SEGURANÇA DIGITAL EM PEQUENOS NEGÓCIOS: DESAFIOS, IMPACTOS E ESTRATÉGIAS PARA MITIGAR AMEAÇAS CIBERNÉTICAS

Henrique Eiji De Oliveira Yoshimoto e Cristiano Morini

Faculdade de Ciências Aplicadas, Universidade Estadual de Campinas

RESUMO: O avanço da transformação digital ampliou a eficiência e o alcance dos pequenos negócios, mas também elevou sua exposição a ameaças cibernéticas. Este artigo, vinculado a uma pesquisa de iniciação científica ainda em desenvolvimento, discute os principais desafios de segurança digital enfrentados por esse segmento e apresenta dois eixos analíticos centrais: a proposta preliminar de um instrumento diagnóstico de maturidade em segurança digital e a análise econômica do trade-off entre crescimento e investimento preventivo. O trabalho é fundamentado na revisão da literatura sobre pequenos negócios, cibersegurança, gestão de riscos e decisão sob incerteza. Como contribuição, organiza uma base teórico-metodológica para as etapas empíricas futuras da pesquisa, sem pressupor a validação do instrumento.

Palavras-chave: segurança digital. Pequenos negócios. cibersegurança. Gestão de riscos.

1 INTRODUÇÃO

A transformação digital alterou profundamente a forma como os pequenos negócios operam, vendem, se relacionam com os clientes e organizam seus processos internos. Ferramentas como sistemas de gestão, aplicativos de mensagens, plataformas de pagamento, armazenamento em nuvem e redes sociais passaram a compor a rotina de micro e pequenas empresas em diversos setores. Esse movimento ampliou oportunidades de eficiência, alcance comercial e flexibilidade operacional, mas também ampliou a superfície de exposição a riscos digitais.

No caso dos pequenos negócios, a incorporação de tecnologia frequentemente ocorre sem o desenvolvimento paralelo de capacidades mínimas de segurança digital. Ao contrário de organizações maiores, esses empreendimentos tendem a operar com recursos financeiros mais restritos, equipes enxutas e menor especialização técnica, o que dificulta a formalização de políticas, a adoção sistemática de controles e a resposta estruturada a incidentes. Em consequência, ameaças como phishing, roubo de credenciais, indisponibilidade de sistemas, vazamento de dados e fraudes digitais podem causar impactos proporcionais bastante severos.

Esse quadro ganhou ainda mais relevância após a aceleração da digitalização observada durante a pandemia de COVID-19, quando muitos negócios precisaram adotar rapidamente canais digitais para manter suas atividades (ALAJMI; ALOTAIBI, 2022). O problema é que a ampliação do uso de tecnologias nem sempre foi acompanhada por rotinas de atualização, de proteção de dados, de controle de acesso e de conscientização dos colaboradores. Assim, a segurança digital deixou de ser um tema periférico e passou a integrar, de forma cada vez mais evidente, a agenda de gestão e sobrevivência organizacional.

Ao adentrar ainda mais no assunto, nota-se que as fontes de informação que chegam aos micro e pequenos negócios são de extrema importância, pois orientam decisões operacionais e de investimento em segurança digital. Contudo, uma parcela significativa dessas empresas não acessa informações ou orientações sobre cibersegurança, com percentual estimado entre 40% e 50% (CARTWRIGHT; CARTWRIGHT; EDUN, 2023). Essa situação revela fragilidades nas campanhas públicas e reforça a importância de mapear a origem dessas orientações, avaliando sua confiabilidade e aplicabilidade ao contexto específico dos pequenos negócios.

Embora existam frameworks amplamente reconhecidos, como o NIST Cybersecurity Framework e a ISO/IEC 27001, sua aplicação integral costuma exigir recursos técnicos, humanos e organizacionais que nem sempre estão disponíveis no contexto de micro e pequenas empresas. Diante dessa lacuna, torna-se relevante desenvolver abordagens mais acessíveis, capazes de traduzir as dimensões essenciais da segurança digital em linguagem operacional para esse tipo de organização.

Diante desse panorama, apesar da grande relevância, observa-se que a maioria dos pequenos negócios carece de políticas consolidadas de segurança da informação. Muitas dessas empresas operam com práticas informais, sem processos definidos para controle de acesso, atualização de sistemas ou gestão de incidentes. A ausência de uma abordagem estruturada compromete não apenas a proteção dos dados, mas também a confiança de clientes e parceiros comerciais. Nesse contexto, essa pesquisa se propõe a identificar os riscos de cibersegurança enfrentados por pequenos e médios negócios, analisar casos e dados para entender quais são e como se realizam os principais ataques cibernéticos, o quanto os negócios afetados são prejudicados, além de buscar e estudar as opções que viabilizem a segurança digital dessas empresas — levando em conta todas as circunstâncias em que elas estão inseridas.

