UNIVERSIDADE FEDERAL DO CEARÁ
FACULDADE DE ECONOMIA, ADMINISTRAÇÃO, ATUÁRIA E CONTABILIDADE
DEPARTAMENTO DE ADMINISTRAÇÃO
CURSO DE CIÊNCIAS ATUARIAIS

LUCAS CISNE CUNHA

ANÁLISE DE RISCOS EMPRESARIAIS E A APLICAÇÃO DO MICROSOFT POWER BI NA GESTÃO DE RISCOS CIBERNÉTICOS

FORTALEZA
2025

LUCAS CISNE CUNHA

ANÁLISE DE RISCOS EMPRESARIAIS E A APLICAÇÃO DO MICROSOFT POWER BI NA GESTÃO DE RISCOS CIBERNÉTICOS

Monografia apresentada ao Curso de Graduação em Ciências Atuariais da Faculdade de Economia, Administração, Atuária e Contabilidade, como requisito parcial à obtenção do grau de bacharel em Ciências Atuariais.

Orientador: Profa. Ma. Alana Katielli Nogueira Azevedo.

FORTALEZA

2025

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

C1a CUNHA, Lucas Cisne.
ANÁLISE DE RISCOS EMPRESARIAIS E A APLICAÇÃO DO MICROSOFT POWER BI NA GESTÃO DE RISCOS CIBERNÉTICOS / Lucas Cisne CUNHA. – 2025.
43 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Economia, Administração, Atuária e Contabilidade, Curso de Ciências Atuariais, Fortaleza, 2025.
Orientação: Prof. Me. Alana Katielli Nogueira Azevedo .
Coorientação: Prof. Dr. Alane Siqueira Rocha.

1. Risco cibernético. 2. Power bi. 3. Risco. I. Título.

CDD 368.01

LUCAS CISNE CUNHA

ANÁLISE DE RISCOS EMPRESARIAIS E A APLICAÇÃO DO MICROSOFT POWER BI NA GESTÃO DE RISCOS CIBERNÉTICOS

Monografia apresentada ao Curso de Graduação em Ciências Atuariais da Faculdade de Economia, Administração, Atuária e Contabilidade, como requisito parcial à obtenção do grau de bacharel em Ciências Atuariais.

Aprovada em: 26/02/2025.

BANCA EXAMINADORA

_____
Profa. Ma. Alana Katielli Nogueira Azevedo (Orientadora)
Universidade Federal do Ceará (UFC)

_____
Profa. Dra. Alane Siqueira Rocha
Universidade Federal do Ceará (UFC)

_____
Prof. Dr. Daniel Tomaz de Sousa
Universidade Federal do Ceará (UFC)

A Deus.
Aos meus pais, e a todos que me apoiaram.

AGRADECIMENTOS

Agradeço a Deus por ter me colocado no caminho da educação e ter me dado tantas oportunidades maravilhosas.

Agradeço ao meu pai que sempre me apoiou e me ajudou e ensinou a ser quem sou hoje.

Agradeço à minha mãe que junto ao meu pai sempre me apoiaram na realização dos meus objetivos, assim como a todos os familiares que me incentivaram de diversas formas.

A todos os colegas e amigos com os quais já aprendi muito da faculdade e das empresas que trabalhei, todos por quem passei na minha carreira profissional e acadêmica que contribuíram de alguma forma.

“Vencer sem correr riscos é triunfar sem glórias” (Ayrton Senna).

RESUMO

O presente estudo tem como objetivo analisar os riscos cibernéticos enfrentados pelas empresas e demonstrar como a ferramenta Microsoft Power BI pode ser utilizada para monitorar e mitigar tais riscos. A pesquisa abrangeu a categorização dos riscos cibernéticos, seus impactos financeiros e estratégicos, além da importância da análise de dados na prevenção e resposta a incidentes. Por meio da aplicação de técnicas de Business Intelligence e modelagem atuarial, foram extraídos insights valiosos sobre a relação entre fraudes, falhas operacionais, número de funcionários e impacto financeiro por setor e região. Os resultados indicam que setores altamente digitalizados, como financeiro, manufatura e tecnologia da informação, são os mais afetados por perdas decorrentes de ameaças cibernéticas. A análise demonstrou que fraudes externas, interrupções operacionais e falhas sistêmicas são os principais vetores de perdas, reforçando a necessidade de uma governança digital robusta. A utilização do Power BI mostrou-se eficaz na identificação de padrões, acompanhamento de métricas e suporte à tomada de decisão estratégica. A ferramenta permitiu a criação de dashboards dinâmicos, facilitando a detecção e mitigação de riscos. No campo atuarial, a pesquisa destaca a importância de modelagens estatísticas na precificação de seguros cibernéticos e na definição de provisões técnicas adequadas. Conclui-se que a gestão eficiente dos riscos cibernéticos demanda uma abordagem multidisciplinar, combinando tecnologia, inteligência de dados e estratégias de segurança digital. O estudo reforça a relevância de soluções baseadas em BI para aprimorar a resiliência organizacional em um ambiente cada vez mais interconectado e vulnerável a ameaças cibernéticas.

Palavras-chave: Risco cibernético, Business Intelligence, Power BI, Análise de dados, Modelagem atuarial.

ABSTRACT

The present study aims to analyze the cyber risks faced by companies and demonstrate how Microsoft Power BI can be used to monitor and mitigate such risks. The research encompassed the categorization of cyber risks, their financial and strategic impacts, and the importance of data analysis in preventing and responding to incidents. By applying Business Intelligence techniques and actuarial modeling, valuable insights were extracted regarding the relationship between fraud, operational failures, workforce size, and financial impact across different sectors and regions. The results indicate that highly digitalized sectors, such as finance, manufacturing, and information technology, are the most affected by losses resulting from cyber threats. The analysis showed that external fraud, operational disruptions, and system failures are the primary loss drivers, reinforcing the need for robust digital governance. The use of Power BI proved effective in identifying patterns, tracking key metrics, and supporting strategic decision-making. The tool enabled the creation of dynamic dashboards, facilitating risk detection and mitigation. In the actuarial field, the research highlights the importance of statistical modeling in pricing cyber insurance and defining adequate technical provisions. It is concluded that efficient cyber risk management requires a multidisciplinary approach, combining technology, data intelligence, and digital security strategies. The study underscores the relevance of BI-based solutions in enhancing organizational resilience in an increasingly interconnected and cyber-vulnerable environment.

Keywords: Cyber risk, Business Intelligence, Power BI, Data analysis, Actuarial modeling.

Lista de Figuras

Lista de Gráficos

LISTA DE ABREVIATURAS E SIGLAS

ANS	Agência Nacional de Saúde Suplementar
API	Application Programming Interface
BI	Business Intelligence
BCBS	Basel Committee on Banking Supervision (Comitê de Supervisão Bancária de Basileia)
DAX	Data Analysis Expressions
DDoS	Distributed Denial of Service (Ataque Distribuído de Negação de Serviço)
DRP	Disaster Recovery Plan (Plano de Recuperação de Desastres)
ERP	Enterprise Resource Planning (Planejamento dos Recursos Empresariais)
GDPR	General Data Protection Regulation (Regulamento Geral de Proteção de Dados – Europa)
LGPD	Lei Geral de Proteção de Dados (Brasil)
NIST	National Institute of Standards and Technology (Instituto Nacional de Padrões e Tecnologia – EUA)
PESTEL	Political, Economic, Social, Technological, Environmental, Legal (Análise Política, Econômica, Social, Tecnológica, Ambiental e Legal)
SUSEP	Superintendência de Seguros Privados
SWOT	Strengths, Weaknesses, Opportunities, Threats (Análise de Forças, Fraquezas, Oportunidades e Ameaças)

SUMÁRIO

1. INTRODUÇÃO

O conceito de risco está presente em diversas áreas do conhecimento e pode ser compreendido como a possibilidade de ocorrer um evento inesperado que impacte negativamente determinado contexto (Lieber; Romano-Lieber, 2002). No campo das Ciências Atuariais, risco é definido como a incerteza em relação a eventos futuros que podem afetar o desempenho financeiro ou operacional de uma organização (Gloeckner; da Silva, 2014). Assim, a gestão de riscos é fundamental para minimizar impactos adversos e garantir a continuidade das atividades empresariais. As empresas estão expostas a diversos tipos de riscos, como os financeiros, operacionais, estratégicos e de conformidade. Esses riscos podem comprometer a rentabilidade, a reputação e a perenidade dos negócios. Com a evolução tecnológica e a crescente digitalização dos processos, um novo tipo de risco vem ganhando destaque: o risco cibernético (Meireles; Pasitto, 2024).

