UNIVERSIDADE FEDERAL DO CEARÁ

FACULDADE DE ECONOMIA, ADMINISTRAÇÃO, ATUÁRIA E CONTABILIDADE

DEPARTAMENTO DE ADMINISTRAÇÃO

CURSO DE CIÊNCIAS ATUARIAS

VICTOR PURCARU FREITAS

UMA INTRODUÇÃO À GESTÃO DE RISCOS CIBERNÉTICOS

FORTALEZA-CE

2023

VICTOR PURCARU FREITAS

UMA INTRODUÇÃO À GESTÃO DE RISCOS CIBERNÉTICOS

Monografia apresentada ao Curso de Ciências Atuariais do Departamento de Administração da Universidade Federal do Ceará, como requisito parcial para obtenção do Título de Bacharel em Ciências Atuariais.

Orientador: Prof. Ms. Alana Katielli Nogueira Azevedo.

FORTALEZA

2023

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)

F1i FREITAS, VICTOR PURCARU.
Uma introdução à gestão de riscos cibernéticos / VICTOR PURCARU FREITAS. – 2023.
80 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, 2023.
Orientação: Prof. Me. Alana Katielli Nogueira Azevedo.

1. gestão de risco. 2. risco cibernético. 3. cyber risk. 4. risco. 5. risk. I. Título.

CDD 368.01

VICTOR PURCARU FREITAS

UMA INTRODUÇÃO À GESTÃO DE RISCOS CIBERNÉTICOS

Monografia apresentada ao Curso de Ciências Atuariais do Departamento de Administração da Universidade Federal do Ceará, como requisito parcial para obtenção do Título de Bacharel em Ciências Atuariais.

Aprovada em: 12/12/2023.

BANCA EXAMINADORA

_____

Profª. Ms. 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, Verônica e Reginaldo

À minha tia, Marionescu.

AGRADECIMENTOS

A todos da minha família, que me apoiaram e incentivaram ao longo dessa jornada. Em especial, aos meus pais Verônica e Reginaldo, e a minha tia Marionescu, por toda dedicação a nossa família, por todo amor direcionado, por me darem a base para que eu chegasse até aqui e encarasse esse desafio.

Aos meus professores que doaram seus conhecimentos e contribuíram para meu crescimento profissional e acadêmico, em especial a Alana, por todo apoio, dedicação e incentivo nessa fase final do curso e pelo paciente trabalho de revisão desta monografia.

Aos professores participantes da banca examinadora Alane Siqueira Rocha e Daniel Tomaz de Sousa pelo tempo, pelas valiosas colaborações e sugestões.

A minha equipe de trabalho, Área Gestão de Riscos e Controles Internos, por todo o aprendizado, todos os momentos de descontração, e pelo conhecimento prático transmitido, contribuindo para a concepção teórica deste projeto.

“O homem não é nada além daquilo que a educação faz dele."

(Immanuel Kant)

RESUMO

A revolução digital está afetando quase todos os aspectos da vida cotidiana. A sociedade e os negócios tornaram-se cada vez mais dependentes da tecnologia e da internet. Como resultado, a disponibilidade e a segurança de todos os serviços de que se depende para a vida diária, especialmente os serviços financeiros, estão expostas a ameaças cibernéticas e riscos associados. Dessa forma, fica clara a necessidade de estruturar e implementar, de forma baseada em dados, o processo de gestão de riscos, por meio do alinhamento dos interesses dos *stakeholders* e da implementação de mecanismos eficazes para recompensar tomadores de decisão prudentes, fundamentado na mobilização de profissionais e na internalização de uma cultura orientada para riscos nos valores fundamentais da organização. Esse trabalho teve como objetivo apresentar, por meio da metodologia de revisão bibliográfica de fontes secundárias, o gerenciamento de riscos cibernéticos de uma perspectiva que ultrapassa a mera função de proteção contra possíveis perdas financeiras decorrentes da materialização desses riscos, estabelecendo e divulgando princípios, diretrizes e responsabilidades a serem observadas no processo de gestão de riscos, de forma a possibilitar a identificação, avaliação, tratamento, monitoramento e comunicação de riscos inerentes às atividades de empresas que possam afetar o atendimento aos seus objetivos e realização de seus negócios, além de propor novos meios e campos de estudos a fim de sanar dificuldades de estimação e quantificação do risco abordado.

Palavras-chave: risco puro; gestão de risco; risco cibernético.

ABSTRACT

The digital revolution is affecting almost every aspect of everyday life. Society and business have become increasingly dependent on technology and the internet. As a result, the availability and security of all services we rely on for our daily lives, especially financial services, are exposed to cyber threats and associated risks. In this way, the need to structure and implement, in a data-based manner, the risk management process is clear, through the alignment of stakeholders' interests and the implementation of effective mechanisms to reward prudent decision makers, based on the mobilization of professionals and the internalization of a risk-oriented culture into the organization's fundamental values. This work aimed to present, through the methodology of a bibliographical review of secondary sources, the management of cyber risks from a perspective that goes beyond the mere function of protection against possible financial losses resulting from the materialization of these risks, establishing and disclosing principles, guidelines and responsibilities to be observed in the risk management process, in order to enable the identification, assessment, treatment, monitoring and communication of risks inherent to the activities of companies that may affect the achievement of their objectives and the performance of their business.

Keywords: pure risk; risk management; cyber risk.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

Dentro do contexto deste texto, denotado como a quarta revolução industrial, temos um mundo cada vez mais conectado na qual é observável a tendência de conjuntos de dados consideravelmente maiores, tanto em cenário nacional quanto mundial, tendo como consequência o aumento na demanda por ferramentas de gestão e análise para lidar com uma quantidade crescente de dados sensíveis, sejam em registros financeiros, legais e médicos conforme destaque em gráfico 2. Além disso, observa-se a comoditização exponencial de mecanismos de ataque no público em geral, o que, financeiramente e em termos de complexidade, reduz drasticamente o custo de entrada para o desenvolvimento de *exploits*. ameaças internas e fraudes.

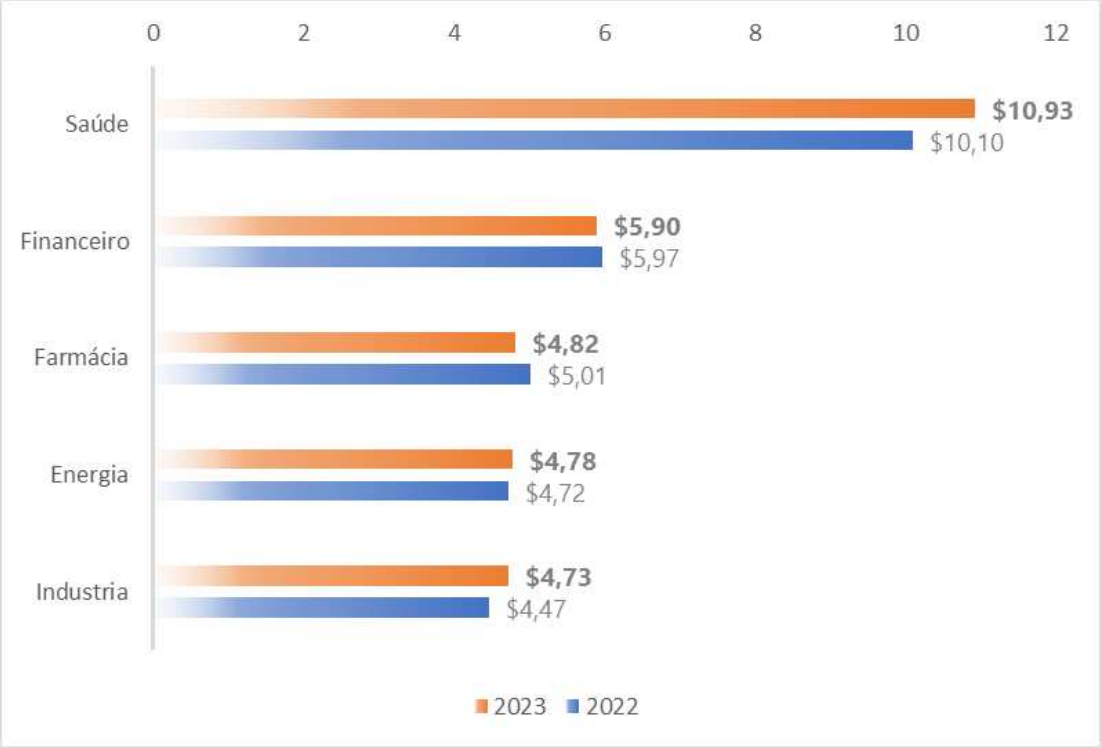
Esses fatores contribuíram para o constante aumento, no exterior, em violações de dados em diversos setores, que prosperaram na última década. Tornou-se difícil ignorar o aumento no custo médio das violações de dados em todo o mundo, que conforme gráfico 1 (IBM, 2023) alcançaram novo patamar de US$ 4,45 milhões no ano de 2023, representando um aumento próximo de US$ 100 mil em relação ao ano de 2022 .

Gráfico 1 – Custo total referente a violação de dados (em milhões de dólares)

Fonte : (IBM, 2023, pg.10).

Tanto nos Estados Unidos quanto na América Latina, que já possuem um alto custo de violações na faixa de US$ 3,69 milhões a US$ 9.48 milhões, é observável um aumento médio de +32% na América Latina e +0.4% nos EUA no período de 2018 e 2019. O Brasil, com um custo médio de US$ 1,22 milhões em violações, apresentou uma redução de -12% em relação ao período anterior, e um aumento de +13% em relação a 2021 (IBM,2023).

Gráfico 2 – Top 5 Indústrias em relação ao custo referente à violação de dados por (em milhões de dólares)



Fonte : IBM (2023).

A evolução dos crimes cibernéticos passou de incidentes como o furto de dados pessoais e de cartões de crédito, considerados ativos informacionais, para a ataques coordenados em infraestruturas críticas. Estes ataques concentram-se principalmente em plataformas de tecnologia e em informações ainda mais valiosas. Atualmente, as organizações encontram-se cada vez mais conectadas, retendo maior quantidade de informações e dados pessoais. Além disso, demonstram maior flexibilidade na troca de conhecimentos, tornando-se mais interdependentes.

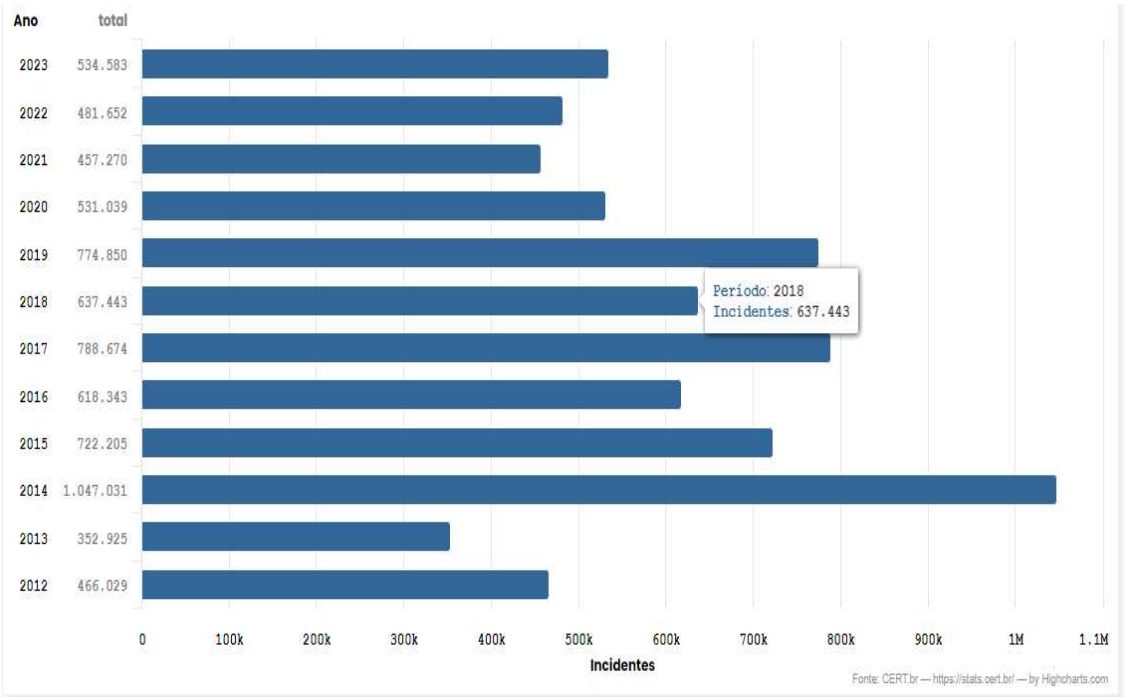
Com base em (Datareportal,2023), é possível constatar que, em 2023, mais de 5.5 bilhões de pessoas estavam online, com um crescimento de 189 milhões em relação ao ano de 2022. Existe assim, um motivo ao aumento do apetite ao crime cibernético, com hackers mais sofisticados, cuja progressão persiste em complexidade e magnitude financeira, com eventos desde vazamentos políticos durante eleições nacionais, ataques de resgate em saúde, educação e setores públicos. Os impactos financeiros são superiores e os reputacionais atingem a grande preocupação para as empresas.

Para Allianz (2022):

> “a cibersegurança é o principal risco de negócios no barômetro da Allianz Risk, ocasionado pelo aumento de ataques de ransomware, comprometimento de e-mails empresariais e ataques à cadeia de suprimentos, acelerados pela inteligência artificial e tecnologia. Em resposta à natureza em constante evolução do risco cibernético, o mercado de seguros cibernéticos amadureceu rapidamente na produção de soluções e abordagens inovadoras”.

Em 2023, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) registrou 534.583 notificações de incidentes de segurança (gráfico 3), ou seja, evento adverso confirmado, relacionado à violação na segurança de dados pessoais (Brasil,2022), ocorridos na internet brasileira. Apresentando além do aumento de 11% em relação aos incidentes registrados em 2022, um aumento de 373% das notificações “outros”, ou seja, sem classificação pela entidade, e uma redução de 21% e 31,5% das notificações de tentativas de fraude e DoS (*Denial of Service*), respectivamente.

Gráfico 3 – Notificações de incidentes recebidos pelo CERT.br (2012 a outubro de 2023)



Fonte: (CERT.br, 2023).

Os ativos de informação são essenciais para a Administração Pública Federal (APF), porém, estão expostos a grandes riscos, observa-se um aumento de 10,9% em notificações de scan, ou seja, além de notificações de varreduras em redes de computadores (*scans*), notificações envolvendo força bruta de senhas, tentativas mal-sucedidas de explorar

vulnerabilidades e outros ataques sem sucesso contra serviços de rede disponibilizados publicamente na Internet. Desse modo, os pilares da segurança da informação – que são a disponibilidade, a integridade, a confidencialidade e a autenticidade – estão sujeitos a vulnerabilidades (Mandarino Júnior; Canongia, 2010).

Juntamente a isso, destacam-se as principais conclusões no relatório de ataques cibernéticos pela (IOCTA, 2023):

a) Ataques cibernéticos baseados em malware continuam sendo a ameaça mais proeminente para a indústria;

b) Programas afiliados de ransomware tornaram-se a principal forma de organização de grupos de ransomware;

c) Táticas comuns de intrusão incluem e-mails de phishing com malware, força bruta no Protocolo de Área de Trabalho Remota (RDP) e exploração de vulnerabilidades em Redes Privadas Virtuais (VPN);

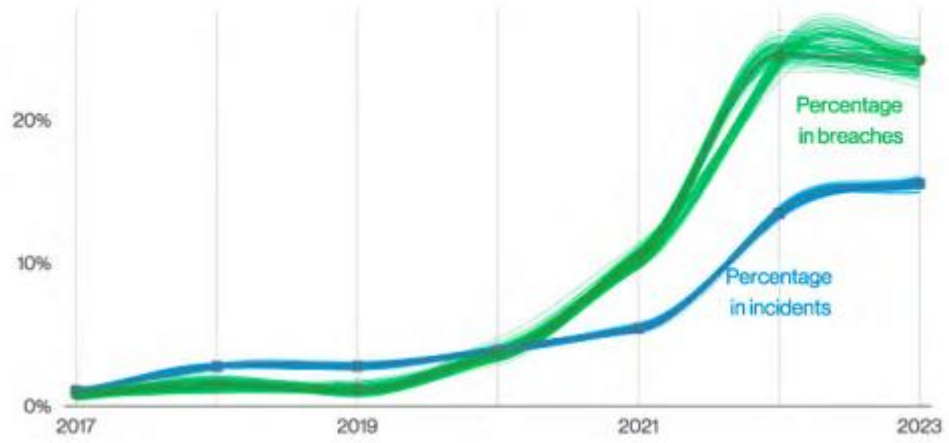
d) A guerra de agressão russa contra a Ucrânia resultou em um aumento significativo nos ataques de Negação de Serviço Distribuído (DDoS) contra alvos da União Europeia;

e) Facilitadores como Corretores de Acesso Inicial (IABs), fornecedores de droppers como serviço e desenvolvedores de crypters desempenham papel crucial na execução de ataques cibernéticos;

f) A guerra de agressão na Ucrânia, juntamente com a política interna da Rússia, levou os cibercriminosos a se deslocarem para outras jurisdições.