Nesse contexto, o presente artigo segue a linha de desenvolvimento adotada no projeto de iniciação científica “Segurança Digital em Pequenos Negócios: Desafios, Impactos e Estratégias para Mitigar Ameaças Cibernéticas”. O texto organiza a discussão em torno de dois eixos complementares. O primeiro é a proposta, ainda em desenvolvimento, de um instrumento diagnóstico simplificado para avaliação preliminar da maturidade em segurança digital em pequenos negócios. O segundo é a análise econômica do trade-off entre crescimento e segurança digital em ambientes marcados por restrições orçamentárias e por decisões sob risco.

2 REFERENCIAL TEÓRICO

2.1 Pequenos e médios negócios (PMEs)

Os pequenos e médios negócios ocupam posição central na economia contemporânea, não apenas por sua expressiva participação no total de empresas, mas também por sua contribuição para a geração de emprego, renda e dinamismo produtivo. Em escala global, esse grupo representa cerca de 90% das empresas e mais da metade dos empregos formais, evidenciando seu papel estrutural no funcionamento das economias (BANCO MUNDIAL, 2025). No Brasil, sua relevância também é significativa, uma vez que micro e pequenas empresas respondem por uma parcela importante do PIB nacional e se destacam especialmente nos setores de comércio e serviços (SEBRAE, 2014).

Apesar dessa importância, PMEs operam, em geral, sob condições mais restritivas do que as das grandes corporações. A literatura mostra que esses negócios convivem com

limitações recorrentes de capital, menor acesso ao financiamento formal, baixa disponibilidade de recursos humanos especializados e maior dificuldade em absorver choques externos (BECK; DEMIRGÜÇ-KUNT, 2006). Em vez de contar com estruturas robustas de gestão e planejamento, muitas dessas empresas dependem de decisões centralizadas, processos mais informais e rotinas operacionais menos padronizadas, o que pode afetar sua capacidade de crescimento e adaptação.

Outro ponto importante é que os desafios enfrentados por PMEs não decorrem apenas de fragilidades internas, mas também de fatores estruturais mais amplos. Há evidências de que o conhecimento produzido sobre pequenas e médias empresas ainda é fragmentado, pouco integrado e, muitas vezes, insuficientemente traduzido em recomendações práticas para gestores e formuladores de políticas públicas. Isso gera um ambiente de desinformação estrutural, no qual os pequenos negócios permanecem sem orientação clara sobre boas práticas de gestão, inovação e competitividade (MASSARO et al., 2016).

No contexto atual, a digitalização passou a integrar, de forma cada vez mais intensa, a realidade desses empreendimentos. Ferramentas digitais ampliam a capacidade de comunicação, gestão, vendas e relacionamento com clientes, ao mesmo tempo em que criam oportunidades de produtividade e expansão. Contudo, a literatura mostra que a transformação digital em PMEs não ocorre sem obstáculos: limitações financeiras, baixa maturidade tecnológica, carência de competências digitais e incertezas quanto ao retorno dos investimentos ainda constituem barreiras relevantes (THRASSOU et al., 2020). Assim, pequenos negócios se veem inseridos em uma dinâmica paradoxal: precisam digitalizar suas operações para permanecerem competitivos, mas frequentemente não dispõem de estrutura suficiente para realizar essa transição de forma plenamente segura e planejada.

Dessa forma, compreender PMEs de maneira integrada — considerando as dimensões econômicas, organizacionais, financeiras e tecnológicas — é condição essencial para analisar os riscos e as vulnerabilidades que emergem no processo de digitalização. Mais do que unidades produtivas de menor escala, esses negócios possuem uma lógica operacional própria, marcada por forte relevância econômica e, ao mesmo tempo, por fragilidades estruturais que influenciam diretamente sua exposição a ameaças digitais.

2.2 Ameaças cibernéticas e Segurança digital (Cybersecurity)

A expansão do uso de tecnologias digitais transformou profundamente a operação das empresas, mas também ampliou sua exposição a ameaças cibernéticas. Nesse novo cenário, incidentes digitais deixaram de ser episódios isolados para se consolidarem como parte de um ambiente permanente de risco, afetando organizações de todos os portes. Relatórios recentes indicam que uma parcela expressiva das empresas já enfrentou algum tipo de ataque cibernético, enquanto o custo econômico médio de vazamentos de dados e incidentes digitais permanece elevado, reforçando a centralidade do tema na gestão contemporânea (PROOFPOINT, 2022; IBM, 2025).

As ameaças cibernéticas podem assumir diferentes formas, mas muitas das mais recorrentes continuam associadas à exploração de vulnerabilidades humanas e organizacionais. Ataques de phishing, engenharia social, roubo de credenciais, malwares e ransomware figuram entre os principais vetores de comprometimento, justamente por explorarem práticas cotidianas, baixa conscientização e falhas de procedimento (DSIT, 2024). Isso mostra que a

vulnerabilidade digital não decorre apenas de insuficiências técnicas, mas também da interação entre tecnologia, comportamento humano e estrutura organizacional.

