diferença entre segurança da informação e Segurança Cibernética pode ser identificada através do objetivo e espaço de atuação de cada uma delas, enquanto a segurança da informação tem o objetivo de preservar a informação dos dados, a Segurança Cibernética tem o objetivo de preservar os dados no formato digital, podemos dizer que a Segurança Cibernética está inserida dentro da segurança da informação.

Figura 1 – Forma de inserção da segurança cibernética

Fonte: Marcondes (2021), adaptado de ISO/IEC 27032 (2012)

Existem muitos tipos de ataques cibernéticos dos quais será mencionado no próximo capítulo, aqui vai um exemplo de uma Ameaça Virtual, ataque de negação de serviço (DoS), segundo Steinberg (2020) o ataque de negação de serviço e o ataque que o invasor tenta travar um computador ou uma rede de computadores para paralisá-la, inundando com solicitações de serviço até que o tráfego não possa ser processado resultando em negação de serviços para usuários, em qualquer ataque de negação de serviço funcionam sobrecarregando as unidades de processamento (CPU).

2.1.1 *Os tipos de ameaças virtuais*

Existem diversos tipos de ameaças que se enquadram em ataques cibernéticos, normalmente são tentativas dos hackers de penetrar dentro de redes e sistemas a fim de causar danos ou roubar informações, esses indivíduos podem estar em 2 grupos ativo ou passivo, no passivo o indivíduo possivelmente é um estudante iniciando na área, no qual acessa o sistema mais não compromete dados ou recursos, já no ativo o indivíduo está disposto a tudo para causar danos, afetando operação e integridade dos dados, até mesmo falsificando e-mails, como exemplo podemos citar o *ransomware* (Rocha, 2021).

A ameaça mais conhecida e o Cavalo de Tróia, de acordo com o site Brasil Paralelo (2021), "o cavalo de Troia é um símbolo de Guerra, uma estratégia decisiva utilizada pelos gregos para derrotar seus inimigos. Na história contada por Homero, autor da Grécia antiga, Troia estava cercada há 10 anos, contudo, não era derrotada. Como suas muralhas eram intransponíveis, os gregos usaram da estratégia que entraria para a história.", mais o que a história tem a ver com um vírus digital?

Bom esse truque ficou conhecido como brilhante e magistral, hoje é sinônimo de uma praga digital maliciosa, sendo o objetivo desse vírus causar danos nos computadores das vítimas sem serem notados, daí vem o nome Cavalo de Troia, as ações podem incluir exclusão de dados, bloqueio de dados, modificar dados e comprometer

o desempenho de computadores e redes (Kaspersky, 2022).

Existem diversos tipos de *trojan* (Cavalo de Troia), *trojan ransom, trojam backdoor*, *trojan* de falso antivírus e *trojan dropper* entre outros, trojan do tipo *backdoor*, são os mais simples, mais e potencialmente o mais perigoso dos *trojans*, segundo a Kaspersky (2022), *trojan* de *backdoor* pode carregar todo tipo de *malware* (software malicioso) para o sistema, agindo como um *gateway* (portal), *backdoor* é frequentemente utilizado para configurar *botnets* (robô de rede), sem que o usuário saiba ele está se tornando parte de uma rede zumbi, usada para ataques, além de permitir que códigos sejam executados no dispositivo ou até o monitoramento de tráfego de rede na internet.

Cavalo de Troia do tipo *dropper* diferente do tipo *backdoor*, ele não pode executar nenhum código, ele é projetado para instalar secretamente programas maliciosos na máquina da vítima ou até mesmo vírus que protejam programas maliciosos, nem todos os antivírus são capazes de detectar todos os arquivos presente dentro desse tipo de trojan (Kaspersky, 2022).

Ataque (DDoS) conhecido como Ataque Distribuído de Negação de Serviço, para Steinberg (2020), um ataque (DDos) e uma distribuição de negação de serviço, e um tipo de (DoS) no qual a uma rede de computadores interligadas em diferentes regiões, do qual inundam simultaneamente a rede alvo com solicitações de serviço, normalmente esses computadores não são do atacante e sim um zumbi conectado à rede, os usuários de computadores nem sabem que estão sendo utilizado para isso, pois ele deve ter sido infectado com um trojan e nem sabe do ocorrido, por isso é difícil para investigadores acharem o hackers, pois os ataques não vem diretamente deles. A Figura 2 demonstra o funcionamento de um ataque DdoS.

Figura 2 - Funcionamento de um ataque DdoS

Fonte: Steinberg (2020)

O objetivo desse tipo de ataque e deixar a vítima offline, a motivação pode variar sendo financeiro ou por "justiça", uma loja ou empresa pode ser prejudicada para um fim objetivo do hacker, sendo deixar sites concorrentes offline afim de ganhar com a queda de ações da empresa concorrente e aumento na empresa onde o hacker tem ações na bolsa de valores, assim como existem hacktivistas que usam esse tipo de ataque para derrubar sites do governo em nome da "justiça", essa aplicação vem após alguém ser desarmado ou morto pela polícia (Steinberg, 2020).

Às vezes um ataque (DDoS) pode deixar a conexão tão lenta que as operações se encerram, após o sistema verificar que as solicitações ultrapassam o tempo limite de espera assim derrubando-o, como mencionado os ataques (DDoS) se utilizam de *botnets* (robô de rede) e zumbis, para Steinberg (2020), os ataques (DDoS) utiliza se o que conhecido como *botnets*, um aglomerado de computadores infectados com *malware* que pertencem a terceiros.

