SEGURANÇA DE DADOS E TURISMO: MODELO TEÓRICO DE PRÁTICAS DE RESPONSABILIDADE SOCIAL CORPORATIVA E CIBERSEGURANÇA EM TRAVEL TECHS

Data security and tourism: theoretical model of corporate social responsibility and cybersecurity practices in Travel Techs

Layrane Mayara Lino Santos[1], Guilherme Bridi[2] & Luiz Augusto Machado Mendes Filho[3]

RESUMO

Os recursos tecnológicos possibilitam o aumento da competitividade, comunicação e expansão de vendas das empresas. No turismo, as Travel Techs aplicam tecnologias inovadoras para otimizar a experiência do viajante e, de certa forma, ajudar as empresas a obterem tecnologia no seu cotidiano melhorando os processos internos. O uso da internet e tecnologias se tornam importantes para a expansão de canais de comercialização, porém a sua utilização possui riscos, dentre eles a violação e vazamento de dados, principalmente por envolver dados financeiros de clientes e empresas. Diante do cenário da segurança de dados, o qual evidencia que as empresas precisam se proteger para que possam garantir serviços de qualidade, o uso da Responsabilidade Social Corporativa (RSC) atrelado a cibersegurança busca reconhecer os desafios inerentes à violação e vazamento de dados que as empresas de turismo enfrentam para manter a qualidade de seus serviços protegendo os seus dados e de seus clientes, além de proteger a imagem da empresa. A RSC no contexto da cibersegurança possui diversos benefícios para as Travel Techs que adotarem suas nuances, pois a não violação ou vazamento de dados implica na imagem da empresa criando assim uma reputação sólida no mercado. Travel Techs que priorizam a segurança de dados proporcionaram um ambiente seguro para os seus clientes e se protegendo de possíveis violações. Portanto, este artigo tem como objetivo propor um modelo teórico que explore a interseção de boas práticas de RSC e a cibersegurança no contexto das Travel Techs. O método adotado para a construção do modelo teórico consistiu em uma pesquisa bibliográfica de natureza teórico conceitual. O estudo teve como principais referências a Teoria da Responsabilidade Social Corporativa, o qual foram organizados e articulados em construtos analíticos. A partir desse procedimento metodológico, foi desenvolvido um modelo teórico composto por cinco hipóteses de pesquisa. Como resultado, o modelo indica que travel techs que adotam políticas de proteção de dados, atuam em conformidade legal e normativa,

[1] **Layrane Mayara Lino Santos –** Doutoranda em Turismo (PPGTUR/UFRN). Universidade Federal do Rio Grande do Norte. Natal, Rio Grande do Norte, Brasil. Lattes: http://lattes.cnpq.br/5154185201017288. ORCID: https://orcid.org/0000-0001-7418-9780. E-mail: layrane16@gmail.com.

[2] **Guilherme Bridi –** Doutor em Desenvolvimento Regional na Universidade Federal de Santa Cruz do Sul (UNISC). Professor do Programa de Pós-Graduação da Universidade Federal do Rio Grande do Norte (PPGTUR/UFRN). Natal, Rio Grande do Norte, Brasil. Lattes: http://lattes.cnpq.br/1626859396401842. ORCID: https://orcid.org/0000-0003-1848-9476. E-mail: guilherme.bridi@ufrn.br.

[3] **Luiz Augusto Machado Mendes Filho –** Doutor em Administração. Professor do Programa de Pós-Graduação da Universidade Federal do Rio Grande do Norte (PPGTUR/UFRN). Natal, Rio Grande do Norte, Brasil. Lattes: http://lattes.cnpq.br/7785924812425468. ORCID: https://orcid.org/0000-0002-9175-8903. E-mail: luiz.mendes@ufrn.br.

mantêm práticas éticas no tratamento das informações de seus clientes tendem a apresentar maior nível de proteção frente a problemas relacionados à segurança de dados no turismo.

PALAVRAS-CHAVE

Turismo; Proteção de Dados; Travel Techs; Cibersegurança; Responsabilidade Social Corporativa.

ABSTRACT

Technological resources enable companies to increase their competitiveness, communication and sales. In tourism, Travel Techs apply innovative technologies to optimize the traveler experience and, in a way, help companies to obtain technology in their daily lives, improving internal processes. The use of the internet and technologies has become important for the expansion of sales channels, but their use has risks, including data breaches and leaks, mainly because they involve financial data of customers and companies. Given the scenario of data protection, which shows that companies need to protect themselves in order to guarantee quality services, the use of corporate social responsibility (CSR) linked to cybersecurity seeks to recognize the challenges inherent to data breaches and leaks that tourism companies face in maintaining the quality of their services, protecting their data and that of their customers, in addition to protecting the company's image. CSR in the context of cybersecurity has several benefits for Travel Techs that adopt its nuances, since the absence of data breaches or leaks affects the company's image, thus creating a solid reputation in the market. Travel Techs that prioritize data security have provided a secure environment for their customers and protected themselves from potential breaches. Therefore, this article aims to propose a theoretical model that explores the intersection of CSR best practices and cybersecurity in the context of Travel Techs. The method adopted for the construction of the theoretical model consisted of a theoretical–conceptual literature review. The study was primarily grounded in the Corporate Social Responsibility Theory, which were organized and articulated into analytical constructs. Based on this methodological procedure, a theoretical model comprising five research hypotheses was developed. As a result, the model indicates that travel tech firms that adopt data protection policies, operate in legal and regulatory compliance, and maintain ethical practices in the handling of their customers' information tend to exhibit higher levels of protection against issues related to data security in tourism.

KEYWORDS

Tourism; Data Protection; Travel Techs; Cybersecurity; Corporate Social Responsibility.

INTRODUÇÃO

Recursos tecnológicos como a internet (e seus serviços) vem trazendo diversos benefícios, tanto para indivíduos, como para empresas, instituições e para a sociedade em geral. Os recursos são

utilizados para fins de entretenimento e lazer, armazenamento de informações, comunicação, comercialização de serviços e produtos, operações financeiras, entre outros.

Quando consideramos o uso de recursos tecnológicos em organizações do setor turístico, esse cenário fica ainda mais evidente. O turismo tem como característica basilar o emprego de tecnologia como aliada para o seu desenvolvimento, tal como afirmam Soares, Albuquerque, Mendes-Filho e Alexandre (2023, p. 3), "O setor de turismo incorpora a tecnologia em seus diversos segmentos visando fornecer informações confiáveis e precisas, e seu crescimento depende da capacidade de inovar e utilizar a tecnologia para melhorar a gestão".

Dessa forma, visando realizar uma abordagem junto às organizações turísticas que se usam da tecnologia, o objeto deste estudo é a organização Travel Tech, que representa um avanço significativo em relação ao modelo clássico de agências de turismo. As Travel Techs aplicam tecnologias inovadoras para otimizar a experiência do viajante e, de certa forma, ajudar as empresas a obterem tecnologia no seu cotidiano melhorando os processos internos. Kuss e Megdalia (2023, p. 8) assinalam que as Travel Techs foram caracterizadas a partir da "transformação digital gerada pelas novas tecnologias e tipos de comércio eletrônico, desenvolveram diversas alterações no âmbito da prestação de serviços. No turismo esses novos modelos têm se consagrado como Travel Techs".

Por ser organizações altamente tecnológicas, às Travel Techs também se caracterizam por gerar grande volume de dados, que podem conter informações sensíveis de empresas e clientes/consumidores, tendo em vista que muitas vezes é necessário realização de cadastro (contendo dados pessoais) para efetivação de uma compra de produtos e serviços no ambiente virtual (Lira & Machado, 2022).