Nesse contexto, a segurança digital não deve ser entendida apenas como um conjunto de ferramentas tecnológicas, mas sim como uma dimensão mais ampla da gestão de riscos. Seu papel não se resume à proteção de sistemas e dados; ele também influencia a continuidade operacional, a confiança de clientes e parceiros, a reputação organizacional e até o desempenho financeiro da empresa. Os impactos de incidentes cibernéticos ultrapassam os custos diretos de restauração de sistemas ou de resposta técnica, alcançando perdas de receita, paralisação de operações, litígios, danos reputacionais e efeitos em cadeia sobre fornecedores e consumidores (VERGARA COBOS; CAKIR, 2024).

Além disso, a literatura recente mostra que a cibersegurança passou a ocupar uma posição mais estratégica nas organizações. Ela deixou de ser vista como uma questão estritamente técnica para ser tratada como um eixo de governança, com implicações para o risco operacional, o reputacional e a sustentabilidade do negócio (WORLD ECONOMIC FORUM, 2025). Paralelamente, o avanço da inteligência artificial reconfigurou ainda mais esse cenário, ampliando tanto a sofisticação dos mecanismos de defesa quanto o potencial ofensivo de agentes maliciosos, especialmente em campanhas automatizadas, fraudes personalizadas e exploração de vulnerabilidades em escala (SINGH et al., 2025).

Assim, a segurança digital precisa ser compreendida como elemento estruturante da operação empresarial em ambientes cada vez mais conectados. Quanto maior a dependência de sistemas digitais, maior a necessidade de incorporar a proteção cibernética à própria lógica organizacional, e não como aspecto periférico ou acessório. Essa constatação torna-se ainda mais relevante quando o foco recai sobre pequenos negócios, cuja capacidade de absorção de perdas tende a ser muito mais limitada.

2.3 Segurança digital em pequenos negócios

A discussão sobre segurança digital ganha contornos específicos quando direcionada aos pequenos negócios. Embora essas empresas também estejam inseridas no processo de transformação digital, sua realidade operacional difere substancialmente daquela observada em grandes corporações. Pequenos negócios passaram a depender cada vez mais de sistemas de gestão, serviços em nuvem, meios eletrônicos de pagamento, marketplaces, redes sociais e canais digitais de comunicação com clientes. Contudo, essa crescente dependência tecnológica não foi necessariamente acompanhada da adoção proporcional de práticas estruturadas de segurança (ENISA, 2021).

A literatura aponta que pequenas empresas frequentemente combinam alta exposição digital com baixa maturidade em cibersegurança. Isso ocorre porque operam com recursos limitados, pouca disponibilidade de pessoal especializado e capacidade reduzida para investir em soluções robustas de proteção. Em muitos casos, sequer existe equipe dedicada de TI e as decisões relacionadas à segurança são tomadas de forma reativa, informal ou terceirizada. Como consequência, controles básicos — como políticas mínimas de acesso, rotinas de backup, atualização regular de sistemas e capacitação de usuários — acabam sendo negligenciados ou implementados de forma incompleta (JUNIOR; BECKER; JOHNSON, 2023).

Esse cenário é agravado por fatores comportamentais e informacionais. Muitos empreendedores ainda operam sob a percepção equivocada de que seus negócios são pequenos demais para se tornarem alvo de ataques, o que contribui para o subinvestimento em medidas

preventivas. Além disso, há evidências de que uma parcela relevante dos micro e pequenos negócios sequer acessa orientações qualificadas sobre segurança digital e, quando o faz, frequentemente depende de fontes limitadas, como prestadores de TI ou conteúdos dispersos, sem garantia de aplicabilidade prática ao seu contexto (CARTWRIGHT; CARTWRIGHT; EDUN, 2023).

A vulnerabilidade desse segmento torna-se ainda mais crítica quando se consideram os potenciais efeitos de um incidente cibernético. Em pequenas empresas, uma paralisação temporária do sistema de vendas, do financeiro ou dos canais digitais de atendimento pode comprometer diretamente o fluxo de caixa e a continuidade operacional. Diferentemente de grandes organizações, que tendem a possuir mais reservas, redundâncias e maior capacidade de resposta, pequenos negócios frequentemente absorvem impactos de forma mais severa e imediata. Por isso, a segurança digital, nesse contexto, não pode ser tratada apenas como um custo adicional, mas como um componente relevante da resiliência e da sobrevivência organizacional (ENISA, 2021).

Outro aspecto importante é que a segurança digital em PMEs gera efeitos que extrapolam o âmbito individual da empresa. Quando um pequeno negócio melhora suas práticas de proteção, reduz não apenas o próprio risco, mas também o risco imposto a clientes, parceiros, cadeias de suprimento e ecossistemas locais. Nesse sentido, a literatura sugere que a cibersegurança em PMEs possui externalidades positivas relevantes, o que reforça a justificativa para políticas públicas, programas de capacitação e instrumentos de apoio direcionados a esse segmento (ARROYABE et al., 2024).