O risco cibernético se refere às ameaças relacionadas à segurança da informação, incluindo ataques hackers, vazamento de dados, fraudes eletrônicas e outras vulnerabilidades digitais. Com a dependência cada vez maior de sistemas informatizados, as empresas se tornam alvos potenciais de ataques, que podem resultar em perdas financeiras, danos à reputação e impactos legais. Dessa forma, estudar e mitigar o risco cibernético é essencial para garantir a segurança e a resiliência das organizações. Nesse contexto, ferramentas de análise de dados desempenham um papel fundamental, permitindo que empresas monitorem ameaças e adotem estratégias eficazes de segurança.

É essencial o uso de ferramentas adequadas para interpretação de dados. O Power BI se enquadra neste contexto como uma ferramenta de Business Intelligence (BI) desenvolvida pela Microsoft que permite a coleta, tratamento, análise e visualização de dados. Sua capacidade de integração com diversas fontes de informação e a possibilidade de criação de dashboards dinâmicos o tornam um recurso valioso para a análise de riscos empresariais, incluindo os cibernéticos. Por meio do Power BI, é possível identificar padrões, acompanhar métricas e tomar decisões embasadas em dados, contribuindo para uma gestão mais eficiente dos riscos.

Diante desse contexto, surge o seguinte problema de pesquisa: como é possível analisar os problemas relacionados aos ataques cibernéticos enfrentados pelas empresas e avaliar se o uso do Power BI permite realizar essa análise de maneira satisfatória.

Este estudo tem como objetivo geral analisar os riscos cibernéticos enfrentados pelas empresas, destacando a utilização da ferramenta Power BI como recurso estratégico para monitorar e mitigar essas ameaças. Os objetivos específicos consistem em identificar as principais ameaças cibernéticas enfrentadas pelas empresas, avaliar os impactos decorrentes desses incidentes e demonstrar, por meio de análises gráficas elaboradas no Power BI, informações que podem subsidiar a tomada de decisões estratégicas em segurança cibernética.

Para atingir os objetivos propostos, utiliza-se uma abordagem metodológica quantitativa, baseada na análise exploratória de dados obtidos de incidentes cibernéticos em diversos setores econômicos, utilizando o Microsoft Power BI como ferramenta analítica. O estudo utiliza técnicas de visualização gráfica e criação de indicadores estratégicos através da linguagem DAX, permitindo uma interpretação dinâmica dos resultados obtidos.

O presente trabalho está estruturado em seis capítulos. O primeiro capítulo corresponde a esta Introdução. O segundo capítulo aborda os conceitos gerais sobre riscos, com destaque especial para os riscos cibernéticos e suas categorias. No terceiro capítulo é realizada uma apresentação sobre o Microsoft Power BI e suas funcionalidades aplicadas à gestão de riscos empresariais. No quarto capítulo é abordado a metodologia do trabalho e as especificidades do banco de dados utilizado. No quinto capítulo são apresentados os resultados obtidos a partir das análises realizadas no Power BI, com destaque para os padrões de perdas financeiras decorrentes de incidentes cibernéticos. Por fim, no sexto capítulo, são feitas as considerações finais, nas quais são discutidas as principais conclusões e recomendações decorrentes do estudo.

2. RISCO

O conceito de risco é amplamente estudado em diversas áreas do conhecimento, sendo de grande relevância para o campo das Ciências Atuariais. De maneira geral, o risco pode ser entendido como a incerteza associada à ocorrência de eventos que podem impactar negativamente indivíduos, empresas e mercados. No ambiente corporativo, a gestão de riscos desempenha um papel essencial na identificação, avaliação e mitigação de ameaças, garantindo a estabilidade e a sustentabilidade dos negócios.

Os riscos empresariais podem ser classificados em diferentes categorias, incluindo riscos financeiros, operacionais, estratégicos e regulatórios. De acordo com Langlois e Cosgel (1993), riscos financeiros estão relacionados a oscilações no mercado, inadimplência e variações cambiais, podendo ser previstos e gerenciados com base em estatísticas e modelos atuariais. Já riscos operacionais, conforme Basel Committee on Banking Supervision (2011), envolvem falhas em processos internos, infraestrutura e tecnologia, estando fortemente associados à governança corporativa. Riscos estratégicos dizem respeito a decisões de negócios que podem impactar o crescimento e a competitividade da empresa, sendo frequentemente analisados por meio de frameworks como SWOT e PESTEL. Por fim, os riscos regulatórios decorrem de mudanças na legislação e exigências de conformidade impostas por órgãos reguladores, como a ANS e a SUSEP no Brasil.

Nos últimos anos, com o avanço da tecnologia e a crescente digitalização das atividades empresariais, os riscos cibernéticos ganharam destaque como uma das principais ameaças enfrentadas pelas organizações. Esses riscos englobam ataques virtuais, violações de dados, espionagem digital e vulnerabilidades em sistemas de informação. Segundo o relatório da Allianz Risk Barometer (2025), o risco cibernético se tornou a principal preocupação para empresas em diversos setores, superando inclusive riscos tradicionais como interrupções na cadeia de suprimentos e crises econômicas. A exposição a ameaças cibernéticas pode resultar em prejuízos financeiros significativos, além de comprometer a reputação e a confiabilidade das empresas.

A gestão eficaz do risco cibernético envolve a implementação de medidas de segurança, como a adoção de protocolos de proteção, criptografia de dados, monitoramento contínuo de sistemas e capacitação de funcionários. Além disso, a

análise de dados desempenha um papel crucial na prevenção e detecção de ameaças. Conforme o National Institute of Standards and Technology (1992), uma abordagem baseada em monitoramento constante e resposta ágil a incidentes reduz significativamente as chances de danos irreversíveis.

Diante desse cenário, a capacidade de monitorar e gerenciar riscos de maneira proativa se tornou um diferencial competitivo para as empresas. Organizações que investem em soluções tecnológicas e em uma cultura de segurança da informação estão mais preparadas para lidar com desafios e minimizar impactos negativos decorrentes de ameaças cibernéticas. Assim, a compreensão aprofundada dos riscos e a adoção de abordagens preventivas são fatores determinantes para a proteção e o sucesso empresarial no ambiente digital.

2.1. Riscos Cibernéticos: Conceitos e Categorização

Com o avanço da digitalização, as organizações passaram a enfrentar desafios relacionados aos riscos cibernéticos, que podem comprometer a segurança, integridade e disponibilidade dos dados e sistemas de uma organização. Segundo Cardoso (2024), esses riscos incluem não apenas ameaças externas, como ataques sofisticados conduzidos por hackers (de Souza *et al.*, 2019; Thomas, 2018), mas também ameaças internas, decorrentes de falhas operacionais, erros humanos e vulnerabilidades tecnológicas internas.

Entre esses riscos destaca-se a fraude interna, definida como eventos criminosos praticados por funcionários ou agentes internos que resultam em perdas financeiras significativas para a organização. Esse tipo de fraude envolve atividades não autorizadas. A fraude computacional relacionada ao roubo direto de ativos financeiros ocorre pela manipulação de sistemas, conforme destacado por Hoffman (2021). Além disso, há danos intencionais aos sistemas por meio da instalação de malware e destruição de dados críticos como retaliação. Outra atividade relevante é a realização de transações financeiras sem aprovação prévia, o que compromete diretamente a segurança financeira da organização. Ainda é importante destacar o roubo de informações estratégicas com objetivo de prejuízo financeiro, como a comercialização de dados sensíveis na dark web (Rizkiana Iskandar *et al.*, 2022).

A fraude externa, por sua vez, refere-se às ações criminosas praticadas por agentes externos, que exploram vulnerabilidades para obter vantagens ilícitas ou

causar danos. Este tipo de evento pode comprometer seriamente a segurança dos sistemas por meio de diversas formas. Primeiramente, o roubo de informações financeiras, como credenciais e dados sensíveis, frequentemente comercializados ilegalmente na dark web. Em segundo lugar, a realização de transações não autorizadas, como extorsões financeiras através de ransomware (Thomas, 2018). A manipulação intencional da posição financeira da empresa também é comum, por meio da alteração fraudulenta de registros contábeis e disseminação de informações falsas. Por fim, danos às operações podem ocorrer por sabotagem ou malware avançado (Velasco, 2022).