A severidade de dados veio a crescer devido a combinação e afiliação de ataques com a aplicação de ransomware (gráfico 4), conforme citado acima por (IOCTA, 2023), o que pode começar como uma invasão em servidor em nuvem, uma ameaça persistente e relativamente complexa, pode se desenvolver para a implementação de um resgate, possibilitando ainda o posterior vazamento de dados em um “Leak after Hack” mesmo sendo pago o resgate.

Gráfico 4 – Violações de *ransomware* ao longo do tempo



Fonte: (Verizon, 2023).

Conforme Brasiliano (2016),

> "A identificação de que há um outro lado da moeda da inovação e que o mundo digital também oferece grande potencial de exploração por parte dos criminosos surgiu muito tarde. As empresas ficaram muito vulneráveis. Adicionalmente, consequências complexas e imprevistas da interconectividade entre as pessoas, as organizações e o ambiente estão emergindo. Antecipar-se aos ataques cibernéticos é a única forma de colocar-se à frente dos criminosos cibernéticos".

Mitigar *cyber risk* é uma prioridade para 2024, conforme pesquisa da PwC Global Digital Trust Insights. Atualmente o risco cyber é o Segundo mais priorizado, atrás apenas de riscos digitais, e segundo (PWC,2023), mais de 30% das companhias não seguem de forma consistente práticas de cybersegurança.

Ainda assim, conforme pesquisa da Tempest Datafolha, 51% das organizações mencionam cybersegurança em seus Mapas Estratégicos, e 73% das empresas planejam Comitê exclusivo de Cyber para assessoramento do Conselho de Administração. Entende-se assim a importância do tema para o mercado, ainda mais explicito em quadro 1, que denota a frequência de temais mais discutidos em pautas estratégicas no Conselho de Administração (ou Comitê Executivo) da organização.

Quadro 1 - Frequência de temais mais discutidos em pautas estratégicas no Conselho de Administração (ou Comitê Executivo) da organização.

Tema	Frequência
O esclarecimento do dimensionamento dos riscos cibernéticos da organização	Mais de 60%
A priorização das ferramentas a implementar	Mais da metade
O esclarecimento das ameaças mais comuns à indústria	Mais da metade
O status da gestão de conformidades de normas e regulamentações	Mais da metade
Indicadores de frequência de incidentes, e status da gestão deles	Mais da metade
Definições de corresponsabilidade do corpo executivo sobre os cyber riscos da empresa	Mais de 1/3
O orçamento de cyber e o equilíbrio em relação ao mercado	Mais de 1/3
A quantificação dos riscos, impacto financeiro e probabilidade de ocorrência	Mais de 1/3
A abordagem de Apetite ao Risco, e a definição de escalas de mensuração que suporte a tomada de decisão	Mais de 1/3
Forma de inclusão da cibersegurança no contexto de negócios	Mais de 1/3
As descobertas de Auditoria Interna e níveis de conformidade regulatória e padrões	Mais de 1/3
Não há discussão de cibersegurança em Comitê Executivo e/ou Conselho	Menos de 1/4

Fonte: 3ª Pesquisa Tempest DataFolha sobre Segurança Cibernética

A medição e avaliação de riscos, observados como tópico atual conforme discutido anteriormente, são a base para a elaboração de planos diante de perigos. O objetivo desse processo é identificar e controlar os riscos para reduzir seu impacto na organização (Hester; Harrisson, 1998). A medição e a avaliação de riscos são de grande importância para organizações, bem como para investidores e empreendedores, que orientarão a tomada de decisões na definição dos tipos e volume de investimento e objetivos de curto e longo prazo (Resnick, 2008).

A medição de riscos também contribui para fornecer sinais de alerta. A medição e avaliação de riscos baseiam-se na ligação entre dados históricos e ferramentas de previsão para formular cenários possíveis que possam representar uma ameaça para a organização. Existem várias ferramentas quantitativas e qualitativas para medir e avaliar riscos (Banks; Dunn, 2003).

Os atuários de *pricing* precisarão considerar como os desenvolvimentos do cybercrime impactam as linhas de negócios existentes e como podem incorporar isso em suas metodologias de precificação. Avaliações de risco podem auxiliar na identificação desses riscos nas linhas de negócios existentes e apoiar o desenvolvimento de métodos de quantificação. Cada linha de negócios será afetada de maneira diferente e em diferentes graus. Por exemplo, em algumas linhas de negócios, os riscos subjacentes estão cada vez mais dependentes de

dispositivos interconectados para alterar a forma como os riscos e as perdas se materializam. Essa avaliação essencialmente verificará como as coberturas existentes são impactadas pelo aumento desse risco.

O presente trabalho tem como objetivo apresentar, por meio da revisão bibliográfica de fontes secundárias, o gerenciamento de riscos cibernéticos de uma perspectiva que ultrapassa a mera função de proteção contra possíveis perdas financeiras decorrentes da materialização desses riscos, estabelecendo e divulgando princípios, diretrizes e responsabilidades a serem observadas no processo de gestão de riscos, de forma a possibilitar a identificação, avaliação, tratamento, monitoramento e comunicação de riscos inerentes às atividades de empresas que possam afetar o atendimento aos seus objetivos e realização de seus negócios.

Esta monografia está dividida como segue: o próximo capítulo aborda o conceito de risco e suas diversas definições, bem como destacar a existência de diferentes metodologias de classificação de riscos; O capítulo 3 categoriza o risco cibernético, suas complexidades e características; O capítulo 4 explana acerca do que se entende por gestão de riscos e sobre os benefícios que sucedem de sua adoção dentro de uma companhia; e, por fim, são feitas as considerações finais.

2 O RISCO PURO

Conforme (ISACA, 2023), uma definição de risco é a combinação da probabilidade de um evento e seu impacto, definição é consoante com o destacado por ISO9001 (2015), risco se refere ao efeito sobre a incerteza relacionado ao resultado esperado de um processo, projeto, ou qualquer objetivo de negócio.

Adicionalmente, diversos autores veem a caracterizar o risco como uma coleção de eventos indesejados (HESTER; HARRISON, 1998), (Malevergne e Sornette, 2005) classificaram risco como eventos aleatórios mensuráveis, enquanto isso, Williams et al. (2006) os classificou como componentes mensuráveis e não mensuráveis. O risco também pode ser classificado como: um declínio na receita total de uma organização (Gregoriou, 2006), risco de perda (Horcher, 2005), a possibilidade de falha de parte ou de todo o sistema levando a resultados indesejáveis (MOLAK, 1997), a incerteza de alcançar os resultados desejados (Keegan, 2004), um evento ou circunstância que, se ocorresse, afetaria a realização dos objetivos do projeto (Chambam, 2003) e uma perda inesperada (Condamin et al., 2006), ou como a perda potencial de fundos de capital entre o início e o final do período de investimento (Warwick, 2003).

Segundo o Tribunal de contas da União (TCU), o risco é conceituado como a possibilidade de que um evento afete negativamente o alcance dos objetivos (TCU, 2020). Juntamente o conceito de risco é definido por COSO (2017, pg.19) como “a possibilidade de que eventos irão acontecer e impactar o desenvolvimento e/ou cumprimento de demandas estratégicas e objetivos do negócio.”

A diferença entre o risco e um evento negativo é que o risco é um termo ligado a eventos inesperados que aconteceram ou podem acontecer no futuro, já o evento, sendo uma ocorrência ou conjunto de ocorrências, é o resultado do risco.

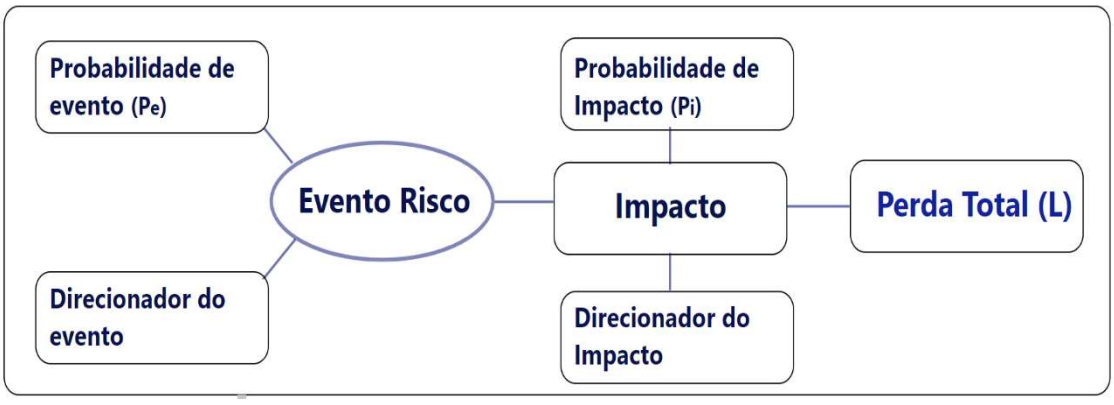
Uma ocorrência ou conjunto de ocorrências que propiciam a materialização do risco, com exemplo o uso inadequado de EPIs ou a ausência dos mesmos em um ambiente, se conceitualiza como um evento de risco (COSO ERM, 2017).

Figura 1 – Componentes do evento de risco

Fonte: ISO31010 (2018).

Observando as Figuras 2 e 3 percebe-se que o evento de risco desencadeia a concepção do risco ao introduzir uma situação ou circunstância que pode ter impactos adversos nos objetivos e operações de uma entidade. Esses eventos podem ser variados, como condições, ações ou fenômenos naturais. A concepção do risco surge da análise da probabilidade e do potencial de danos associados ao evento. Essa avaliação permite à organização determinar a magnitude do risco e implementar estratégias de gerenciamento adequadas.

Figura 2 – Modelo padrão de risco



Fonte: Smith e Merrit (2002).

Considerando o apontado acima, denotam-se diversas semelhanças entre as definições de risco, se consolidando em eventos prováveis ou não com possibilidade de falha ou interrupção dos objetivos traçados de forma completa.

A aplicação do conceito de risco requer uma definição de 'risco' que se adeque à definição de análise de portfólio apresentada ao contexto avaliado, conforme Hester e Harrison

(1998), o conceito de risco e o grau de acreditabilidade na qual ele é considerado dependem do setor e período na qual se é analisado, já de acordo com COSO (1992) e FERMA (2003), a classificação dos riscos avaliados depende do ambiente interno e do ambiente externo à entidade analisada.

A redução da exposição ao risco implica na diminuição do potencial de oportunidade. Portanto, para alcançar ganhos substanciais, é necessário demonstrar disposição para uma exposição significativa aos riscos (DAMODARAN, 2007).

2.1 Tipos de riscos

O primeiro passo para criar um sistema de gerenciamento de risco eficaz, para fim de aplicar tratamentos específicos e precisos para cada exposição (Nunes, 2009) , é entender as distinções qualitativas entre os tipos de riscos que as organizações enfrentam (KAPLAN; MIKES, 2012) , visto que conforme o cenário avaliado, a organização, o mercado de atuação, além de uma série de outros fatores, se torna difícil uma organização utilizar somente um único conceito de risco para suas atividades de forma eficiente a fim de competir no mercado corporativo (CAVALCANTI, 2009).

Conforme Brasiliano (2012), entende-se que os riscos são ordenados em estratégicos, financeiros, operacionais, de gestão do conhecimento e riscos de conformidade. Porém,

> Não há um tipo de classificação de riscos que seja consensual, exaustivo e aplicável a todas as organizações; a classificação deve ser desenvolvida de acordo com as características de cada organização, contemplando as particularidades da sua indústria, mercado e setor de atuação (BRASILIANO, 2012).

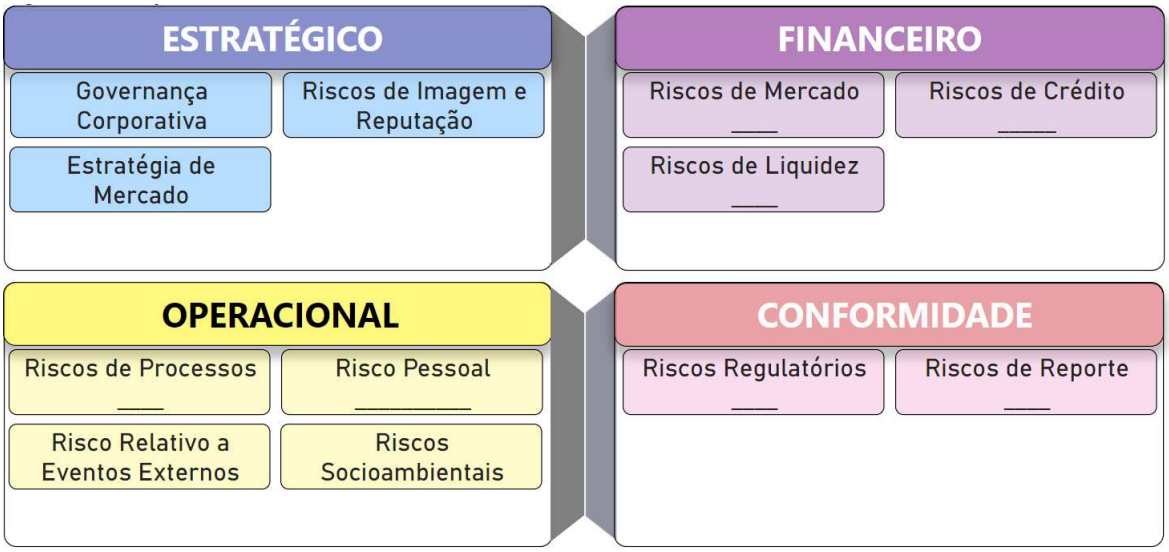
Pesquisadores classificam o risco de diferentes maneiras conforme cenário abordado, Campbell (2008) classificou o risco com base em seu tipo de efeito: risco estratégico, risco financeiro, risco operacional e risco de desastres.

As empresas estão expostas a vários tipos de riscos, que podem ser comerciais, como os riscos do negócio, e financeiros. Dentre os riscos financeiros, estão os riscos de mercado, riscos de liquidez, riscos operacionais e risco de crédito (BASILEIA III, 2010).

Independentemente das diferenças de classificação, os pesquisadores concordam que a classificação de risco ajuda as organizações a entender e analisar os riscos e contribui para o desenho e implementação de planos preventivos e corretivos.

Para a avaliação do presente documento, será considerado a classificação de riscos conforme Figura 4.

Figura 3 – Principais riscos



Fonte: Brasiliano (2012, p. 61).

Conforme FERMA (2003), riscos tem também fatores externos à organização, como o risco financeiro ou estratégico sendo influenciados por não somente a entidade, mas o mercado ou setor financeiro como um todo, ou seja, não dependendo da própria organização ou entidade para ser considerado.

2.1.1 Riscos estratégicos

Se refere à aqueles diretamente relacionados à alta administração da companhia na busca de desenvolvimento, manutenção e crescimento de valor e competitividade ao tempo, podendo levar desde a ruptura da conexão com o mercado até a diluição dos lucros essenciais. Em casos extremos, esses riscos têm o potencial de comprometer todos os pilares que sustentam os objetivos da empresa. É influenciado pela dinâmica de mercado e escassez de recursos, meio político e econômico, fusões e aquisições e avaliação do portfólio e da entidade como um todo em meio social (BRASILIANO,2018).

Conforme Slywotzky (2007) existem sete grandes tipos de riscos estratégicos que empresas devem estar preparadas para enfrentar, abrangendo a maioria das ameaças ao modelo de negócio, incluindo falhas em grandes iniciativas, perda de clientes devido a mudanças inesperadas em preferências, bifurcações no setor devido a mudanças tecnológicas, concorrentes aparentemente invencíveis, enfraquecimento da marca, setores com lucros reduzidos e estagnação no crescimento da empresa.

Ainda segundo Slywotzky, cada um desses riscos pode ter um impacto devastador no negócio, e muitas vezes são subestimados ou ignorados pela gestão. Reconhecer e gerenciar esses riscos é essencial para a sustentabilidade e o sucesso a longo prazo da empresa, e conforme o autor, ignorar ou subestimar esses riscos pode ter consequências sérias para a continuidade do negócio

2.1.2 Riscos operacionais

Se refere à aqueles que envolvem ou estão relacionados à operação, dentre sua eficácia e eficiência, tal quanto seus sistemas e processos, auditorias, controles e pipelines de informação, clientes internos ou externos, e o tangível diretamente dentre os processos que possa gerar receitas, despesas, ativos e passivos, ou impacto contábil direto, com destaque “se referindo às perdas potenciais resultantes de sistemas inadequados, falhas de gestão, controles viciosos, fraude e erro humano” (CROUHY; GALAI; MARK, 2008).

Conforme (UK, 2023. Pg 55),

> riscos decorrentes de liderança e envolvimento ineficazes, cultura subótima, comportamentos inadequados, a falta de disponibilidade de capacidade e capacidade suficientes, ação industrial e/ou não conformidade com a legislação relevante de emprego/políticas de RH resultando em um impacto negativo no desempenho.