Phishing é uma técnica direcionando para alguém um link malicioso, vem do termo utilizado nos anos 90 e uma alteração do nome *fishing* (pescaria em inglês), o *phishing* tem como objetivo coletar os dados da vítima, a vítima pode receber um e-mail dizendo para ela redefinir a senha ou o usuário do banco, ao abrir o link é direcionado a um site clone do banco em questão, podendo se passar pelo banco original a vítima coloca seus dados pessoais, e o hacker acaba podendo roubar dinheiro da sua conta bancária ou até mesmo podendo ter o número do cartão de crédito (Gilmore, 2014).

Para se proteger do *phishing* é preciso ter um bom senso ao usar a internet, deve se pensar bem antes de inserir informações, até mesmo em sites que se pareçam confiáveis, já que é possível clonar a aparência do site e ludibriar o usuário comum, deve se ficar atento a URL do site, para verificar se o site e verdadeiro, outro indicador e erro de digitação e o site não parecer profissional, como são criados com uma devida pressa muitos destes podem ser significativamente diferentes do original (Kaspersky, 2022).

O Brasil e o país mais atingido por phishing, de acordo com um levantamento de dados da Kaspersky em 2022, segundo esses dados a porcentagem de brasileiros que tentou abrir pelo menos uma vez esses links enviados e de 19,9%, em segundo lugar vem Portugal (19,7%), seguido da França (17,9%), Tunísia (17,6%), Camarões (17,3%) e da Venezuela (16,8%), esses golpes foram aplicados por meio de links que se passam por empresas grandes e conhecidas, como a Amazon e entre outras empresas. A Figura 3 ilustra a tentativa de *phishing*.

Figura 3 - Tentativa de phishing

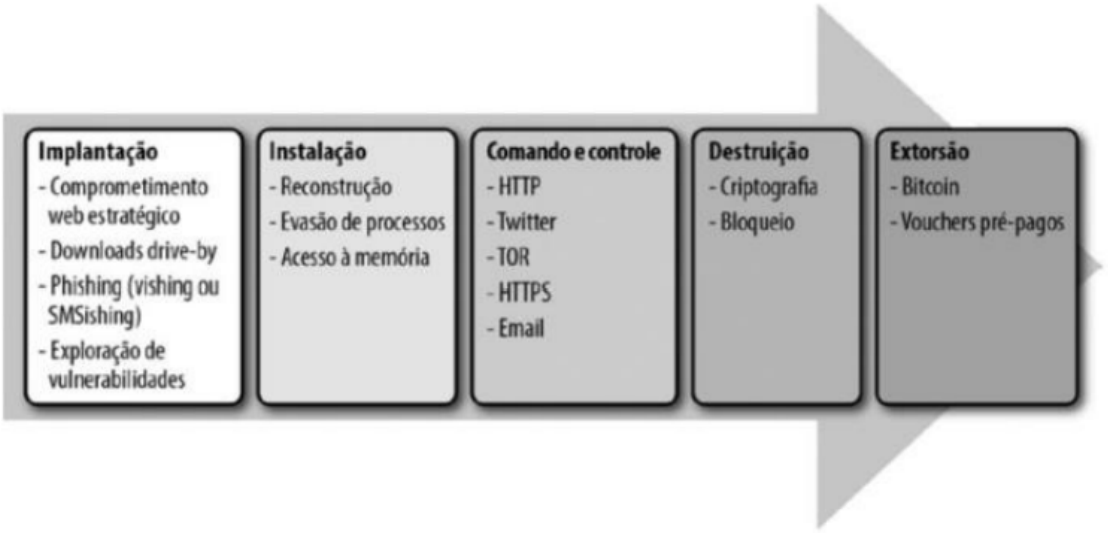
Fonte: Hostinger (2022).

Phishing não tem prazo para acabar já que se baseia no bom senso das pessoas, e fácil criar e divulgar essa tentativa, muitas pessoas não sabem desses ataques, e para outras pode parecer bem óbvio as pistas deixadas por quem criou, e por isso que se deve aprender sobre mesmo que seja pouco, é preciso educar pessoas que são novas em ambientes virtuais, para que não caia nesse tipo de armadilha digital (Steinberg, 2020).

Malware (*software* malicioso), e bem abrangente quando se fala em *softwares* mal intencionados, normalmente não se tem ideia de que está infectado, e que estão executando algo em sua máquina, esse termo engloba vírus, *Worms*, Cavalos de Tróia, *ransomware, scareware*, *spyware, adware* dentre outros softwares maliciosos, o vírus de computador ele quando é executado se replica, executando e inserindo o próprio código nos computadores, já *Worms* são peças de *malware* independentes, que se propagam pela conexão, afetando a segurança dos computadores conectados na rede, pode causar danos ao sistema ou até mesmo roubar dados (Steinberg, 2020).

Ransomware em sua essência é uma forma de extorsão, pode ser subdivididas conforme suas respectivas famílias representativas, as principais formas de *ransomware*, são aquelas que restringem ou bloqueiam o acesso dos usuários nos dispositivos, o método para desbloqueio dos dados, e pago e em sua maioria por criptomoeda geralmente Bitcoin, mais esse não é o único método para desbloqueio, alguns serviços de voucher pré-pagos, atualmente o *ransomware* é considerado uma das formas predominantes de ataque contra sistemas de computadores, estima-se que uma das variantes mais conhecidas foi o *CryptoWall* (atualmente extinto), ele foi capaz de extorquir cerca de 18 milhões de dólares até meados de julho de 2015 (Liska; Gallo, 2017). A figura 4 mostra a anatomia básica de um *ransomware*.

Figura 4 - Anatomia de um ataque ransomware



Fonte: Liska; Gallo (2017).