Além das fraudes internas e externas, as organizações enfrentam riscos relacionados à interrupção de negócios e falhas de sistemas, que podem ocorrer devido a problemas técnicos. Esses eventos incluem a falha de hardware, quando componentes físicos essenciais apresentam defeitos resultando na interrupção de serviços críticos (Koks *et al.*, 2019). Também há falha de software, caracterizada por bugs e erros críticos que prejudicam processos automatizados e a segurança operacional (Zahid *et al.*, 2018). A prevenção dessas falhas demanda monitoramento constante e estratégias eficazes de manutenção dos sistemas.

Outro aspecto relevante é a execução, entrega e gestão de processos empresariais, que podem ser impactados por falhas não intencionais em diversas atividades operacionais. Dentre essas, destacam-se problemas na captura, execução e manutenção de transações. Um exemplo são os erros na gestão de colateral, que afetam diretamente a liquidez financeira. Outra questão comum envolve a realização de entradas incorretas ou incompletas de dados críticos nos sistemas. Além disso, falhas na entrega ou atraso de serviços podem prejudicar a experiência dos clientes.

Ademais, o monitoramento inadequado e problemas nos relatórios também representam uma ameaça significativa, podendo comprometer a transparência e conformidade regulatória das organizações. Falhas comuns nesta área incluem não reportar informações regulatórias no prazo exigido, falta de transparência durante auditorias internas e externas e erros críticos na geração de relatórios obrigatórios.

Finalmente, as falhas na gestão de contas e segurança dos dados de clientes surgem como uma preocupação constante no contexto digital atual. A má gestão dessas informações pode resultar em eventos como vazamento de dados pessoais, roubo de credenciais e acessos não autorizados, gerando prejuízos financeiros e perda de confiança junto aos clientes (Koks *et al.*, 2019; Zahid *et al.*,

2018). Dessa forma, torna-se essencial que as organizações adotem estratégias robustas e integradas de gestão de riscos cibernéticos, com foco na prevenção, monitoramento e rápida resposta frente a possíveis ameaças.

3. MICROSOFT POWER BI

3.1. Business Inteligence

Nos últimos anos, a evolução tecnológica e o grande volume de dados gerados diariamente impulsionaram a necessidade de ferramentas que auxiliem na tomada de decisão baseada em dados. Nesse contexto, o Business Intelligence (BI) surge como um conjunto de processos, metodologias e tecnologias utilizadas para coletar, integrar, analisar e apresentar informações que auxiliam nas decisões estratégicas de uma organização.

O BI tem como objetivo principal transformar dados brutos em insights valiosos por meio de dashboards interativos, relatórios dinâmicos e análises preditivas. Dessa forma, ele permite que empresas melhorem sua eficiência operacional, identifiquem padrões e antecipem possíveis problemas (Gonçalves, 2024).

Além de sua função essencial de transformar dados em insights estratégicos, a técnica de Business Intelligence apresenta grande versatilidade em sua aplicação. Ela pode ser adotada tanto como uma filosofia orientada por dados quanto como uma prática operacional através de ferramentas especializadas. Essa diversidade de abordagens reflete a expansão dinâmica do mercado de soluções de BI, que tem acompanhado a demanda por inovação e maior precisão analítica.

Nesse cenário, o Quadrante de Gartner (Ruvolo, 2024) emerge como uma referência internacional, classificando fornecedores com base em critérios rigorosos de desempenho, visão de mercado e capacidade de execução. Assim, a posição de uma marca, quanto mais elevada e deslocada para a direita no gráfico indica um reconhecimento superior em termos de qualidade e confiabilidade, conforme mostra a Figura 1.

Figura 1 – Quadrante de Gartner

Fonte: Gartner (2024).

3.2. Características e funcionamento do Power BI

O avanço tecnológico e a necessidade de tomada de decisões baseada em dados levaram ao desenvolvimento de ferramentas especializadas em análise e visualização de informações. Nesse contexto, conforme mostrado na Figura 1, o Power BI se destaca como uma das soluções mais amplamente utilizadas para transformar dados brutos em insights valiosos para as organizações.

O Power BI é uma plataforma de Business Intelligence (BI) desenvolvida pela Microsoft, que permite a coleta, organização, análise e visualização de dados de maneira interativa e dinâmica. A ferramenta oferece uma interface intuitiva e conectividade com diversas fontes de dados, permitindo a criação de relatórios personalizados e dashboards interativos para auxiliar na interpretação de informações complexas.

A principal vantagem do Power BI é sua capacidade de integrar grandes volumes de dados de diferentes origens, como bancos de dados, planilhas e sistemas de gestão empresarial (ERP). Além disso, a ferramenta possibilita a aplicação de modelos estatísticos e métricas para avaliar tendências e prever cenários futuros, auxiliando na identificação de padrões e na mitigação de riscos operacionais e financeiros.

Dentre suas funcionalidades, o Power BI oferece ferramentas de integração com diversas fontes de dados e funcionalidades avançadas de análise.

Suas principais características incluem:

a) Integração com Múltiplas Fontes de Dados: O Power BI permite conexões com bancos de dados, arquivos Excel, serviços em nuvem e APIs, garantindo uma ampla gama de possibilidades para consolidação de dados.
b) ETL (Extract, Transform, Load): Possui um mecanismo robusto de extração, transformação e carga de dados, permitindo a modelagem e limpeza de informações antes da análise.
c) Criação de Dashboards Interativos: Com o Power BI, é possível desenvolver dashboards visuais altamente dinâmicos, permitindo a exploração de dados de maneira visual e intuitiva.
d) Linguagem DAX (Data Analysis Expressions): Utiliza expressões de análise de dados para criar cálculos complexos e métricas personalizadas.
e) Compartilhamento e Publicação: As análises podem ser compartilhadas na nuvem através do Power BI Service, facilitando a colaboração entre equipes.

Com isso, empresas de diversos segmentos conseguem utilizar a plataforma para aprimorar a gestão estratégica, otimizar operações e fortalecer a tomada de decisão baseada em evidências.

Assim, o Power BI se tornou uma ferramenta essencial para organizações que buscam monitorar indicadores de desempenho e riscos, oferecendo suporte para análises aprofundadas e permitindo uma visão holística do cenário corporativo.

Para a realização dos cálculos e a criação de indicadores analíticos apresentados neste estudo, utiliza-se a linguagem de programação fundamental do

Power BI: a Data Analysis Expressions (DAX). Conhecida como Expressões de Análise de Dados, essa linguagem desempenha um papel essencial na manipulação e modelagem de dados tabulares.

A DAX possui funcionalidades comparáveis às fórmulas do Microsoft Excel, mas sua aplicabilidade estende-se à análise de grandes volumes de dados, tornando-a indispensável na construção de relatórios e painéis interativos. Sua utilização viabiliza a criação de métricas e cálculos customizados, otimizando a análise de dados e aprimorando a capacidade de tomada de decisão.

Para a correta elaboração de expressões DAX, algumas regras devem ser seguidas, conforme orientações da Microsoft (2024):

a) As fórmulas devem iniciar com o símbolo de igual (=);
b) Os nomes das funções podem ser digitados manualmente ou selecionados a partir de uma lista de opções disponíveis;
c) A funcionalidade autocomplete permite sugerir funções, tabelas e colunas, facilitando a construção de expressões sem erros sintáticos;
d) Os argumentos devem ser informados corretamente, seja digitando diretamente ou selecionando em listas suspensas;
e) É necessário validar a sintaxe da expressão, garantindo a correta estruturação dos parênteses e a referência precisa às tabelas e colunas envolvidas;
f) Para confirmar e aplicar a fórmula, basta pressionar a tecla ENTER.

A DAX contém um vasto repertório de funções, categorizadas conforme sua aplicabilidade. Segundo a Microsoft (2024), essas funções podem ser classificadas em diversas áreas, incluindo:

a) Funções de agregação: possibilitam cálculos como soma, média, contagem, mínimo e máximo em colunas de tabelas;
b) Funções de data e hora: semelhantes às do Excel, mas baseadas no formato DateTime a partir de 1º de março de 1900;
c) Funções de filtro: permitem modificar o contexto de cálculos para criar métricas dinâmicas;
d) Funções financeiras: utilizadas para cálculos como valor presente líquido e taxa de retorno, semelhantes às do Excel;
e) Funções informativas: verificam e identificam tipos de valores específicos em células ou colunas;

f) Funções lógicas: avaliam expressões e retornam valores condicionais;
g) Funções matemáticas e trigonométricas: incluem operações como arredondamento, raiz quadrada, seno e cosseno;
h) Funções de relação: facilitam a busca de valores em tabelas relacionadas e a definição de vínculos entre dados;
i) Funções estatísticas: aplicáveis ao cálculo de distribuições, probabilidades e medidas de dispersão;
j) Funções de texto: permitem manipulação de cadeias de caracteres, incluindo concatenação e extração de trechos específicos;
k) Funções de inteligência temporal: possibilitam comparações baseadas em períodos de tempo, essenciais para análises históricas;
l) Funções de manipulação de tabelas: geram novas tabelas ou modificam as já existentes, permitindo análises segmentadas e detalhadas.