A crescente quantidade de dados gerados evidencia a ampla utilização da internet por diversos setores e usuários, quanto mais sensível ao consumidor, maior é a possibilidade de invasão aos sistemas (Bamiatzi, Dowling, Gogolin, Kearney & Vigne, 2023), o que abre caminho para que esses dados sejam ser usados de formas criminosas. Os ataques ocorrem de diversas formas em empresas de todo mundo. De acordo com a Verizon (2023, p. 24, tradução nossa), "o roubo de dados mais comum em empresas é o tipo Ransomware (vírus malware que rouba os dados das empresas), ao ano são cerca de 3.966 incidentes, sendo 1.944 com dados de invasão divulgados e 97% desses ataques são ligados ao setor financeiro".

Visando mitigar os impactos negativos gerados por essa realidade, é essencial para as empresas desenvolverem ações e estratégias com responsabilidade, o que converge para a ideia de Responsabilidade Social Corporativa (RSC). Porém, a RSC vai além de obrigações previstas em leis. Uma empresa não apenas cumpre as leis estabelecidas pelo governo, é necessário também a utilização de obrigações morais, assim assumindo boas práticas para o desenvolvimento social das pessoas (Primolan, 2004). A atuação da RSC nas empresas também implica na qualidade da prestação de serviços para a sociedade. Entende-se que uma empresa que se preocupa com questões sociais e no bem-estar do consumidor, ofertam um produto ou serviço de melhor qualidade o qual influencia diretamente em sua imagem (Primolan, 2004).

Porém, há diversas leis que convergem no consumidor, e consequentemente isso resulta que as empresas também precisam ser responsáveis pelos seus clientes, e por informações e dados gerados do usuário em ambiente virtual. Considerado o vazamento e a segurança de dados gerados, a empresa torna-se responsável por zelar e tratar de informações sensíveis dos clientes, nisto levanta-se que a RSC poderá vir a ser aplicada nesse sentido.

Nesse cenário, destaca-se a necessidade de implementar medidas robustas de segurança de dados nos níveis organizações das empresas, considerando o crescente número de ataques de invasões no setor turístico. Com a sensibilidade dos consumidores em relação aos riscos financeiros decorrentes de ataques cibernéticos, principalmente no que concerne a roubo de informações pessoais, diante disso, levanta-se o questionamento: Seria possível estabelecer, por meio de uma análise da literatura existente, conexões teóricas entre Responsabilidade Social Corporativa e segurança de dados em Travel Techs?

A revisão da literatura conduzida na base de dados Web of Science, demonstrou incipiência nas pesquisas relacionando os temas de segurança de dados, turismo e responsabilidade social corporativa. Evidenciando uma lacuna teórica, o qual reforça a relevância do estudo, ao indicar a necessidade de avanços conceituais sobre o tema. Desta maneira, esse artigo tem como objetivo propor a criação de um modelo teórico que explore a interseção de boas práticas de RSC e a segurança de dados no contexto das Travel Techs, contribuindo para a sistematização e ampliação do conhecimento existente e oferecendo bases para pesquisas futuras.

O estudo adota uma abordagem qualitativa de construção teórica, fundamentada na revisão estruturada e na síntese crítica da literatura acadêmica. Permitiu identificar que a RSC e suas

dimensões de responsabilidade econômica, ética, legal e filantrópica podem ser aplicadas no contexto da segurança de dados. Esse processo permitiu o desenvolvimento de um modelo teórico estruturado com cinco hipóteses de pesquisa, evidenciando a relação prática entre RSC e a segurança de dados no contexto das Travel Techs.

TECNOLOGIA, CIBERSEGURANÇA E TRAVEL TECHS

A tecnologia moldou a nova forma de fazer, vender e distribuir no turismo, melhorando a competitividade das empresas, automatizando processos e armazenando informações, permitindo que o setor se usufrui de várias ferramentas tecnologias em suas operações cotidianas (Dorcic, Komsic & Markovic, 2019). Além disso, a difusão tecnológica fez com que mais pessoas permanecem conectadas, principalmente devido aos avanços da internet e tecnologias móveis, Dorcic, Komsic e Markovic (2019, p. 9, tradução nossa) corroboram nessa questão, afirmando que “os turistas hoje estão mais conectados, tecnologicamente sofisticados e interessados na interação com as tecnologias móveis”.

Por conseguinte, pode-se observar novas formas de consumo no turismo também, fazendo com que as empresas precisem se adaptar ao novo estilo de vida do comprador e facilitar o processo de compras em seus canais de distribuição (Lohmann, 2006). Diante disso, o mercado turístico enfrenta desafios com o crescimento do turismo digital, sendo necessário se adaptar para atender a demanda de mercado. Santa Ana (2019, p. 12) afirma que “o crescimento do turismo teve como um dos grandes impulsionadores a transformação digital ou a digitalização da economia”.

Kuss e Megdalia (2023, p. 5) afirmam que “a indústria do turismo migra então para uma nova fase, a do Turismo 4.0, um novo ecossistema de valor turístico que está sendo construído sob um paradigma de produção de serviços altamente baseado em tecnologia e apoiado pelos princípios comuns de outras indústrias 4.0”. Logo, a digitalização do turismo permite a oportunidade de expansão de organizações e aumento da competitividade, originando assim as Travel Techs.

De acordo com Lino Santos (2025, p. 52) “as travel techs se configuram como organizações turísticas com base tecnológica que distribuem e comercializam seus produtos e serviços turísticos de forma virtual. São empresas rentáveis e escaláveis, seguindo o padrão de negócios de startups”. A autora ainda aborda que as plataformas online são o tipo de tecnologia

desenvolvida por essas empresas e que o foco da ferramenta é utilizado para a gestão de negócios, como empresas de eventos, hotéis, guias e agências de turismo receptivo.

Em 2020, a empresa Onfly (2020, s.p) realizou um mapeamento de Travel Techs e se referiu ao termo como empresas que tem como objetivo solucionar problemas de viagens, turismo e mobilidade a partir do desenvolvimento de tecnologias. Corroboram nessa questão Kuss e Magdalia (2023, p. 9) as quais acreditam que "as tecnologias desenvolvidas pelas empresas de Travel Techs, facilitam o mercado e resultam em uma economia de viagens mais eficiente e acessível para os consumidores". A constante evolução tecnológica traz consigo a necessidade de mudanças no comportamento do consumidor e das empresas. Como contraponto, Martins & Denkewicz (2021, p. 54, tradução nossa) afirmam que "as Travel Techs são oportunidades para a criação de novos produtos para atender a novos segmentos".

Por se caracterizar em uma empresa responsável por criar soluções e oportunidades a segmentos do turismo, as Travel techs se diferenciam das Online Travel Agency e agências tradicionais, pois elas possuem maior foco em tecnologia, com o intuito do turismo usufruir de suas soluções para o desenvolvimento e gestão da atividade (Mizrachi & Gretzel, 2020).

O desenvolvimento de novas tecnologias trouxe diversos benefícios para as operações do turismo, facilitando a vivência e contato entre turistas e empresas. Contudo, pouco se fala sobre impactos negativos da tecnologia, no que tange proteção de dados gerados pelo usuário, e seu armazenamento em grandes escalas (Li, Xu, Tang, Wang, & Li, 2018; Demirol, Das & Hanbay, 2023). No turismo, a geração de dados é diversa e ampla, o qual pode beneficiar o trade, as pesquisas e muito mais (Li, Xu, Tang, Wang, & Li, 2018).