A primeira fase de um ataque de *ransomware* é a instalação dos componentes necessários para infectar a máquina, para se proteger existem métodos específicos, usar uma proteção de navegador, nunca clicar em links inseguros em mensagens de spam ou em sites desconhecidos, se caso clicar em algum link o download automático pode ser iniciado, levando a infecção do seu computador, evite

divulgação de informações pessoais, já que pode ser montado mensagens de *phishing* especificamente para você, não abrir e-mails suspeitos, sempre se deve verificar o remetente antes de tomar qualquer ação, não utilizar pendrives ou USB desconhecidos, pessoas maliciosas podem infectar seu dispositivo em locais públicos, ou até mesmo ser infectado por um amigo, que não sabe que o pendrive está infectado, passando para várias máquinas sem sequer saber, usar VPN em redes públicas, o uso consciente do WI-FI público é uma medida de proteção contra os *ransomware* (Liska; Gallo, 2017)

2.2 *E-commerce*

O advento da internet trouxe consigo uma revolução em diversas áreas de nossas vidas, dentre elas uma nova maneira de comprar e vender produtos e serviços, o *e-commerce*. Seu início está datado entre os anos 1995 e 2000, mas sua consolidação só ocorreu por volta de 2007 devido o maior acesso da população a aparelhos eletrônicos que proporcionaram uma maior inclusão digital, de acordo com Laudon e Traver (2017).

Segundo publicação do Ministério da Saúde (2020) a covid-19 é uma infecção respiratória que é causada pelo vírus SARS-CoV-2 e potencialmente grave pois tem uma elevada transmissibilidade e pode gerar complicações, levando ao óbito.

Devido à sua alta taxa de transmissão, uma das maiores recomendações desde a descoberta do vírus em dezembro de 2019 foi o distanciamento social. Assim, durante o ano de 2020 e ainda em 2021, as lojas físicas e outros estabelecimentos, ou buscaram formas alternativas de venda para manter o negócio ou encerraram o atendimento. Onde, o e-commercese destacou como sendo a principal alternativa tanto de compra como de venda.

Nesse sentido, considerando conjuntamente a rápida expansão dessa modalidade de venda e quanto aos cuidados demandados pela pandemia, torna-se cada vez mais importante o conhecimento do comportamento do consumidor. Neste cenário, Salgado (2019) apontam que o marketing 4.0 é uma ferramenta fundamental para o desenvolvimento do comércio via internet. Os autores ainda definem o marketing 4.0 como sendo mais horizontal, incluso e social, por conta da significativa influência trazida pelas mídias digitais, já que atualmente a informação está a um clique.

Segundo e Salgado (2019) o *e-commerce* possibilita se ter um ambiente favorável a essa horizontalização integrando fornecedores, varejistas, distribuidores e clientes em um único lugar, uma vez que a internet facilita o rápido acesso a diversas informações e aproxima pessoas tornando cada vez mais simples essa integração de todos os pontos.

Contudo, devido a toda essa agilidade e visibilidade que a tecnologia proporciona, o e-commerce tem como principal desafio ser cada vez mais transparente, competitivo e atencioso, proporcionando um ambiente confiável e que supere as expectativas de seus consumidores.

2.2.1 *O crescimento do e-commerce nos últimos 10 anos*

O aumento significativo no número de vendas reflete o aumento no número de pedidos, a exemplo do Mercado Livre, que ganhou 2,5 milhões de novos compradores em 2020. Como a pandemia segue em 2021, imagina-se que esse índice continue crescendo, aponta Novaes (2021). Na opinião do autor, as compras via celular irão dominar esse mercado, e muitas lojas que ainda não otimizaram o seu site para o dispositivo móvel estão perdendo dinheiro.

O resultado da presença digital das empresas tem sido tão grande que tende a crescer ainda mais nos próximos anos. Para Tomé (2018, p. 1), "mesmo em períodos de instabilidade, o comércio eletrônico vem apresentando crescimento, na contramão da crise". O *e-commerce* busca se adaptar às necessidades dos consumidores em diferentes setores para atender a grande demanda, e com isso seu crescimento é inevitável. O Código de Defesa do Consumidor e o Decreto n.º 7962/2013 regulamentam as transações comerciais em ambiente eletrônico e regem essas relações de negócios virtuais.

Lemos e Góes (2015) explicam sobre o funcionamento desse mercado no Brasil: produtos são expostos em um site, o pagamento do pedido é feito online e as mercadorias são entregues no endereço cadastrado. Contudo, para ocorrer esse processo do início ao fim, existem ações como o planejamento de marketing, atendimento ao consumidor, logística e pós-venda. Ainda, os autores comparam as páginas com vitrines de um shopping, em que são disponibilizadas fotos e especificações técnicas dos produtos, além do preço.

Após a escolha dos produtos, o consumidor deve seguir para a etapa do pagamento em que ele faz um breve cadastro e fornece informações básicas e endereço para entrega. Pode ou não haver a cobrança de frete, e então com o valor final calculado, escolhe-se a forma de pagamento, sendo mais comum utilizar um cartão de crédito ou boleto. Após confirmado o pagamento, basta aguardar que a mercadoria seja entregue no local indicado (Lemos; Góes, 2015).

Na opinião de Soares *et al.* (2015), a evolução do comércio eletrônico no Brasil exige das empresas que elas se reestruturem de modo a atender essa demanda com agilidade. Para os autores, não é possível atualmente que uma empresa se mantenha competitiva sem atuar no comércio eletrônico, pois por mais que ainda haja uma pessoa ou outra com receio de comprar pela internet e que prefira se deslocar fisicamente, esse número fica menor a cada dia. Ainda, o e-commerce tem o potencial de gerar mais vendas para as empresas, e mais facilidade para os consumidores.