Outro conceito indispensável na aplicação da DAX no Power BI é o contexto de cálculo, que define a maneira como os dados são filtrados e processados para a geração dos resultados esperados. A Microsoft (2025) classifica os contextos em três principais tipos:

a) Contexto de linha: reflete os cálculos aplicados a cada linha individualmente dentro de uma tabela;
b) Contexto de consulta: refere-se ao subconjunto de dados extraído para determinada fórmula, dependendo de sua posição na análise;
c) Contexto de filtro: determina o escopo dos dados considerados em uma expressão, sendo influenciado por filtros aplicados diretamente no modelo ou nos relatórios.

O uso eficiente da DAX, aliado à compreensão do contexto de cálculo, possibilita a construção de análises sofisticadas e aprofundadas, garantindo maior assertividade e dinamismo na interpretação dos dados. Assim, a integração dessa linguagem ao Power BI torna-se essencial para aprimorar a modelagem de dados e contribuir para tomadas de decisão estratégicas baseadas em informações concretas.

4. METODOLOGIA

Para a realização do estudo, foram aplicadas técnicas de Business Intelligence, permitindo a extração, transformação e visualização de dados estratégicos. O armazenamento original foi realizado em um arquivo Excel, contendo 908 registros distribuídos em 16 colunas. A criação dos indicadores foi feita utilizando a linguagem DAX (Data Analysis Expressions) no Power BI, garantindo uma análise dinâmica e interativa.

A estrutura do banco de dados inclui as seguintes colunas: 'Reference ID Code' (código de identificação do evento), 'Industry Sector Name' (setor da indústria), '# of Employees' (número de funcionários), 'Region of Domicile' (região da entidade), 'Country of Legal Entity' (país da entidade legal), 'Event Risk Category' (categoria de risco do evento), 'Sub Risk Category' (subcategoria de risco), 'Activity' (atividade relacionada ao evento), 'Month & Year of Settlement' (mês e ano do acordo), 'Month and year' (mês e ano do evento), 'Loss Amount ($M)' (valor da perda em milhões), 'CPI Adjustment' (ajuste de índice de preços ao consumidor), 'Current Value of Loss ($M)' (valor atual da perda), 'Revenue ($M)' (receita em milhões), 'Current Value of Revenue ($M)' (valor atual da receita) e 'Assets ($M)' (ativos em milhões).

Além disso, o banco de dados contém uma tabela auxiliar denominada 'Categorization Table', que possui registros distribuídos em 3 colunas para as definições dos Riscos abordados. Essa tabela desempenha um papel importante na categorização dos eventos de risco, permitindo a segmentação e análise detalhada dos diferentes tipos de incidentes registrados.

A base de dados reflete informações relacionadas a incidentes cibernéticos, fraudes, falhas sistêmicas e suas consequências financeiras e operacionais. A estrutura do banco inclui registros de eventos de risco, detalhando a categoria do incidente, o setor afetado e o impacto econômico associado. A abordagem analítica empregada permitiu a identificação de padrões e tendências, fornecendo insights relevantes sobre a gestão de riscos cibernéticos e suas implicações para diferentes setores da economia.

Os dados foram tratados e modelados com o objetivo de oferecer suporte à tomada de decisão baseada em evidências, permitindo a visualização de informações estratégicas para a mitigação de riscos. Dessa forma, este estudo contribui para o entendimento dos desafios enfrentados pelas empresas na era digital,

ressaltando a importância de estratégias eficazes de segurança da informação e governança de riscos.

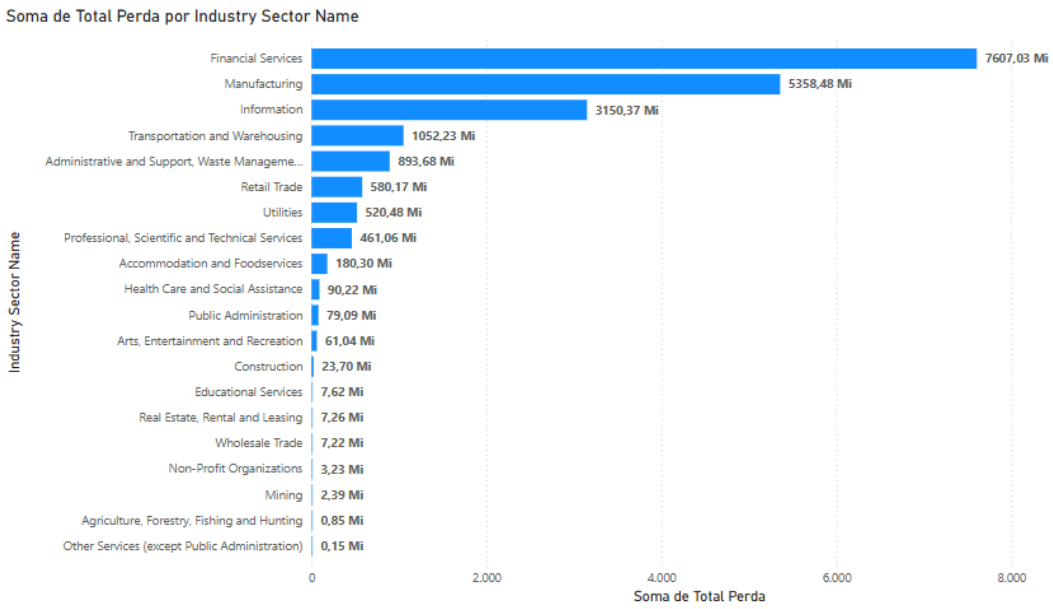
5. ANÁLISE DE RESULTADOS

A crescente digitalização dos processos empresariais tem exposto organizações de diferentes setores e regiões a riscos financeiros significativos, tornando essencial a análise detalhada desses eventos para aprimorar estratégias de mitigação. Este estudo busca identificar padrões de perdas financeiras globais e os principais fatores que influenciam sua ocorrência, proporcionando uma visão abrangente sobre a relação entre fraudes, falhas operacionais, número de funcionários e impacto financeiro por região.

5.1. Análise da Perda por Setor

A análise dos dados de perdas por setor econômico evidencia a relevância da gestão de riscos cibernéticos, especialmente nos setores financeiro, de manufatura e de tecnologia da informação. O Gráfico 1 demonstra que os setores mais impactados em termos absolutos foram serviços financeiros (7,6 bilhões), manufatura (5,3 bilhões) e tecnologia da informação (3,1 bilhões). Essas perdas substanciais refletem a criticidade dessas indústrias na economia e o grau de exposição a riscos cibernéticos.

Gráfico 1 – Perda por Setor



Fonte: Dados de empresas afetadas por ataques cibernéticos

Os três setores com as maiores perdas são caracterizados por alta digitalização, grandes volumes de dados sensíveis e interdependência com outras indústrias. No caso dos serviços financeiros, a crescente dependência de transações digitais e sistemas automatizados de crédito e pagamento aumenta a vulnerabilidade a ataques cibernéticos, fraudes e vazamentos de dados. A manufatura, por sua vez, enfrenta riscos elevados devido à crescente adoção da Indústria 4.0, que integra automação e conectividade, tornando as operações suscetíveis a ransomware e sabotagem industrial (Lezzi; Lazoi; Corallo, 2018). Já o setor de tecnologia da informação, sendo fundamental na infraestrutura digital, está exposto a incidentes que podem ter efeitos cascata sobre outras indústrias (Von Solms; Van Niekerk, 2013).

Setores como transporte e armazenamento (1,05 bilhão), gestão de resíduos (893 milhões) e varejo (580 milhões) também registram perdas significativas. Isso pode estar relacionado à integração de cadeias logísticas e ao uso crescente de sistemas interconectados. No varejo, por exemplo, o comércio eletrônico e os pagamentos digitais ampliam a superfície de ataque para fraudes financeiras e violações de dados de clientes.

Já os setores como agricultura (850 mil) e mineração (2,39 milhões) apresentaram perdas relativamente baixas. Isso pode ser explicado por um menor nível de digitalização e menor volume de informações sigilosas armazenadas digitalmente. Entretanto, com o avanço das tecnologias agrícolas e mineração autônoma, esses números podem aumentar nos próximos anos.