O texto sublinha os desafios resultantes de liderança menos eficaz, cultura organizacional menos otimizada, condutas inapropriadas e insuficiência de recursos. Também destaca a imperatividade da conformidade legal e regulatória, enfatizando que uma organização deve compreender e implementar controles para assegurar essa conformidade. Adicionalmente, aponta que em situações excepcionais, o custo de mitigar um risco pode ser substancialmente superior ao próprio risco.

Mais especificamente, Brasiliano (2018) destaca se referir à medida da incerteza nos retornos de uma instituição quando seus sistemas, práticas e controles podem falhar diante de diversos fatores, como falhas humanas, danos à infraestrutura, mau uso de modelos ou produtos, mudanças no ambiente de negócios e situações adversas de mercado.

As principais subcategorias desses riscos incluem sobrecarga nos sistemas, obsolescência de equipamentos, atrasos ou falhas na prestação de serviços, falhas em equipamentos, erros não intencionais, fraudes, falta de qualificação dos funcionários, inadequação de produtos e serviços, questões de regulamentação, problemas na modelagem, falhas na liquidação financeira, riscos sistêmicos, concentração operacional, danos à imagem e

riscos de catástrofe. Estes riscos, muitas vezes, podem ser subestimados ou negligenciados pela gestão, o que pode resultar em graves consequências para a instituição (BRASILIANO, 2018).

2.1.3 Riscos de conformidade

Segundo Assi (2012), o risco de conformidade é a “possibilidade de perda ocasionada pela inobservância, violação ou interpretação indevida de regulamentos e normas”. Com isso, o risco de conformidade é rapidamente associado ao setor jurídico da empresa, que, habitualmente, é o responsável por fiscalizar e garantir o cumprimento de leis e regulamentações aplicáveis à organização.

Conforme (COSO, 2020), os riscos de conformidade se referem a possíveis violações de leis aplicáveis, regulamentações, termos contratuais, padrões ou políticas internas, onde tal violação pode resultar em responsabilidade financeira direta ou indireta, penalidades civis ou criminais, sanções regulatórias ou outros efeitos negativos para a organização ou seus funcionários.

Juntamente, embora os atos subjacentes (ou omissões) sejam realizados por indivíduos, as violações de conformidade geralmente são atribuíveis à organização quando são praticadas por funcionários ou agentes da organização no curso normal de suas funções. O escopo exato dos atos atribuíveis a uma organização pode variar dependendo das circunstâncias. Em alguns casos, o funcionário também pode ter responsabilidade como indivíduo.

Embora a maioria dos riscos de conformidade esteja relacionada a leis ou regulamentações específicas, outros não estão. Esses outros riscos, referidos como "riscos relacionados à conformidade", podem incluir riscos associados a falhas em cumprir padrões profissionais, políticas internas de uma organização (incluindo códigos de conduta e ética nos negócios) e obrigações contratuais (COSO,2020).

2.1.4 Riscos financeiros

Conforme World Bank (2013), o risco financeiro é visto como a potencialidade de perdas financeiras provenientes de várias fontes, incluindo flutuações de mercado, exposição ao crédito, falhas operacionais e outras incertezas que podem impactar o desempenho financeiro e a estabilidade de uma instituição.

O Corporate Finance Institute (CFI, 2023) define o risco financeiro como a potencialidade de perdas ou falhas financeiras resultantes da incerteza nos preços de mercado, taxas de juros, taxas de câmbio, preços de commodities ou estabilidade financeira de outras

partes. De acordo com o CFI, o risco financeiro abrange diversos tipos, incluindo risco de mercado, risco de crédito, risco de liquidez, risco operacional e risco sistêmico.

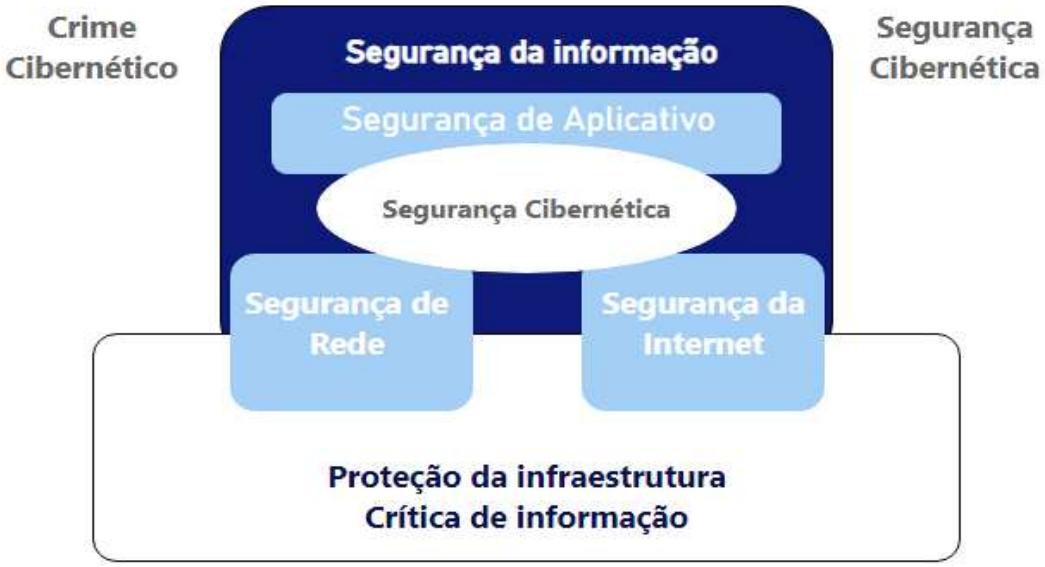
3 O RISCO CIBERNÉTICO

O risco cibernético é, em conceito, o conglomerado dos riscos presentes na gerência e controle de dados em um ambiente "*cyber*", incluindo em negócios ou serviços (CRO Forum, 2014).

O termo se refere a um risco amplamente estabelecido, em constante evolução, emergente, com efeito sistémico em ambos pequena ou grande escala, com rápido aprimoramento de técnicas e dissipação, não somente reconhecido como um risco de TI, mas empresarial no nível executivo (MARSH, 2016).

Em termos mais específicos, vemos na figura 5 que o risco cibernético se trata de qualquer risco que emana do uso de dispositivos eletrônicos e sua transmissão de dados. Também danos físicos que podem ser causados por ataques cibernéticos, fraudes cometidas pelo uso indevido de dados, qualquer responsabilidade decorrente do armazenamento de dados, disponibilidade de rede e a disponibilidade, integridade e confidencialidade de informações eletrônicas - seja relacionada a indivíduos, a internet, empresas ou governos (CRO Forum, 2014).

Figura 4 – Relação entre Segurança Cibernética e outros domínios de Segurança da Informação



Fonte: ABNT NBR ISSO/IEC 27032:2015.

Conforme exposto por Barzilay (2013), “nos referimos a esses riscos como um conglomerado dado a duas características similares: a) todos tem um potencial de alto impacto, b) todos foram um dia considerados improváveis [...] cybersegurança é a soma de esforços investidos em denotar o risco cibernético, o mesmo que, a pouco tempo atrás , era considerado como tão improvável que dificilmente requereria nossa atenção”.

Os riscos e impactos podem ser causados por erro humano ou de sistema, mas também por atividades cibernéticas muitas vezes impulsionadas por motivos criminais tradicionais, como roubo, assalto ou sabotagem, que podem ser executados sem a necessidade de proximidade física (CRO Forum, 2014).

Dentre os ataques, cita-se Intrusão no Sistema, Negação de Serviço, Perda e Roubo de Ativos, Uso Indevido de Privilégios ou Engenharia Social, visando principalmente aplicações web, seguindo um padrão de "entrar, obter os dados e sair" (ZARGAT *et al.*, 2013). Eles abrangem desde tentativas de negação de serviço até a exploração de erros diversos e o uso indevido de privilégios. Cada ataque busca comprometer a disponibilidade ou segurança da aplicação web, mas não requerem uma grande quantidade de ações após a invasão inicial (VERIZON, 2022).

Apesar da abundância de desafios em segurança digital, existem diversas abordagens para enfrentá-los, ainda que não sigam um padrão específico. De acordo com Brasiliano (2023), os pontos cruciais na guerra cibernética incluem:

a) Ataques de software maliciosos e potencialmente indesejados;

b) Ataques de engenharia social;

c) Compartilhamento e coordenação de informações.

As estatísticas dessas questões chaves com os principais riscos cibernéticos em 2021 podem ser vistas no quadro 2, e em empresas que sofreram ataques no ano de 2017 podem ser vistas no Gráfico 5.

Quadro 2 – Principais riscos cibernéticos, 2021

Risco	Posição
Engenharia Social	#1
Ransomware	#2
Vazamento de dados	#3
Brechas de supply-chain	#4
Ataques à privacidade	#5

Fonte: Relatório de ameaças 2021 – Gat Infosec.

Gráfico 5 – Tipos de incidentes cibernéticos reportados à AIG, 2017

Fonte: AIG SEGUROS BRASIL (2019).

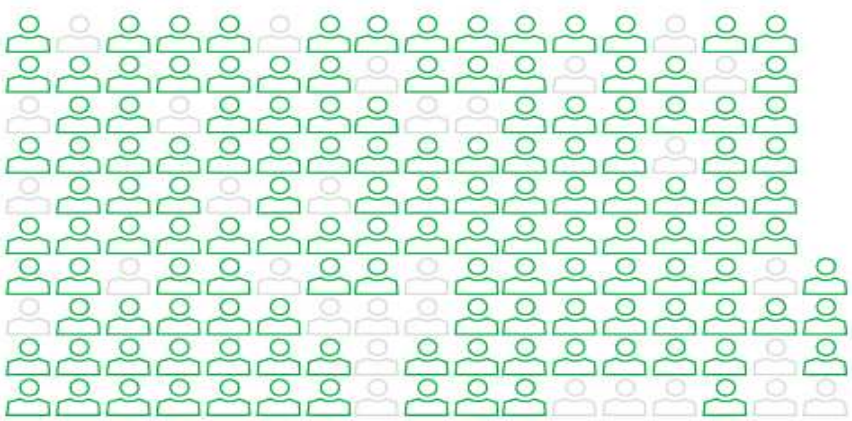
O crime cibernético evoluiu de algo altamente disruptivo e sofisticado, para algo com um amplo e crescente espectro de sofisticação e determinação, uma vez que, enquanto empresas usam grande cautela ao compartilhar informações sobre sua tecnologia - tanto interna quanto externamente - para proteger suas operações comerciais, os atacantes cibernéticos têm o luxo de operar no extremo oposto do espectro, compartilhando informações abertamente por meio da dark web, com pouco receio de repercussões legais, e frequentemente operam com um alto grau de anonimato (CRO Forum, 2014).

Os atacantes cibernéticos alavancam a tecnologia e buscam explorar falhas em políticas e procedimentos de segurança para atacar virtualmente de qualquer lugar e visar virtualmente qualquer tipo de dados. O agressor pode ser uma ameaça interna ou externa, e seus motivos podem variar (DELOITTE, 2019).

Como exposto em Ponemon (2021), as violações de dados custam às organizações ao redor do mundo uma média de US$ 4,24 milhões de dólares por incidente, o maior valor em 17 anos do relatório. O levantamento ouviu mais de 500 organizações ao redor do mundo e

destaca que a complexidade da resolução dos problemas de Segurança contempla as mudanças operacionais drásticas durante a pandemia, com aumento de custo e do tempo de resposta. Em média, as empresas levam 212 dias para detectar uma violação e 75 dias para conter.

Figura 5 – O fator humano nas violações



Fonte: Verizon (2022).

O elemento humano continua sendo um fator chave em 82% das violações, conforme estudo da (Verizon, 2022) em destaque na figura 1, esse padrão engloba uma grande porcentagem dessas violações, destacando: "Seja o uso de credenciais roubadas, phishing, uso indevido ou simplesmente um erro, as pessoas continuam desempenhando um papel muito significativo em incidentes e violações". Além disso, malware e credenciais roubadas fornecem um segundo passo significativo após um ataque social abrir a porta para o invasor, o que destaca a importância de ter um programa de conscientização de segurança robusto.

Avaliando em termos de perdas, a falha de segurança resultante de um data breach resulta em inúmeros custos, podendo provocar perdas financeiras diretas por extorsão (ramsomware), perda de hardware, despesas legais e de perícia, juntamente com perdas financeiras indiretas por meio do vazamento ou perda de dados, podendo ocasionar em danos reputacionais, de litígio ou confiança do consumidor, perda de vantagem comercial, multas ou interrupção do negócio por meio de sanções regulamentares, roubo de identidades, roubo de controle de sistemas vitais ou secundários, perda de acessos, falhas na TI, falhas de processos ou compliance (CRO Forum, 2014) ou perda de disponibilidade devido a ataques DoS (REFSDAL; SOLHAUG; STOLEN, 2015).

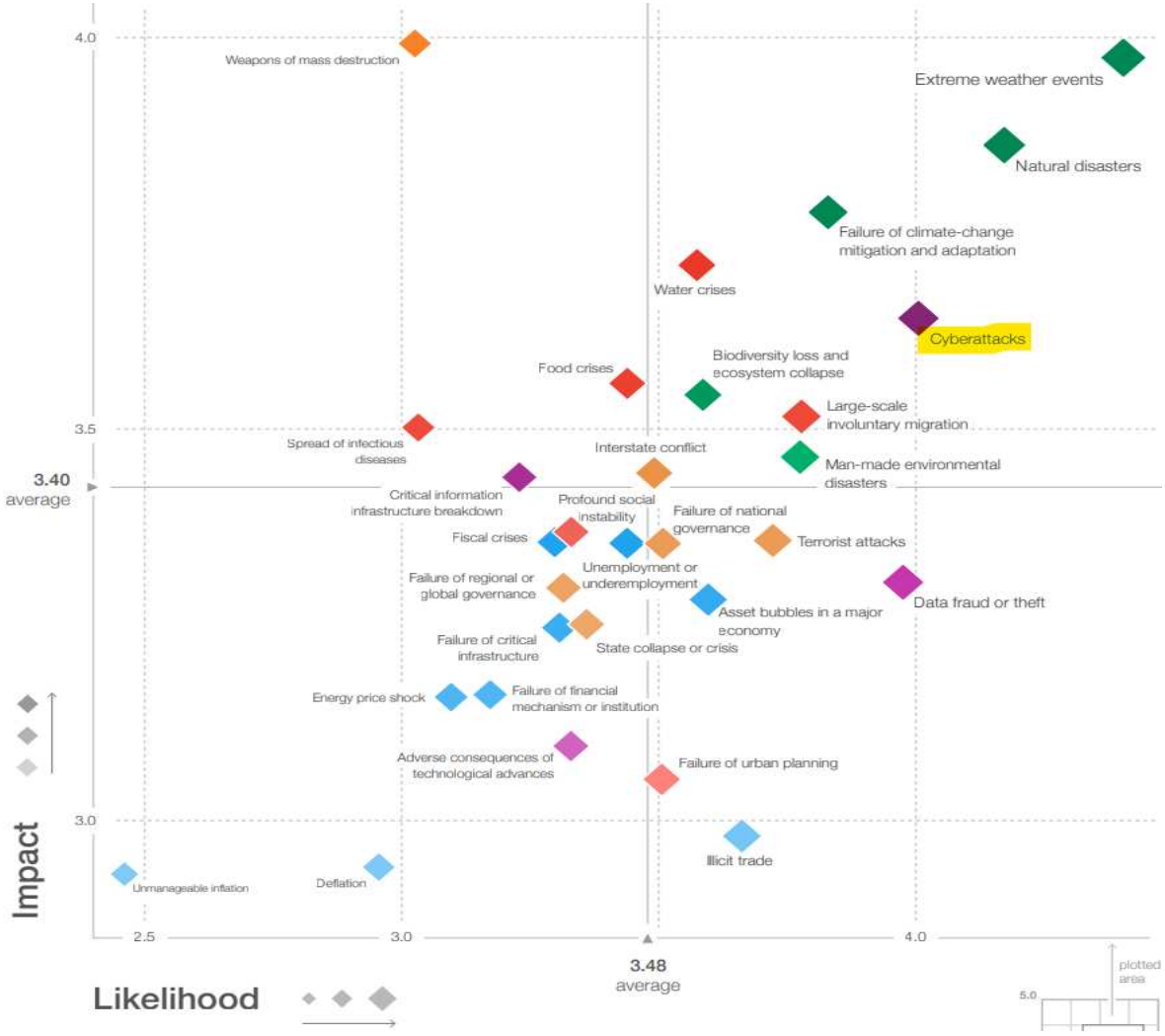
Um estudo conduzido pela KPMG (2016) no Reino Unido revela que os atacantes tendem a se agrupar em três principais categorias, utilizando abordagens "comoditizadas", "direcionadas" ou "de alto padrão" na seleção e exploração de vítimas.

Segundo a pesquisa, há três níveis distintos de crimes digitais, definidos pelos seus alvos. No nível mais alto, criminosos realizam ataques direcionados de alto nível ao sistema financeiro, como o recente ataque de 81 milhões de dólares ao banco central de Bangladesh, que, não fosse pela vigilância de outros bancos centrais, poderia ter sido de 951 milhões de dólares. No segundo nível, há os ataques regulares a empresas e indivíduos de alta renda. E, finalmente, existem ataques comoditizados que afetam o maior público.