Além disso, o uso crescente de soluções em nuvem e de modelos SaaS introduz novas possibilidades e riscos. Tais ferramentas podem ser vantajosas para pequenos negócios por reduzirem a necessidade de infraestrutura própria e ampliarem a flexibilidade operacional. Entretanto, sua adoção não elimina a necessidade de práticas mínimas de segurança. Pelo contrário, erros simples de configuração, compartilhamento indevido de credenciais, ausência de autenticação adicional e revisão insuficiente de permissões podem criar brechas significativas para vazamentos de dados e acessos indevidos (WOJCIECHOWSKI et al., 2012).

Portanto, a segurança digital em pequenos negócios deve ser analisada a partir de sua realidade específica, como recursos escassos, processos frequentemente informais, forte dependência de ferramentas digitais e baixa margem de absorção de perdas. Essa combinação faz com que incidentes relativamente comuns tenham potencial para gerar efeitos desproporcionais. Por isso, discutir segurança digital nesse universo significa não apenas proteção técnica, mas também capacidade de continuidade, sustentabilidade e competitividade em um ambiente econômico cada vez mais digitalizado.

3 OBJETIVO

Este artigo tem como objetivo geral discutir os desafios e os impactos da segurança digital em pequenos negócios e organizar, com base no desenvolvimento atual da pesquisa, duas frentes analíticas centrais: a proposta de um instrumento diagnóstico simplificado para avaliação preliminar da maturidade em segurança digital e a formalização econômica do trade-off entre crescimento e investimento preventivo. De modo mais específico, busca-se compreender os principais tipos de vulnerabilidade enfrentados por esses empreendimentos,

traduzir dimensões teóricas em categorias observáveis e oferecer uma base conceitual para futuras etapas de refinamento e de aplicação empírica da pesquisa.

4 DESENVOLVIMENTO DO QUESTIONÁRIO DIAGNÓSTICO

4.1 Apresentação da ideia

A crescente digitalização dos pequenos negócios ampliou significativamente sua exposição a riscos cibernéticos e, ao mesmo tempo, evidenciou a ausência de mecanismos estruturados e acessíveis para avaliação interna da maturidade em segurança digital. Embora existam frameworks consolidados internacionalmente, muitos deles apresentam elevado grau de complexidade técnica e operacional, o que reduz sua aplicabilidade em micro e pequenas empresas com recursos financeiros, humanos e técnicos limitados.

Diante dessa lacuna, a pesquisa propõe o desenvolvimento de um instrumento diagnóstico simplificado, voltado especificamente à realidade dos pequenos negócios. A ideia não é substituir auditorias técnicas, certificações formais ou análises especializadas, mas sim oferecer um mecanismo preliminar de autodiagnóstico organizacional. Em termos práticos, trata-se de uma ferramenta pensada para ajudar gestores a visualizar vulnerabilidades estruturais e priorizar ações compatíveis com sua capacidade operacional.

Desde o início, a concepção do instrumento foi guiada pelo esforço de equilibrar rigor conceitual e aplicabilidade prática. Por isso, a proposta parte de categorias já consolidadas na literatura de cibersegurança e de gestão de riscos, mas busca traduzi-las em uma linguagem objetiva, acessível e operacionalizável no contexto dos pequenos negócios. Nesta etapa da pesquisa, o instrumento deve ser entendido como uma estrutura em desenvolvimento, ainda não validada empiricamente.

4.2 Fundamentação teórica

A construção do instrumento diagnóstico foi fundamentada em referenciais consolidados da literatura de cibersegurança e de gestão de riscos organizacionais, adaptados à realidade operacional dos pequenos negócios. Frameworks reconhecidos, como o NIST Cybersecurity Framework e a ISO/IEC 27001, oferecem estruturas abrangentes de governança, controle e gestão da segurança da informação, mas sua aplicação integral costuma demandar recursos nem sempre disponíveis nesse tipo de organização (NIST, 2024; ISO, 2013). Por essa razão, optou-se por uma síntese conceitual das dimensões consideradas essenciais e viáveis, em diálogo com recomendações operacionais de referências aplicadas, como o Cybersecurity Blue Team Toolkit (TANNER, 2019).

Com base na convergência desses referenciais, a proposta em desenvolvimento aborda cinco dimensões centrais. A primeira diz respeito à governança e cultura organizacional, uma vez que a segurança digital não depende apenas de mecanismos técnicos, mas também de liderança, definição de responsabilidades e disseminação de práticas de conscientização interna. Em pequenos negócios, marcados por estruturas mais informais e centralizadas, a existência de diretrizes mínimas e de atribuição de responsabilidade já constitui um indicador relevante de maturidade.

A segunda dimensão refere-se à gestão de acessos e ao controle de privilégios. A literatura mostra que credenciais comprometidas, permissões excessivas e controles de

autenticação fracos figuram entre os fatores mais recorrentes em incidentes cibernéticos. Assim, medidas como autenticação multifator, definição de critérios mínimos para senhas e limitação de privilégios administrativos aparecem como elementos de alto impacto e baixo custo.