Para o campo das Ciências Atuariais, a análise dessas perdas se traduz diretamente em desafios para a precificação de seguros cibernéticos, avaliação de provisões técnicas e desenvolvimento de estratégias de mitigação de riscos. Algumas implicações incluem:

a) precificação mais alta de seguros cibernéticos para setores mais afetados, como serviços financeiros e tecnologia da informação.
b) adoção de modelos preditivos baseados em machine learning para estimar perdas futuras e identificar padrões de ataques cibernéticos.
c) revisão dos níveis de capital regulatório exigidos para empresas altamente digitalizadas, garantindo que estejam preparadas para possíveis eventos extremos.

Com base nos setores analisados, algumas estratégias podem ser adotadas para mitigação e gestão dos riscos. Para setores financeiro e de tecnologia

da informação, recomenda-se o fortalecimento da segurança cibernética com sistemas de detecção de intrusão, autenticação multifatorial e criptografia avançada. No caso da manufatura e transporte, é essencial implementar redes segmentadas para evitar ataques em cadeia e ampliar o monitoramento de dispositivos conectados. Já o setor de varejo deve focar na proteção de dados dos clientes e aprimorar sistemas antifraude para evitar perdas financeiras.

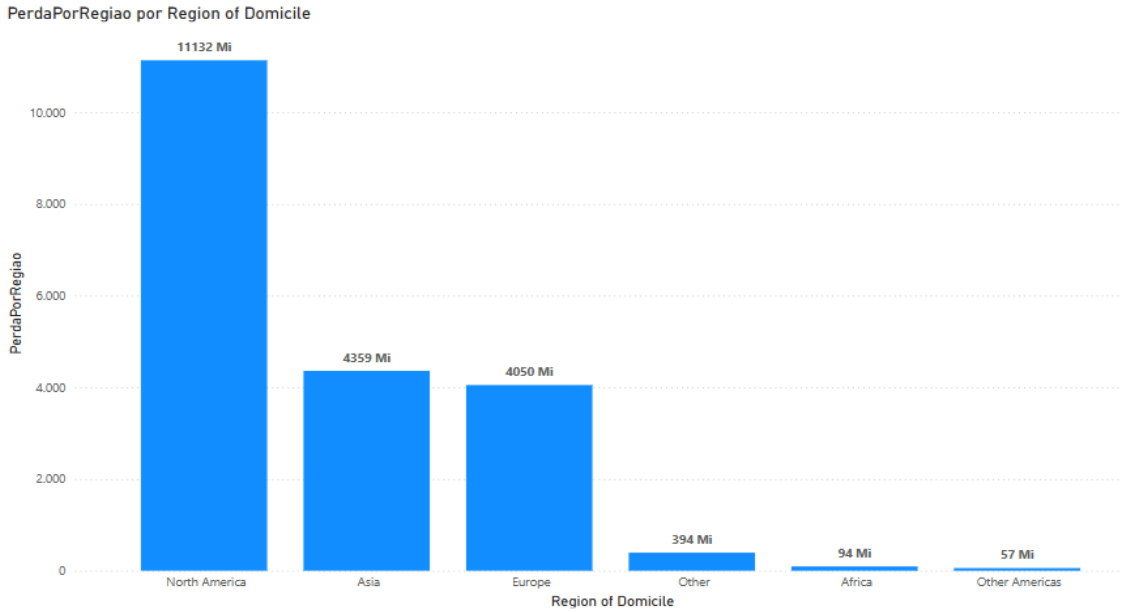
Conforme evidenciado no Gráfico 1, as perdas variam conforme a exposição digital e a criticidade do setor na economia. A alta correlação entre setores mais impactados e o volume de transações digitais reforça a necessidade de estratégias robustas de mitigação e avaliação atuarial precisa para lidar com riscos cibernéticos de forma sustentável. A gestão preventiva, aliada ao uso de análise de dados em tempo real, será essencial para reduzir essas perdas no futuro.

5.2. Análise sobre Perdas por Continente

A análise dos dados apresentados no Gráfico 2 evidencia uma disparidade significativa nas perdas registradas por diferentes regiões do mundo. A América do Norte se destaca como a região com as maiores perdas, totalizando 11,13 bilhões, seguida pela Ásia (4,36 bilhões) e pela Europa (4,05 bilhões). Regiões como África (94 milhões), outras partes das Américas (57 milhões) e "Outros" (394 milhões)

apresentam perdas consideravelmente menores. Essa distribuição pode ser atribuída a diversos fatores estruturais, econômicos e tecnológicos.

Gráfico 2 – Perda por Continente



Fonte: Dados de empresas afetadas por ataques Cibernéticos

A América do Norte concentra um grande volume de empresas multinacionais, transações digitais, bancos e instituições financeiras altamente digitalizadas, tornando-a um alvo prioritário para ataques cibernéticos e fraudes financeiras. Além disso, a regulamentação rigorosa sobre a divulgação de violações de dados pode inflar os números da região, já que incidentes são obrigatoriamente reportados e contabilizados.

A Ásia aparece como a segunda região com maiores perdas, refletindo o crescimento da digitalização e a adoção de tecnologias avançadas. Países como China, Japão, Índia e Coreia do Sul possuem grandes setores tecnológicos e industriais, além de um mercado financeiro robusto (Junior; Lima, 2010). Contudo, a variação nos níveis de regulamentação e segurança cibernética pode contribuir para vulnerabilidades exploradas por cibercriminosos.

A Europa, apesar de possuir uma regulamentação forte (como o GDPR - Regulamento Geral de Proteção de Dados), ainda registra perdas elevadas. Isso pode ser explicado pela elevada interconectividade entre países da União Europeia, a digitalização de seus setores bancário e industrial, além do impacto de ataques cibernéticos direcionados a infraestruturas críticas.

Regiões como África, América Latina e outras partes do mundo registram valores significativamente menores, o que pode ser explicado por diversos fatores. Primeiramente, muitas economias emergentes possuem infraestruturas digitais menos avançadas, reduzindo a exposição a riscos cibernéticos massivos devido à menor digitalização e bancarização. Além disso, a subnotificação é outro fator importante, já que a ausência de regulações rígidas sobre incidentes cibernéticos pode levar muitas perdas a não serem oficialmente registradas. Outro aspecto relevante é a menor concentração de grandes empresas globais nessas regiões, resultando em menor volume de transações digitais e menor dependência tecnológica.

Para a área de Ciências Atuariais, essas diferenças regionais são fundamentais para a modelagem de riscos, precificação de seguros cibernéticos e provisão de capital para perdas inesperadas. As principais implicações incluem:

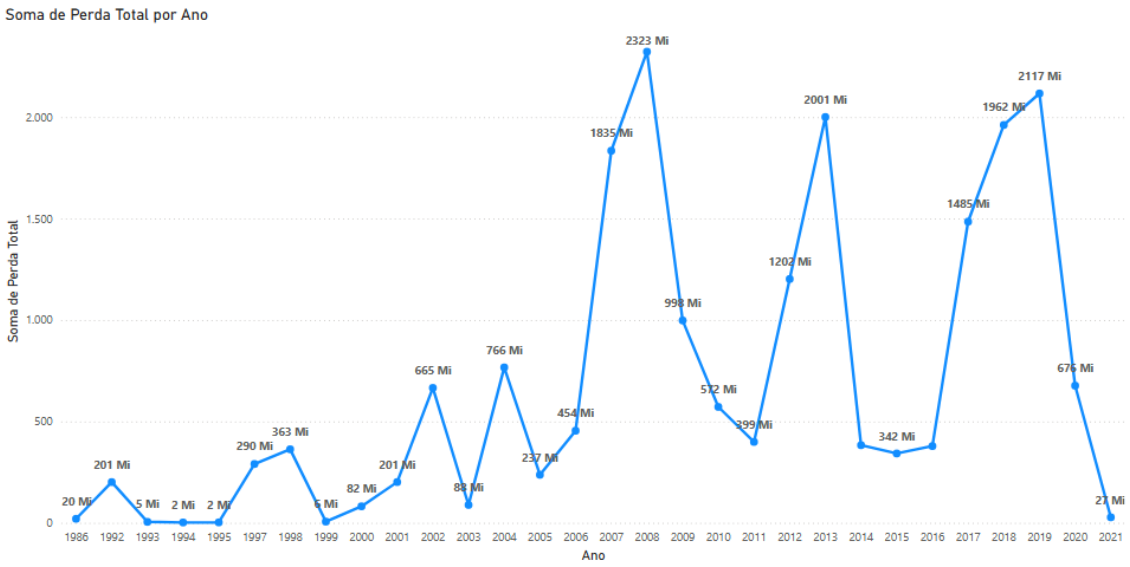
a) precificação diferenciada de seguros cibernéticos, com regiões como América do Norte apresentando prêmios mais altos, enquanto mercados emergentes podem necessitar de maior incentivo à contratação de seguros contra ataques.
b) necessidade de modelagem estatística por região, com criação de modelos preditivos específicos que ajudem seguradoras e empresas a identificarem padrões e tendências de perdas, reduzindo a exposição financeira.
c) incentivo à regulamentação mais rigorosa em regiões com menores perdas, fortalecendo o monitoramento e a transparência dos incidentes cibernéticos e garantindo maior confiabilidade dos dados.