Contudo, esse medo por parte de alguns consumidores e a resistência às compras eletrônicas ainda é uma realidade, afirmam Azevedo, Odone e Coelho (2014). A resistência às compras se dá principalmente pela insegurança de fornecer seus dados pessoais, endereço e cartão de crédito, diante de tantos golpes e crimes cibernéticos noticiados com mais frequência nos últimos 10 anos, há uma insegurança de comprar o produto e não o recebê-lo e do compartilhamento dos seus dados pessoais e financeiros. Essa resistência advém principalmente dos indivíduos com mais de 40 anos, um público que ainda desconfia do comércio eletrônico, segundo a pesquisa de Azevedo, Odone e Coelho (2014).

Ainda, na visão dos autores, esse é um desafio que as empresas precisam superar, sendo capazes de oferecer um ambiente virtual seguro para seus clientes, e meios de comprovar a sua veracidade como empresa virtual (como certificado de segurança dos sites e instruções de verificação do site original), de modo que eles tenham acesso aos produtos e serviços que chegam simultaneamente em alta velocidade pelo mundo.

Como explica Guerreiro (2006), a internet proporcionou tudo isso, ela é a grande responsável, e juntamente com o avanço da tecnologia, possibilita que as empresas trabalhem com maior flexibilidade e eficiência, aproximando-as de seus fornecedores e tornando-as mais ágeis em atender às demandas dos consumidores. Sem dúvida, o comércio eletrônico é algo que veio para ficar, revolucionado as transações de compra e venda no mundo todo, tornando o processo mais confortável, rápido e com menor custo.

Teixeira Filho (2001) destaca que as organizações utilizam cada vez mais a internet como infraestrutura para realizar seus negócios, se favorecendo do *e-commerce* e compreendendo a importância dele para seu sucesso e crescimento no mercado. Vieira (2003) afirma que o comércio eletrônico possibilita negócios que no passado não eram nem pensados, e que todas as empresas precisam aderir, mesmo as menores ou de administração familiar. É fundamental vencer essa resistência ou o resultado será a perda de espaço no mercado.

No entendimento de Siqueira (2008), o comércio eletrônico, de maneira geral, apresenta algumas características importantes, tais como a comunicação (existe a troca de informações à distância entre o fornecedor e o consumidor); os dados (deve haver o gerenciamento das informações dos clientes de modo a manter a base de dados); a segurança (esta é a mais importante de todas as características que um *e-commerce* precisa ter, pois a empresa deve ser capaz de garantir a privacidade das informações transmitidas a ela no momento da transação. O cliente precisa ter a certeza de que seus dados não serão utilizados para outros fins ou repassados a terceiros).

Nas palavras de Albertin (2000, p. 100), "o comércio eletrônico no mercado brasileiro está consolidado e apresenta claros sinais de evolução, mesmo que ainda possa ser considerado em um estágio intermediário de expansão". Para que as organizações consigam se manter competitivas no mercado, elas precisam ter um diferencial, apresentar novidades constantemente, ou pelo menos, não se manter atrasadas quanto às novas tecnologias em relação às suas concorrentes. Seguindo esse raciocínio, é de se esperar que o comércio eletrônico no Brasil ainda cresça muito, aproximando-se da realidade dos países desenvolvidos.

Limeira (2007) considera importante acrescentar que o próprio perfil do consumidor também mudou com o passar dos anos e acredita que a geração de pessoas mais engajada na internet e nas compras online se deve a dois fatores principais: a conveniência e facilidade que a compra online oferece, e a economia de recursos, já que a internet apresenta uma gama de opções de um mesmo produto com grande diferença de preço, dependendo do fornecedor, mas consideravelmente menor do que o preço praticado na loja física.

É claro que atualmente leva-se em conta a pandemia, sendo que alguns consumidores têm tanto medo do contágio que se sentiram praticamente obrigados a aderir ao comércio eletrônico, mas mesmo antes da pandemia espaço do *e-commerce* já vinha sendo conquistado, aponta Ratten (2020). As populações dos grandes centros urbanos estão sempre correndo contra o tempo para dar conta de tantos afazeres, sendo assim, a possibilidade da economia de tempo é algo valorizado por essa parcela da população.

Já para os habitantes de cidades pequenas, é comum que não exista grande variedade de produtos nas lojas físicas, ou diferentes faixas de preço. Nestes casos, contar com o comércio eletrônico abre um leque de possibilidades, em que o consumidor tem um número muito maior de opções e também de preços, destaca Speranza (2012). Para Rosa (2007), há que se considerar também que a população brasileira em sua maioria não dispõe de muitos recursos financeiros, aí o comércio eletrônico frequentemente leva vantagem com seus preços mais baixos e seus fretes gratuitos.

Diversos autores corroboram com a ideia de que os processos eletrônicos de compra têm muito a agregar na vida de todo mundo, desde a rapidez na transação, a flexibilidade e a eficiência do processo, o alcance de grandes massas que sem a internet jamais seria possível, redução nos custos de venda e distribuição. É inesgotável a fonte de informações que o consumidor passa a ter, podendo comparar de forma rápida e fácil os

preços, os prazos de entrega, a qualidade entre o produto de uma empresa e o de sua concorrente, vantagens, desvantagens, rede de assistência técnica, entre outros fatores. E o benefício para o consumidor vai além, pois as empresas têm que se esforçar muito mais hoje em dia para entregar bons produtos e serviços (Herzer, 2013).

3 METODOLOGIA

O presente trabalho se baseia em uma revisão bibliográfica, de metodologia qualitativa, com foco no caráter subjetivo da bibliografia analisada, por uma pesquisa literária. Ressalta-se que o estudo foi delimitado com foco na temática, selecionando livros, publicações periódicas (jornais e revistas, impressas ou virtuais), artigos científicos e trabalhos acadêmicos.

