South American Development Society Journal

Vol.: 10 | Nº.: 29 | **Ano:** 2024 | **ISSN:** 2446-5763 | **DOI:** 10.24325/issn.2446-5763.v10i29p99-115
Data de Submissão: 06/05/2024 | **Data de Publicação:** 31/08/2024

ESTRATÉGIAS DE SEGURANÇA DA INFORMAÇÃO NAS ATIVIDADES TURÍSTICAS

Eliacy Cavalcanti Lélis (FATEC São Paulo / FATEC Zona Leste) – eliacylelis@gmail.com
Beatriz Maximiano Batista (FATEC São Paulo) – bemaximianob@gmail.com

Resumo

A evolução da tecnologia trouxe transformação digital para a sociedade e suas organizações, com impactos diretos e indiretos. No turismo, essa transformação trouxe mudanças que contribuíram com ganhos, mas que também, problemas com a criminalidade na internet. Esta pesquisa visa apresentar um estudo sobre as estratégias de segurança da informação na área de turismo. A metodologia de pesquisa inclui um levantamento bibliográfico e uma pesquisa de campo com estudantes da área de turismo, turistas e profissionais de turismo na cidade de São Paulo. Os resultados tipificam alguns tipos de crimes e apontam as estratégias de segurança da informação nas atividades turísicas. O estudo tem a função de alertar profissionais, estudantes, internautas e gestores sobre o seu papel na prevenção de crimes eletrônicos na área de turismo ao compreender a tipologia dos crimes e as estratégias de segurança que precisam de mais investimento.

Palavras-chaves: Crimes eletrônicos; estratégias de segurança da informação, atividades turísticas.

Abstract

The evolution of technology has brought digital transformation to society and its organizations, with direct and indirect impacts. In tourism, this transformation brought changes that contributed to gains, but also problems with internet crime. This research aims to present a study on information security strategies in the tourism area. The research methodology includes a bibliographic survey and field research with tourism students, tourists and tourism professionals in the city of São Paulo. The results typify some types of crimes and point out information security strategies in tourist activities. The study aims to alert professionals, students, internet users and managers about their role in preventing electronic crimes in the tourism sector by understanding the typology of crimes and the security strategies that need more investment.

Keywords: Electronic crimes; information security strategies, tourist activities.

1. INTRODUÇÃO

O turismo contribui para a economia e tem relação com diversos setores com parcerias que estruturam fluxos de negócios pelo mundo, vinculados à hospedagem, transporte, alimentação, lazer e entretenimento. Segundo a Organização Mundial do Turismo (OMT, 2001), o turismo é um fênomeno de aspecto social, cultural, econômico relacionado ao fluxo de visitantes para outros lugares, fora de seu ambiente pessoal, independentemente da distância.

Nesta era da internet, há transformações digitais nos negócios e no comportamento da sociedade pelas aplicações das inovações tecnológicas que mudam a experiência do turista contemporâneo.

A internet pode ser uma grande facilitadora para o turista conduzir sua experiência, sem ficar dependente de terceiros para montar um pacote turístico, pesquisar novos destinos e definir seu roteiro de viagem. Entretanto, essas pessoas que tem acesso a dispositivos móveis e internet estão vulneráveis a riscos de crimes eletrônicos que crescem a cada ano.

Na área de turismo, há algumas peculiaridades neste tipo de crime, que está atrelado à produtos e serviços oferecidos neste setor que podem ser investigadas.

Há um aumento do número de usuários na internet, e consequentemente, a crescente da tecnologia e suas ferramentas, o Jornal Exame (2022) juntou os seguintes dados “em 2021, 84,7% (ou 155,7 milhões) de pessoas de 10 anos ou mais, na população brasileira de 183,9 milhões, acessaram a internet. Esse percentual vem crescendo desde 2016, quando 66,1% da população nessa faixa etária tinha utilizado a rede, passando para 79,5%, em 2019, e 84,7% no ano passado.”

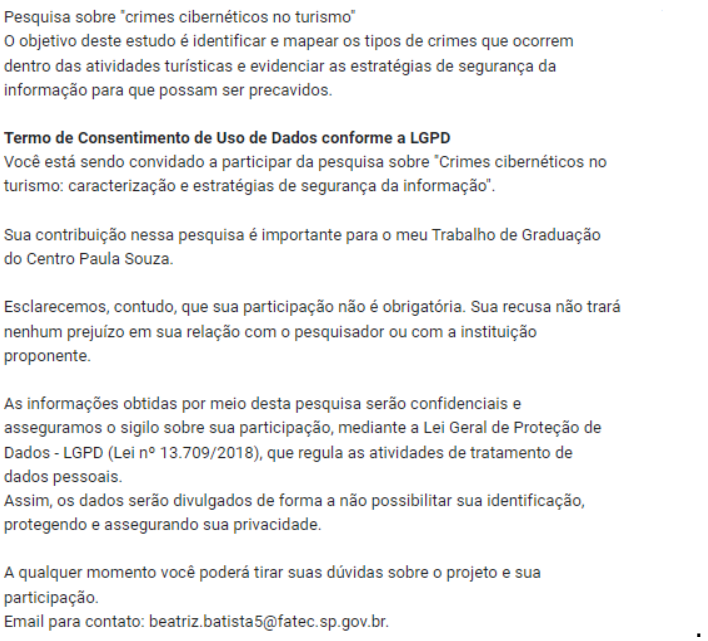
O objetivo desse trabalho é identificar crimes eletrônicos e estratégias de segurança da informação na área de turismo na perspectiva de profissionais e estudantes da área.