A terceira dimensão envolve a proteção técnica e a manutenção de sistemas. Atualizações regulares, uso de antivírus, presença de firewall e rotinas mínimas de monitoramento constituem a camada inicial de defesa contra ameaças recorrentes. Já a quarta dimensão contempla a gestão e a proteção de dados, incluindo a identificação de informações sensíveis, o controle de acesso a dados financeiros e de clientes e práticas adequadas de armazenamento e recuperação. Mesmo os pequenos negócios estão submetidos a responsabilidades relacionadas à proteção de dados, o que reforça a relevância dessa dimensão (BRASIL, 2018).

Por fim, a quinta dimensão trata da capacidade de resposta e de recuperação diante de incidentes. Nenhum sistema é completamente imune a ataques; por isso, a existência de procedimentos mínimos para resposta, registro de ocorrências e restauração de backups é decisiva para a resiliência organizacional. A partir dessas cinco dimensões, busca-se estruturar um instrumento sintético e operacionalizável, capaz de representar fatores centrais da vulnerabilidade cibernética sem pretender esgotar a complexidade do tema.

4.3 Metodologia de desenvolvimento

Após a definição das dimensões teóricas, passou-se à etapa metodológica de construção e de operacionalização dos itens. O desenvolvimento do questionário seguiu uma lógica dedutiva, partindo de construtos conceituais amplamente reconhecidos na literatura e convertendo-os em variáveis observáveis no contexto organizacional. Em vez de formular perguntas de modo arbitrário, a proposta procura assegurar que cada item corresponda diretamente a um construto previamente fundamentado.

A operacionalização consistiu em transformar conceitos abstratos — como governança, controle de acesso, proteção técnica ou capacidade de resposta — em indicadores concretos e verificáveis. Assim, o construto “gestão de acessos”, por exemplo, pode ser observado por meio de elementos como a utilização de autenticação multifator, a definição de critérios mínimos para a definição de senhas e a limitação de privilégios administrativos. A mesma lógica vale para as demais dimensões.

Nesta fase da pesquisa, a estrutura preliminar do instrumento consiste em vinte itens distribuídos entre as cinco dimensões anteriormente definidas. Também se propõe, de maneira exploratória, uma escala simples de três pontos: 0 para prática inexistente, 1 para prática parcialmente implementada ou informal e 2 para prática formalmente implementada e institucionalizada. A escolha por essa escala reduzida decorre da necessidade de simplicidade operacional e de compatibilidade com a realidade dos pequenos negócios.

A partir da pontuação atribuída aos itens, propõe-se a construção de um índice composto denominado Índice de Vulnerabilidade Cibernética (IVC), calculado pela razão entre a soma das pontuações obtidas e a pontuação máxima possível. Em termos formais, a proposta preliminar pode ser expressa como:

$$IVC = (\Sigma x_i) / 40$$

Em que x_i representa a pontuação atribuída a cada item e 40 corresponde à pontuação máxima total, considerando vinte itens com valores entre 0 e 2. Para fins interpretativos exploratórios, sugere-se a classificação em três faixas: de 0 a 0,33, alta vulnerabilidade; de 0,34 a 0,66, vulnerabilidade moderada; e acima de 0,67, maturidade básica estabelecida. Essas faixas têm caráter indicativo e poderão ser revistas em etapas posteriores de refinamento metodológico.

4.4 Limitações metodológicas e possibilidades futuras

Apesar do rigor conceitual empregado até aqui, é importante reconhecer que o instrumento permanece em estágio exploratório. Até o presente momento, não houve validação estatística, aplicação em amostra de organizações reais nem testes formais de confiabilidade interna ou de estrutura dimensional. Desse modo, não seria adequado tratar o questionário como uma ferramenta concluída ou empiricamente validada.

Outra limitação diz respeito à adoção deliberada de uma escala simplificada de três pontos. Embora essa escolha favoreça clareza, aplicabilidade e maior facilidade de resposta, ela reduz a granularidade do instrumento e pode limitar a captura de diferenças mais sutis entre organizações. Ainda assim, essa simplificação parece coerente com o objetivo de elaborar uma proposta preliminar de autodiagnóstico adequada ao contexto dos pequenos negócios.

Como possibilidades futuras, recomenda-se a realização de estudos quantitativos voltados à avaliação da consistência interna do índice, à verificação da robustez das dimensões propostas e ao eventual refinamento dos itens. A aplicação em diferentes setores econômicos também poderá contribuir para ajustes contextuais e para o aprimoramento da utilidade analítica do instrumento.

Em termos de pesquisa, a etapa empírica deve ser compreendida como posterior ao trabalho ora apresentado. Qualquer aplicação junto a organizações reais dependerá tanto do amadurecimento metodológico do instrumento quanto das autorizações éticas e institucionais pertinentes.

5 ANÁLISE ECONÔMICA PROFUNDA DO TRADE-OFF

5.1 Apresentação do problema

Pequenos negócios operam, em geral, sob restrições significativas de recursos financeiros, humanos e técnicos. Nesses contextos, decisões de investimento exigem priorização entre alternativas que competem entre si. No âmbito da transformação digital, um dos dilemas centrais enfrentados por empreendedores consiste na alocação de recursos entre iniciativas voltadas ao crescimento do negócio — como expansão comercial, marketing ou aquisição de novos clientes — e investimentos em segurança digital, cujo retorno não costuma se manifestar diretamente no aumento da receita, mas sim na redução da probabilidade ou da severidade de perdas futuras.