A busca na literatura se deu por materiais publicados nos últimos 15 anos, embora também tenha sido selecionado materiais com datas posteriores em razão de conceituação de termos e de contexto histórico do assunto, em português e inglês, online, gratuitos e completos, através das palavras-chave: Segurança Cibernética. Tecnologia. *E-commerce*., nos bancos de dados do Google Scholar, Google Books e SCIELO, juntamente com alguns principais autores, nesta pesquisa são: Gilmore (2014); Steinberg (2020); Kaspersky (2022); Marcondes (2021); Forças Armadas (Brasil, 2007); Liska e Gallo (2017); Kovacs (2005); McAfee (2017); Barro (2022).

4 RESULTADOS E DISCUSSÃO

Com tantas mudanças na tecnologia e no mercado de trabalho, espera-se que as oportunidades mudem, assim como mudou o perfil do profissional e dos gestores. No passado, empreender era pra normalmente para quem já tinha posses, pois iniciar um negócio demandava grandes montantes. As pessoas de origem de classes sociais mais humildes conformavam-se em trabalhar para alguém, e ter o próprio negócio não passava de um sonho muito distante e praticamente inalcançável (Marthe; Betti, 2012).

Com o crescimento do *e-commerce* o mercado de trabalho também cresceu. A possibilidade de negociar através da internet abriu ainda mais as portas para novas oportunidades de trabalho, aumentando a competitividade e criando até mesmo novas profissões. O ambiente virtual já é visto como um mercado de trabalho online, uma vez que tem a capacidade de criar conexões entre empregadores e trabalhadores. "O mercado de empregos on-line é especialmente atuante na área de tecnologia, porque as empresas e os trabalhadores interessados utilizam a internet regularmente. Contudo, há milhares de tipos de empresas que anunciam cargos disponíveis". (Turban; King, 2004, p. 84).

Conforme destacam Cardoso e Araújo (2013), o mercado de trabalho de alguns anos atrás estava dividido entre empregadores e empregados, mais especificamente entre aqueles com recursos para abrir uma empresa e gerar empregos e aqueles que precisavam de uma vaga de trabalho. No entanto, hoje se pode afirmar que a internet mudou essa realidade e revolucionou o mercado de trabalho.

O *e-commerce* trouxe consigo novas perspectivas de trabalho, melhorando a comunicação entre os agentes envolvidos, facilitando a distribuição de produtos e a disponibilização de bens e serviços, acesso à informação, além do próprio processo comercial. Para o mercado de trabalho, essa dinâmica proporcionou novas oportunidades, inclusive a possibilidade do home-office (escritório em casa), que é uma modalidade de trabalho sem a necessidade de se deslocar até a empresa fisicamente, uma das muitas vantagens da era digital, sendo o comércio eletrônico a ferramenta que

mais propicia isso, pois é o que efetivamente gera a renda e o lucro das empresas e colaboradores.

Com a revolução do digital, empreender se tornou uma realidade possível para praticamente qualquer pessoa que possua internet e um dispositivo como computador ou celular. O comércio eletrônico é apenas uma das diversas alternativas para quem deseja iniciar um negócio gastando pouco, pois para qualquer pessoa é possível montar uma loja online e despachar a mercadoria para qualquer lugar do Brasil, afirma Almeida (2005).

Ser dono do próprio negócio é um sonho para muita gente, muitos inclusive cursam Administração visando a capacitação para gerir o negócio da família ou o negócio que ainda pretendem abrir. É fato que uma grande parcela da população não está satisfeita em trabalhar para alguém e sonha dar adeus ao chefe e ao registro de ponto, conseguindo fazer dinheiro de maneira independente. E a internet e o meio digital oferecem esse espaço praticamente gratuito para as pessoas mostrarem seus produtos e serviços e serem capazes de assim gerar renda (Garcia, 2008).

Desde o final de 2019 o mundo trava uma batalha contra a COVID-19. O ano de 2020 foi extremamente difícil e desafiador para muitas pessoas, especialmente para muitos brasileiros que muito rapidamente se viram desempregados e sem uma fonte de renda para prover o sustento de suas famílias. Muitos empresários também tiveram que fechar as portas e encerrar as atividades, colocando milhares de trabalhadores nas ruas.

A pandemia mudou a realidade de diversas pessoas, que se viram sem emprego, sem renda fixa e tiveram que buscar diferentes alternativas. Observando a dificuldade de conseguir uma colocação profissional neste momento, mesmo para as pessoas mais qualificadas, e com anos de experiência, muitas pessoas começam a empreender devido à necessidade. E se de um lado as portas do comércio físico estão se fechando, as portas do eletrônico vêm com novas oportunidades todos os dias, afirmam Tobler e Bittencourt (2020).

A solução para sair da dificuldade financeira pode ser, sim, empreender, mas ressalta-se que o empreendedorismo deve vir acompanhado de planejamento, essencialmente financeiro, essa percepção muita das vezes é desconhecida, principalmente por aqueles que empreendem por necessidade. Apesar da crise, sabe-se que alguns segmentos não pararam de ganhar dinheiro, apenas desaceleraram um pouco. Então, a solução é estudar e pesquisar, identificar uma oportunidade no bairro, na cidade, de um produto ou serviço que apresenta demanda e investir nisso. Recomenda-se pesquisar o mercado e estudar os concorrentes, os preços praticados por eles, o que eles têm de bom e em que são insuficientes (Bessant; Tidd, 2009).

Logo, constata-se que o *e-commerce* contribui para novas oportunidades no mercado de trabalho, gerando emprego, renda e viabilizando novos caminhos de crescimento profissional.

E o principal, para qualquer negócio, é a presença digital. Seguindo esse raciocínio, pode-se compreender como o comércio eletrônico movimentou o mercado de trabalho, e continua oferecendo oportunidades mesmo durante a pandemia e a crise econômica. Ainda, se não fosse pela possibilidade de empreender online, muito mais pessoas estariam fora do mercado de trabalho atualmente, comenta Marino (2020).