Em cada um desses níveis, os criminosos digitais mapeiam os custos e riscos envolvidos em comparação com o pagamento provável, assim como qualquer empreendedor faria.

O Relatório de Riscos Globais (2018) mais uma vez salienta a criticidade e impacto desse risco, o colocando em foco no quesito de risco "muito alto" ao destacar alta probabilidade e impacto inerente ao risco, como pode ser visto na Figura 6.

Figura 6 – Matriz de probabilidade x impacto



Fonte: Global Risk Report (2018).

Aqueles que têm como alvo o sistema de saúde vem a executar um investimento maior em malwares personalizados e em pesquisas e desenvolvimento, juntamente com a infiltração de pessoas em organizações-alvo. O investimento dos criminosos em tempo e esforço é grande, mas também são os seus retornos. O custo para as vítimas de 2023 está em média 10.93 Milhões de dólares mundialmente, e os alvos que falham em proteger seus sistemas também enfrentam multas dos reguladores (IBM, 2023).

Segundo (IBM, 2023), esta é a área de maior risco para os criminosos. As autoridades têm priorizado os ataques para derrubadas de alto perfil, e os criminosos podem ter dificuldade em lavar o dinheiro que conseguiram. Ainda assim, dados do estudo mostram que organizações que envolveram representantes da lei obtiveram *savings* consideráveis em relação aos demais, obtendo em média uma redução de custos de 9.6% or USD 470 mil, juntamente com tempo médio para identificar e conter ataque reduzido em 11.4% ou 33 dias.

As causas mais comuns exploradas pelos criminosos cibernéticos são os fatores humanos de todos os tipos, como engenharia social, erros, mal uso de privilégios de sistemas de segurança mal configurados, uso de credenciais roubadas, links a banco de dados, acesso telefônico ou conexões de gerenciamento de rede secundária e VPNs, citando apenas algumas. De forma geral, as três principais formas de invasão de uma organização são uso de credenciais roubadas, phishing e exploração de vulnerabilidades (Verizon, 2023).

Figura 7 – Diagrama de causa e efeito com a lógica de ataque e as consequências para a empresa

Fonte: Brasiliano (2021)

3.1 Ataques *maware* e APT

Conforme a Europol's European Cybercrime Centre (EC3, 2016), "malware" é um termo abrangente que descreve software malicioso que se infiltra em sistemas de computadores ou dispositivos móveis para roubar informações valiosas ou causar danos aos dados. Existem vários tipos de malware que podem atuar em conjunto durante um ataque. Um exemplo é a "*botnet*", uma rede de computadores interconectados pela internet, controlada por um centro de comando e controle para realizar atividades maliciosas como envio de spam e ataques DDoS. Outros tipos de *malware* incluem "*rootkits*", "*worms*", "cavalos de Troia", "infectores de arquivos", "*trojans* de acesso remoto/*backdoor*", "*ransomware*", "*scareware*", "*spyware*" e "*adware*", cada um com funções específicas.

Os ataques APT (ameaça persistente avançada) seguem geralmente uma estrutura composta por seis etapas: identificação, entrega, exploração, execução, aquisição de dados e exfiltração (GIURA; WANG, 2012). A Figura 8 ilustra um esquema desses estágios conforme descrito pelos autores. Dentre os algoritmos de árvore de decisão (ID3, C4.5, C5.0, CART), destacam-se ID3 (Iterative *Dichotomiser* 3) e C4.5 como os mais utilizados (ANURADHA; VELMURUGAN, 2014).

Figura 8 – Etapas do ataque de hacker

Fonte: montagem do autor com base em (Arcon serviços gerenciados de segurança, 2017).

Em conclusão, o malware representa uma categoria abrangente de softwares maliciosos que visam danificar sistemas, roubar informações e realizar ações prejudiciais sem o consentimento do usuário (ROUSE, 2021). Por outro lado, os ataques APT representam uma forma altamente sofisticada e direcionada de ciberataque, muitas vezes realizada por agentes cibernéticos experientes e bem financiados, com o objetivo de obter informações estratégicas ou sensíveis (EDWARDS, 2017). Ambos os fenômenos são representativos da crescente sofisticação e complexidade do cenário de segurança cibernética, exigindo respostas cada vez mais robustas e proativas por parte das organizações e usuários. A compreensão e a vigilância contínua são essenciais para se proteger contra essas ameaças em constante evolução.

Executivos C-Level, CISOs e líderes do Conselho de Administração das organizações devem estabelecer a tolerância ao risco e identificar quais dados e informações são pertinentes para a empresa. Esta pertinência é fundamental para a organização priorizar seus ativos em relação aos investimentos em segurança cibernética, implementando camadas adicionais de proteção (DELLOITE, 2019). Com esses parâmetros, a alta gestão está preparada para tomar medidas decisivas diante de qualquer incidente

4 A GESTÃO DE RISCO CIBERNÉTICO

A gestão de riscos é a integração da cultura organizacional e dos recursos disponíveis com a estratégia e execução utilizadas pelas organizações para gerenciar riscos na criação, preservação e obtenção de valor (COSO, 2017).

A gestão do risco de uma organização pode ser entendida como a gestão da incerteza e determinação das ações necessárias para que esta possa ser minimizada ou reduzida para níveis considerados aceitáveis por parte da organização. É um exercício sistematizado, no âmbito do qual a organização identifica possíveis ameaças que possam construir sobre as vulnerabilidades dos ativos, bem como quais os níveis do risco associado, avaliando-se a probabilidade de ocorrência e possíveis impactos.

Conforme Vieira *et al.* (2019), a gestão de riscos é o processo que trata dos riscos e oportunidades que afetam a criação, a destruição ou a preservação de valor nas organizações. A premissa inerente ao gerenciamento de riscos é a de que toda a agência, pública ou corporativa, existe para gerar valor às partes interessadas (stakeholders). O entendimento de (FERMA, 2003) quando destaca que a gestão de riscos é um processo vital na gestão estratégica das organizações, e que a ele devem alocar os devidos recursos para que funcione de forma eficaz.

Ao longo dos anos, as organizações têm refinado suas estratégias de defesa para lidar com as ameaças em constante evolução que surgem diariamente (EY, 2016). Esse progresso foi impulsionado por uma série de eventos significativos, incluindo avanços na inovação digital, a Lei Sarbanes-Oxley, a expansão dos produtos conectados, mudanças no cenário regulatório e o constante crescimento de cibercrimes. Esses acontecimentos exigiram medidas de proteção efetivas e formalizadas.

A exposição a riscos é uma realidade comum para todas as organizações do meio corporativo, independentemente de serem entidades financeiras ou não. Mesmo ao conduzir pesquisas de mercado, desenvolver estratégias sólidas e elaborar planejamentos eficazes, todas as empresas enfrentam algum grau de incerteza residual. Assim, surge a necessidade de gerenciar os riscos empresariais, visando prever eventos que possam resultar em ganhos ou perdas, e buscando antecipar-se à concretização de riscos prejudiciais, ao mesmo tempo que se impulsiona a materialização de riscos positivos (DELLOITE, 2019).

Nesta perspectiva, Chakraborty *et al.* (2019) afirmam que os principais impulsionadores da gestão de riscos são os requisitos de governança corporativa e as pressões regulatórias, aliados à demanda de administradores e investidores por uma compreensão mais ampla dos riscos estratégicos e operacionais.

É importante ressaltar que a gestão de riscos não tem como objetivo eliminar completamente os riscos empresariais de uma organização. Para minimizar os possíveis impactos, o processo deve se concentrar na identificação, medição e controle dos riscos (SAEIDI *et al.*, 2019). Dessa forma, a gestão de riscos se torna uma ferramenta importante para os gestores tomarem as decisões mais apropriadas em suas empresas. É por isso que as organizações adotam políticas voltadas para a implementação de uma função de gerenciamento de riscos específica (OLECHOWSKI *et al.*, 2016).

De acordo com Rêgo (2014), nas últimas décadas a gestão de riscos nas instituições financeiras tem sido foco de investigação, pois com a boa gestão de riscos pode ser criado valores para acionistas, que a ideia principal de instituições financeiras é a maximização do seu valor. Segundo Pena (2013), a gestão dos riscos vai mais além da avaliação das possibilidades dos vários cenários de investimentos, é ter conhecimento das limitações dentro da instituição sobre o risco, é ter fatores tradicionais que analisam a viabilidade do mesmo, fatores relacionados com a incerteza.

Durante a pandemia de covid-19, o Brasil testemunhou um aumento nas ameaças cibernéticas e se tornou um dos principais alvos desses ataques (TREND MICRO, 2022). Conforme Brasiliano (2023), causa é resultante de uma falta de visão e conscientização por parte dos executivos de alto escalão e do Conselho de Administração nestas organizações, A ausência de uma Avaliação de Riscos em Segurança Cibernética nas empresas e instituições brasileiras reflete uma certa imaturidade ao risco, agravando ataques, causando impactos significativos em diversos setores, incluindo o hospitalar e a cadeia de suprimentos.

4.1 Metodologia da gestão de risco

Destaca-se aqui a relação entre gestão de riscos e os objetivos da empresa, que é um fator chave nas organizações (Andrade Abreu; Zotes; Ferreira, 2018). Esse papel também surge da percepção de que os riscos devem ser gerenciados de maneira integrada, com foco na estratégia da empresa.

De acordo com as observações de Aven e Zio (2014), devido ao fato de que a gestão de riscos está cada vez mais integrada à cultura das instituições, as técnicas de avaliação e gestão amadureceram por meio de pesquisa e aplicação de resultados. Novas tecnologias e estruturas conceituais estão surgindo. Empresas que não adotam as melhores práticas de mercado e não respeitam as normas impostas podem sofrer ao risco, como dano reputacional, operacional, de mercado ou financeiro (Safa; Von Solms; Furnell, 2016).

A organização deve determinar os recursos humanos e materiais necessários para conduzir efetivamente o processo de gestão de risco. Isso inclui a definição de uma metodologia adequada, a identificação das partes interessadas, a escolha do modelo de governança e o estabelecimento de papéis e responsabilidades. Todas as decisões devem ser aprovadas pela alta administração (BRASILIANO, 2023).

Avaliando práticas exemplares de segurança cibernética a nível internacional com o intuito de abordar a gestão de riscos cibernéticos, temos as seguintes metodologias:

a) COBIT 5: Responsabilidade do ISACA1, o COBIT é um framework de boas práticas para governança de TI. Ajuda as organizações a criar valor a partir da TI e contribui para o equilíbrio entre os benefícios, a otimização dos níveis do risco e a utilização dos recursos disponíveis pelas organizações (ISACA, 2012);

b) ISO/IEC 27001: A norma ISO/IEC 27001 especifica os requisitos para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um sistema de gestão de segurança da informação, bem como os requisitos para os controles de segurança a serem implementados, de acordo com as necessidades e a realidade da organização (ISO, 2013);

c) ISO/IEC 27032: A norma de Tecnologia da Informação, Diretrizes para Segurança Cibernética especifica os requisitos para estabelecer, implementar, operar, monitorar, rever, manter e melhorar um sistema de gestão de segurança cibernética a serem implementados de acordo com as necessidades e realidade da organização (ISO, 2012);

d) ISO/IEC 27005:: A norma ISO/IEC 27005 fornece diretrizes para o estabelecimento de uma abordagem sistemática para o gerenciamento de riscos da Segurança da Informação (ISO, 2018);

e) NIST SP-800-53 Rev4: Publicado pela NIST 93, é um catálogo de controles de segurança e de privacidade para redes e sistemas de informação de infraestruturas críticas, usadas também pelas empresas privadas e públicas. Disponibiliza, também, um processo de seleção de controles para proteção da operação e dos ativos das organizações, de incidentes, desastres naturais, falhas estruturais ou erro humano (NIST, 2013);

f) CIS CSC 7.0: O Catálogo de controles críticos de segurança cibernética (CSC) é publicado pelo Center for Internet Security (CIS). E juntamente com COBIT 5 vem a promover um ciclo de melhorias contínuas em gestão e mitigação de riscos (CIS, 2018);

g) O COSO ERM, disponibiliza um conjunto de Orientações sobre como as organizações podem integrar efetivamente a gestão de riscos em sua estratégia global e desempenho (COSO, 2017);

h) A ISO/IEC 31000 disponibiliza um conjunto de princípios e de orientações genéricas sobre gestão do risco para as organizações. Por outro lado, a ISO/IEC 27005 específica orientações e processos para gestão do risco de segurança dos sistemas de informação de uma organização, apoiando-se, em particular, nos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI), implementado de acordo com a norma ISO/IEC 27001 (ISO, 2018).

O processo de gestão de riscos pode ser visualizado na Figura 9 e de forma mais completa na Figura 10.

Figura 9 – Processo de gestão de riscos

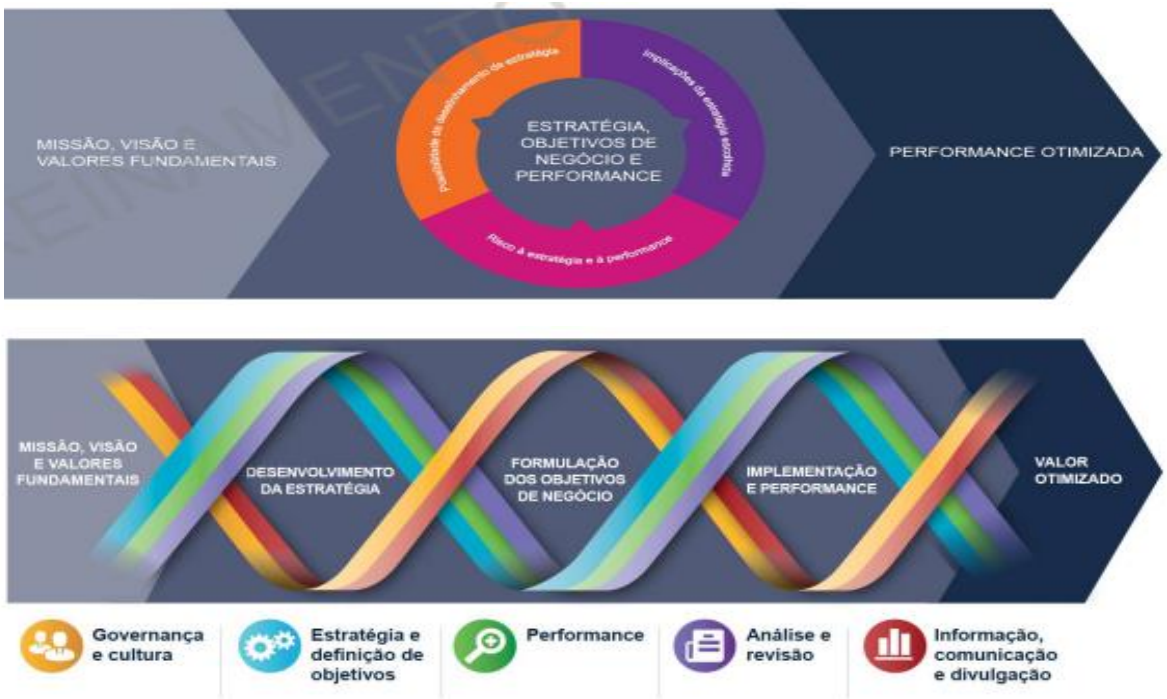
Fonte: ISO 31000 (2018).

Figura 10 – Processo de gestão de riscos em segurança da informação

Fonte: ISO/IEC 27005: 2019

Posteriormente, o processo de Gerenciamento Integrado de Riscos (em inglês ERM) proposto por COSO (2017) pode ser visualizado de forma mais completa na Figura 11.

Figura 11 – Gerenciamento Integrado de Riscos COSO



Fonte: (COSO, 2017).

Descrevendo o modelo conforme COSO (2017), a governança estabelece para o ERM o tom da entidade, enfatizando a importância da vigilância cibernética e atribuindo responsabilidades de supervisão. A estratégia e definição de objetivos integram a gestão de riscos cibernéticos ao plano estratégico, considerando o contexto de negócios e definindo o apetite por risco.

No desempenho, a organização identifica e avalia os riscos que podem impactar a realização da estratégia e objetivos de negócios, incluindo os riscos cibernéticos. A priorização desses riscos é feita com base na gravidade e no apetite de risco cibernético da entidade. A seleção de respostas aos riscos e o monitoramento contínuo permitem desenvolver uma visão do portfólio de riscos assumido pela entidade.

A avaliação e revisão contínuas avaliam como os recursos e práticas de gerenciamento de riscos cibernéticos contribuem para o valor ao longo do tempo, adaptando-se a mudanças substanciais. No âmbito da informação, comunicação e relatório, a organização utiliza um processo contínuo e iterativo para obter e compartilhar informações em toda a

entidade. A administração utiliza informações relevantes para apoiar o gerenciamento de riscos cibernéticos, empregando sistemas de informação para capturar, processar e gerenciar dados. A comunicação abrange riscos, cultura e desempenho, aplicando informações que se aplicam a todos os componentes do ERM (COSO, 2017).