2. METODOLOGIA

A metodologia abordada parte de un levantamento bibliográfico e pesquisa empírica na qual foram coletadas repostas de usuários da internet que já possuem contato com o turismo e para obter esses dados, foi elaborado um questionário semiaberto para embasar os riscos que se corre com os crimes cibernéticos no turismo. Foi realizada uma pesquisa pelo formulário do Google em novembro de 2023, onde foram feitas 10 perguntas aos respondentes – majoritariamente estudantes da área de turismo, turistas e profissionais de turismo.

No início do questionário foi apresentado um Termo de consentimento para atendimento à Lei Geral de Proteção de Dados (LGPD). A Figura 1 apresenta o termo. Todos os participantes da pesquisa neste levantamento empírico deram o aceite no termo e os dados foram tratados sem a identificação das pessoas, garantindo o sigilo e o devido cuidado na proteção dos dados.

Figura 1 – Termo de consentimento do questionário



Pesquisa sobre "crimes cibernéticos no turismo"
O objetivo deste estudo é identificar e mapear os tipos de crimes que ocorrem dentro das atividades turísticas e evidenciar as estratégias de segurança da informação para que possam ser precavidos.

Termo de Consentimento de Uso de Dados conforme a LGPD
Você está sendo convidado a participar da pesquisa sobre "Crimes cibernéticos no turismo: caracterização e estratégias de segurança da informação".

Sua contribuição nessa pesquisa é importante para o meu Trabalho de Graduação do Centro Paula Souza.

Esclarecemos, contudo, que sua participação não é obrigatória. Sua recusa não trará nenhum prejuízo em sua relação com o pesquisador ou com a instituição proponente.

As informações obtidas por meio desta pesquisa serão confidenciais e asseguramos o sigilo sobre sua participação, mediante a Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/2018), que regula as atividades de tratamento de dados pessoais.
Assim, os dados serão divulgados de forma a não possibilitar sua identificação, protegendo e assegurando sua privacidade.

A qualquer momento você poderá tirar suas dúvidas sobre o projeto e sua participação.
Email para contato: beatriz.batista5@fatec.sp.gov.br.

Fonte: Autoras (2023)

Os resultados da pesquisa foram tratados com estatística descritiva com gráficos e nas questões fechadas e análise de conteúdo nas questões abertas.

3. FUNDAMENTAÇÃO TEÓRICA

3.1 Atividades Turísticas

Como dito na introdução, existem diversas definições de turismo construída ao longo dos anos por diversos autores. É fato que, para entender e estudar essa ciência social, há muitas perspectivas, tendo em vista a amplitude da área e, consequentemente, o seu relacionamento com inúmeras outras dimensões econômicas, sociais, ambientais, éticas, políticas e simbólicas.

Para Beni (2001), as motivações são as razões pelas quais os indivíduos realizam uma viagem, ou seja, os fatores pessoais que no nosso interior incitam a ação. O motivo também deve ser entendido como uma necessidade ou desejo do turista, que poderá ser satisfeito por meio de um deslocamento. De acordo com a conceituação de turismo da OMT (2001), possíveis motivos de viagens turísticas são: diversão, descanso, desenvolvimento pessoal, religião, negócios, tratamento de saúde, entre outros.

Na classificação da OMT (2001), há seis grupos para o turismo receptor, emissor e interno, são eles: a) lazer, recreação e férias; b) visitas à parentes e amigos; c) negócios e motivos profissionais; d) tratamentos de saúde; e) motivos religiosos e f) outras motivações.

As atividades turísticas tem uma cadeia de suprimentos com diversos setores: hospedagem, meios de transporte, fornecedores de alimentos & bebidas, operadoras de turismo, consolidadoras, agências e eventos. Esse é o contexto em que podem surgir os crimes eletrônicos específicos da área.

3.2 Crimes Eletrônicos e Legislação Brasileira

Com o avanço da internet, mais pessoas tem acesso à dispositivos e esse é o ambiente que tem o espaço para o crescimento da criminalidade. Com isso tem-se a criação de novas leis para garantir a segurança dos internautas consumidores e regularizar a prática de segurança pelas empresas.

Em 30 de novembro de 2012, foi publicada a Lei n° 12.737, também conhecida por “Lei Carolina Dieckmann”, que tipifica as condutas delituosas no âmbito informático e dispõe de outras providências, como a penalidade quando estes são cometidos, e também trouxe diversas alterações no Decreto-Lei nº 2.848/40 em nosso Código Penal, em seu artigo 154-A bem como:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (BRASIL, 2012, s.p.).