Sendo assim, o mercado eletrônico encontra-se em fase de crescimento, impulsionado pela tecnologia e a popularidade da internet, gerando renda e oportunidades de negócios para os mais diferentes profissionais. Todor (2016) acrescenta que com o conhecimento de marketing que se tem hoje, é muito mais fácil conseguir resultados com o comércio eletrônico, pois o empreendedor tem

aprendido a falar sobre seu produto para o público certo, aquele que está realmente interessado.

Sobre isso, ressalta-se a estratégia de marketing através dos algoritmos[2] que registram a temporalidade (uso da internet e horários), engajamento (comentários, curtidas, determinados usuários de influência), e relacionamento (contas com as quais o usuário mais engaja) dos seus usuários, a fim de criar anúncios pagos e direcionados a cada usuário baseado nessas informações. Basicamente, o algoritmo das redes sociais e de sites de busca da internet, agrupa os interesses do usuário e o potencial de engajamento de determinados conteúdos, a fim de conseguir mais índices de engajamento, e consequentemente, de anúncios direcionados especificamente para aquele usuário considerando as suas preferências.

O comércio eletrônico movimenta bilhões de dólares, e a expectativa é de que cresça exponencialmente. O ciberespaço prenuncia uma era em que o de compra e venda torna-se mais automatizado e conveniente. As empresas conectam-se entre si e com os clientes em uma rede virtual homogênea. A informação na Internet flui pelo planeta em um instante e sem custo. As partes vendedoras têm mais facilidade para identificar as melhores partes vendedoras e os melhores produtos. O tempo e a distância, que representaram grandes custos e barreiras comerciais no passado, encolhem imensamente. Os comerciantes que continuarem a vender nas formas antigas lentamente desaparecem de cena (Kotler, 2009, p. 257).

Paes (2016) destaca que o comércio, de forma geral, é o grande responsável por satisfazer as necessidades do consumo no mercado, oferecendo experiências de compra satisfatórias e levando o produto do fabricante até o consumidor final. O autor reconhece que com o passar dos anos ocorreram mudanças significativas, e estas levaram o comércio tradicional a se adaptar de modo a conseguir atender de forma mais eficiente às demandas do novo perfil de consumidor.

Portanto, é preciso que o profissional atual, seja ele empreendedor ou funcionário, entenda que o comércio eletrônico é que garantirá renda daqui por diante. Não que as lojas físicas irão desaparecer por completo, mas a tendência é que cada vez mais o online tome o espaço do físico, e compreender isso é a melhor forma de permanecer ativo no mercado de trabalho. Ou seja, o comércio eletrônico por si só não é garantia de sucesso, já que é preciso de estratégias de marketing assertivas, mas fugir dele certamente é o caminho para perder vendas.

Assim, as contribuições do e-commerce para essas novas modalidades de trabalho advêm, principalmente, do grande lucro que esse mercado gera. O comércio eletrônico consegue alcançar o maior número de clientes possíveis e oferecer exatamente o que eles buscam. O resultado é um mercado cada vez maior, competitivo, lucrativo e crescente.

5 CONSIDERAÇÕES FINAIS

O presente estudo revisitou o tema Segurança Cibernética. Justificou-se o tema escolhido por se tratar de um problema para a sociedade, uma vez que tais riscos comerciais são semelhantes aos profissionais para um indivíduo, existem medidas a serem tomadas em um ambiente empresarial em relação à Segurança Cibernética, muitas pessoas armazenam informações privadas em seus dispositivos eletrônicos.

O objetivo do presente trabalho foi de analisar as possíveis mudanças ocasionadas pelo *e-commerce* no atual mercado de trabalho, sobretudo

2 Algoritmo é uma série de instruções em formato de código, realizadas em uma determinada ordem, para executar uma ação ou resolver um problema na internet.

durante a pandemia do Covid-19, onde o mercado precisou se reorganizar, fechando temporariamente as lojas físicas e mantendo os atendimentos virtuais. Além disso, mostrou-se o histórico do *e-commerce* ao longo das décadas, seu crescimento e benefícios que as vendas online trazem para as pequenas empresas. Para isso, o trabalho foi desenvolvido por meio de uma revisão da literatura que analisou as principais características de evolução do comércio eletrônico.

Sobre as decisões a serem tomadas em um ambiente empresarial, são elas obter determinado desenvolvimento quanto a implementação de uma Política de Segurança da Informação adequada, elaborar de um Plano de Gestão da Segurança Cibernética adequado às necessidades da empresa, estabelecer de boas práticas na gestão dos ativos de informações da empresa, que deve ser dimensionadas mediantes, análise de riscos adequadas.

Mediante ao estudo realizado, as demonstrações contábeis podem viabilizar as tomadas de decisões assertivas por parte dos gestores nas organizações, deve-se conhecer o indicador adequado para cada decisão a ser tomada, ter parâmetros para serem comparados, realizar análises e diagnósticos, para então, tomar decisões, à luz das teorias, exploradas na fundamentação teórica desta pesquisa bibliográfica, torna-se possível afirmar que os objetivos específicos e geral foram alcançados neste estudo científico.

Por mais que tenham ficado explícitos os perigos de um ambiente virtual, por meio deste estudo bibliográfico, são possíveis avanços em novos estudos que possibilitem mostrar como lidar com possíveis ameaças. Assim, como propostas para futuras pesquisas, sugere-se que novos estudos mais aprofundados possam ser realizados como: os benefícios da segurança da informação em pequenas empresas; os principais causadores de invasão dos computadores; como combater os cibercriminosos.