Conforme destacado por Li, Xu, Tang, Wang, e Li (2018, p. 302), "o turismo é um sistema complexo que abrange uma série de operações (ou seja, transações, atividades ou eventos no mercado de turismo), como pesquisa na web, visita a páginas da web, reservas e compras online, etc". Assim, permitindo uma maior geração de dados no turismo permite também o seu armazenamento, como informa Buhalis (2000, p. 44), "o banco de dados gerados por clientes permite que as empresas possam usar os dados para traçar estratégias de comunicação com o consumidor. permitindo também flexibilidade e dinamicidade ao tarifário e melhor gerenciamento de reservas".

O armazenamento de informações pode ser benéfico para o turismo, pois ao ser utilizado da forma correta, permite que as empresas e destinos tracem suas estratégias competitivas para se destacar no mercado. Li, Xu, Tang, Wang e Li (2018) abordaram quais são os principais dados gerados por turistas, geralmente voltados para dados de vendas, incluindo dados pessoais, estes considerados sensíveis.

O fato de operar com dados sensíveis gera um alerta para as empresas do setor turístico no tocante a violações de dados. Conforme Bamiatzi, Dowling, Gogolin, Kearney e Vigne (2023, p. 3), "o impacto negativo de uma violação de segurança será exacerbado numa indústria sensível ao consumidor". A violação de dados ou de segurança ocorre quando o sistema de uma empresa é invadido e terceiros têm acesso a informações, Knight e Nurse (2020, p. 2) afirmam que "os incidentes de segurança podem ser caracterizados pela sua natureza maliciosa ou não intencional" fazendo com que o autor chama de crise cibernética.

A crise cibernética, como descrita por Knigth e Nurse (2020) pode trazer diversos impactos para as organizações, principalmente impactos negativos no setor financeiro. Nesse sentido, o Relatório de Data Breach da IBM (2023, p. 5) informa que "O custo médio da violação de dados atingiu o valor mais alto de todos os tempos em 2023, chegando a US$ 4,45 milhões. Isso representa um aumento de 2,3% em relação ao custo de US$ 4,35 milhões em 2022", o que corrobora com o proposto por Slapničar, Vuko, Cular e Drašček (2022, p. 1), no sentido de que "apesar da crescente conscientização e de numerosos mecanismos avançados de defesa tecnológica e de processos, o crime cibernético está aumentando".

Diante do cenário de aumento de incidentes e violações online, surge a preocupação dos empresários em se proteger dos riscos cibernéticos. O Relatório de Data Breach IBM (2023) evidencia que 51% das empresas planejam aumentar o investimento em proteção de dados. A constante preocupação e o cuidado com os dados é o que os autores chamam de gestão de risco aplicado a cibersegurança (Slapničar, Vuko, Cular & Drašček, 2022; Bamiatzi, Dowling, Gogolin, Kearney, & Vigne, 2023).

A gestão de risco na cibersegurança reflete as boas práticas de proteção de dados de seus usuários. A União internacional de telecomunicações da ITU-T (2009, p. 2) afirma que a "cibersegurança é o conjunto de ferramentas, políticas, conceitos de segurança, diretrizes,

abordagens de gerenciamento de risco, ações, treinamento, melhores práticas, garantia e tecnologias que podem ser usadas para proteger o ambiente cibernético [...]".

Conforme apontado pelo autor, a cibersegurança é entendida como um conjunto integrado de políticas e ações que inclui a adoção de medidas de segurança com intuito de proteção de dados. No contexto da cibersegurança, no Brasil, a lei de referência é a Lei Geral de Proteção de dados (LGPD) de Nº 13.709 de 2018. O governo brasileiro ainda realizou mais dois decretos específicos para garantir a segurança de dados, o primeiro trata-se da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC) pelo Decreto nº 10.748, de 16 de julho de 2021 e o Decreto de nº 11.856, de 26 de dezembro de 2023 que institui a Política Nacional de Cibersegurança.

Ademais, Lino Santos (2025) destaca a necessidade de adequação das travel techs em pensar na gestão de dados seguros com a utilização e compreensão da responsabilidade social corporativa para a gestão de risco em consonância com a LGPD, com realização de treinamentos internos e auditórias dos sistemas desenvolvidos por essas empresas. Consequentemente, a gestão de risco para ambientes online mostra-se essencial diante da constante evolução de ameaças virtuais. Além de implementar as ferramentas e tecnologias citadas pela ITU-T, é crucial adotar medidas e estratégias que antecipem os riscos potenciais de violações e incidentes. No turismo, é comum ocorrer ataques de roubo de dados online de clientes em agências de viagens, principalmente com clientes que fazem uso de cartão de crédito (Grubor, Ristić, Simeunović, Adamović, Sinergija, & Bijeljina, 2016).

Um exemplo no turismo que teve repercussão foi o caso da rede de hotéis Marriott, quando em 2018 assumiu-se que houve um roubo de dados de 500 milhões de clientes da rede de hotéis (Bamiatzi, Dowling, Gogolin, Kearney & Vigne; 2023). Em um e-mail enviado pela Marriott para os seus clientes, foi admitido o erro e foi informado aos clientes que as medidas de investigação e seguranças estavam sendo tomadas, devido à um acesso não autorizado ao banco de dados das propriedades Starwood (Marriott International, 2018). O relatório da Verizon (2023, p. 53) investiga ataques por áreas e informa que o setor de acomodações e serviços de alimentos sofreram ataques voltados para "Pagamentos (41%), Credenciais (38%), Pessoal (34%), Outros (26%)", e ainda informa que "100% dos ataques teve motivação financeira".

A partir desses dados, constata-se que o setor do turismo apresenta uma vulnerabilidade acerca dos dados gerados pelas empresas e usuários, logo, ressalta-se a importância em possuir uma

gestão de risco para minimizar os impactos e a cibersegurança. Diante desse contexto, parte da necessidade de medidas que impliquem em boas práticas e proteção de dados, pois Bamiatzi, Dowling, Gogolin, Kearney e Vigne (2023, p. 2) afirmam que "reconhecer e antecipar os riscos do negócio é imperativo para o sucesso futuro". Assim, é necessário desenvolver ações responsáveis que protejam a empresa e os dados gerados por ela.

RESPONSABILIDADE SOCIAL CORPORATIVA

A Teoria da Responsabilidade social corporativa refere-se a ideia do retorno que a empresa dá à sociedade e ao meio ambiente, uma vez que entende que as empresas geram impactos ao desenvolver suas atividades e ser responsável social é dar uma devolutiva à sociedade (Primolan, 2004). Isto implica a todos os impactos gerados para a sociedade e seus clientes. Schroeder e Schroeder (2004, p. 2) afirmam que "A responsabilidade social corporativa é justificada e defendida, tanto pelas empresas, sociedade e Estado, como um fenômeno que delimita as ações empresariais".

As empresas são uma parte da sociedade que busca a geração de bens e possui fins de lucratividade (Carrol, 1991; Schroeder & Schroeder 2004), logo, o surgimento da RSC parte da ideia de que as empresas não possuem apenas esse caráter de geração de bens, mas também tem que prestar serviços à sociedade se envolvendo em causas sociais (Schroeder & Schroeder 2004).

Para buscar envolvimento com a sociedade e ao mesmo tempo gerar lucros, a RSC apresenta orientações e critérios para que as empresas possam seguir para melhoria do desempenho comercial, tal como afirma o Carrol (1991, p. 40), "com foco nos resultados, a RSC sugere uma orientação abrangente para critérios normais pelos quais avaliamos o desempenho comercial, incluindo quantidade, qualidade, eficácia e eficiência".