Além disso, o autor também irá destacar que a organização deve identificar os recursos necessários para definir e implementar políticas, processos e procedimentos de gestão de risco, realizar o levantamento e o plano de tratamento de riscos, monitorar os controles implementados e avaliar a eficácia do plano de tratamento de risco.

Essa abordagem estruturada, também guiada pela ISO/IEC 27005, destaca a importância de uma integração sistemática de estratégias de gestão de riscos no dinâmico cenário da Segurança da Informação. Ao aderir a essas fases meticulosamente delineadas, as organizações podem fortalecer suas defesas e navegar no complexo terreno de riscos com vigilância e eficácia.

4.1.1 Identificar

Existe uma variedade de abordagens para a identificação dos riscos, variando de acordo com o segmento, tamanho, a localização geográfica, a complexidade de uma entidade etc. Dependendo desses fatores, a administração pode utilizar múltiplas técnicas. Por exemplo, uma entidade pode reunir dados internos referentes ao histórico de incidentes e perdas, analisando-os para identificar riscos novos, emergentes e em evolução.

Para Pena (2013) o processo deve ter início com o conhecimento dos possíveis riscos ligados as decisões na instituição e a avaliação dos seus possíveis impactos, buscando medir e analisar a exposição dos mesmos, deve-se buscar medidas para diminuir o impacto e a gravidade do risco.

Os riscos emergentes, como o cyber, se manifestam quando o contexto de negócios muda e eles podem alterar o perfil de risco da entidade no futuro. É possível que os riscos emergentes não sejam suficientemente bem compreendidos para serem identificados e avaliados com precisão no início, o que pode justificar maior frequência de novos processos de identificação. Além disso, as organizações devem comunicar a evolução das informações sobre os riscos emergentes.

Conforme COSO (2017), identificar riscos novos, emergentes ou alterações nos riscos existentes possibilita que a organização projete-se no futuro, dispondo de tempo para avaliar a potencial gravidade desses riscos. Isso não apenas permite antecipar respostas aos

riscos, mas também oferece a oportunidade de revisar a estratégia e os objetivos de negócio da entidade, quando necessário.

Quadro 3 – Método de identificação de riscos de acordo com o tipo de risco

Tipo de risco	Computação cognitiva	Rastreamento de dados	Entrevistas	Indicadores-chave	Análise de processo	Seminários
Existente	☑	☑	☑	☑	☑	☑
Novo	☑	☑			☑	☑
Emergente	☑		☑	☑		☑

Fonte: Elaboração do autor baseado em COSO (2017).

A computação cognitiva permite que as organizações analisem grandes volumes de dados de forma eficiente para identificar tendências futuras e informações cruciais sobre riscos emergentes. O uso de dados históricos, seja de bancos de dados terceirizados ou consórcios setoriais, é valioso para prever ocorrências futuras e entender interdependências. Entrevistas, questionários e pesquisas são métodos para obter conhecimento sobre eventos passados, enquanto indicadores-chave ajudam a identificar mudanças nos riscos existentes. A análise de processo, através de diagramas, ajuda a mapear riscos em relação aos objetivos de negócio. Workshops reúnem indivíduos para aproveitar o conhecimento coletivo, desenvolvendo listas de riscos relacionados à estratégia ou objetivos de negócio da entidade (COSO,2017).

4.1.2 Avaliar

Parenty e Doment (2020) destacaram que a prioridade ao avaliar os riscos cibernéticos deve ser a identificação das vulnerabilidades nas atividades essenciais da empresa, ou seja, aquelas relacionadas ao seu "core business", e não apenas nas tecnologias em si.

É necessário que haja comunicação dos impactos, e das medidas para diminuição dos mesmos, bem como da identificação dos riscos para os agentes de decisões, que as decisões sejam tomadas com maior segurança e conhecimento possível (PENA, 2013).

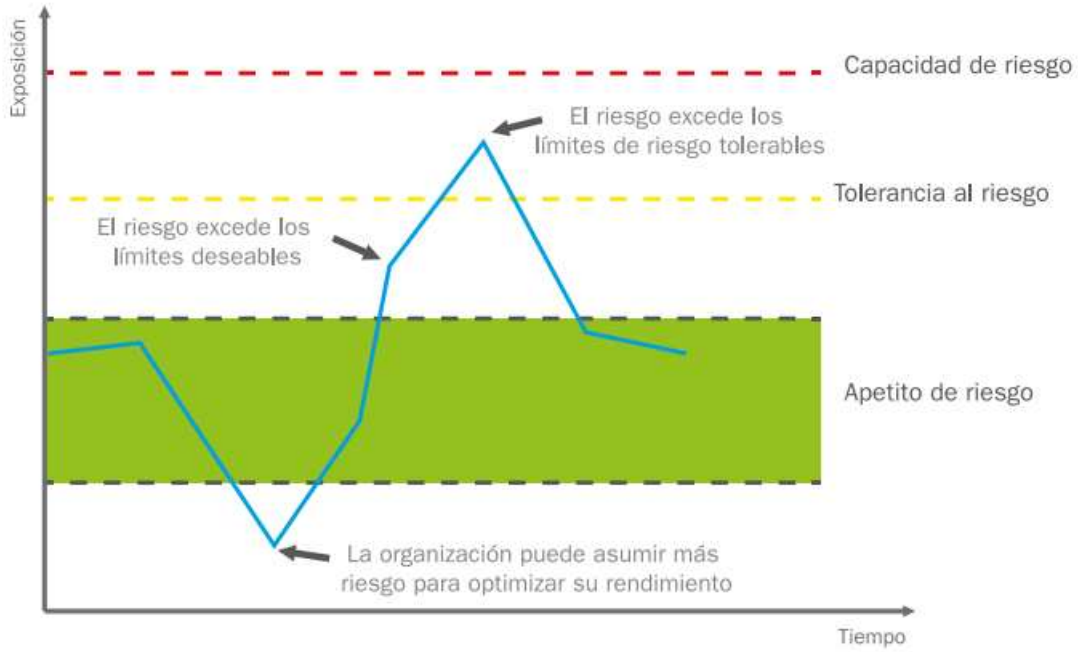
Destaca-se aqui o chamado apetite de risco, que reflete a disposição de uma agência pública em assumir riscos para alcançar seus objetivos e agregar valor às partes interessadas, está diretamente ligado à estratégia organizacional, influenciando a alocação de recursos e a harmonização entre pessoas e processos na agência.

Conforme Brasiliano (2023), destaca-se que a organização deve definir o escopo e as fronteiras do seu sistema de gestão de risco, levando em conta seus objetivos estratégicos,

processos, funções, estrutura interna, política de segurança da informação, expectativas das partes interessadas, ambiente sociocultural e ativos de informação.

Conforme COSO (2009), o termo se refere ao tipo e a quantidade de riscos que em conjunto a organização está preparada para buscar, reter ou assumir correspondem à atitude da agência pública perante o risco e reflete toda a filosofia da organização, influenciando sua cultura e estilo gerencial

Gráfico 6 – Apetite ao risco



Fonte : La Fábrica de Pensamiento - Instituto de Auditores Internos de España, 2013

Dessa forma, os gestores podem alinhar o nível aceitável de variação em relação às metas estabelecidas para o cumprimento de cada objetivo específico, definindo assim a tolerância ao risco, às variações aceitáveis no desempenho, de acordo com o apetite ao risco de toda a organização.

Conforme Brasiliano (2023), sugere-se a responsabilidade da definição do Apetite ao Risco da empresa ser do Conselho de Administração da Empresa, sugerido pela Diretoria Executiva, através do seu Presidente.

Além disso, conforme COSO (2017), a organização deve estabelecer critérios de aceitação de risco, identificando a partir de que nível de risco a aprovação da alta administração é necessária. Esses critérios devem considerar diferentes limites de aceitação e podem incluir requisitos para tratamento adicional no futuro.

Nem todos os tipos de Riscos são passíveis de aceitação. Portanto, em conformidade com (CRO Forum, 2014), a proposta de limites deverá obrigatoriamente ser fundamentada e formalizada pelas seguintes análises:

a) Avaliação do retorno tangível e intangível relacionado ao limite de Risco proposto;

b) Capacidade da Companhia de suportar o impacto do limite de Risco proposto

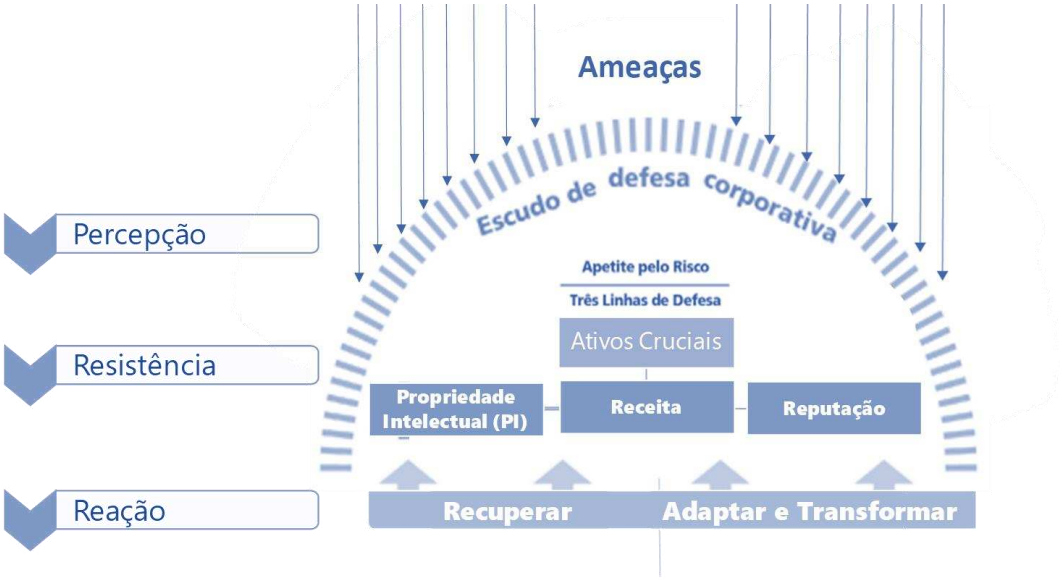
c) Decisão se o Risco deve ou não ser aceito conforme sua tipologia;

d) Viabilidade da implantação das iniciativas de mitigação (custo e esforço) versus efeito na mitigação do Risco e respectivo retorno; e

e) Disponibilidade de recursos (investimento e esforço) para implantação.

Resiliência cibernética (Figura 8) tem uma relação direta com o tópico b). Por isso é preciso investir nessa jornada a fim de ganhar experiência e inteligência, com visão 360º em gestão de risco e priorização.

Figura 12 – Resiliência cibernética



Fonte: EY (2016).

Conforme Brasiliano (2023), os critérios de avaliação de risco devem ser estabelecidos considerando o valor estratégico dos processos, a criticidade dos ativos de informação, a importância operacional e comercial em termos de confidencialidade, integridade e disponibilidade da informação, bem como as expectativas das partes interessadas. A organização também deve definir os critérios de impacto, determinando os níveis de danos ou custos que um evento de segurança da informação pode ter. Isso deve levar em conta a

importância e classificação dos ativos de informação, falhas na segurança de informação, custos, disrupção de planos e prazos, e danos à reputação.

Probabilidade refere-se à probabilidade de um risco se materializar. Avaliar a probabilidade de um risco muitas vezes envolve uma avaliação subjetiva. No entanto, mesmo que seja subjetiva, uma avaliação sistemática pode ser aplicada.

Normalmente, o avaliador faz suposições sobre a eficácia dos controles em vigor, como políticas e procedimentos, e avalia a probabilidade conforme figura 13 de forma qualitativa, como remota ou esperada, de forma quantitativa, com um percentual esperado, ou via frequência, ex. uma vez a cada 12 meses (COSO, 2017).

Figura 13– Expectativa de ocorrência do sinistro

Escala	Probabilidade	Expectativa
Muito Alto	Maior ou igual a 80%	Ocorrencia esperada (certa ou quase certa)
Alto	60% a 79%	Grandes chances de ocorrer
Médio	30% A 59%	Pode ocorrer em alguma circunstância
Baixo	10% a 29%	Pode ocorrer em alguma circunstância excepcional
Muito Baixo	Menor do que 10%	Chance remota de ocorrer

Fonte: Elaboração do autor a partir de COSO (2017).

O segundo aspecto relacionado à gravidade do risco diz respeito ao impacto. O impacto é o resultado ou efeito do risco em termos da estratégia e dos objetivos de negócio da organização (COSO,2020). No contexto do risco cyber, imediatamente se pensa em resgates ou multas civis, bem como nas possíveis consequências financeiras diretas da invasão. Outro fator significativo pode ser o impacto na reputação decorrente de questões de dados e ética. Essas e outras consequências (como sanções, suspensões e impedimentos) podem ter um impacto financeiro indireto e mensurável, assim como afetar o moral e outros fatores de difícil avaliação, conforme destaque em figura 15.

Figura 14 – Expectativa de severidade do sinistro

Escala	Financeira	Continuidade	Reputação e imagem da marca	Litigações	Conformidade
Muito Alto	Redução do Lucro Líquido maior do que 10%	Paralização integral por mais de 3 meses	Perda de confiança da marca pelo público, stakeholders e pela mídia em escala internacional	Alto recorrente de litigações causado por falhas sistêmicas ou erro humano	Envolvimento do C-Level ou acima em grandes escândalos, prisões, paralisações, multas e/ou impedimento de operações Perda de contratos
Alto	Redução do Lucro Líquido entre 7% e 8%	Paralização parcial por mais de 3 meses	Perda de confiança da marca pelo público, uma parcela dos stakeholders e pela mídia em escala internacional	Considerável fluxo de litigações ou Autos causado por falhas sistêmicas ou erro humano	Envolvimento do V-Level ou acima em escândalos, prisões, paralisações, multas e/ou impedimento de operações Bloqueio ou paralização de contratos
Médio	Redução do Lucro Líquido entre 4% e 5%	Paralizações severas em um objeto da companhia mensal	Perda de confiança da marca pelo público, uma parcela dos stakeholders e pela mídia em escala nacional	o fluxo de litigações ou Autos causado por falhas sistêmicas ou erro humano	Autos de infração, processos judiciais, notificações com necessidade de provisionamento / dispêndio de caixa para órgãos competentes
Baixo	Redução do Lucro Líquido entre 2% e 3%	Interrupções de baixa escala em um objeto vital da companhia mensal	Perda de confiança da marca pelo público, uma pequena parcela dos stakeholders e pela mídia em escala nacional	Baixo fluxo de litigações ou Autos causado por falhas sistêmicas ou erro humano	Processos judiciais ou notificações com necessidade de provisionamento / dispêndio de caixa para órgãos competentes
Muito Baixo	Redução do Lucro Líquido abaixo de 1%	Interrupções de baixa escala em um objeto da companhia mensal	Baixa negatividade ou somente em escala interna, sem comprometimento da confiança da marca	Fluxo muito baixo/ inconsiderável de litigações ou Autos causado por falhas sistêmicas ou erro humano	Sem Autos, processos ou notificações avaliadas

Fonte: Elaboração do autor a partir de (COSO, 2017).

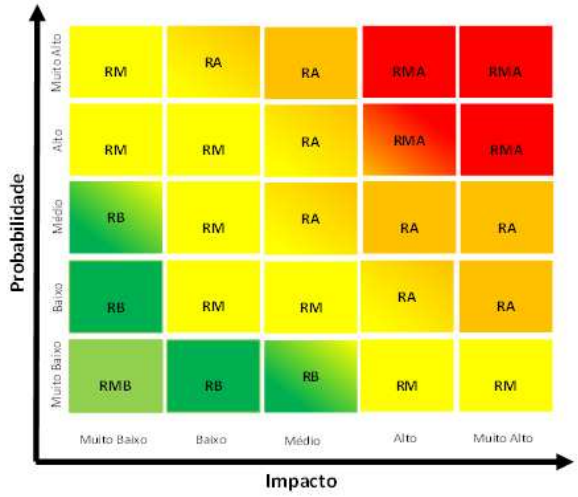
Também explica COSO (2020) que avaliações dos riscos em relação à probabilidade e ao impacto permitem a priorização em toda a organização. Uma abordagem utilizada para capturar e resumir a avaliação de gravidade envolve a criação de uma matriz de inventário de riscos.

A matriz de risco (Figura 13), também conhecida como matriz de probabilidade e impacto (SCHWALBE, 2005), é uma ferramenta simples utilizada para compreender e contribuir para a classificação dos riscos em uma organização com base no valor de cada risco.

Probabilidade refere-se à probabilidade de um risco se materializar (COSO,2020). Esse valor é calculado de acordo com a seguinte relação:

Valor = probabilidade (risco de) X (o grau de severidade do impacto do risco) (1)

Figura 15 – Matriz de risco



Fonte:Elaboração do autor com base em (COSO, 2017).