Esse cenário pode ser compreendido como um problema de decisão sob risco. Considere-se um empreendedor que dispõe de um orçamento total B para um determinado período. Esse montante pode ser alocado entre duas categorias principais: G, que representa investimento em crescimento, e S, que representa investimento em segurança digital, de modo que $B = G + S$. A decisão econômica relevante consiste em determinar a combinação entre essas parcelas que maximize o resultado esperado da empresa.

O investimento em crescimento tende a gerar retorno positivo relativamente previsível, ainda que sujeito a incertezas de mercado. Já o investimento em segurança digital não produz, em regra, incremento imediato de receita, mas atua como mecanismo de mitigação de risco, reduzindo a probabilidade e/ou a severidade de perdas decorrentes de ataques cibernéticos. Assim, a insuficiência de investimento em segurança pode expor a empresa a eventos adversos capazes de comprometer receitas, gerar custos operacionais inesperados e afetar a reputação organizacional.

Forma-se, então, um trade-off intertemporal e probabilístico: priorizar investimentos com retorno mais visível no curto prazo ou alocar parte do orçamento para reduzir a exposição a riscos cuja materialização é incerta, porém potencialmente severa. A formalização desse dilema contribui para compreender em que condições o investimento em segurança deixa de ser percebido apenas como custo e passa a ser interpretado como um instrumento racional de preservação de valor.

5.2 Fundamentação teórica

A análise do trade-off entre crescimento e segurança digital pode ser fundamentada na teoria econômica da decisão sob risco, segundo a qual agentes econômicos alocam recursos escassos de modo a maximizar sua utilidade ou lucro esperado diante de incertezas. Em contextos empresariais, especialmente em pequenas organizações, decisões de investimento frequentemente envolvem escolhas entre aplicações com retorno esperado positivo e previsível e investimentos de caráter preventivo, cujo benefício se manifesta principalmente na redução da probabilidade ou da severidade de perdas futuras (VON NEUMANN; MORGENSTERN, 1944).

Sob a perspectiva da teoria do valor esperado, investimentos em segurança podem ser compreendidos como mecanismos de mitigação de risco, reduzindo a perda esperada associada a eventos desfavoráveis. A perda esperada é definida como o produto da probabilidade de ocorrência de um evento e do impacto financeiro decorrente desse evento (HULL, 2018). Assim, ainda que a segurança digital não gere receita adicional direta, sua função econômica reside na preservação de valor e na redução da variância dos resultados organizacionais (DAMODARAN, 2014).

Em pequenas empresas, esse dilema tende a ser mais acentuado devido à restrição orçamentária mais severa e à maior sensibilidade a choques negativos. Enquanto grandes corporações podem diluir perdas decorrentes de incidentes cibernéticos em estruturas financeiras robustas, pequenos negócios frequentemente enfrentam impactos proporcionais significativamente maiores, podendo inclusive comprometer a continuidade das atividades. Nesse sentido, o investimento em segurança assume o caráter de proteção patrimonial e de garantia da sobrevivência organizacional.

Além disso, a literatura de economia comportamental sugere que decisões sob risco não são tomadas exclusivamente com base na racionalidade perfeita. Pequenos empreendedores podem subestimar as probabilidades de eventos raros, apresentar viés de otimismo ou priorizar retornos imediatos em detrimento da proteção contra riscos futuros. Esses elementos contribuem para um possível subinvestimento em segurança digital, mesmo quando a análise racionalmente estrita indicaria maior alocação preventiva (KAHNEMAN; TVERSKY, 1979).

A fundamentação teórica do trade-off, portanto, combina elementos da teoria da decisão sob risco, da análise de valor esperado e da economia comportamental. Essa abordagem

permite estruturar formalmente o problema de alocação de recursos entre crescimento e segurança, fornecendo uma base conceitual para a modelagem quantitativa apresentada na subseção seguinte.

5.3 Formalização analítica do trade-off

Com base na fundamentação teórica apresentada, a análise econômica do trade-off entre crescimento e segurança digital pode ser estruturada a partir de um modelo de lucro esperado sob risco. A ideia central é representar, de forma simplificada, a decisão do pequeno negócio diante de um orçamento limitado, no qual os recursos precisam ser distribuídos entre investimentos voltados à expansão da operação e à proteção contra ameaças cibernéticas.

O ponto de partida dessa modelagem consiste em tratar o investimento em crescimento como um fator gerador de retorno econômico esperado, associado à ampliação da capacidade operacional, ao aumento de receitas, à melhoria de processos ou à expansão comercial. Em paralelo, o investimento em segurança digital é compreendido não como fonte direta de receita, mas como mecanismo de mitigação de risco, na medida em que reduz a probabilidade de ocorrência de incidentes ou atenua a magnitude de suas perdas potenciais. Dessa forma, a segurança digital passa a ser interpretada economicamente como um instrumento de preservação de valor.