Logo, o uso da RSC nas corporações possui o objetivo de ser um bom cidadão corporativo (Carrol, 1991) com a utilização de quatro critérios, sendo eles a responsabilidade econômica, legal, ética e filantrópica, estabelecidos por Carroll (1991) para desenvolver as competências necessárias para esse objetivo.

Ademais, Primolan (2004, p. 125) cita que "as organizações que desenvolvem ações de responsabilidade social conseguem diferenciar-se de seus concorrentes e são valorizadas por

seus clientes". Consequentemente, a empresa que realizar o cumprimento dos 4 pressupostos será considerada um bom cidadão corporativo, além de se valorizar no mercado e se destacar entre os consumidores.

METODOLOGIA

Este trabalho utilizou-se de pesquisa bibliográfica. Conforme Sousa, Oliveira e Alves (2021, p.65), "a pesquisa bibliográfica está inserida principalmente no meio acadêmico e tem a finalidade de aprimoramento e atualização do conhecimento, através de uma investigação científica de obras já publicadas." Com o intuito de investigar a proteção de dados nas empresas de turismo, especificamente em Travel Techs, como anteriormente mencionado, faz-se uma revisão da literatura na Web of Science utilizando de termos que se remetem ao turismo, segurança de dados e RSC.

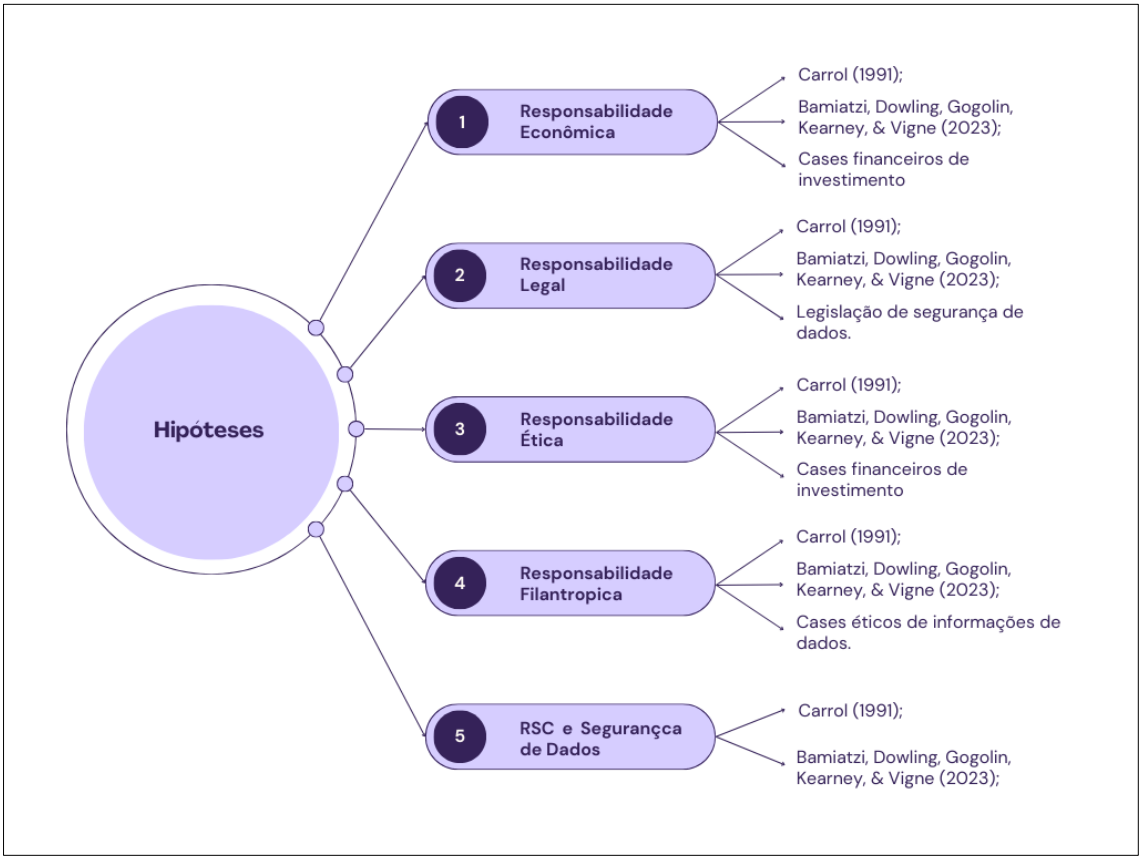
O levantamento dos estudos foi realizado na base de dados da Web Of Science, selecionada por sua relevância e abrangência no campo da gestão. Foram pesquisados termos em língua portuguesa: "turismo", "segurança de dados" e "responsabilidade social corporativa", não foi encontrado nenhum documento. Logo optou-se por utilizar os termos em idioma inglês e separados. Dessa forma, foi pesquisado "tourism, data, breach, and security", resultando num total de 23 documentos encontrados. Visando expandir as possibilidades de obter novos trabalhos, foi realizada nova pesquisa, utilizando os termos "corporate social responsibility, data, breach e security", com o total de 13 documentos.

Como critério de inclusão, foram considerados artigos científicos publicados em periódicos, disponíveis na íntegra e alinhados tematicamente à segurança de dados e a responsabilidade social corporativa aplicados ao setor do turismo. Foram excluídos artigos duplicados e trabalhos que não abordavam diretamente a temática da pesquisa. Ao final, foram analisados 20 artigos que subsidiaram a construção dos construtos analíticos e o desenvolvimento do modelo teórico proposto.

Em sequência, para a construção do modelo teórico e suas respectivas hipóteses foram empregados a Teoria da Responsabilidade Social Corporativa baseada em Carrol (1991), e a Responsabilidade social corporativa como seguro contra incidentes de segurança cibernética dos autores Bamiatzi, Dowling, Gogolin, Kearney & Vigne (2023), além da utilização de dados

empíricos de casos de proteção de dados que ocorreram em áreas distintas ao turismo, tal como apresentado na figura 1 abaixo:

Figura 1. Desenvolvimento de hipóteses



Fonte: Autores da pesquisa, 2025.

Acredita-se que o uso da RSC pode ser aplicado para a segurança de dados dos usuários em ambientes online, de modo a estimar em uma pesquisa empírica futura se o uso de boas práticas da responsabilidade social corporativa implica na cibersegurança e segurança de dados em Travel Techs.

MODELO TEÓRICO RESPONSABILIDADE SOCIAL CORPORATIVA: DESENVOLVENDO HIPÓTESES

A construção das hipóteses foi baseada nos estudos de Carrol (1991) e de Bamiatzi, Dowling, Gogolin, Kearney e Vigne (2023). Além disso, diante da dificuldade de encontrar na literatura exemplos concretos do setor turísticos (o que revela a existência de lacunas), optou-se por utilizar exemplos concretos advindos de áreas distintas.

O uso da RSC nas corporações possui o objetivo de ser um bom cidadão corporativo realizado devolutivas a sociedade (Carrol, 1991) com a utilização de quatro critérios estabelecidos para desenvolver as competências necessárias para ser tornar um bom cidadão. Além do mais, Primolan (2004, p. 125) cita que "as organizações que desenvolvem ações de responsabilidade social conseguem diferenciar-se de seus concorrentes e são valorizadas por seus clientes". Consequentemente, a empresa que realizar o cumprimento dos quatro pressupostos será considerada um bom cidadão corporativo além de se valorizar no mercado e se destacar entre os consumidores.