Conforme anteriormente destacado, a Gestão do Risco no âmbito da Segurança da Informação, definido em ISO/IEC 27005, denota os seguintes estágios. Estabelecimento do Contexto (Fase 1), Avaliação de Riscos abrangente (Fase 2). Essa fase envolve a identificação (2.1), análise (2.2) e avaliação (2.3) meticulosa dos riscos potenciais.

4.1.3 Priorizar

Além da gravidade e apetite de risco, algumas organizações consideram outros fatores na priorização de riscos. Ajustes podem ser feitos nos riscos com base na velocidade, persistência e recuperação. Velocidade é a rapidez com que um risco afeta a organização, como uma violação grave de segurança alimentar que exigiria o fechamento imediato de uma planta de processamento de alimentos. Persistência refere-se a quanto tempo o risco afeta a organização, como a cobertura midiática de violações criminais que dura quatro ou cinco anos.

Figura 16 - Priorização de Avaliação de Risco

Fonte: (Delloite,2019)

Recuperação se refere ao tempo necessário para corrigir o problema (ou seja, o tempo necessário para gerenciar o risco para níveis toleráveis), como o tempo necessário para implementar critérios e processos aprimorados de diligência devida do fornecedor para reduzir o risco de transações com empresas de fachada (BRASILIANO, 2018).

Por exemplo, no exemplo fornecido na Figura 18, os riscos nas áreas verdes seriam periodicamente reavaliados, mas nenhuma ação de resposta específica ou ação de monitoramento extensivo seria tomada. Nas áreas amarelas, os proprietários de riscos seriam obrigados a desenvolver um plano de mitigação de riscos para reduzi-los ou eliminá-los sem a necessidade de recursos significativos adicionais.

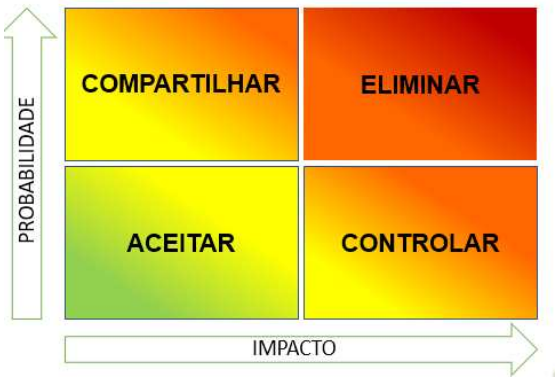
Quanto aos riscos nas áreas vermelhas, comitês de conformidade seriam designados para colaborar com os proprietários de riscos na elaboração de planos de resposta abrangentes. Esses planos definiriam claramente a propriedade do risco, atribuiriam responsabilidades para as respostas aos riscos e delineariam estratégias de monitoramento e auditoria para os esforços de remediação.

As fases subsequentes abrangem o tratamento estratégico dos riscos (Fase 3) e a necessária aceitação dos riscos identificados (Fase 4). A narrativa se desenrola ainda mais com as etapas fundamentais de comunicação e consulta (Fase 5), destacando a importância de práticas transparentes e colaborativas de gestão de riscos. A jornada conclui com as fases críticas de monitoramento e revisão de riscos (Fase 6), garantindo uma abordagem contínua e adaptativa à mitigação de riscos.

4.1.4 Tratar

O plano de tratamento dos riscos é executado tendo por base a avaliação realizada pela organização sobre riscos identificados, no âmbito do processo de análise. Existem quatro opções disponíveis para tratamento do risco: Evitar, Aceitar, Mitigar e Transferir.

Figura 17 – Contexto organizacional



Fonte: ISO/IEC 27005

As respostas ao risco podem vir na forma de aceitação do risco, onde a organização pode tolerar os resultados, transferindo o risco quando outros podem gerenciar os riscos de forma mais eficaz ou eficiente, ou agindo para mitigar ou reduzir tais riscos. Como a avaliação de risco direciona essas decisões, é importante considerar que tais respostas são apropriadas para o apetite de risco da organização. Quando decisões são tomadas para agir sobre tais riscos, uma organização normalmente implementa atividades de controle. As atividades de controle são as ações realizadas por indivíduos dentro da organização que ajudam a garantir que as diretrizes da administração sejam seguidas para mitigar os riscos para o alcance dos objetivos. Essas atividades de controle devem ser documentadas em políticas para ajudar a garantir que as atividades de controle sejam realizadas de forma consistente em toda a organização (Delloite, 2019).

A gestão de riscos em uma organização na forma de aceitação do risco deve ocorrer de acordo com a gravidade do risco identificado. É sugerido para riscos muito altos, o Conselho de Administração é responsável, enquanto a Diretoria Executiva lida com riscos altos. O CEO cuida de riscos médios, e os Diretores de Área assumem a responsabilidade por riscos baixos e muito baixos. Essa abordagem hierárquica visa garantir uma gestão estratégica e eficaz de riscos em todos os níveis da organização.

No âmbito do tratamento do risco, COSO (2020) denota que a organização deve definir qual a opção de tratamento considerada adequada, deve proceder à identificação dos controles que podem ser implementados para mitigar, evitar ou transferir o risco, bem como definir um plano para seu tratamento. Na escolha das opções de tratamento do risco, deve-se tomar em consideração:

a) Como o risco é percebido pelas partes interessadas afetadas;
b) A forma mais adequada para comunicar-se com as partes interessadas.

Figura 18 – Framework de controles internos

Fonte: (COSO, 2011).

Conforme COSO (2011), as atividades de controle compreendem ações que visam assegurar a adequada execução e prontidão das respostas aos riscos avaliados, bem como de outras diretrizes de gestão, como o estabelecimento de padrões de conduta no Ambiente de Controle.

Como exemplo de controle, consideremos uma empresa que estabelece o objetivo gerencial de enfrentar riscos de engenharia social para o próximo resultado. A administração identifica um risco relacionado à falta de conhecimento do pessoal sobre ameaças de engenharia social e tentativas de manipulação.

Para combater a engenharia social, uma entidade pode seguir práticas como promover a conscientização e fornecer treinamento regular aos funcionários, implementar políticas de segurança da informação claras, estabelecer controles de acesso rigorosos, verificar a identidade em solicitações de informações sensíveis, utilizar comunicação segura, realizar simulações de ataques, incentivar relatos de incidentes, e manter sistemas atualizados. Adaptar essas medidas às necessidades específicas da organização e garantir uma abordagem contínua e dinâmica são cruciais para lidar com as ameaças em constante evolução da engenharia social.

Assim que o plano de tratamento do risco for definido, os riscos residuais devem ser determinados. Este processo envolve uma atualização ou uma nova iteração com a fase de avaliação, tendo por base os efeitos esperados pelo tratamento do risco proposto.

Ainda conforme COSO, a avaliação de riscos é aplicada primeiramente aos riscos inerentes, visando identificar quais são os riscos inerentes críticos, pois são estes que o gestor deve monitorar e tratar. Para isso, é necessária a implantação de sistemas e controles, e a tendência é reduzir a criticidade dos riscos inerentes a níveis aceitáveis, dentro do apetite de risco que a empresa impôs.

4.1.4.1 Riscos inerentes e residuais

Destacam algumas das melhores práticas do mercado, juntamente com os modelos internacionais de gestão de riscos destacados anteriormente, a sugestão de forma enfática que a área de gestão de riscos trabalhe com um processo estruturado, independentemente da disciplina, em que efetue de duas maneiras a avaliação do risco: a avaliação de riscos inerentes e a avaliação de riscos residuais (ISO, 2013, 2018; COSO, 2017; CIS, 2018).

Conforme COSO (2007), o risco inerente é definido como o nível de risco que uma entidade enfrentaria se não implementasse medidas de resposta a riscos. Em outras palavras, é o risco associado a uma atividade ou processo antes de considerar os efeitos de controles internos específicos ou ações de gestão de riscos.Assim, o risco inerente é a avaliação do risco

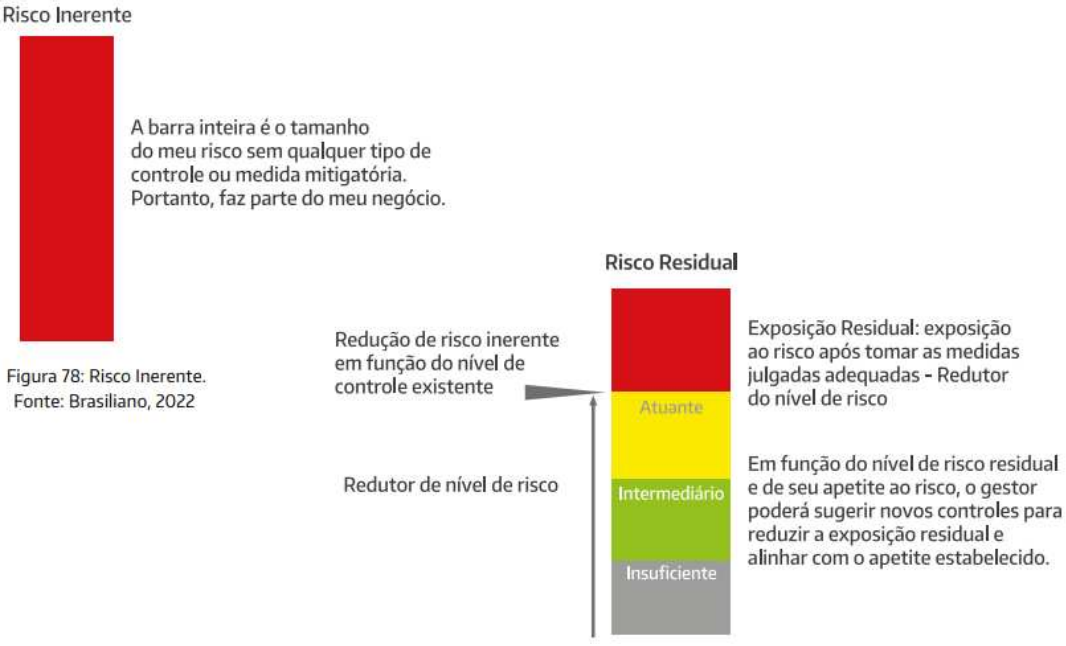
sem levar em conta as estratégias de mitigação ou os controles implementados. Isso fornece uma base para entender a exposição inicial a riscos antes de aplicar quaisquer medidas para reduzi-los ou gerenciá-los.

Conforme Brasiliano (2018), avaliar o risco inerente significa avaliar a probabilidade e impacto da ocorrência de um risco, desconsiderando a estrutura existente de sistemas de TI, no caso cibernético, tanto preventivo como contingencial. Ou seja, avaliamos os riscos sem levar em consideração seus controles e sistemas. Temos que enxergar os riscos sem qualquer tipo de controle ou sistema que possa reduzi-los.

Risco residual é o risco que permanece após as respostas da gestão às ameaças e contramedidas de risco terem sido aplicadas. Haverá virtualmente sempre algum nível de risco residual (COSO, 2007).

Na segunda avaliação de riscos, o processo de gestão de riscos deve prever a avaliação dos sistemas e dos controles existentes e implantados, para determinar se a estrutura que a empresa possui é eficaz o suficiente para manter seus riscos críticos dentro do nível requerido. Se estiver dentro do apetite ao risco, o gestor irá apenas monitorar. Já se estiver fora do apetite ao risco, terá que implantar, desenhar e/ou implantar novos sistemas e/ou controles até que o residual do risco esteja dentro do respectivo apetite (COSO, 2004).

Figura 19– Risco residual



Fonte: Brasiliano (2018).

Caso o risco residual ainda não satisfaça os critérios de aceitação do risco da organização, poderá ser necessária uma análise adicional do tratamento do risco antes de se proceder à sua aceitação.

Quadro 4 – Tratamento do risco residual

Risco Residual	Status
Muito Alto	Sem possibilidades de mitigar ou tratar o risco, ações e controles não são suficientes Não existem controles ou ações para tratar risco Ações não foram efetivas
Alto	Com possibilidades de mitigar ou tratar o risco, mas parcialmente implementadas Ações e controles não são suficientes. Ações não foram efetivas. Existem controles ou ações para tratar risco, mas necessitam de melhoria
Médio	Com possibilidades de mitigar ou tratar o risco implementadas em alguns casos Ações e controles não são suficientes. Ações nem sempre foram efetivas. Existem controles ou ações para tratar risco
Baixo	Ações mitigam o risco e/ou reduzem constantemente a probabilidade ou impacto Controles maduros. Ações foram efetivas de forma consistente Existem controles ou ações para tratar risco
Muito Baixo	Ações mitigam o risco e/ou reduzem constantemente a probabilidade para remota ou impacto para muito baixo Controles maduros.

Fonte: Elaboração do autor a partir de (COSO,2013)

4.1.5 Monitoramento

A organização deve desenvolver planos de comunicação de apoio aos processos de gestão do risco, comuns e de emergência. Desta forma, a atividade de comunicação deve ser realizada de forma contínua (COSO, 2020).

Conforme destacado pelo IBGC (2007, p. 16), “é importante ressaltar que sempre existirão riscos desconhecidos pela organização”. Disso conclui-se que a atividade de identificação de riscos requer monitoramento contínuo por parte da equipe responsável, pois com o passar do tempo, e o aprimoramento do processo de gestão de riscos, é comum que o número de riscos desconhecidos diminua, desde que mantidas constantes as demais conjunturas do mercado.

Conforme observado no Quadro 5, presente processo de verificação da execução do plano de ação desempenha um papel crucial, conforme princípio de monitoramento do

COSO, visando não apenas a efetiva implementação das medidas propostas, mas também a avaliação contínua dos resultados e a pronta adoção de ações corretivas quando necessário, enfatizando a importância da vigilância e validação na garantia de uma gestão eficiente e alinhada aos padrões de governança.

Quadro 5 – Monitoramento do plano de ação.

<table>
<tr><th>PLANO DE AÇÃO</th><th>PRAZO DE IMPLANTAÇÃO</th><th>RESULTADOS</th><th>DIFICULDADES</th><th>AÇÕES CORRETIVAS</th></tr>
<tr><td rowspan="5">1. Tipo do plano de ação - nome</td><td>Implantado</td><td>Eficaz</td><td rowspan="5">Descrever as dificuldades encontradas, como recursos humanos, tecnológicos e orçamentários</td><td rowspan="5">Quais ações são necessárias para que o Plano de Ação seja eficaz e anule as dificuldades</td></tr>
<tr><td>Fora do prazo - não implantado</td><td>Ineficaz</td></tr>
<tr><td>Dentro do prazo - em implantação</td><td rowspan="3">Cumpriu com seus objetivos?</td></tr>
<tr><td>Atrasado - em implantação</td></tr>
<tr><td>Paralisado</td></tr>
</table>

Fonte: (Brasiliano, 2023)

No cenário em constante expansão da globalização, as complexidades dos riscos empresariais tornam-se mais intricadas e exigentes, apresentando um desafio considerável para a mitigação eficaz. Essa complexidade amplia os níveis de vulnerabilidade aos quais as organizações precisam se adaptar. Em resposta, as empresas se veem pressionadas a explorar não só o monitoramento eficiente dos riscos, mas também o aprimoramento das estratégias gerais de gestão de riscos e a integridade estrutural dos controles corporativos dentro de seus processos operacionais (BRASILIANO, 2020).

Entretanto, caso o equilíbrio não seja mantido, tem-se o exemplo mencionado por Damodaran (2009, p. 308), ao afirmar que “não causa surpresa que os riscos que enfrentamos tornem-se mais numerosos e complexos à medida que expandimos nossas operações em diferentes produtos e mercados”. Logo, caso a empresa opte por ingressar em um novo setor de atuação, decida lançar um produto inovador no mercado, ou até mesmo ocorram alterações na legislação em vigor, consequentemente se tornará vulnerável a riscos desconhecidos.

Conforme Pereira (2014), “Isso permite que a organização agrupe os riscos com base em como e quando serão abordados, bem como o nível de atenção que cada um receberá. Embora possa ser argumentado que idealmente a organização poderia lidar com todos os seus riscos de conformidade, na prática, é necessária uma atenção mais direta e imediata para os riscos mais graves. Como isso é feito dependerá do apetite e tolerâncias de risco da organização e dos recursos disponíveis.”

Realizados os esforços para a criação dos registros de informações acerca dos riscos identificados, analisados, avaliados e tratados, o monitoramento destes pode ser efetuado de duas formas, como recomenda o COSO (2007, p. 83), “mediante atividades contínuas ou de avaliações independentes”

Mesmo com a importância do gerenciamento de riscos, muitas organizações ainda falham por diversos motivos (BORODZICZ, 2005; JEYNES, 2002). Estes incluem a falta de experiência na área de gestão de risco, escassez de sistemas de monitoramento e controle, falhas inesperadas em sistemas de comunicação, falha dos funcionários em reconhecer a importância da gestão de risco, ignorar o desenvolvimento histórico ou gestão de risco e otimismo excessivo. As causas do fracasso estão relacionadas a fatores cognitivos, como falta de experiência ou falta de consciência, bem como falhas em fatores relacionados aos sistemas de comunicação e controle.

Consequentemente, as estratégias atuais para lidar com os riscos cibernéticos concentram-se principalmente na remediação após o fato (LECHLER *et al.*, 2017).