E 154-B:

> Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos (BRASIL, 2012, s.p.).

Esta lei descreve o crime de invasão à privacidade e roubo de dados pessoais a fim de utilizá-los maliciosamente, alterando os artigos supracitados no código penal, prevendo às punições cabidas a quem os comete.

Publicada em 23 de abril de 2014, o Marco Civil da Internet é a lei federal nº 12.965, que visa estabelecer os princípios, garantias, direitos e deveres fundamentais para o uso de Internet do Brasil, determinando as diretrizes para atuação da União, dos Estados, dos Distrito Federal e dos Munícipios em relação à matéria, conforme seu art. 1º. Esta, também dispõe em seus artigos e incisos, os direitos do cidadão perante à

internet e a asseguração da proteção à privacidade e aos dados pessoais inseridos nas redes.

Outra legislação de destaque é a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), que visa garantir a segurança dos dados dos clientes das empresas privadas e entidades públicas, conforme seu art. 1º (BRASIL, 2018, s.p.):

> Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A identificação e a tipificação desses crimes são o primeiro passo para o desenvolvimento de estratégias de segurança da informação para que as organizações do setor de turismo possam investir em soluções de proteção e mitigação de riscos.

Antes de tudo, deve-se considerar o crime de invasão de dados e compartilhamento destes de forma prejudicial, acontece em todo e qualquer tipo de empresa ou órgão público, sendo assim, agências de viagens, operadoras de turismo, estabelecimentos de hotelaria, estão sujeitos a esse tipo de crime.

Além disso, é necessário entender o conceito de Engenharia Social, pois esta influencia fortemente nas práticas dos crimes cibernéticos. Segundo Gonçalves, Ogawa, Lima (2022), a engenharia social na internet é uma forma de pessoas mal intecionadas envolverem potenciais vítimas em golpes ou ataques à segurança da informação visando obter alguma vantagem sobre organizações ou internacionais.

Neste sentido, Fontes (2012, p. 119) conceitua engenharia social como

> […] o conjunto de procedimentos e ações que são utilizados para adquirir informações de uma organização ou de uma pessoa por meio de contatos falsos sem o uso da força, do arrombamento físico ou de qualquer brutalidade.

O Observatório de Crimes Cibernéticos (OCC), em 2022 tem divulgado dados sobre os crimes eletrônicos, contribuindo para a identificaçãoe e quantificação dessas ocorrências. O Comitê Gestor de Internet no Brasil, em 2012, divulga a Cartilha de Segurança da Internet para ajudar nas estratégias de segurança da informação. A gestão da segurança da informação deve planejar e executar ações que possam prevenir e mitigar os riscos de crimes eletrônicos, para isso, entender como o crime acontece e qual o papel das partes interessadas é fundamental para que hajam ações inteligentes e efetivas.

3.3 Estratégias de Segurança da Informação

5. ESTRATÉGIAS DE SEGURANÇA DA INFORMAÇÃO

É necessário que as empresas invistam mais em estratégias de segurança da informação para que evitem que seus clientes sejam vítimas destes crimes e mediante ao resultado da pesquisa empírica realizada, não manche o nome da empresa. Neste contexto, Gonçalves, Ogawa e Lima (2022) relacionam a segurança da informação à métodos, ferramentas e ações que possam contribuir com a segurança visando proteger as informações de ameaças, sejam físicas ou eletrônicas.

Fontes (2006, p.10) afirma que,

> "segurança da informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada."

Assim, em conjunto com o CGI (2012) juntamente da EGI (2014), que dispõem de algumas práticas e investimentos que devem ser realizados por partes das empresas para diminuir até mitigar a ocorrência desses crimes.

CGI (2012, p. 67) define a criptografia como:

> "(..) considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código, é um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso da Internet."

Todavia, dentro da criptografia, há algumas dimensões em que ela se divide, conforme mostra o Quadro 2.

Quadro 2 - Criptografia

Tipos de criptografia:	Definição:
Chave	Similar a uma senha, é utilizada como elemento secreto pelos métodos criptográficos.
Certificado Digital	Registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública. É emitido por uma autoridade certificadora.
Assinatura Digital	Código usado para comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isso e que ela não foi alterada.
Pretty Good Privacy - PGP	Programa que implementa operações de criptografia, como cifrar e decifrar conteúdos e assinatura digital. Normalmente utilizado em e-mails.

Fonte: Adaptado de EGI (2024)

Esta estratégia de segurança da informação é bastante viável para autenticação da identidade de usuários, autenticação de transações bancárias; proteção da

integridade de transferências eletrônicas de fundos, e proteção do sigilo de comunicações pessoais e comerciais. Em relação às estratégias de segurança da informação nas redes, que podem ser implementadas pelas empresas, existem:

a. ***Firewall*****:** este é utilizado para dividir e controlar o acesso entre redes de computadores com acessos não autorizados vindos da internet. A implementação deste previne crimes como *phishing*.

b. **Virtual Private Network – VPN:** CGI, 2012, p. 121, define:

> Termo usado para se referir a construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

c. ***Intrusion Detection System*** **– IDS:** programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas geralmente implementado com base na análise de logs ou de tráfego de rede, em busca de padrões de ataque pré-definidos. (EGI, 2014, p. 35).

d. **Antimalware:** procura detectar e, então, anular ou remover os códigos maliciosos de um computador. Antivírus, *antispyware*, *antirootkit* e *antitrojan* são exemplos de ferramentas deste tipo. (CGI, 2012, p. 55). Neste caso, existem diversos programas que cumprem essa função, é parte da empresa escolher qual melhor se encaixa.