Ao seguir os critérios estabelecidos por Carrol (1991) as empresas se caracterizam como responsáveis, a RSC parte dos pressupostos de responsabilidade filantrópica, responsabilidade ética, responsabilidade legal e responsabilidade econômica e juntas elas formam a pirâmide da responsabilidade social corporativa. A pirâmide parte do pressuposto de boas práticas aplicadas em cada item, sendo a base a **responsabilidade econômica - RE** (grifo nosso) é responsável por gerir as demais voltada pela lucratividade da empresa, a **responsabilidade legal - RL** (grifo nosso) se refere ao cumprimento de leis estabelecidas pelo governo, a **responsabilidade ética - RET** (grifo nosso) refere-se a padrões e expectativas de preocupações da empresa para com os seus consumidores e a **responsabilidade filantrópica - RF** (grifo nosso) é aquela que está voltada para ações sociais gerando benefícios e caracterizando a empresa como bons cidadãos corporativos (Carrol, 1991).

RESPONSABILIDADE ECONÔMICA

A responsabilidade econômica (RE) está voltada para o processo de lucratividade da empresa na teoria original de Carrol (1991), e é vista como a base para as demais, pois a partir da obtenção de lucro existe a possibilidade em investir em melhorias que sejam aplicáveis na proteção de dados dos clientes que fazem o uso da ferramenta.

Uma determinada empresa, ao traçar investimentos e melhorias de segurança, está se protegendo de futuros ataques e assim traçando estratégias para reduzir os impactos negativos decorrentes de uma invasão Bamiatzi, Dowling, Gogolin, Kearney e Vigne (2023). A performance das corporações depende desses investimentos, tendo em vista que a responsabilidade econômica é a base para que as demais possam ser sustentadas, logo, aquelas empresas que

priorizam o investimento em segurança tem a possibilidade de diminuir os efeitos negativos da invasão de cibercriminosos.

Pesquisas demonstram que as invasões geram alto prejuízo econômico, como indica o Relatório da Verizon (2024), evidenciando 83% dos ataques possuem motivações financeiras. Devido às invasões prejudicarem as organizações financeiramente, o Relatório da Verizon (2023, p. 57, tradução nossa) ainda identificou que "51% das empresas pretendem aumentar o investimento em proteção". Outra pesquisa realizada pela Secure Way (2023, s.p.) apresentou que "79% dos líderes só aprovam o orçamento para proteção de dados somente após a ocorrência de uma violação de dados, enquanto o número de corporações atacadas chega a 92%".

A responsabilidade econômica constitui a base do modelo de RSC proposto por Carroll (1991), ao estabelecer que as finanças de uma organização é condição necessárias para o cumprimento das demais responsabilidades empresariais. Nessa perspectiva, instituições financeiras como o Banco Bradesco vêm investindo em cibersegurança, com a utilização de computação cognitiva para monitorar ameaças globais aos seus serviços (Security Leaders, 2024). Assim, dados do Ranking das reclamações do Banco Central (relativas a Irregularidades relativas à integridade, confiabilidade, segurança, sigilo ou legitimidade das operações no internet banking) demonstram que o Bradesco possui 17 reclamações, enquanto como Bancos concorrentes possuem índices de reclamações bem superiores (Banco Central, 2023).

No contexto das Travel Techs, a alocação de recursos financeiros em infraestrutura tecnológica e mecanismos de proteção de dados representa uma decisão orientada para diminuição de gastos financeiros e mitigação de invasões, como apontado pelo Banco Central (2023). Assim, as decisões econômicas incorporam a gestão responsável dos riscos digitais e passam a possuir alinhamento com a Responsabilidade Social Corporativa.

Consequentemente, constata-se que empresas que têm a visão em investir em proteção de dados, têm maior responsabilidade econômica ao que concerne ao seu produto e dados gerados por seus usuários. Isso posto, propõe-se a seguinte hipótese, correlacionada com o tema da pesquisa:

Hipótese 1: Travel Techs que priorizam o investimento em responsabilidade econômica impactam positivamente a RSC.

RESPONSABILIDADE LEGAL

Em termos de responsabilidades legais, de acordo com Carrol (1991, p. 41, tradução nossa), "espera-se que os negócios cumpram as leis e regulamentos promulgados pelos governos federal, estadual e local como as regras básicas sob as quais o negócio deve funcionar". Assim, as responsabilidades legais das empresas estão diretamente relacionadas ao cumprimento das leis gerais, funcionando como Carrol (1991) chama de "contrato social".

O cumprimento das leis não só respalda o consumidor, mas também a própria empresa, tendo em vista que as leis agem como molde, a base de direitos e deveres que o cidadão corporativo deve possuir para funcionar dentro das regularidades presentes em determinado país e região.

A proteção de dados é uma constante preocupação dos governos. Nos EUA, a proteção de dados é regida pela Lei Americana de Proteção de Privacidade de dados (H.R.8152, 2022, s.p, tradução nossa) tendo como objetivo "fornecer aos consumidores direitos fundamentais de privacidade de dados, criar mecanismos de supervisão fortes e estabelecer uma aplicação significativa". Já a Europa segue o Regulamento do Parlamento Europeu (2018, s.p, tradução nossa) o qual estabelece no "Art. 16º, nº 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelece que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito".

No Brasil, o cumprimento da legislação de proteção de dados se refere à Lei Geral de Proteção de Dados (LGPD) nº 13.853, de 2019. A LGPD parte do princípio de proteção e privacidade dos usuários em meio online, direcionada apenas para pessoas jurídicas de direito público ou privado, como informado Brasil (2019, art 1º): "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". Ou seja, as empresas que trabalham com dados sensíveis de clientes têm o dever previsto em lei garantir a segurança dos dados gerados online ou não. Ademais a LGPD tem como objetivo, Brasil (2019, Art 1º) "[...] proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

Recentemente, um assunto que ganhou destaque na mídia brasileira foram os incidentes ocorridos pela empresa META, G1 (2023, s.p): "a empresa META foi condenada pelo Tribunal de Justiça de Minas Gerais (TJMG) a pagar 20 milhões por vazamento de dados de usuários brasileiros ocorridos nos anos de 2018 e 2019".

Considerando que a legislação do país desempenha um papel fundamental na regulamentação e funcionamento das empresas, as leis referentes à proteção de dados (LGPD e Política Nacional de Cibersegurança) seguem um conjunto de regras que respaldam seus clientes e que permitem operar de maneira transparente. A responsabilidade legal, é compreendida como uma dimensão fundamental da RSC, considerando sua função estruturante na proteção de direitos e na prevenção de danos à sociedade, conforme abordado por Carroll (1991). No âmbito das Travel techs, o cumprimento das legislações relacionadas à proteção de dados, como a adequação da LGPD representa um compromisso com a empresa e seus usuários na garantia da proteção de dados (Lino Santos, 2025).

Consequentemente, o cumprimento das responsabilidades legais, além de evitar as penalidades legais e financeiras, surge como um construto que assegura as travel techs protejam seus dados e usuários do sistema, sob essa perspectiva o cumprimento das leis está intrinsicamente relacionado à cibersegurança, logo o estudo propõe a seguinte hipótese:

Hipótese 2: Travel Techs que cumprem as responsabilidades legais impactam positivamente a RSC.