Conforme observado, o Gráfico 2 revela que as perdas não são distribuídas uniformemente pelo mundo, sendo concentradas nas regiões mais desenvolvidas e altamente digitalizadas. Esse fenômeno reforça a importância da gestão estratégica de riscos e do desenvolvimento de mecanismos de mitigação adequados para cada contexto regional. Do ponto de vista atuarial, essas disparidades devem ser incorporadas nas metodologias de precificação e análise de solvência das seguradoras e empresas que lidam com riscos cibernéticos.

5.3. Evolução das Perdas por Ano

O Gráfico 3 apresenta a evolução das perdas totais ao longo dos anos, evidenciando um padrão cíclico de crescimento e queda nas perdas, com picos significativos em anos específicos. Esses ciclos indicam que fatores externos, como avanços tecnológicos, mudanças regulatórias, crises financeiras e evolução das ameaças cibernéticas, podem ter impacto direto nas perdas registradas.

Gráfico 3 – Evolução das Perdas por ano de 1986 a 2021



Fonte: Dados de empresas afetadas por ataques cibernéticos

A análise sugere que as perdas eram relativamente baixas antes dos anos 2000, mas começaram a crescer rapidamente após esse período. Esse crescimento pode ser explicado por diversos fatores:

a) digitalização e globalização das economias, uma vez que o aumento da interconectividade entre empresas e governos tornou os sistemas mais vulneráveis a ataques cibernéticos e fraudes.
b) adoção de novas tecnologias, considerando que sistemas mais complexos e automatizados ampliam a exposição a falhas e ataques.
c) aumento da regulamentação e transparência, com obrigatoriedade de reportar incidentes financeiros e cibernéticos, aumentando assim a visibilidade das perdas.

A partir de 2002, observa-se um aumento significativo, com picos em 2007 (2,32 bilhões), 2013 (2,00 bilhões) e 2018 (2,11 bilhões), momentos que podem

coincidir com eventos globais como crises financeiras, ataques cibernéticos massivos ou fraudes de grande escala.

O comportamento do Gráfico 4 sugere um padrão de crescimento rápido seguido por quedas bruscas. Algumas hipóteses podem explicar esse comportamento cíclico:

a) eventos isolados de grande impacto, como fraudes massivas, colapsos financeiros ou ataques cibernéticos amplamente divulgados, podem causar picos nas perdas.
b) regulações mais rígidas após grandes incidentes tendem a reduzir temporariamente os impactos.
c) crescimento da resiliência das empresas, que adotam melhores práticas de segurança e gestão de riscos após episódios de perdas elevadas.

Em 2015 e 2021, por exemplo, há quedas expressivas após anos de alta, sugerindo que medidas de controle foram implementadas nesses períodos.

Do ponto de vista atuarial, a variação das perdas por ano reforça a importância de modelos probabilísticos e preditivos para prever períodos de alta exposição ao risco. Algumas implicações incluem:

a) precificação dinâmica de seguros cibernéticos e financeiros, ajustando prêmios em períodos de alta exposição para refletir o risco elevado.
b) provisão de capital regulatório para riscos inesperados, garantindo que empresas e seguradoras mantenham reservas suficientes para lidar com eventos extremos.
c) modelagem de riscos baseada em ciclos, utilizando análises preditivas para antecipar futuros ciclos de crescimento de perdas.

A evolução das perdas ao longo do tempo mostra que os riscos financeiros e cibernéticos estão crescendo de forma cíclica. As grandes oscilações sugerem que eventos específicos podem impactar significativamente os valores anuais. Para empresas, seguradoras e gestores de riscos, a chave para lidar com essa variabilidade é investir continuamente em segurança, conformidade regulatória e estratégias de mitigação de riscos. A análise também indica que não basta olhar apenas para os valores médios das perdas, mas sim entender os padrões de longo prazo. O uso de ferramentas como Business Intelligence (Power BI) e modelagem estatística atuarial pode proporcionar uma visão mais estratégica e eficiente para prevenir futuras oscilações negativas.

5.4. Perdas por Evento de Risco

O Gráfico 4 apresentado destaca as principais categorias de risco operacional e suas respectivas perdas globais. As quatro categorias analisadas são:

a) Fraude Externa - 7,16 bilhões.

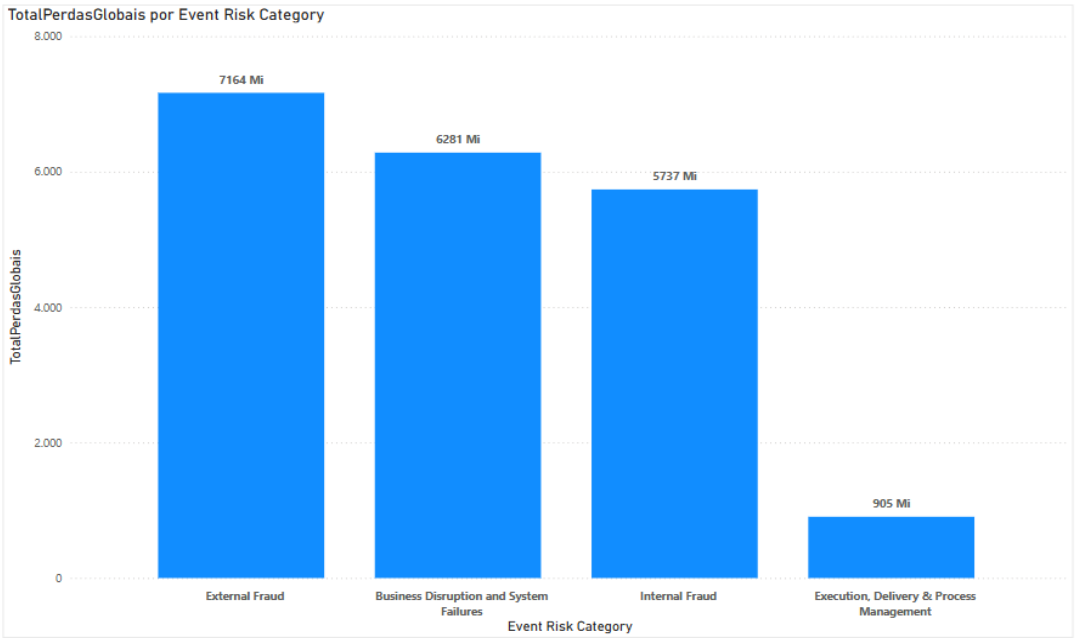
b) Interrupção de Negócios e Falhas de Sistema - 6,28 bilhões.

c) Fraude Interna - 5,73 bilhões.

d) Execução, Entrega e Gestão de Processos - 905 milhões.

A distribuição dessas perdas evidencia que as fraudes e falhas nos sistemas têm grande impacto financeiro, enquanto problemas relacionados à execução e gestão de processos apresentam menor impacto.

Gráfico 4 – Perdas Globais por Evento de Risco



Fonte: Dados de empresas afetadas por ataques cibernéticos

A fraude externa se destaca como a maior fonte de perdas globais, indicando desafios significativos na segurança digital, identidade corporativa e controle de acessos externos. Este tipo de fraude pode incluir:

a) ataques como phishing, ransomware e hacking.

b) roubo de informações financeiras e fraude financeira.

c) engenharia social e manipulação de informações sensíveis.

A crescente digitalização das empresas aumenta sua exposição a cibercriminosos que exploram falhas em segurança.

As implicações atuariais incluem:

a) necessidade de modelagem de risco cibernético para precificação de seguros.
b) desenvolvimento de estratégias de mitigação, como autenticação multifatorial e monitoramento contínuo.
c) cumprimento de regulamentações como LGPD e GDPR.

A segunda categoria com maior impacto financeiro está relacionada a problemas técnicos, indisponibilidade de sistemas e falhas na infraestrutura digital. Os principais fatores incluem:

a) falhas em data centers e sistemas críticos de TI.
b) ataques que comprometem disponibilidade dos sistemas, como DDoS.
c) falhas graves de infraestrutura, como energia e telecomunicações.
d) problemas em sistemas críticos que afetam a continuidade operacional.