Esses são alguns exemplos dos vários tipos de estratégias de segurança da informação, é válido ressaltar, que se desmembram em vários outros conceitos a serem estudados para melhor aplicá-los. As estratégias destacadas até aqui, podem impedir crimes como a invasão de dados e os outros crimes já citados nesta monografia.

4. RESULTADOS DA PESQUISA DE CAMPO

Os resultados da pesquisa de campo iniciam traçando o perfil do respondente com uma coleta de 50 respostas, em uma amostragem por conveniência nesta pesquisa não probabilística.

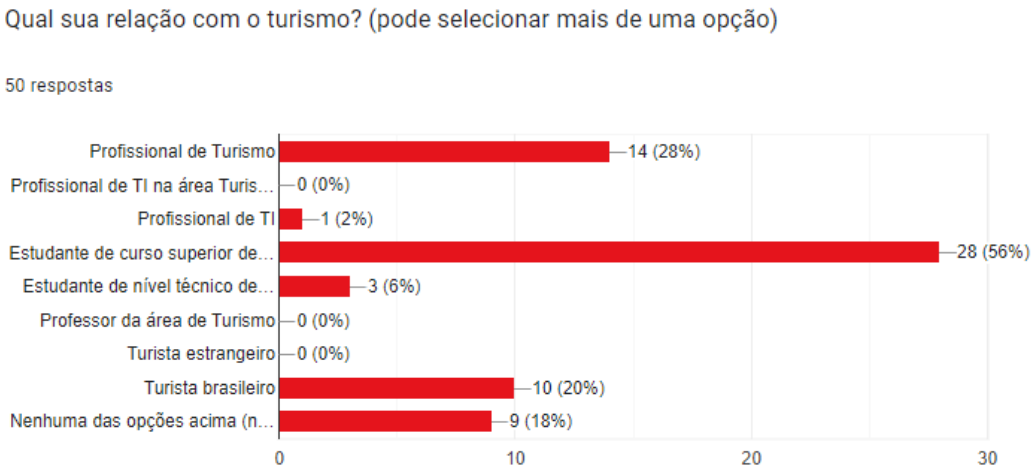
A faixa etária dos respondentes é apresentada na Figura 2.

Figura 1 - Questão 1 da pesquisa

Fonte: *Autoras* (2023)

Uma grande parcela dos respondentes possui idade entre 18 a 21 anos (38%), em seguida é entre 22 a 32 anos (34%), 33 a 45 anos (16%) e 46 a 60 anos (12%).

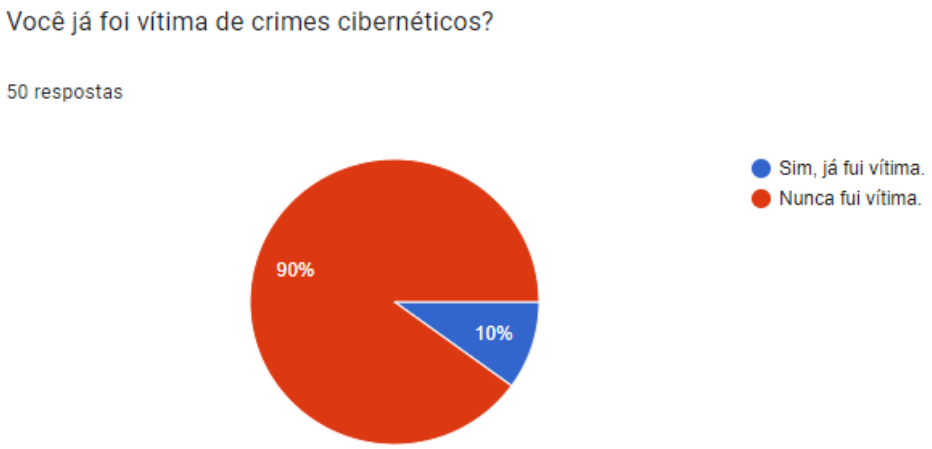
Figura 2 - Questão 2 da Pesquisa



Fonte: *Autoras* (2023)

A terceira questão (Figura 3) busca identificar quais são as relações dos respondentes com o turismo, sendo que estes poderiam selecionar mais de uma resposta. Ela é necessária para entender sob quais parâmetros as pessoas entendem de turismo e os crimes acerca dele. Mais de 56% das pessoas são estudantes do curso superior de turismo, em seguida, 28% são de profissionais de turismo, 20% são turistas brasileiros, 18% não se encaixavam em nenhuma das opções anteriores, 6% eram estudantes de nível técnico da área de turismo e 2% profissionais de TI.