RESPONSABILIDADE ÉTICA

A ideia de responsabilidade ética se relaciona com o construto que as empresas precisam seguir para serem bons cidadãos corporativos. A ética é essencial e um componente legítimo da RSC (Carrol, 1991), estando intrinsecamente relacionada aos valores das corporações. Isso posto, a proteção de dados é uma temática atualmente indispensável de ser incorporada aos valores das empresas, afirmação esta que se ancora nos pressupostos de Carrol (1991, p. 41, tradução nossa), “As responsabilidades éticas incorporam aqueles padrões, normas ou expectativas que refletem uma preocupação com o que consumidores”. Pode-se considerar que essa preocupação citada por Carrol (1991) correlaciona-se com a proteção de dados, uma vez que esta vai além de indicadores econômicos e se refere ao padrão de serviço oferecido.

A responsabilidade ética surge na perspectiva de cuidado com o consumidor, principalmente ao que refere a atingir as expectativas dos produtos e serviços ofertados, porém, também afeta na imagem que as empresas passam para a sociedade. Por serem socialmente responsáveis, a responsabilidade ética (RET) reflete que o foco da empresa é priorizar a preferência de seus clientes (Primolan, 2004).

A forma com que as empresas oferecem seus serviços reflete no seu sucesso e afeta diretamente a sua imagem e o seu papel na sociedade, ou seja, empresas que têm cuidado com os dados dos clientes tendem a ofertar serviços mais seguros. No que concerne a segurança de dados, o foco reside na preocupação com os dados gerados pelo usuário, tal como afirma Grubor, Ristić, Simeunović, Adamović, Sinergija e Bijeljina (2016, p. 01, tradução nossa), "roubo online de dados pessoais e credenciais de cartões de crédito diretamente relacionados com agências de turismo, onde os clientes pagam contas com cartões".

Dessa forma, as empresas precisam ter cuidado com as informações geradas pelos seus clientes para que não ocorra nenhum vazamento de dados. Contudo, muitas vezes não é isso que se observa na realidade. A Autoridade Nacional de Proteção de Dados (2023, s.p) afirma que "que algumas práticas de tratamento de dados pessoais ainda não estavam em completa conformidade com a legislação, incluindo o tratamento de dados pessoais para finalidades diferentes daquelas indicadas aos titulares e indícios de coleta excessiva de dados".

Isso está diretamente relacionado à proteção ética dos dados, onde as empresas fazem o uso de dados de forma incorreta, como é o caso de uma empresa líder em vendas online de serviços turísticos no Brasil, a qual recebeu milhares de reclamações de clientes sobre vazamento de dados, como afirma o CNN Brasil (2023).

As empresas têm como dever proteger os dados dos clientes, comprometendo-se com a ética da segurança. Por conseguinte, propõe-se a seguinte hipótese:

Hipótese 3: Travel Techs que tem responsabilidade ética com as informações dos clientes impactam positivamente a RSC.

RESPONSABILIDADE FILANTRÓPICA

A responsabilidade filantrópica se refere a ações sociais feitas pelas empresas, a fim de cumprir seu papel de bom cidadão corporativo. Ao seguir determinadas normas e regras, é necessário que as empresas também participem de ações sociais que contribuam de alguma forma para o desenvolvimento humano (Carrol, 1991).

O principal objetivo das empresas que fazem ações filantrópicas é atender as expectativas da sociedade (Carrol, 1991). Uma das expectativas da sociedade é a própria geração de emprego Primolan (2004, p. 128) ainda afirma que "a responsabilidade social difere da filantropia porque

reflete consciência social e dever cívico". Ao empregar os moradores do local onde ela está inserida, a empresa passa a desempenhar geração de emprego para aquelas pessoas. Logo, para ser responsável filantrópico é necessário cumprir os requisitos sociais, gerar esta devolutiva e isso consequentemente reflete no papel da empresa como cidadão corporativo (Zanandrea, Haag & Bitencourt 2022).

Porém, a responsabilidade filantrópica pode ir além da geração de emprego, atendendo também a qualidade de vida e satisfação e interação de seus colaboradores. Isso posto, cabe a empresa zelar por todos esses aspectos. Ademais, cabe ressaltar que, os funcionários (especialmente os descontentes) podem ser agentes de vazamento de informações sigilosas, como informa a Forbes Brasil (2023, s,p.) "os comportamentos dos funcionários têm sido a principal causa de entrada de criminosos aos dados das empresas, seja por violações de credenciais (29%), como senhas, ou por e-mails maliciosos (18%) e phishing (13%), que consiste em clicar em links perigosos".

Assim sendo, a empresa também precisa gerar um ambiente que atenda às expectativas de seus funcionários e os treinar para terem responsabilidade filantrópica que estimulem a segurança de dados. Propõe, assim, a seguinte hipótese:

Hipótese 4: Travel Techs que proporcionam ações de responsabilidade filantrópica aos seus funcionários impactam positivamente a RSC.

RESPONSABILIDADE SOCIAL CORPORATIVA

Considerando o que é necessário para as empresas possuírem para proteção de dados, Bamiatzi, Dowling, Gogolin, Kearney e Vigne (2023, p. 01, tradução nossa) afirmam que "utilização das medidas de responsabilidade social corporativa permite que as empresas se protejam de eventos de invasão e pode oferecer um melhor controle de expectativas de partes interessadas em situações de crises".

Carrol (1991) em suas pesquisas, trata da reputação em ser um bom cidadão corporativo que as empresas precisam dispor. Logo, com a geração de dados online e a comercialização de produtos e serviços pela internet, as corporações passam a ter um novo papel e uma nova responsabilidade a ser gerida.

Conforme anteriormente exposto, atualmente a RSC correlaciona-se também com a ideia de empresas que desenvolvem ações de proteção de dados virtuais. Nesse sentido, considerando que as Travel Techs possuem a característica intrínseca de serem empresas que fazem o uso de tecnologia como suporte para vendas de produtos e serviços, entende-se que a proteção de dados seja primordial para o desenvolvimento seguro do setor turístico. Em complemento, Bamiatzi, Dowling, Gogolin, Kearney e Vigne (2023, p. 03, tradução nossa) ainda retratam que "as atividades de RSC diminuem as implicações negativas de uma crise cibernética violação, agir como um escudo contra a opinião pública e protestos, e preservar a reputação corporativa".

Dessa maneira, as práticas da RSC estão relacionadas com a gestão empresarial, a ética e a segurança de dados, de acordo com Lino Santos (2025) afirma que as práticas da RSC permitem a empresa ter transparência e responsabilidades em termos de comunicação, experiência do cliente e credibilidade, com o intuito de garantir o armazenamento de informações de forma segura. Assim, pressupõe que uma travel tech que integra a RSC às suas práticas empresariais tendem a alcançar resultados significativos no que concerne a segurança de dados. Seguindo esse aspecto levanta-se a última hipótese desta pesquisa:

Hipótese 5: Travel Techs com maior adaptabilidade da Responsabilidade social corporativa tem melhor desempenho na segurança de dados.

MODELO PROPOSTO DO USO DA RSC E CIBERSEGURANÇA EM TRAVEL TECHS: CONSIDERAÇÕES TEÓRICAS

As pesquisas indicam que a utilização da RSC é adequada para o desenvolvimento empresarial para garantir a segurança de dados (Bamiatzi, Dowling, Gogolin, Kearney & Vigne, 2023; Lino Santos, 2025). Logo, ao considerar que o modelo teórico se refere à qualidade de serviços, ao uso ético dos serviços e produtos ofertados pelas empresas, entende-se assim que a RSC e sua aplicabilidade beneficiam a segurança de dados.