Implicações atuariais e gerenciamento de risco nesta categoria envolvem:

a) fortalecimento dos planos de contingência e recuperação de desastres.
b) aprimoramento na análise de risco operacional para ajustar adequadamente prêmios de seguros.
c) investimento em redundância e proteção cibernética para evitar falhas críticas.

A fraude interna representa perdas substanciais devido a desvios financeiros, corrupção e uso indevido de informações privilegiadas. Entre suas principais causas estão:

a) desfalques e apropriação indébita de recursos.
b) manipulação contábil e fraudes fiscais.
c) conflitos de interesse e abuso de poder, facilitados pela ausência de auditorias eficazes.

As implicações atuariais para fraudes internas incluem:

a) implementação de modelos de risco internos e auditoria contínua.
b) uso de inteligência artificial para identificar transações suspeitas.
c) desenvolvimento de seguros contra fraudes internas, protegendo a organização contra danos financeiros.

As perdas relacionadas à execução, entrega e gestão de processos são as menores registradas, embora incluam problemas operacionais significativos como:

a) falhas manuais na execução de serviços.
b) descumprimento de regulamentações.
c) controle inadequado nas entregas de produtos e serviços. Tais falhas podem gerar perdas indiretas significativas por insatisfação de clientes e sanções regulatórias.

Implicações atuariais nesta categoria destacam:

a) automação dos processos para minimizar erros humanos.
b) auditorias internas contínuas para identificação de ineficiências.
c) criação de seguros para cobrir perdas operacionais.

O Gráfico 4 revela que fraudes (externas e internas) e falhas sistêmicas representam grandes riscos financeiros para as empresas. A dependência crescente de tecnologia expõe as empresas a ataques cibernéticos e interrupções operacionais, exigindo estratégias robustas de mitigação, segurança tecnológica avançada e políticas rigorosas de governança corporativa. Na perspectiva atuarial, são essenciais:

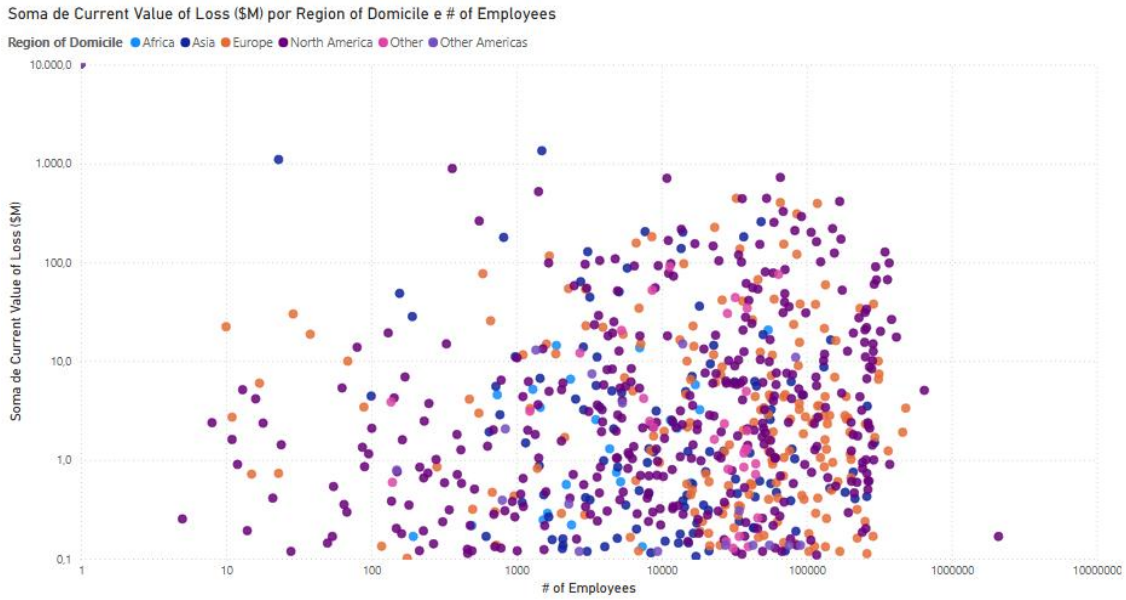
a) precificação adequada de seguros cibernéticos.
b) utilização de modelos preditivos avançados para antecipar fraudes e falhas.
c) implementação rigorosa de auditoria e compliance.

Portanto, o investimento constante em segurança digital, políticas antifraude e infraestrutura resiliente é fundamental para garantir sustentabilidade financeira e operacional a longo prazo.

5.5. Relação entre Perdas Financeiras e Número de Funcionários

O Gráfico 5 apresenta a relação entre o número de funcionários de uma empresa e o valor das perdas financeiras (em milhões de dólares), segmentado por região de domicílio. A análise visual revela que empresas com maior número de funcionários tendem a registrar perdas financeiras mais elevadas, embora haja uma variabilidade significativa entre diferentes regiões.

Gráfico 5 – Relação Perda por quantidade de Funcionários



Fonte: Dados de empresas afetadas por ataques cibernéticos

A distribuição dos pontos sugere uma correlação positiva, mas não linear, entre o número de funcionários e o valor das perdas. Algumas observações importantes incluem:

a) empresas com poucos funcionários (menos de 100) geralmente apresentam perdas menores, frequentemente abaixo de 10 milhões de dólares.
b) empresas com mais de 10.000 funcionários exibem uma grande dispersão de perdas, que variam de pequenas quantias até casos extremos superiores a 1 bilhão de dólares.
c) a dispersão dos dados sugere que outras variáveis, como setor de atuação, nível de digitalização e robustez dos controles internos, podem influenciar significativamente as perdas.

Tal relação é lógica sob a perspectiva atuarial, pois empresas maiores realizam um número mais elevado de transações e têm maior dependência de infraestrutura tecnológica, tornando-se mais vulneráveis a fraudes internas e externas.

No gráfico 5 também são observados pontos extremos (outliers), especialmente em empresas de grande porte, associados a eventos catastróficos, tais como:

a) fraudes massivas, como esquemas Ponzi e manipulações contábeis.

b) ciberataques de grande escala, especialmente ransomwares com prejuízos bilionários.
c) falhas sistêmicas significativas, como colapsos de infraestrutura tecnológica ou crises bancárias.

Esses eventos ressaltam a necessidade de seguros especializados, provisões atuariais robustas e políticas eficazes de mitigação de riscos em empresas maiores.

Do ponto de vista atuarial e de gerenciamento de riscos, os padrões observados indicam importantes conclusões, como:

a) necessidade de precificação diferenciada de seguros com base no porte da empresa.
b) importância da inclusão de variáveis como setor de atuação e nível de digitalização nos modelos atuariais.
c) essencialidade de planos de contingência robustos contra fraudes e ciberataques.
d) implementação de auditorias internas rigorosas para prevenir perdas operacionais decorrentes de falhas nos processos.

Em resumo, o Gráfico 5 demonstra que, apesar da relação entre o tamanho da empresa e as perdas financeiras, outros fatores regionais e operacionais também são relevantes. A abordagem atuarial precisa considerar todas essas variáveis para desenvolver modelos de risco mais eficazes, precificar seguros adequadamente e estabelecer estratégias eficientes de mitigação para empresas em escala global.

6. CONSIDERAÇÕES FINAIS

A crescente digitalização dos processos empresariais e a consequente exposição a riscos cibernéticos reforçam a importância de um monitoramento eficiente dessas ameaças. Ao longo deste estudo, buscou-se compreender a dinâmica dos riscos cibernéticos e demonstrar como ferramentas de Business Intelligence, com ênfase no Microsoft Power BI, podem auxiliar na gestão e mitigação desses riscos.

A análise realizada evidenciou que os riscos cibernéticos têm impacto significativo sobre a estabilidade financeira e operacional das empresas, podendo resultar em perdas bilionárias, danos à reputação e prejuízos regulatórios. Os setores mais afetados, como serviços financeiros, manufatura e tecnologia da informação, demandam uma abordagem mais rigorosa na prevenção e resposta a incidentes. Observou-se que a maior incidência de perdas está associada a fraudes externas, interrupções de negócios e falhas sistêmicas, o que reforça a necessidade de investimentos em segurança da informação e infraestrutura resiliente.