Figura 3 - Questão 3 da Pesquisa

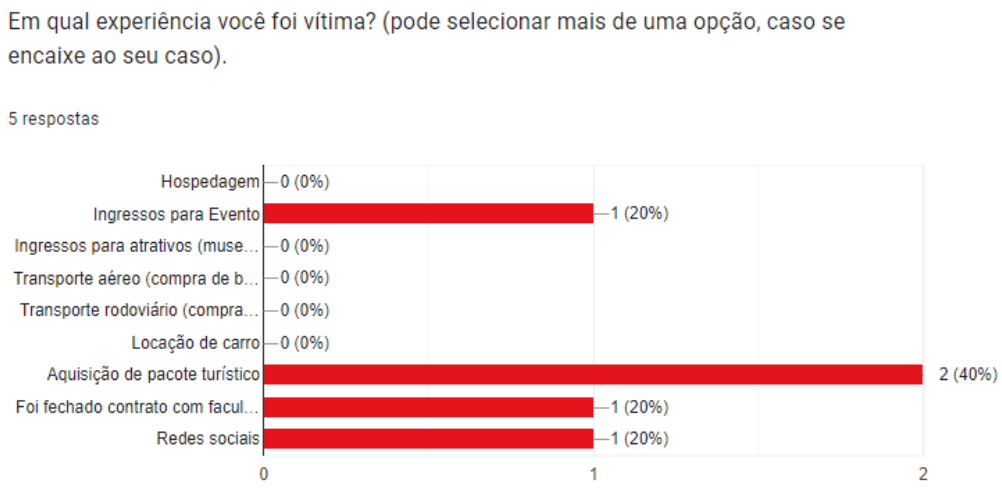


Fonte: *Autoras* (2023)

Nesta questão da Figura 4 busca-se verificar se os respondentes foram vítimas de crimes cibernéticos, e observa-se que 90% nunca foi vítima e 10% já foi vítima.

Em caso de selecionar a resposta “sim, já fui vítima”, o respondente é direcionado à próxima pergunta para entender em qual crime ele já foi vítima, conforme mostra a Figura 5.

Figura 4 - Questão 4 da Pesquisa

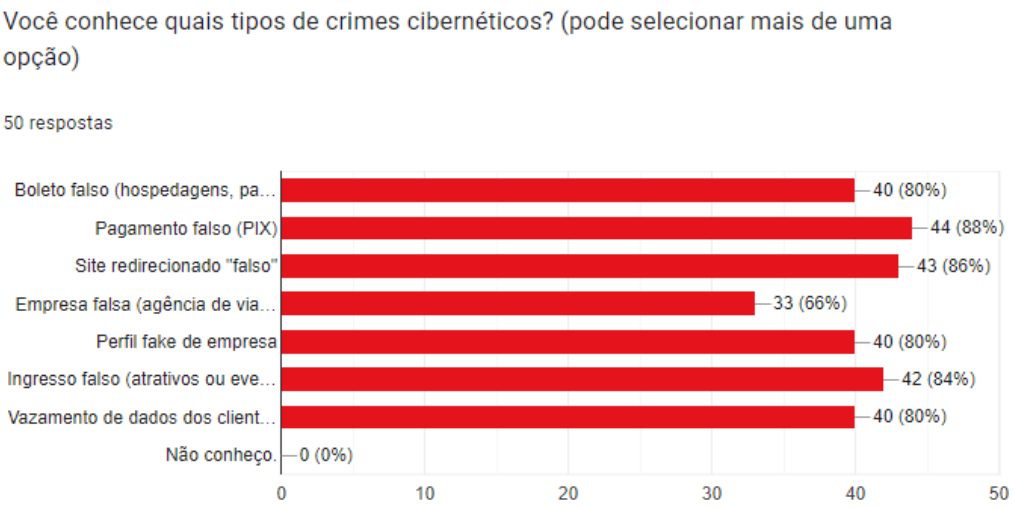


Fonte: *Autoras* (2023)

Nesta questão foram obtidas 5 respostas, sendo que 2 pessoas foram vítimas de crimes cibernéticos na aquisição de pacotes turísticos (40%), 1 pessoa foi vítima de crimes na aquisição de ingressos falsos para eventos (20%), 1 pessoa em perfil de redes sociais (20%) e uma última em um fechamento de contrato pela faculdade onde a mesma não acordou e não assinou contrato (20%). Observa-se o resultado de 3

pessoas vítimas de crimes cibernéticos no turismo e o restante em crimes cibernéticos mais gerais.