Considerado a ampla aplicabilidade da RSC, como citado por Bamiatzi, Dowling, Gogolin, Kearney e Vigne (2023, p. 1, tradução nossa) "a utilização das medidas de RSC permite que as empresas se protejam de eventos de invasão e pode oferecer um melhor controle de expectativas de partes interessadas em situações de crises", compreende-se que a sua utilização permite certa segurança para proteção dos dados gerados pelos usuários. Contudo, as pesquisas realizadas com o uso da RSC na tecnologia e proteção de dados são relativas ao setor financeiro,

focado na lucratividade das empresas e na área computacional de ciência de tecnologia e informação.

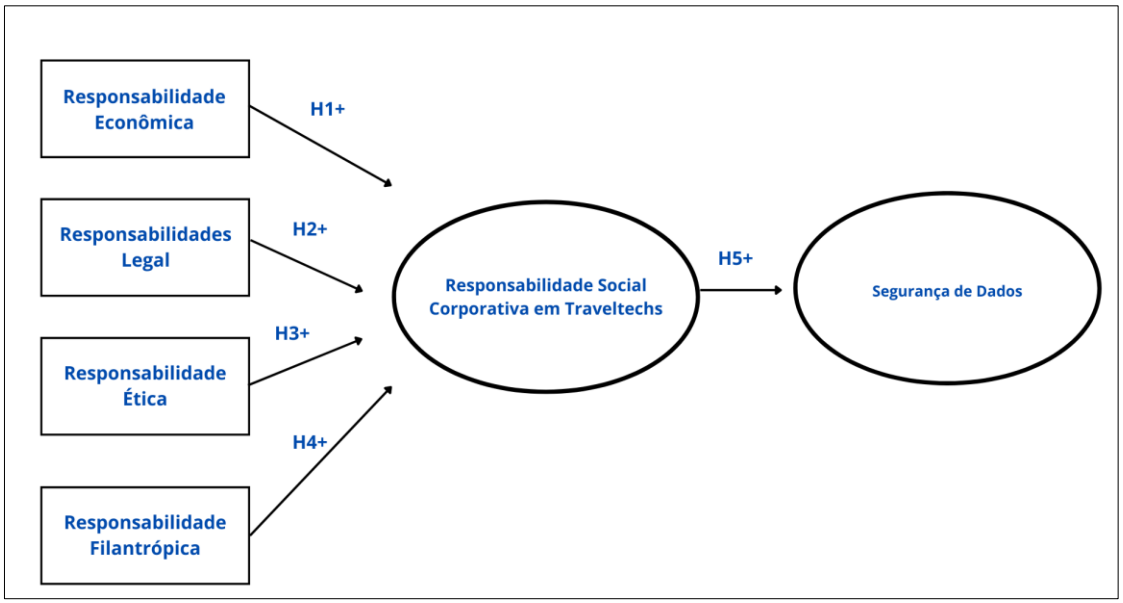
Portanto, para o presente estudo optou-se em ampliar a visão da RSC para além da questão da lucratividade. Assim, o modelo proposto parte do uso da Responsabilidade social corporativa em Travel Techs, empresas que ofertam serviços tecnológicos e objetivam inovação para o setor turístico. Isso já pode ser considerado um avanço teórico na literatura, visto que, tradicionalmente, no setor do turismo a abordagem da RSC concentra-se em práticas ambientes, verdes e sustentáveis dentro dos hotéis e com destaques de seus impactos dos hotéis e os benefícios para os seus clientes (Reinert, 2012).

A perspectiva da RSC tem foco em práticas sustentáveis, porém pode ser aplicada em relação aos serviços oferecidos pela empresa, como afirma Carrol (1991, p. 40, tradução nossa), “uma orientação abrangente para critérios normais pelos quais avaliamos os negócios desempenho para incluir quantidade, qualidade, eficácia e eficiência”.

Compreende-se que a empresa que tiver políticas de proteção de dados, seguir as normas estabelecidas em leis, ser ética com os dados dos seus clientes e ser uma boa cidadã corporativa estará menos suscetível a ter problemas relacionados à segurança de dados em geral, e, oferecendo um nível de proteção mais elevado quanto ao vazamento de dados.

No modelo proposto (Figura 2), optou-se seguir as dimensões da RSC abordada por Carrol (1991) e Bamiatzi, Dowling, Gogolin, Kearney & Vigne (2023), porém, tendo como enfoque o uso de RSC em segurança de dados, para assim tornar um modelo mais adequado para a cibersegurança em Travel Techs.

Figura 2. Desenvolvimento de hipóteses



Fonte: Autores da pesquisa, 2025.

O modelo proposto indica a interseção entre os construtos e como sua aplicabilidade tende a influenciar na segurança de dados em Travel techs. Lino Santos (2025, p. 78) aborda que "os riscos online estão se tornando cada vez mais comuns, principalmente no setor turístico devido a suas características de realização de transações online e fragilidade de informações". Logo, esse estudo aborda a necessidade de fortalecimento das organizações turísticas em segurança de dados, por meio da incorporação e aplicabilidade do modelo teórico.

Assim, compreende-se que o modelo teórico entre RSC e Travel Techs estejam corporificadas por meio da construção das cinco hipóteses apresentadas neste trabalho, bem como a respectiva discussão das mesmas à luz dos preceitos da RSC.

CONCLUSÕES E PESQUISAS FUTURAS

O presente estudo procurou despertar o interesse em explorar as práticas essenciais para que as corporações e Travel Techs se protejam das violações e ataques cibernéticos. Nesse contexto, o principal objetivo deste artigo teórico foi a criação de um modelo teórico que explorou a interseção de boas práticas da responsabilidade social corporativa está intrinsecamente ligada à cibersegurança no setor de Travel Techs como abordado por Lino Santos (2025).

Logo, neste estudo foi explorado as interconexões entre a responsabilidade social corporativa e a cibersegurança, visando proporcionar contribuições valiosas que orientem a formulação de

estratégias para as Travel Techs se protegerem no cenário digital. Assim, analisando o uso da responsabilidade econômica, responsabilidade legal, responsabilidade ética, responsabilidade filantrópica e a segurança de dados, acredita-se que juntas venham beneficiar as corporações com ações efetivas de proteção de dados.

Dito isso, destacamos a RSC no contexto da cibersegurança, possuindo diversos benefícios para as Travel Techs que adotarem suas nuances, pois a não violação ou vazamento de dados implica na imagem da empresa criando assim uma reputação sólida no mercado. Portanto, Travel Techs que priorizam a segurança de dados proporcionaram um ambiente seguro para os seus clientes e se protegendo de possíveis violações.

Em termos de contribuição teórica, a pesquisa aborda a Responsabilidade social corporativa em outra perspectiva proposta por Carroll (1991), pois, a expande além da área ambiental e destacando que as empresas que fazem o uso de dados, são responsáveis pelas informações geradas e por sua segurança. Enquanto as contribuições práticas, a pesquisa destaca a necessidade das travel techs se adequarem para que garantam a segurança de dados de seus usuários.

No entanto, é fundamental reconhecer as limitações inerentes a esta pesquisa. A principal limitação é o fato desta pesquisa ser teórica-conceitual, e assim, sugere-se a realização de uma pesquisa empírica com o modelo aqui elaborado com a construção de pesquisas futuras com a abordagem quantitativa, as quais terão como objetivo validar se esse modelo de fato consegue atender a proteção de dados em Travel Techs.