Conforme pontuado por Igarapé (2021) sobre segurança cibernética, os principais desafios para mitigação de riscos cibernéticos são:

a) A ausência de uma linguagem compartilhada para se referir às questões de segurança cibernética/digital na sociedade;

b) A associação de segurança cibernética com assuntos, responsabilidades e competências de instituições militares;

c) Desconhecimento de riscos específicos e compartilhados entre setores;

d) Ausência de mecanismos para o compartilhamento de informações sobre riscos/ameaças e conhecimento em segurança entre setores;

e) Falta de alinhamento normativo, estratégico e operacional para responder a incidentes; e

f) Existência de diferentes níveis de maturidade da sociedade em segurança cibernética.

Banks e Dunn (2003) sugeriram que o mecanismo de tomada de ação inclui uma série de ações que a organização deve aplicar para minimizar falhas na gestão de riscos. A sugestão foi a seguinte:

> Definindo os fatores de risco em categorias claramente distinguíveis, como liquidez, mercado e credores. Escolha um cenário para analisar cada risco. Calcule o valor esperado de lucros e perdas para cada cenário de risco. Compilando os resultados da análise por seções (organização, departamento, etc.) Compare os resultados de cada risco com o guia de gerenciamento de riscos da organização. Diariamente, assegure-se de que as perdas para cada fator de risco não ultrapassem o máximo. Revise

> regularmente para garantir que os limites de risco estejam em conformidade com as diretrizes da organização. Usando os indicadores de Banks e Dunn, é importante que as organizações criem um guia de gerenciamento de riscos para ajudar a treinar os funcionários sobre a importância do gerenciamento de riscos e como implementá-lo. O guia de gerenciamento de risco organizacional deve incluir vários elementos: O efeito do risco em dificultar os objetivos da organização. Formas de determinar quais riscos devem ser o foco para evitá-los ou minimizar sua probabilidade e reduzir seu impacto negativo na organização. Garante que os riscos do foco da organização sejam importantes para os atores externos para garantir que os atores terceirizados entendam como esses riscos podem afetar o desempenho da organização (Banks; Dunn, 2003).

4.2 Seguro cibernético – Transferência de riscos

Antecipar riscos e amparar prejuízos econômicos incertos é a principal função do seguro, vindo a desenvolver planos de sobrevivência às mesmas, ações coincidem com o conceito de Gerenciamento de Riscos (DORFMAN, 1998).

Tem-se, além do seguro cibernético, uma gama de demais modalidades ofertadas em mercado, dentre os mais populares sendo o seguro automotivo e o seguro de vida, quanto também os mais específicos como o seguro de riscos de petróleo ou de Responsabilidade Civil Geral.

> “O seguro marítimo, o mais antigo entre os ramos modernos do seguro, tem suas raízes na Itália durante o século XIII. A partir dali, difundiu-se pelos demais países do continente e, posteriormente, alcançou a Inglaterra por meio dos mercadores da Lombardia. Estes últimos exerceram considerável influência sobre o comércio e as finanças britânicas ao longo do século XV. Inicialmente, o seguro marítimo não era formalizado por companhias de seguro, mas sim por indivíduos. Um armador ou comerciante interessado em assegurar seu navio ou carga preparava e distribuía um documento com informações detalhadas sobre a embarcação, sua carga, destino e demais dados pertinentes. Aqueles que aceitavam compartilhar o risco colocavam seus nomes abaixo da descrição do risco e dos termos do acordo. Essa prática de "inscrever-se sob" o acordo deu origem ao termo "subscritor", que mantém sua definição como aquele que decide sobre a aceitação ou recusa dos riscos” (VAUGHAN; VAUGHAN, 2008, tradução livre).

Dorfman (1998) define seguro como sendo um contrato, com regras específicas e validade legal, que compromete o segurador a absorver parte dos custos de prejuízo no caso de alguma ocorrência possível e incerta que venha a confirmar o risco, mediante recolhimento de um pagamento estipulado pelo segurador chamado prêmio, estipulado para cada segurado conforme os riscos cobertos, caso o evento aleatório previsto no contrato, ou seja, o sinistro, venha a se concretizar, seguradora passará a indenizar o segurado nas despesas para o segurado e seus beneficiários, conforme delimitado no constante da apólice do seguro acordada.

Apesar do início das atividades de seguros no Brasil remontar ao século XVI, o estabelecimento do Sistema Nacional de Seguros Privados e a regulamentação abrangente de seguros e resseguros, substituindo o Departamento Nacional de Seguros Privados e Capitalização (DNSPC), foi promulgado em 1996 por meio do Decreto-Lei 73/66 (BRASIL,

1966). Este marco instituiu o Conselho Nacional de Seguros Privados (CNSP) como órgão normativo, sob a supervisão da Superintendência de Seguros Privados (SUSEP). Abaixo da SUSEP estão as Corretoras de Seguros e as Empresas de Seguros, Previdência Complementar Aberta e Capitalização (FENASEG, 2001).

O Decreto-Lei 73 e a SUSEP promoveram a segregação de ramos e grupos de seguros, com as operações de seguros englobando uma ampla gama de categorias, como seguros de coisas, pessoas, bens, responsabilidades, obrigações, direitos e garantias. Além disso, a diversidade de classificações abrange até 95 ramos e 16 grupos, conforme estabelecido pelo Circular 445/12, devidamente registrados e categorizados pela Superintendência de Seguros Privados (SUSEP). Um exemplo notável é o seguro de responsabilidade civil, que possui 12 ramos distintos, incluindo o seguro compreensivo de Riscos Cibernéticos, cada vez mais crescente, oferece proteção ao segurado contra danos diretos causados por ataques cibernéticos que gerem perdas materiais, imateriais e de conteúdo informacional ou mesmo ressarcimento por reclamações de terceiros por violação da privacidade e de direitos de propriedade intelectual ,ou uso indevido de informações.

Indicando uma tendência ascendente no interesse e investimento nesse produto, a Allianz Global Corporate & Specialty projeta que o mercado global de seguros cyber atinja uma cifra superior a 20 bilhões de dólares até o ano de 2025. Essa estimativa reflete o contínuo crescimento e expansão do setor (AGCS , 2015).

Assim, de forma geral, as apólices de seguro têm cinco itens principais a serem analisados na hora de sua contratação:

a) Coberturas referem-se aos riscos assumidos pela seguradora e podem ser classificadas como "básicas" - cobrindo automaticamente os riscos fundamentais do ramo de seguros em questão - ou "adicionais" - opcionalmente adicionadas à apólice mediante negociação e cobrança de prêmio adicional;

b) Limites representam os valores máximos em termos monetários que a seguradora irá desembolsar em caso de sinistro. As apólices possuem um Limite Máximo de Garantia (LMG) e as coberturas individuais podem ter limites específicos, conhecidos como Limite Máximo de Indenização por Cobertura (LMI);

c) Franquias são valores monetários fixos que, em caso de sinistro, representam a parte do prejuízo apurado que poderá não ser coberta pela seguradora;

d) Exclusões referem-se a coberturas ou eventos que não estão incluídos no escopo da apólice, sendo previamente definidos pela seguradora e, portanto, não sujeitos a reclamação pelo segurado em caso de sinistro;

e) Prêmios são os valores monetários pagos pelos segurados ou pelas partes interessadas (como estipulantes ou proponentes) à seguradora para que ela assuma os riscos aos quais os segurados estão expostos.

No Brasil, o seguro voltado ao risco cibernético vem ganhando forma desde 2020, mas foi a partir da Circular Susep nº 637, de 27 de julho de 2021, que a matéria ganhou contornos regulatórios. Tal circular distinguiu o seguro de responsabilidade compreendendo riscos cibernéticos como ramo específico do grupo responsabilidades, favorecendo a segregação destes riscos pelas seguradoras, de modo que estas uniformizem suas carteiras segundo critérios estatísticos mais precisos e, assim, afastem a incerteza latente do *silent cyber risk*, assim, o risco cibernético é coberto e precificado, ou está excluído.

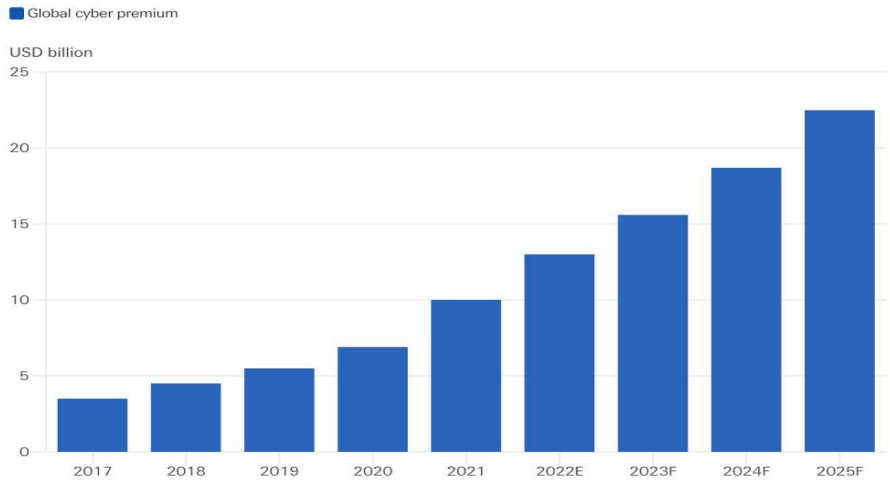
Adicionalmente, é possível observar uma concentração de influência em alguns países, incluindo o Brasil, no que se refere à cibersegurança, como apontado por Kuerbis *et al*. (2017). Segundo os autores, 70% das empresas especializadas nesse setor estão concentradas em apenas três países, Os restantes 30% das empresas estão espalhados por diversos outros países. Além disso, de acordo com a mesma fonte, países como China, Brasil e Rússia juntos contribuem com pouco mais de 2,5% da participação nesse mercado. Já os Estados Unidos lideram estatística, representando sozinho 60% do mercado, seguido pelo Reino Unido com 7% e o Canadá com 3%.

4.2.1 Características do ramo de seguro cibernético

Conforme dados globais do instituto Swiss Reinsurance Company Ltd, observamos no gráfico 7 constante tendência de crescimento em prêmios pagos e projetados de acordo com percepções de mercado e adoção de políticas cyber. (Swiss Re, 2022).

Ainda em dados globais, corroborando com a tendência ascendente no interesse e investimento no produto de segurança cyber, a Allianz Global Corporate & Specialty projeta que o mercado global de seguros cyber atinja uma cifra superior a 20 bilhões de dólares até o ano de 2025. Essa estimativa reflete o contínuo crescimento e expansão do setor (AGCS , 2015).

Gráfico 7 – Premios pagos e estimados para seguro cyber global



Fonte: (Swiss Re , 2022).

Utilizando a base de dados nacional disponível no site da SUSEP, é possível perceber em tabela 2 e 3 os valores de prêmios e sinistros do seguro compreensivo de riscos cibernéticos para o período de 2019 a 2022. Observa-se notável variação entre anos anteriores e o período de 2023, sendo o ano analisado separadamente para melhor calibre da análise.

Tabela 1 – Prêmios ganhos e sinistros ocorridos, seguro cibernético, 2019 -2023

Ano	Prêmio Ganho [1]	Sinistro Ocorrido [3]
2019	R$ 11.631.824,00	R$ 811.476,00
2020	R$ 30.750.663,00	R$ 31.617.316,00
2021	R$ 77.084.205,00	R$ 74.513.761,00
2022	R$ 145.174.466,00	R$ 63.941.061,00
2023	R$ 153.731.235,00	R$ 11.651.209,00

Fonte: SUSEP (2023).

Tabela 2 – Prêmios ganhos e sinistros ocorridos, seguro cibernético, 2023

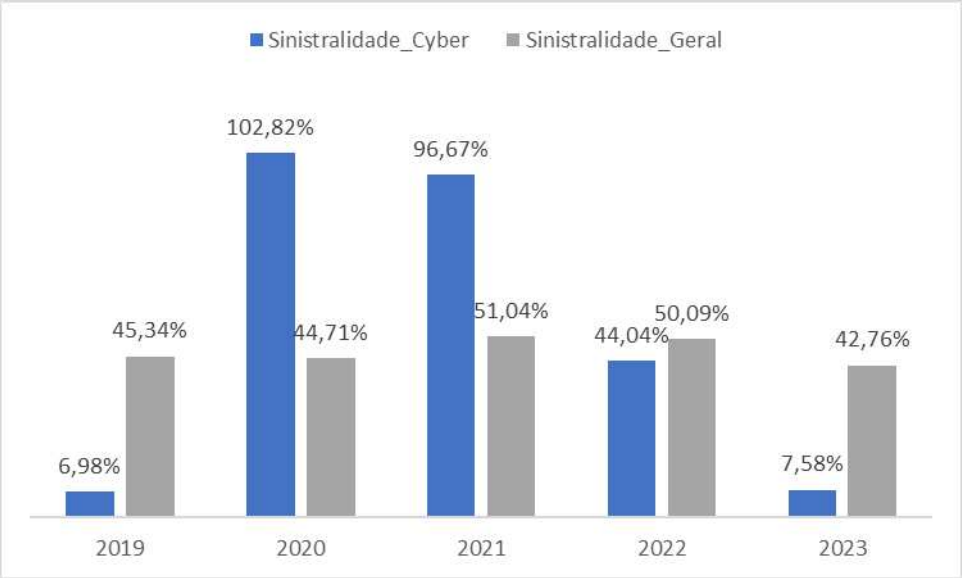
Mês	Prêmio Ganho [1]	Sinistro Ocorrido [3]
janeiro	R$ 15.438.156,00	R$ 3.896.377,00
fevereiro	R$ 14.243.006,00	R$ 3.779.796,00
março	R$ 13.038.955,00	-R$ 16.233.038,00
abril	R$ 16.725.549,00	R$ 4.450.190,00
maio	R$ 15.485.128,00	R$ 6.518.216,00
junho	R$ 16.169.515,00	-R$ 8.062.562,00
julho	R$ 16.341.958,00	R$ 4.238.483,00
agosto	R$ 15.773.303,00	R$ 1.356.464,00
setembro	R$ 15.397.498,00	R$ 2.964.695,00
outubro	R$ 15.118.167,00	R$ 8.742.588,00

Fonte: SUSEP (2023).

A partir desses dados, pode-se verificar o grande crescimento dos prêmios e sinistros no período analisado. Descontando-se a inflação, INPC (Índice Nacional de Preço ao Consumidor) divulgado mensalmente pelo IBGE, os prêmios ganhos cresceram 542% no período de 2019 a 2021; enquanto para todos os ramos de seguros, nesse mesmo período, os prêmios ganhos tiveram queda de 5,64%.

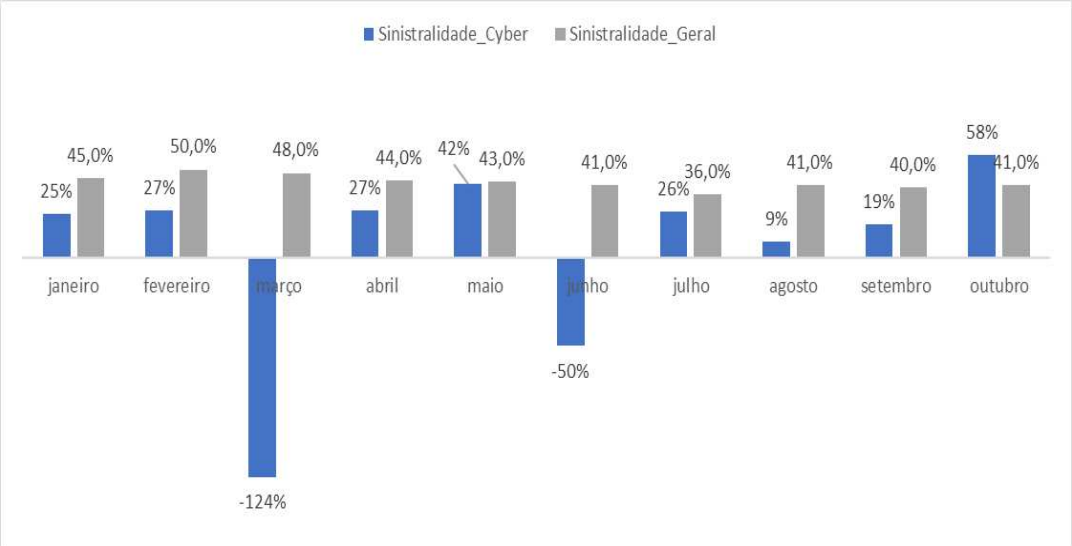
No Gráfico 8 é apresentada a sinistralidade (Sinistro ocorrido/prêmio ganho) do período de 2019 a 2022 do seguro de riscos cibernéticos, que representa quanto do prêmio ganho foi destinado para o pagamento de sinistros. É possível notar crescimento da sinistralidade no período pós 2019, e posterior redução da sinistralidade em 2022, com seus meses de variação (Gráfico 9), esse indicador está abaixo da estatística para todo o mercado de seguros listados em base de dados Susep. Destaca-se que essa sinistralidade apresentada pelo seguro cibernético em 2022, abaixo de 45%, irá permitir o investimento das seguradoras na ampliação das coberturas e do público-alvo.