A utilização do Power BI provou ser um diferencial estratégico na identificação de padrões e tendências de risco, permitindo que empresas monitorem indicadores críticos em tempo real. A implementação de dashboards dinâmicos e modelos preditivos com base na linguagem DAX possibilitou uma análise mais aprofundada das perdas financeiras e sua relação com fatores como número de funcionários e região geográfica. A dispersão das perdas entre diferentes setores e continentes indica que a vulnerabilidade às ameaças cibernéticas é um fenômeno global e deve ser tratada de forma personalizada para cada contexto.

Do ponto de vista atuarial, este estudo reforça a necessidade de modelagens estatísticas mais precisas para a precificação de seguros cibernéticos e provisões técnicas. A análise de dados e o uso de ferramentas de BI são fundamentais para apoiar decisões que minimizem os impactos financeiros e fortaleçam a resiliência organizacional. Modelos preditivos devem ser aprimorados para antecipar possíveis ciclos de aumento nas perdas e permitir uma resposta mais eficiente aos riscos emergentes.

Em suma, a gestão eficaz dos riscos cibernéticos exige uma abordagem multidisciplinar que combine tecnologia, análise atuarial e estratégias de segurança digital. O uso de ferramentas como o Power BI se apresenta como um aliado indispensável para a análise e tomada de decisão baseada em dados, promovendo

maior segurança e estabilidade para as organizações em um cenário cada vez mais digital e interconectado.

REFERÊNCIAS

ALLIANZ RISK BAROMETER. Berlim, Alemanha, 2025. Disponível em: https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html. Acesso em: 23 fev. 2025.

CARDOSO, Luiz Henrique Filadelfo. Gestão do risco cibernético à implantação ADS-B no âmbito do SISCEAB por meio do método de Gerenciamento de Riscos à Segurança Operacional (GRSO). Brasília, 2024. Disponível em: http://www.rlbea.unb.br/jspui/handle/10482/47944. Acesso em: 10 fev. 2025.

DAVIDISEMINGER. **O que é Power BI? - Power BI**. Redmond, Estados Unidos, 2024. Disponível em: https://learn.microsoft.com/pt-br/power-bi/fundamentals/power-bi-overview. Acesso em: 23 fev. 2025.

DE SOUZA, Deywisson Ronaldo Oliveira *et al.* Guerra híbrida e ciberconflitos: uma análise das ferramentas cibernéticas nos casos da síria e conflito rússia-ucrânia. **Revista Eletrônica da Estácio Recife**, Recife, v. 5, n. 3, 2019. Disponível em: https://reer.emnuvens.com.br/reer/article/view/346. Acesso em: 23 fev. 2025.

GLOECKNER, Ricardo Jacobsen; DA SILVA, David Leal. Criminal Compliance, controle e lógica atuarial: A relativização do Nemo tenetur se detegere. **Revista de Direito da Universidade de Brasília**, Brasília, 2014. Disponível em: https://repositorio.pucrs.br/dspace/bitstream/10923/11366/2/Criminal_Compliance_Controle_e_Logica_Atuarial_a_relativizacao_do_nemo_tenetur_se_detegere.pdf. Acesso em: 23 fev. 2025.

GONÇALVES, Maria Sofia de Nóbrega Malça. **Implementação de um Scorecard utilizando o Power BI: Um estudo de caso**. 2024. Master's Thesis - Universidade do Porto (Portugal), Porto, Portugal, 2024. Disponível em: https://search.proquest.com/openview/09ea717674e23c426ae4024fd8ea5452/1?pq-origsite=gscholar&cbl=2026366&diss=y. Acesso em: 23 fev. 2025.

HOFFMAN, Karen Epper. The Financial Fraud Epidemic. **American Bankers Association. ABA Banking Journal**, New York, v. 113, n. 2, p. 20–23, 2021. Disponível em: https://search.proquest.com/openview/3d18c942a84a900f54653aee6d4630d7/1?pq-origsite=gscholar&cbl=47754. Acesso em: 26 fev. 2025.

JUNIOR, Augusto Wagner Menezes Teixeira; LIMA, Marcos Costa. Cooperação, Regionalismo e Desenvolvimento Econômico: Brasil, Índia e Coréia do Sul Comparados. **SÉCULO XXI: Revista de Relações Internacionais-ESPM**, Pernambuco, Brasil, v. 1, n. 1, p. 29–63, 2010. Disponível em: https://sumario-periodicos.espm.br/xxi/article/view/5. Acesso em: 10 mar. 2025.

KOKS, Elco *et al.* Understanding Business Disruption and Economic Losses Due to Electricity Failures and Flooding. **International Journal of Disaster Risk Science**, Berlin, Germany, v. 10, n. 4, p. 421–438, 2019. DOI: 10.1007/s13753-019-00236-y.

LANGLOIS, Richard N.; COSGEL, Metin M. FRANK KNIGHT ON RISK, UNCERTAINTY, AND THE FIRM: A NEW INTERPRETATION. **Economic Inquiry**, Fountain Valley, California, v. 31, n. 3, p. 456–465, 1993. DOI: 10.1111/j.1465-7295.1993.tb01305.x.

LEZZI, Marianna; LAZOI, Mariangela; CORALLO, Angelo. Cybersecurity for Industry 4.0 in the current literature: A reference framework. **Computers in Industry**, Amsterdã, Países Baixos, v. 103, p. 97–110, 2018. Disponível em: https://www.sciencedirect.com/science/article/pii/S0166361518303658. Acesso em: 10 mar. 2025.

LIEBER, Renato Rocha; ROMANO-LIEBER, Nicolina Silvana. O conceito de risco: Janus reinventado. **MINAYO, MC de Souza; MIRANDA, AC de. Saúde e ambiente sustentável: estreitando nós. Rio de Janeiro: ABRASCO/FIOCRUZ**, Rio de Janeiro, v. 15, 2002. Disponível em: https://books.scielo.org/id/xkvy4/pdf/minayo-9788575413661.pdf#page=70. Acesso em: 23 fev. 2025.

MEIRELES, Isys Gonzaga; PASITTO, Fernando Teles. ESTELIONATO E SUAS IMPLICAÇÕES: O CONSTANTE CRESCIMENTO DOS GOLPES VIRTUAIS. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo,SP, v. 10, n. 11, p. 6303–6316, 2024. Disponível em: https://periodicorease.pro.br/rease/article/view/17063. Acesso em: 23 fev. 2025.

RIZKIANA ISKANDAR *et al.* Determinants of Auditor's Ability to Detect Fraud: Internal and External Factors. **International Journal of Science, Technology & Management**, Indonesia, v. 3, n. 1, p. 179–195, 2022. DOI: 10.46729/ijstm.v3i1.452.

RUVOLO, Alberto. **Business Intelligence: concepts and application-Implementation of an Intelligent Planning through software Board**. 2024. PhD Thesis - Politecnico di Torino, Turim, Itália, 2024. Disponível em: https://webthesis.biblio.polito.it/31168/. Acesso em: 23 fev. 2025.

SUPERVISION, Banking. Basel committee on banking supervision. **Principles for Sound Liquidity Risk Management and Supervision (September 2008)**, Basileia, Suiça, 2011. Disponível em: https://www.academia.edu/download/45696423/bcbs213.pdf. Acesso em: 23 fev. 2025.

THOMAS, Jason. Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. **Thomas, JE (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal of Business Management**, Canadá, v. 12, n. 3, p. 1–23, 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3171727. Acesso em: 26 fev. 2025.

UNITED STATES SUPERINTENDENT OF DOCUMENTS. **National Institute of Standards and Technology**. Washington, D.C: US Government Printing Office, 1992. Disponível em: https://books.google.com/books?hl=pt-BR&lr=&id=sZxmn_7z1SUC&oi=fnd&pg=PA4&dq=National+Institute+of+Standards+

and+Technology&ots=Qru6rgln3e&sig=svVpBTjO2RVclYskZzAXTUYacXI. Acesso em: 23 fev. 2025.

VELASCO, Cristos. Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. **ERA Forum**, Berlin, Germany, v. 23, n. 1, p. 109–126, 2022. DOI: 10.1007/s12027-022-00702-z.

VON SOLMS, Rossouw; VAN NIEKERK, Johan. From information security to cyber security. **computers & security**, Amsterdã, Países Baixos, v. 38, p. 97–102, 2013. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404813000801. Acesso em: 10 mar. 2025.

ZAHID, Amjad Hussain Afzal *et al.* A critical analysis of software failure causes from project management perspectives. **VFAST Transactions on Software Engineering**, Lahore, Pakistan, v. 6, n. 1, p. 62–68, 2018. Disponível em: https://vfast.org/journals/index.php/VTSE/article/view/512. Acesso em: 26 fev. 2025.