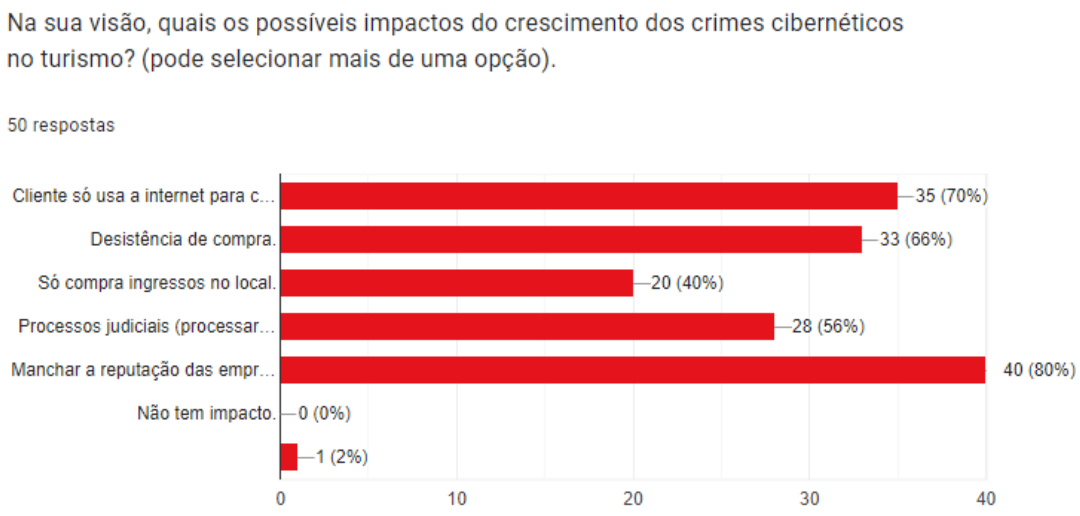
Figura 5 - Questão 5 da Pesquisa



Fonte: *Autoras* (2023)

Nesta questão da Figura 6 com múltiplas escolhas, foi possível entender quais crimes cibernéticos os respondentes conhecem, nenhum deles não conheciam os tipos de crimes cibernéticos no turismo e grande parte deles conheciam na sequência decrescente: pagamento falso via PIX (88%); site redirecionado “falso” – *pharming* (86%); ingressos falsos de atrativos ou eventos (84%); vazamento de dados de clientes (80%); perfis *fakes* de empresas (80%); boleto falso para hospedagens, passagens aéreas e outros serviços turísticos (80%); empresa falsa, como agência de viagens, operadoras de turismo e estabelecimentos de hotelaria (66%).

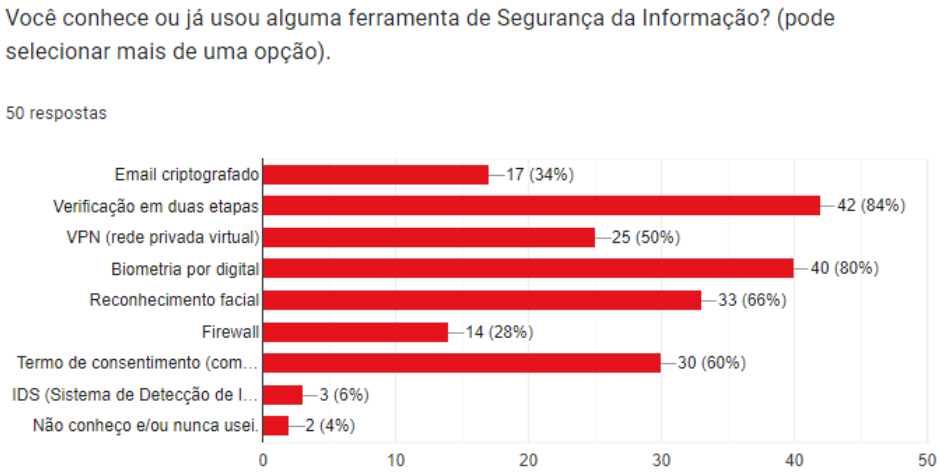
Figura 6 - Questão 6 da Pesquisa



Fonte: *Autoras* (2023)

Na sexta pergunta da pesquisa apresentada na Figura 7, tem-se a visão dos respondentes, quais são os possíveis impactos do crescimento de crimes cibernéticos no turismo, sendo que há unanimidade na crença de impactos, assim, 80% deles acreditam na transformação de uma imagem negativa às empresas fornecedoras de serviços turísticos; 70% acredita que o cliente só utiliza a internet para consultas, mas não finaliza a compra, consequentemente diminuindo os lucros; 66% visualiza a desistência da compra; 56% acredita na ação de processos judiciais contra a empresa; 40% visa a compra de ingressos somente no local.