A construção analítica desse trade-off pode seguir quatro etapas complementares. A primeira é a modelagem do lucro esperado, na qual se busca representar a relação entre o retorno econômico, a exposição ao risco e a restrição orçamentária. Nessa etapa, o objetivo é mostrar que a decisão de investimento não deve ser avaliada apenas pelo potencial de geração de receita, mas também pela capacidade de evitar perdas futuras decorrentes de falhas de segurança.

Em seguida, dá-se início à condição de otimalidade, isto é, o ponto em que a alocação de recursos entre crescimento e segurança se torna economicamente racional. O raciocínio subjacente é que a empresa deve ampliar o investimento em segurança até o momento em que o benefício marginal de reduzir o risco deixe de compensar o custo de oportunidade de retirar recursos de atividades diretamente voltadas ao crescimento. Essa formulação permite interpretar a segurança digital como parte de uma decisão econômica de equilíbrio, e não apenas como um gasto adicional ou acessório.

Também deve ser levada em conta a questão das distorções comportamentais, uma vez que decisões reais nem sempre seguem a lógica da racionalidade estrita. Pequenos empreendedores podem subestimar a probabilidade de ataques, supervalorizar os retornos de curto prazo ou adiar medidas preventivas diante de pressões imediatas de caixa. Assim, a modelagem não deve ser entendida apenas como exercício abstrato de maximização, mas também como ferramenta útil para evidenciar porque, na prática, pode haver subinvestimento em segurança mesmo quando a alocação preventiva seria economicamente justificável.

É interessante também contar com uma análise de cenários, que permite explorar como diferentes combinações de orçamento disponível, nível de digitalização, probabilidade de incidente e magnitude das perdas podem alterar a decisão ótima de investimento. Esse tipo de abordagem é especialmente relevante no contexto dos pequenos negócios, pois evidencia que a relação entre crescimento e segurança não é fixa, mas depende das condições específicas enfrentadas por cada organização.

Assim, a proposta é demonstrar que a segurança digital pode ser tratada como uma variável estratégica na alocação de recursos escassos. O que contribui para uma análise mais realista das escolhas de pequenos negócios, dado o contexto de ambientes marcados por restrições orçamentárias e por exposição crescente a riscos cibernéticos.

5.4 Implicações gerenciais da análise econômica

A formalização econômica do trade-off também acarreta implicações gerenciais importantes. Em vez de tratar a segurança digital como um gasto residual, a modelagem ajuda a enquadrá-la como um investimento voltado à redução da perda esperada. Essa mudança de enquadramento é particularmente relevante para pequenos negócios, nos quais decisões financeiras costumam ser fortemente pressionadas por necessidades imediatas de caixa e por objetivos visíveis de expansão.

Sob essa ótica, a segurança digital deixa de ocupar uma posição meramente defensiva e passa a integrar a própria lógica de sustentabilidade econômica do negócio. Ao evitar interrupções operacionais, custos emergenciais de recuperação e danos reputacionais, controles básicos podem preservar os fluxos de receita e reduzir a volatilidade dos resultados. Em linha semelhante, estudos recentes sugerem que a cibersegurança pode desempenhar um papel econômico mais amplo nas PMEs, ao influenciar a resiliência, a capacidade de continuidade e a qualidade das relações com clientes e parceiros (ARROYABE et al., 2024).

Essa interpretação é útil porque aproxima a discussão de segurança das decisões reais do empreendedor. Em muitos contextos, o problema não é simplesmente desconhecer o risco, mas conciliar múltiplas prioridades sob forte escassez de recursos. Quando a segurança é apresentada apenas como obrigação técnica, tende a perder espaço para investimentos com retorno mais tangível no curto prazo. Quando é apresentada como proteção do valor e redução da exposição a perdas potencialmente severas, a alocação preventiva passa a ser mais inteligível do ponto de vista econômico.

6 CONSIDERAÇÕES FINAIS

A crescente digitalização dos pequenos negócios tem ampliado oportunidades de operação, comunicação e crescimento, mas também vem tornando essas organizações mais expostas a riscos cibernéticos que podem comprometer sua estabilidade e continuidade. Nesse contexto, discutir segurança digital em PMEs significa ir além de uma abordagem puramente técnica e reconhecer que o tema também envolve gestão, tomada de decisão, alocação de recursos e capacidade de adaptação em ambientes de incerteza.

Ao longo do trabalho, buscou-se demonstrar que a segurança digital pode ser compreendida como uma dimensão relevante da resiliência organizacional em pequenos negócios. Mais do que uma despesa acessória, ela pode ser interpretada como um elemento de proteção econômica e operacional, especialmente em contextos marcados por restrição orçamentária, informalidade de processos e dependência crescente de ferramentas digitais. Essa perspectiva se torna ainda mais importante quando se considera que, para empresas de menor porte, incidentes relativamente comuns podem gerar impactos desproporcionais.