Os resultados encontrados apontam que o *e-commerce* vem trazendo novas perspectivas de trabalho, acesso à informação, desenvolvendo a comunicação entre empresas e profissionais, facilitando a distribuição de produtos e a disponibilização de bens e serviços, além do próprio processo comercial. Para o mercado de trabalho, essa dinâmica proporcionou novas oportunidades de crescimento e uma recolocação em um mercado que tende a se expandir devido sua atual evolução.

O comércio eletrônico possui a habilidade de alcançar um número maior de clientes potenciais e oferecer o que eles buscam por meio de mecanismos de marketing. Com isso um mercado digital fica cada vez mais lucrativo, competitivo e com inclinação ao progresso. O mercado de trabalho então abre novas possibilidades devido à expansão das transações comerciais online.

As operações comerciais realizadas virtualmente não se limitam apenas à venda e compra de produtos, serviços ou bens de consumo. Elas também abrangem todos os processos envolvidos nestas operações, como a logística, a gestão do estoque, o relacionamento com o cliente e com a empresa, dentre outros. Desse modo, o *e-commerce* acaba contribuindo para o mercado de trabalho.

Por fim, o mercado do *e-commerce* já vinha crescendo, isso é fato, mas espera-se que as pessoas entendam que mesmo com o fim da pandemia e a retomada das atividades de forma presencial ele não deve desacelerar, muito pelo contrário. O medo de exposição ao vírus pode ter forçado alguns a aderirem às compras online, mas uma vez que se conhece essa facilidade, a tendência é que ela passe a ser cada vez mais utilizada.

Dessa maneira, o trabalho conclui o objetivo central de analisar o crescimento do *e-commerce* nos últimos anos, sobretudo no tocante ao mercado de trabalho, haja visto que o comércio

online e digital fez com que as relações trabalhistas passam por profundas modificações, além de trazer visibilidade para o pequeno empreendedor, que agora está disponível para uma gama quase infinita de público, aumentando seu faturamento mesmo diante de um cenário de crise econômica durante a pandemia do Covid-19.

Por fim, pode-se apontar a dificuldade de pesquisar o assunto quando se relaciona o mercado durante a Covid -19 pelo fato de a pandemia ainda estar em andamento durante a confecção desse trabalho, tendo poucos materiais disponíveis na literatura acadêmica, porém, dessa maneira o presente estudo auxilia novos trabalhos que visam compreender o panorama do *e-commerce*, percepções trabalhistas e do pequeno empresário, especialmente durante a pandemia.

REFERÊNCIAS

ALBERTIN, A. Comércio eletrônico: seus aspectos de segurança e privacidade. **Revista de Administração de Empresas - RAE**, São Paulo, v. 38, n. 2, 2000.

ALMEIDA, Mário. **O comércio no Brasil**. Rio de Janeiro, 2005.

AZEVEDO, Cristiano Oliveira; ODONE, Marcos Paulo; COELHO, Marcos Antônio Pereira. **Estudo sobre a evolução do comércio eletrônico, suas formas de pagamentos digitais e suas preocupações quanto à segurança e a privacidade**. XI EVIDOSOL e VIII CiltecOnline, junho, 2014.

BARRO, Bruna. O Que são os Vírus Cavalo de Troia e Como se Proteger Deles. 17 maio 2022. Disponível em: https://www.hostinger.com.br/tutoriais/cavalo-detroia-virus. Acesso em: 14 set. 2023.

BESSANT, John; TIDD, Joe. **Inovação e empreendedorismo**. [*S. l.*]: Bookman, 2009.

BRASIL. Ministério da Defesa. **Glossário das Forças Armadas – MD35-G-01**. Apresenta definições de termos comuns às Forças Armadas. Brasília, 2007.

BRASIL. Ministério da Saúde. Orientações sobre COVID-19 e infecção respiratória por SARS-CoV-2. Brasília: Ministério da Saúde, 2020. Disponível em: http://www.gov.br/saude/pt-br/centrais-de-conteudo/publicacoes/svsa/vigilancia-laboratorial/guia-de-vigilancia-genomica-do-sars-cov-2-uma-abordagem-epidemiologica-e-laboratorial/@@download/file. Acesso em: 14 set. 2023.

BRASIL PARALELO, O que foi o Cavalo de Troia? Entenda a história do mito de guerra mais famoso da Antiguidade. 2021. Disponível em: https://www.brasilparalelo.com.br/artigos/cavalo-de-troia. Acesso em: 14 set. 2023.

CARDOSO, A.; ARAÚJO, R. **Vantagens competitivas na internet**. Rio de Janeiro, 2013.

GARCIA, L. F. Conduta ou personalidade de um empreendedor. **Empreendedor**, São Paulo, n. 169, p. 76, nov. 2008.

GILMORE, Georgina; BEARDMORE, Peter. **Simplificando a Segurança de TI para Leigos**. Moscou: Kaspersky Lab, 2014.

GUERREIRO, A. S. **Análise da Eficiência de Empresas de Comércio Eletrônico usando Técnicas da Análise Envoltória de Dados**. 2006. Dissertação (PósGraduação em Engenharia de Produção) - Departamento de Engenharia Industrial, PUCRio, Rio de Janeiro, 2006.

HERZER, Anderson. **Fidelizando clientes no comércio eletrônico**. [*S. l.*: *s. n.*], 2013.

HOSTINGER. **Tentativa de Phishing**. 2022. Disponível em: https://www.hostinger.com.br/tutoriais/o-que-e-phishing-e-como-se-proteger-degolpes-na-internet. Acesso em: 14 set. 2023.

KASPERSKY. **As sete principais ameaças virtuais que merecem atenção.** 2022. Disponível em: https://www.kaspersky.com.br/resource-center/threats/top-7-cyberthreats. Acesso em: 14 set. 2023.