Além disso, as dinâmicas do cibercrime estão em constante evolução, podendo repercutir em futuras adaptações diante das mudanças do cenário digital. Portanto, este estudo não busca abordar exaustivamente toda complexidade inerente aos temas abordados. Pelo contrário, destaca-se a necessidade de desenvolver novos modelos que integrem outras teorias para investigar a cibersegurança, de modo a servir de base para a condução de outras pesquisas sobre o tema.

Além disso, pretende-se realizar uma pesquisa empírica futura com as Travel Techs em busca de analisar como a integração efetiva das práticas de RSC fortalecem a resiliência das organizações diante as ameaças digitais, e contribui para a construção de uma reputação sólida no mercado. Corroborando com Bamiatzi, Dowling, Gogolin, Kearney e Vigne (2023), a RSC não atua apenas

como uma barreira defensiva contra potenciais incidentes de cibersegurança, mas também demonstra o compromisso da empresa com os dados de seus clientes.

REFERÊNCIAS

Autoridade Nacional de Proteção de Dados (ANPD). (2023). ANPD divulga nota técnica sobre tratamento de dados pessoais no setor farmacêutico. Recuperado de Link. Acesso em 08 abr. 2024

Bamiatzi, V., Dowling, M., Gogolin, F., Kearney, F., & Vigne, S. (2023). Are the good spared? Corporate social responsibility as insurance against cyber security incidents. Risk Analysis, 43(12), 2503-2518.

Banco Central do Brasil. (2023). Ranking de domínios de internet por volume de requisições ao Sistema de Pagamentos Brasileiro. Recuperado de Link. Acesso em 03 abr. 2024.

Brasil. (2019, 16 de dezembro) Lei nº 13.853, de 08 de julho de 2019. Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Presidência da República. Recuperado de Link .

Brasil (2019, 29 de fevereiro). Decreto nº 10.748, de 13 de julho de 2021. Dispõe sobre Rede Federal de Gestão de Incidentes Cibernéticos. Diário Oficial da União, Brasília, DF. Recuperado de Link

Brasil (2023, 29 de janeiro). Decreto nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Diário Oficial da União, Brasília, DF, n. 308, p. 1-10. Recuperado de https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm

Buhalis, D. (2000). Marketing the competitive destination of the future. Tourism management, 21(1), 97-116.

Carroll, A. B. (1991). The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders. Business horizons, 34(4), 39-48.

Congresso dos Estados Unidos. (2022). Lei Americana de Proteção e Privacidade, H.R.8152, 117º Congresso, 2D. Link

CNN Brasil. (2023, 04 de abril). Clientes prejudicados e queda do CEO: Entenda o caso Hurb. Recuperado de Link

Demirol, D., Das, R. & Hanbay, D. (2023) A key review on security and privacy of big data: issues, challenges, and future research directions. SIViP, 17, 1335–1343.

Dorcic, J., Komsic, J. and Markovic, S. (2019), "Mobile technologies and applications towards smart tourism – state of the art", Tourism Review, Vol. 74 No. 1, pp. 82-103.

Forbes Brasil. (2023, 09 de abril). Seus funcionários podem tornar a empresa menos vulnerável a ciberataques. Forbes. Recuperado de Link

G1. (2023, 09 de abril). Meta deve pagar ao todo R$ 20 milhões para usuários brasileiros que tiveram dados vazados; veja se você será indenizado. G1. Recuperado de Link

Grubor, G., Ristić, N., Simeunović, N., Adamović, S., Sinergija, U., & Bijeljina, B. (2016) Optimizacija zaštite turističkih agencija od kompjuterskog kriminala Security optimization of travel agencies from cyber crime. Uloga i značaj turizma u privrednom rastu i razvoju, 72.

IBM. (2023, 13 de dezembro). Data breach trends. Recuperado de https://www.ibm.com/br-pt/reports/data-breach.

ITU-T. (2009, 08 de janeiro). Recommendation ITU-T X.1205: Overview of Cybersecurity Recuperado de Link.

Knight, R., & Nurse, J. R. (2020). A framework for effective corporate communication after cyber security incidents. Computers & Security, 99, 102036. ISSN 0167-4048.

Kuss, A. C., & Medaglia, J. (2023). Turismo e tecnologia da informação: das agências tradicionais às Travel Techs. Revista Brasileira de Pesquisa em Turismo, 16, 2668.

Li, J., Xu, L., Tang, L., Wang, S., & Li, L. (2018). Big data in tourism research: A literature review. Tourism management, 68, 301-323.

Lira, B. & Machado, D. C. (2022). Tratamento e proteção de dados no comércio eletrônico. In: Vigliar, J. (Org.) LGPD e a Proteção de Dados Pessoais na Sociedade em Rede: Dados de Crianças e Adolescentes na Internet; Tratamento de Proteção de Dados no Comércio Eletrônico. Grupo Almedina.

Lino Santos, L. M. (2025). O Papel da Responsabilidade Social Corporativa no desenvolvimento de Ações de Cibersegurança: um estudo em Travel Techs de Natal-RN.

Marriott International. (2018, 30 de novembro). Marriott announces Starwood guest reservation database security incident. Recuperado de Link. Acesso em 13 dez. 2023

Martins, B. M. L., & Denkewicz, P. (2021). Clusterização da tecnologia aplicada ao turismo por meio do mapeamento das Travel Techs brasileiras. Revista Acadêmica Observatório de Inovação do Turismo, 15(3), 52-71.

Mizrachi, I., & Gretzel, U. (2020). Collaborating against COVID-19: Bridging travel and travel tech. Information Technology & Tourism, 22(4), 489-496.

Onfly (2020, 10 de agosto). Mapa das Traveltechs brasileiras. Recuperado de Link.

Parlamento Europeu, Conselho da União Europeia. (2018). Regulamento (Ue) 2018/1725 Do Parlamento Europeu E Do Conselho De 23 De Outubro De 2018 relativo à proteção das

pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) nº 45/2001 e a Decisão nº 1247/2002/CE. Jornal Oficial da União Europeia, L 295/39.

Primolan, L. V. (2004). A responsabilidade social corporativa como um fator de diferenciação na competitividade das organizações. Revista Ibero-Americana de Estratégia, 3(1), 125-134.

Reinert, F (2012). Responsabilidade social corporativa e a gestão de stakeholders no turismo.

Santa Ana, A. G. (2019). Turismo Brasileiro 4.0: do analógico ao digital. A digitalização e a mudança na venda de "pacotes" de viagens nas operadoras de turismo do Brasil [Tese de doutorado, Fundação Getúlio Vargas]

Schroeder, J. T., & Schroeder, I. (2004). Responsabilidade social corporativa: limites e possibilidades. RAE eletrônica, 3.

Security Leaders. (2024, 03 de abril). Case de sucesso: Bradesco mapeia ameaças globais com inteligência cognitiva. Disponível em Link.

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44, 100548.

Soares, R, Albuquerque, T, Mendes-Filho, L, & Alexandre, M. (2023). Revisão sistemática da produção científica brasileira sobre turismo e tecnologia da informação e comunicação (TIC). Revista Brasileira de Pesquisa em Turismo, 16, e-2629.

Sousa, A. S., Oliveira, G. S., & Alves, L. H. (2021). A pesquisa bibliográfica: princípios e fundamentos. Cadernos da FUCAMP, 20(43).

Verizon (2023, 13 de dezembro). Relatório de investigações de violação de dados. Recuperado de Link.

Zanandrea, G., Haag, R., & Bitencourt, C. C. (2022). E, Agora, Para Onde Vamos? Inovação Social Como Um Caminho Para A Mudança. Desvendando a Inovação Social Casos de Ensino, 95.