O estudo também buscou avançar na organização de uma base teórica e analítica capaz de apoiar futuras investigações sobre o tema. Ao articular a discussão sobre ameaças cibernéticas, as especificidades das PMEs e os trade-offs de investimento, o trabalho reforça a

importância de desenvolver abordagens mais ajustadas à realidade desses negócios, evitando a mera transposição de modelos concebidos para grandes corporações.

De forma mais ampla, a pesquisa aponta para a necessidade de ampliar o debate sobre segurança digital no universo dos pequenos negócios, tanto no campo acadêmico quanto no prático. Em um cenário em que a transformação digital se intensifica, compreender como essas organizações percebem riscos, definem prioridades e estruturam mecanismos mínimos de proteção torna-se essencial para pensar a competitividade, a sustentabilidade e a sobrevivência empresarial no longo prazo.

Como limitação, trata-se de um estudo ainda em fase de validação. O questionário a ser aplicado foi encaminhado ao comitê de ética em pesquisa. Assim que aprovado pelo comitê, será iniciada a coleta de dados para validação (ou não) da proposta.

7 REFERÊNCIAS

ALAJMI, Mona; ALOTAIBI, Mohammad. A deeper look into cybersecurity issues in the wake of the COVID-19 crisis. Journal of Cloud Computing, v. 11, n. 1, p. 1-16, 2022.

ARROYABE, M. F. et al. Exploring the economic role of cybersecurity in SMEs. Technology in Society, v. 79, 102539, 2024.

BANCO MUNDIAL. Small and Medium Enterprises (SMEs) Finance. Washington, DC: World Bank, 2025. Disponível em: https://www.worldbank.org/en/topic/smefinance. Acesso em: 30 mar. 2026.

BECK, Thorsten; DEMIRGUC-KUNT, Asli. Small and medium-sized enterprises: access to finance as a growth constraint. Journal of Banking & Finance, v. 30, n. 11, p. 2931-2943, 2006.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: Brasília, DF, 2018.

CARTWRIGHT, Anna; CARTWRIGHT, Edward; EDUN, Esther Solomon. Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. Computers & Security, v. 131, p. 103288, 2023.

DAMODARAN, Aswath. Applied Corporate Finance. 4. ed. Hoboken: Wiley, 2014.

DEPARTMENT FOR SCIENCE, INNOVATION AND TECHNOLOGY. Cyber Security Breaches Survey 2024. London: DSIT, 2024.

EUROPEAN UNION AGENCY FOR CYBERSECURITY. Cybersecurity for SMEs: Challenges and Recommendations. Luxembourg: ENISA, 2021.

HULL, John C. Risk Management and Financial Institutions. 4th ed. Hoboken: Wiley, 2018.

IBM. Cost of a Data Breach Report 2025. Armonk, 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements. Geneva: ISO, 2013.

JUNIOR, C. R.; BECKER, I.; JOHNSON, S. Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity. arXiv, 2023.

KAHNEMAN, Daniel; TVERSKY, Amos. Prospect theory: an analysis of decision under risk—Econometrica, v. 47, n. 2, p. 263-292, 1979.

MASSARO, Maurizio; HANDLEY, Karen; BAGNOLI, Carlo; DUMAY, John. Knowledge management in small and medium enterprises: a structured literature review. Journal of Knowledge Management, v. 20, n. 2, p. 258-291, 2016.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: NIST, 2024.

PROOFPOINT. 2022 State of the Phish Report. Sunnyvale, 2022.

SEBRAE. Participação das micro e pequenas empresas na economia nacional. Brasília: SEBRAE, 2014.

SINGH, Geetika; SHARMA, Deepak Kumar. Advancements in Cybersecurity: A Comprehensive Survey of AI-Driven Solutions. Procedia Computer Science, v. 259, p. 1296-1305, 2025.

TANNER, N. H. Cybersecurity Blue Team Toolkit. [S.l.], 2019.

THRASSOU, A.; UZUNBOYLU, N.; VRONTIS, D.; CHRISTOFI, M. Digitalisation of SMEs: a review of opportunities and challenges. In: THRASSOU, A.; VRONTIS, D.; WEBER, Y.; SHAMS, R.; TSOUKATOS, E. (org.). The Changing Role of SMEs in Global Business: Contextual Evolution Across Markets, Disciplines and Sectors. Cham: Springer, 2020. p. 179-200.

VERGARA COBOS, Estefanía; CAKIR, Selcen. A Review of the Economic Costs of Cyber Incidents. Washington, DC: World Bank, 2024.

VON NEUMANN, John; MORGENSTERN, Oskar. Theory of Games and Economic Behavior. Princeton: Princeton University Press, 1944.

WOJCIECHOWSKI, R.; STRYKOWSKI, S.; WILUSZ, D.; ŚWIERZOWICZ, J. Security challenges in cloud computing for small and medium enterprises. Informatyka Ekonomiczna – Business Informatics, n. 4(26), p. 100-111, 2012.

WORLD ECONOMIC FORUM. Global Cybersecurity Outlook 2025. Geneva: World Economic Forum, 2025.