Figura 7 - Questão 7 da Pesquisa



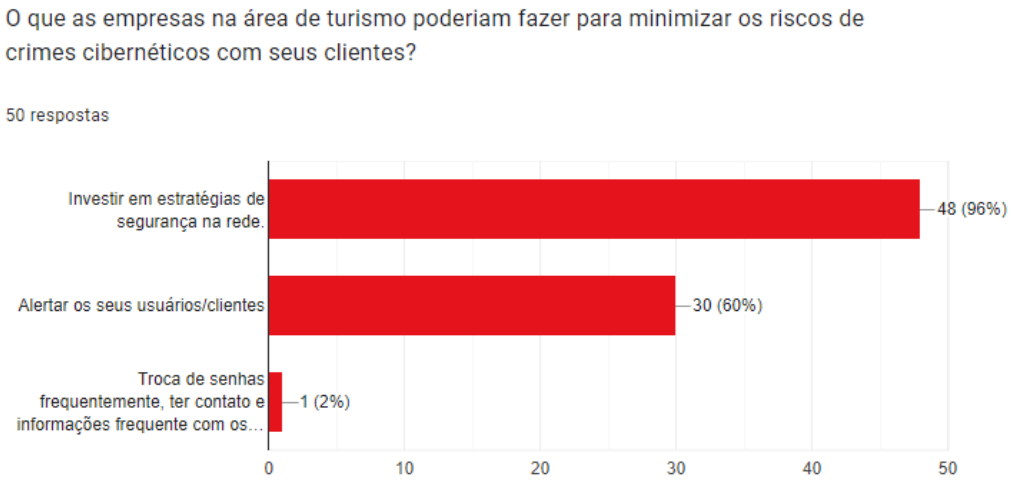
Fonte: *Autoras* (2023)

Na sétima questão da Figura 8 foram identificadas as estratégias de segurança da informação os respondentes conhecem ou já utilizaram. Neste sentido, 84% conhecem a verificação em duas etapas; 80% a biometria por digital; 66% conhece o reconhecimento facial e 60% os termos de consentimento (como LGPD, por exemplo, observamos que grande parte dos respondentes conhecem as estratégias de segurança da informação mais comuns e que usamos no dia a dia. Em seguida, temos o sistema de VPN (en-us: *Virtual Private Network*; pt-br: Rede Privada Virtual) conhecido por 50% dos respondentes; o e-mail criptografado conhecido por 34% dos respondentes; o *Firewall* com 28%; o IDS (en-us: *Intrusion Detection System*; pt-br: Sistema de Detecção de Intrusão) com 6% de seleção; 2% dos respondentes não conhecem ou nunca utilizaram nenhuma ferramenta de Segurança da Informação. Neste âmbito, observa-se que poucas pessoas conhecem estratégias de segurança da informação que podem e devem ser utilizadas pelas empresas fornecedoras de

serviços e produtos turísticos, em sua maioria, são as estratégias de segurança para as redes que protegem os dados pessoais de seus clientes.

É importante entender o que os respondentes acreditam que as empresas da área de turismo podem fazer para minimizar ou até mitigar os riscos de crimes cibernéticos aos seus clientes, conforme mostra a Figura 9.

Figura 8 - Questão 8 da Pesquisa



Fonte: *Autoras* (2023)

Nesta questão, onde podiam ser escolhidas mais de uma opção, 96% dos respondentes acreditam no investimentos em estratégias de segurança na rede, estratégias essas, pouco conhecidas pelos mesmos e que serão evidenciadas no próximo capítulo. Após, 60% deles acreditam que alertar os seus usuários/clientes é importância para que fiquem atentos a não caírem nesses tipos de crimes, o que pode ser trabalhoso e não chegar a todos. Por fim, 2% dos respondentes inseriram uma resposta livre sugerindo a troca de senhas, o contato e as informações frequentes com os clientes.

A questão na Figura 10 tem resposta dissertativa, onde desta vez, foi questionado o que os consumidores internautas poderiam fazer para minimizar os riscos de cair em crimes cibernéticos, vide figura 10.

Figura 9 - Questão 9 da Pesquisa

Fonte: *Autoras* (2023)

Metade dos respondentes, que representa 50% acreditam na realização de estudos e pesquisa sobre a empresa (como referências, comentários, avaliações, o uso da plataforma Reclame Aqui, entre outros); 12% crê na ciência a adoção de medidas de segurança; 10% em resolver presencialmente ou entrar em contato com a empresa a fim de verificar a veracidade do produto oferecido; 6% em buscar conhecimento (citado de forma geral); 6% em ler os termos com mais atenção; 6% na compra com parceiros, indicações ou já ter uma agência de confiança; 4% em estar bem informado sobre as práticas criminosas para não cair em golpes; 4% na certificação dos sites acessados e não confiar em propagandas “vantajosas; 2% visualiza o tráfego digital mais consciente como um fator para minimizar esses riscos.

Por fim, a Figura 11 mostra a resposta da última pergunta onde é possível entender, na ótica dos respondentes, se a falta de investimento em segurança da informação pode ou é um fator prejudicial às empresas fornecedoras de serviços turísticos.

Figura 10 - Questão 10 da Pesquisa

Fonte: *Autoras* (2023)

Nesta questão, 96% dos respondentes acreditam que pode sim ser um fator prejudicial, enquanto os outros 4% não acreditam.

Os resultados desta pesquisa mostram informações que podem auxiliar os gestores, internautas e profissionais da área de turismo a enfrentar os crimes eletrônicos com um conjunto de ações que podem mitigar problemas e perdas para os envolvidos em situações onde ocorrem os crimes na internet.