KASPERSKY. ***Ransomware*: definição, prevenção e remoção**. 2022. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware. Acesso em: 14 set. 2023

KASPERSKY. **O que é *phishing***. 2022. Disponível em: https://www.kaspersky.com.br/resource-center/preemptive-safety/what-is-phishingand-how-does-it-affect-email-users. Acesso em: 14 set. 2023.

KASPERSKY. **O que são crimes cibernéticos? Como se proteger dos crimes cibernéticos**. 2022. Disponível em: https://www.kaspersky.com.br/resourcecenter/threats/what-is-cybercrime. Acesso em: 14 set. 2023.

KOVACS, Leandro. Qual a origem e história do grupo Anonymous? **Tecnoblog**, 2005. Disponível em: https://tecnoblog.net/responde/qual-a-origem-e-historia-do-grupo-anonymous/#:~:

text=Leandro%20Kovacs%20%C3%A9%20jornalista%20e,sobre%20softwares%2C%20ciberseguran%C3%A7a%20e%20jogos. Acesso em: 14 set. 2023.

KOTLER, P. **Marketing para o século XXI**: como criar, conquistar e dominar o mercado. São Paulo: Ediouro, 2009.

LAUDON, Kenneth C.; TRAVER, Carol Guercio. ***E-commerce***. 13. ed. [*S. l.*]: Pearson Education, 2017.

LEMOS, F. GÓES, L. F. Avaliação do comportamento de consumidores no processo de decisão de compra no M-Commerce e no E-commerce. Trabalho apresentado no XI Brazilian Symposium on Information System. Goiânia. p. 127 – 134, 2015.

LIMEIRA, Tania. ***E-marketing***. São Paulo: Saraiva, 2007.

LISKA, Allan; GALLO, Timothy. **Ransomware**: Defendendo-se da extorsão digital. São Paulo: Novatec Editora, 2017.

MARCONDES, José Sérgio. **Segurança Cibernética**: O que é, Objetivos, Importância, Medidas, 2 fev. 2021. Disponível em: https://gestaodesegurancaprivada.com.br/seguranca-cibernetica-o-que-e-objetivosimportancia-medidas/. Acesso em: 14 set. 2023.

MARINO, Caroline. O trabalho depois do Coronavírus. **Você S/A**, jun. 2020.

MARTHE, M.; BETTI, R. **Estratégia Digital**. São Paulo, 2012.

MCAFEE. **O impacto econômico do crime cibernético: sem indícios de desaceleração**. McAfee, 2017. Disponível em: https://www.mcafee.com/enterprise/ptbr/assets/executive-summaries/es-economic-impact-cybercrime.pdf. Acesso em: 14 set. 2023.

NOVAES. V. *E-commerce* brasileiro tem alta de 26% no primeiro trimestre. **Economia e Política/Portal Panrotas**, 2021.

PAES, F. **Análise multicritério para estratégia de varejo Omnichanncel**. Curitiba: Instituto de Tecnologia para Desenvolvimento, 2016.

RATTEN, V. Coronavirus and international business: An entrepreneurial ecosystem perspective. **Thunderbird International Business Review**, n. 62, v. 5, p. 629-634, 2020.

RELATÓRIO DO DIRETOR-GERAL. Trabalho em tempos de COVID. Conferência Internacional do Trabalho, 109ª sessão, Genebra, 2021.

ROCHA, Aldry. **Principais tipos de ataques virtuais**. 23 mar. 2021. Disponível em: https://www.opservices.com.br/tipos-de-ataques-virtuais/. Acesso em: 14 set. 2023.

ROSA, A. C. **Gestão do transporte na logística**. [*S. l.; s. n.*]: 2007.

SIQUEIRA, Ethevaldo. **Para compreender o mundo digital**. [*S. l.*]: Ed.Globo, 2008.

SOARES; Carlos H. Hentz; BATISTA, Lucas Pelegrinelli B.; SCANDIUZZI, Fernando. Comércio eletrônico: fatores que estimulam e desestimulam os consumidores. **Rev. Científica Eletrônica UNISEB**, Ribeirão Preto, v. 5, n. 5, p. 34-52, jan./jun. 2015.

SPERANZA, M. G. **New Trends in Distribution Logistics.** [*S. l.*]: Springer Science & Business Media. 2012.

STEINBERG, Joseph. **Cibersegurança Para Leigos**: Os Primeiros Passos Para o Sucesso. Rio de Janeiro: Alta Books, 2020.

TEIXEIRA FILHO, Jayme. **Comércio eletrônico**. [*S. l.*]: Ed. Senac, 2001.

TOBLER, Rodolpho; BITTERNCOURT, Viviane Seda. **Blog do Ibre**: Os impactos do Coronavírus nas empresas e nos consumidores, 2020.

TODOR, D. Blending traditional and digital marketing. **Bulletin of the Transilvania University of Braşov**, 2016.

TOMÉ, Luciana Mota. Comércio Eletrônico. **Caderno Setorial ETENE,** ano 3, n. 43, p. 1- 9, set. 2018.

TURBAN, Efraim; KING, David. **Comércio eletrônico**: estratégia e gestão. São Paulo: Prentice Hall, 2004.

VIEIRA, Eduardo. **Os bastidores da internet no Brasil.** [*S. l.*]: Ed. Saraiva, 2003.

WIKIPÉDIA. **Anonymous**, 13 nov. 2022. Disponível em: https://pt.wikipedia.org/wiki/Anonymous. Acesso em: 14 set. 2023.

NOTAS

Conflito de interesse: Não há conflito de interesse entre os autores.

Contribuição dos autores: Todos os autores participaram da elaboração, redação e Revisão e aprovação final do artigo.

Informar se a publicação é oriunda de uma dissertação ou tese: Não se aplica.

Aprovação Ética: Não se aplica