5. CONSIDERAÇÕES FINAIS

Esta pesquisa traz à reflexão a questão da criminalidade na internet no contexto das atividades turísticas para aprofundar a discussão sobre as estratégias de segurança da informação que precisam de mais atenção e investimento.

Os crimes eletrônicos no turismo precisam de mais atenção e prevenção para que os benefícios e ganhos do setor sejam usufruídos com tranquilidade e segurança para todos os envolvidos.

Entender como o crime acontece é o ponto de partida para que o planejamento em estratégias de segurança da informação seja desenvolvido e atrelado à forma como a atividade turística acontece. A pesquisa apresenta estas estratégias na perspectiva de profissionais, estudantes da área e turista pois o conhecimento e vivência destas pessoas podem ajudar na elaboração de estratégias adequadas à especificidade da área.

Como limitação de pesquisa, os resultados apresentados nesta pesquisa não podem ser generalizados pois estão restritos ao contexto dos respondentes.

Para estudos futuros, recomenda-se o estudo de caso em agência de viagens e turismo e uma análise comparativa de boas práticas de segurança da informação no turismo.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Haian de Assis Lopes de; OLIVEIRA, Tamar Ramos de. **Crimes virtuais**: o avanço dos crimes eletrônicos e a evolução das leis específicas no Brasil. 2022. Disponível em: doi.org/10.51891/rease.v8i11.7554. Acesso em: 17 ago. 2023.

BARRETO, Alessandro Gonçalves; SILVA, Natália Siqueira da. **É bom demais para ser verdade?** 2022. Disponível em: https://occ.org.br/e-book-50-tipos-golpes-digitais/. Acesso em: 18 ago. 2023.

BENI, Mário Carlos. Análise estrutural do Turismo. 6. ed. São Paulo: SENAC, 2001

BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Acesso em: 01 nov. 2023.

BRASIL. **Lei nº 12.737,** de 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 15 de ago de 2023.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 24 ago. 2023.

(CGI) BRASIL. COMITÊ GESTOR DA INTERNET NO BRASIL. **Cartilha de Segurança para Internet**. 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 03 nov. 2023.

CRISTINE HOEPERS (EGI). Escola de Governança da Internet no Brasil. **Fundamentos de Segurança da Informação**. 2014. Disponível em: https://www.cert.br/docs/palestras/certbr-egi2014.pdf. Acesso em: 03 nov. 2023.

EXAME, Revista. **Quase 85% das pessoas de 10 anos ou mais acessam internet no Brasil**. 2022. Disponível em: https://exame.com/brasil/quase-85-das-pessoas-de-10-anos-ou-mais-acessam-internet-no-brasil/. Acesso em: 20 out. 2023.

FONTES, Edison Luiz G. Segurança da informação - 1ª edição. Editora Saraiva, 2012. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502122185/. Acesso em: 03 nov. 2023.

GONÇALVES, Gabriel Vinicius Costa; OGAWA, Kenichi Roberto Lino; LIMA, Mateus Alves de. **Engenharia Social e a Segurança da Informação**. 2022. Disponível em: https://dspace.uniceplac.edu.br/bitstream/123456789/2099/1/Gabriel%20Vínicius%20Costa%20Gonçalves_Kenichi%20Lino%20Ogawa_Mateus%20Alves%20de%20Lima.pdf.pdf. Acesso em: 10 nov. 2023.

INFOMONEY. **Brasil aparece em 2º em ranking de ataques cibernéticos; como se proteger.** Disponível em https://www.infomoney.com.br/negocios/brasil-aparece-em-2o-em-ranking-de-ataques-ciberneticos-como-se-proteger/ Acesso em 01 de set. 2023.

OCC (Brasil). Observatório de Crimes Cibernéticos. **Página principal.** Disponível em: https://occ.org.br. Acesso em: 20 ago. 2023.

Infomoney. **Brasil aparece em 2º em ranking de ataques cibernéticos; como se proteger.** Disponível em https://www.infomoney.com.br/negocios/brasil-aparece-em-2o-em-ranking-de-ataques-ciberneticos-como-se-proteger/ Acesso em 01 de set. 2023.

OMT. Introdução ao turismo. São Paulo: Roca, 2001

RIBEIRO, Ma. Lore Manica. ARTIGO DE TCC PROCEDIMENTOS BÁSICOS. Taguatinga. 2011.

SAFERNET (Brasil) (org.). **Delegacias cibercrimes.** Disponível em: https://new.safernet.org.br/content/delegacias-cibercrimes. Acesso em: 20 ago. 2023.

SANTOS, Glauber Eduardo de Oliveira. **Modelo gravitacional do turismo: proposta teórica e estudo empírico dos fluxos turísticos no Brasil**. São Paulo, 2004. Dissertação (Mestrado em Ciências da Comunicação) – Escola de Comunicações e Artes, Universidade de São Paulo, São Paulo, 2004. Disponível em https://www.teses.usp.br/teses/disponiveis/27/27148/tde-12032005-122024/publico/Glauber.pdf. Acesso: 02 nov. 2023

VERGARA, S. **Projetos e relatórios de pesquisa em administração.** São Paulo: Atlas, 2007.