Gráfico 8 – Sinistralidade cibernética em relação à sinistralidade geral, 2019 - 2023



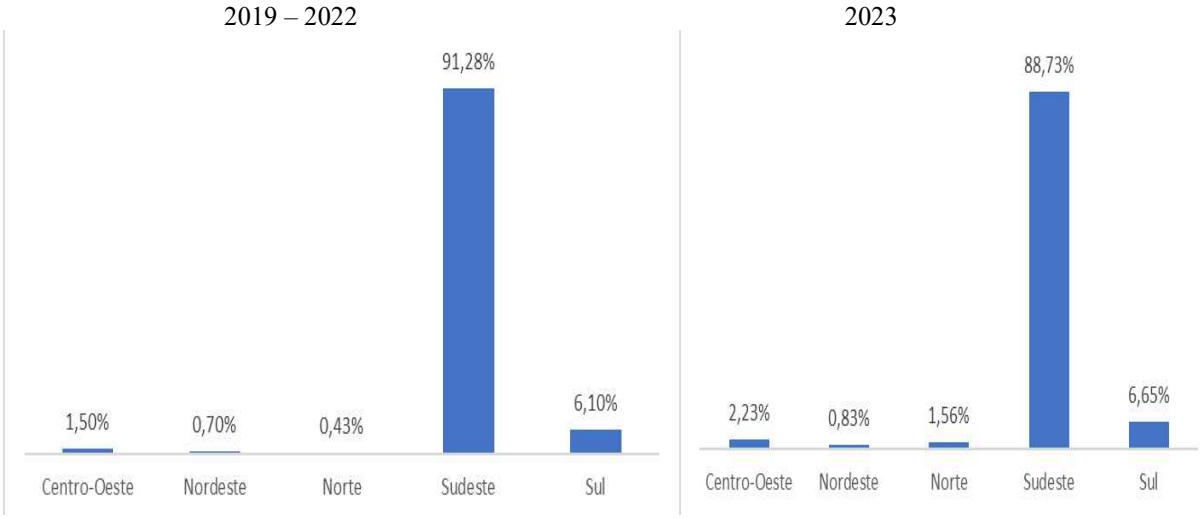
Fonte: SUSEP (2023).

Gráfico 9 – Sinistralidade cibernética em relação à sinistralidade geral, 2023



Fonte: elaboração do autor a partir de SUSEP (2023).

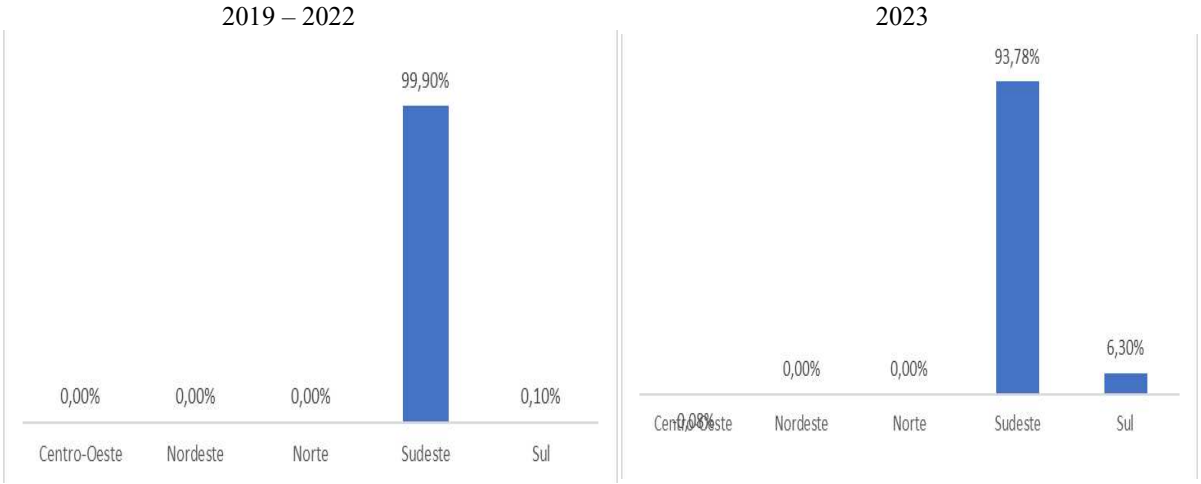
Gráfico 10 – Prêmios ganhos, seguro cibernético, por região



Fonte: SUSEP (2023).

No Gráfico 10 visualiza-se para o seguro cibernético, a participação dos prêmios de cada região no período analisado. Verifica-se que a região sudeste detém a maior participação nos prêmios ganhos, 89,79% apresentando queda de aproximadamente 3% em 2022, já que nesta região, com alto desenvolvimento econômico, estão os principais centros de negócios e principais pontes áreas do país. A região sul concentra 7,97% dos prêmios ganhos, apresentando aumento em relação a 2021, enquanto as demais regiões apresentam apenas 2% desse indicador.

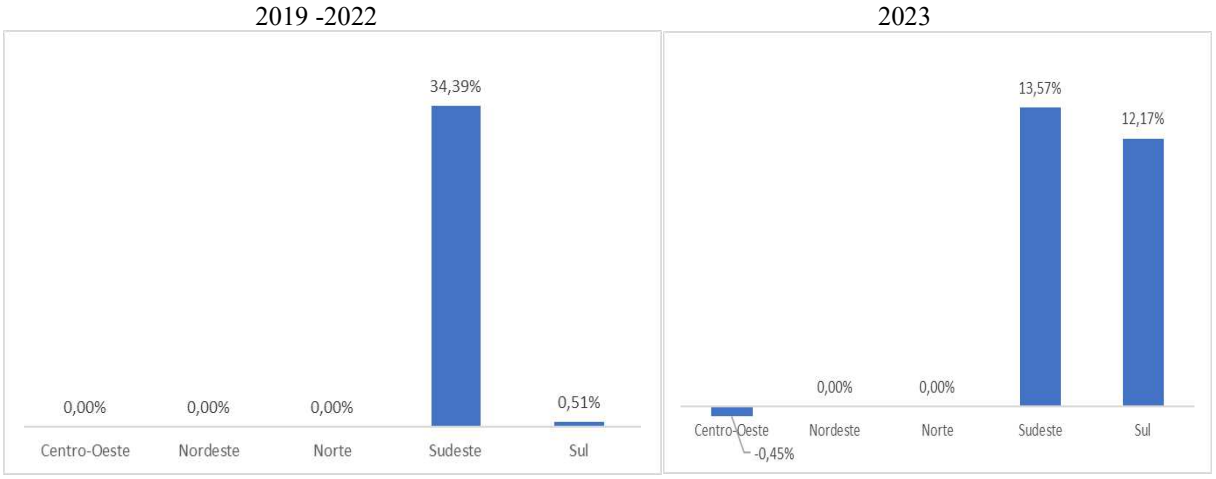
Gráfico 11 – Sinistros ocorridos, seguro cibernético, por região



Fonte: SUSEP (2023).

O Gráfico 11 apresenta a participação por região dos sinistros ocorridos no período de 2019 a 2021. É perceptível que a proporção é basicamente a mesma da apresentada pelos prêmios, com a região sudeste, possuidora da maior participação dos prêmios. O Gráfico 12 irá apresentar a sinistralidade, com a região sudeste apresentando maior percentual, juntamente com redução da sinistralidade conforme período. Observa-se também o aumento da expressividade da região sul, com sinistralidade semelhante à sudeste.

Gráfico 12 – Sinistralidade, seguro cibernético, por região



Fonte: SUSEP (2023).

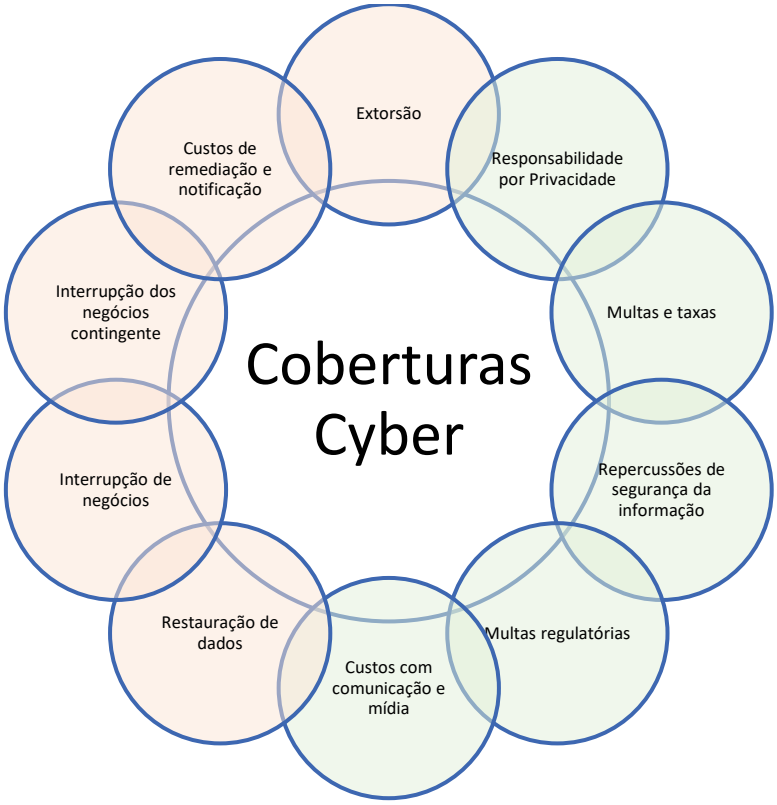
Por fim, devido às incertezas e riscos significativos associados ao ciberseguro, este tipo de seguro é atualmente mais caro do que outras formas de cobertura. Conforme dados de SUSEP (2023), observa-se o seguro cibernético pode ser até três vezes mais caro que o seguro de responsabilidade geral e seis vezes mais caro que o seguro de propriedade.

4.2.2 Coberturas do seguro cibernético

Esta seção oferece um mapeamento detalhado dos diferentes tipos de coberturas relatadas pelas empresas. Um resumo dos tipos de cobertura ofertados em mercado nacional (AIG) e internacional (EIOPA e Swiss Re).

O seguro cibernético pode ser oferecido como um produto independente ou como uma cobertura adicional às linhas de negócios tradicionais. Ele pode incluir cobertura para responsabilidades tanto de primeira quanto de terceira parte. A maioria das empresas oferece soluções personalizadas e algumas disponibilizam seus produtos por meio de parcerias com outras seguradoras. Todos os grupos na amostra oferecem cobertura para responsabilidades de primeira e terceira partes e/ou uma combinação de ambas (EIOPA, 2018).

Figura 20 – coberturas do seguro cibernético comumente comercializadas



Fonte: (Swiss Reinsurance institute,2023)

Os tipos mais comuns de cobertura oferecidos são interrupção de negócios (BI) e restauração de dados. Cobertura contra extorsão cibernética e suporte legal também são fornecidos pela maioria das empresas de seguro, embora em menor escala.

Conforme AIG (2023), atualmente principal player no mercado de seguros Cyber conforme dados da SUSEP, o seguro teria a responsabilidade e cobertura relacionadas a dados pessoais e corporativos. Isso inclui situações como a divulgação pública de dados privados e corporativos, a contaminação de dados por software não autorizado, roubo físico de hardware, violações por empresas terceirizadas e custos associados à defesa legal e investigação.

Conforme AIG, o seguro também cobre despesas para mitigar danos à reputação, notificação de violações de dados aos usuários e a recuperação de dados eletrônicos após uma violação de segurança. Em suma, o objetivo é proteger a empresa contra diversas formas de perda ou dano relacionados à segurança e confidencialidade de dados.

Juntamente a isso, conforme AIG, clientes têm a opção de adicionar extensões ao Seguro de Riscos Cibernéticos. Uma dessas extensões cobre perdas resultantes de extorsão na internet, proporcionando pagamento exclusivamente em resposta a ameaças de segurança. Outra extensão abrange perdas decorrentes de atos relacionados à mídia, como violações de

direitos autorais, marcas registradas, plágio ou divulgação imprópria de informações. Além disso, o seguro oferece cobertura para interrupção de rede, compensando o lucro líquido e as despesas operacionais que seriam obtidos caso haja uma interrupção ou suspensão dos negócios causada diretamente por falha de segurança, sendo essa interrupção real e mensurável.

No que diz respeito a violações de dados, persistem preocupações quanto à precisão na quantificação de seu impacto, uma vez que as consequências desses eventos podem envolver perdas financeiras e outras implicações nas receitas futuras. Outro desafio é identificar se a perda é permanente ou temporária, e determinar o impacto preciso na imagem da marca. Na maioria dos casos, observou-se uma redução nos preços das ações após violações de dados (principalmente com base na experiência dos Estados Unidos). No geral, o mercado para cobertura de danos reputacionais ainda não é considerado maduro (EIOPA, 2018).

Diferentes apólices podem vir a possibilidade de engajar um consultor de relações públicas ou um assessor de imprensa, visando mitigar o impacto na reputação da empresa que tenha sido alvo de uma violação de segurança, dado que a reputação representa um dos ativos intangíveis mais substanciais para uma organização (EIOPA, 2018). Estes serviços suplementares oferecem ao segurado um recurso adicional para a administração de seu perfil de risco, embora possam vir a custar um valor adicional sobre o prêmio.

Conforme CRO Forum (2023), no caso de ransomware deve-se considerar a cobertura do seguro cibernético com certo cuidado, diferentes aspectos devem ser incluídos, como os custos judiciais associados à violação de dados, custos para gestão de crises (por exemplo, forense de TI, aconselhamento jurídico e comunicações), custos para restaurar os dados e o sistema, a perda de lucro atribuível ao evento de ransomware, e também a cobertura do pagamento de resgate

Atualmente, na legislação vigente, são estabelecidos padrões em relação ao Marco Legal e à responsabilização. A Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), demonstra uma inspiração fortemente consumerista. Foi empreendido um esforço substancial, especialmente por parte da Secretaria Nacional do Consumidor (SENACOM), para moldar a legislação, e muitos dos preceitos da lei guardam notável semelhança com as disposições do Código de Defesa do Consumidor.

Conforme LGPD, para o indivíduo cujos dados tenham sido objeto de violação, o direito de acionar tanto o ente que efetuou a coleta da informação quanto aquele que a processou é assegurado - o último podendo ser, inclusive, uma terceira parte, como, por exemplo, o local de armazenamento, incluindo serviços em nuvem, entre outros agentes cuja identidade o titular dos dados porventura desconheça.

Ainda assim, é válido destacar que a lei estabelece uma responsabilidade solidária entre tais entidades. O titular dos dados pode, eventualmente, ter consentido com a política da empresa à qual confiou suas informações, ciente de que haveria um compartilhamento da referida informação. No entanto, em virtude da responsabilidade solidária, a empresa detentora dos dados deve possuir um entendimento claro acerca de seus parceiros de negócios, com o intuito de mitigar, ao menos em parte, o risco associado a tais operações (Brasil, 2018).

Percebe-se, conforme destacado por (EIOPA, 2018), caso o segurado se associe a um colaborador desprovido de um nível de segurança adequado, ou que não detenha uma apólice com uma cobertura ideal capaz de prover a devida compensação em caso de eventualidades, sem garantias de solvência e responsabilidade por parte da empresa, estar-se-á assumindo um risco substancialmente maior do que o ordinário.

Por fim, parece não haver disposição para oferecer cobertura potencial relacionada a transações envolvendo criptomoedas no momento, visto que os riscos envolvidos ainda não são plenamente compreendidos (EIOPA, 2018).

4.2.3 Risco de subscrição no seguro cibernético

Conforme demonstrado pelo estudo da Global Digital Trust Insights Survey de 2024, em ressonância com uma visão internacional pelo relatório publicado em 2018 pela EIOPA(European Insurance and Ocupational Pensions Authority), o maior risco apontado por seguradoras do mercado é o risco de subscrição (PWC, 2024; EIOPA, 2018).

Entende-se como risco de subscrição o risco inerente à atividade de seguradoras de que a probabilidade de sinistros futuros venha a superar as expectativas da seguradora enquanto processo de montagem de um prêmio, sendo risco comummente ligado à incapacidade de cálculo de um prêmio puro adequado ou de provisões técnicas necessárias para acomodar o risco contratado em processo de subscrição (ou fechamento de contrato) (REJDA; MCNAMARA, 2018).

Dada a escassez de dados de sinistros e de ferramentas de benchmark para sinistros, o método qualitativo é adotado para gestão de riscos na maioria das empresas, havendo geralmente a falta de modelos robustos e em fase de uso para precificação de sinistros cibernéticos (EIOPA , 2018).

No âmbito do mercado de seguros, como previamente discutido, surge a indagação de como quantificar o risco. De forma simplificada, é comum a distinção entre os riscos inerentes à própria entidade segurada, denominados "riscos de primeira parte" ou First-Party Risk , e os riscos associados à responsabilidade civil ou aos danos ocasionados a terceiros, como

vendedores, parceiros ou prestadores de serviços, chamados de “Riscos de terceira parte” ou Third-Party Risk. No contexto do risco de responsabilidade civil tradicional, é imperativo avaliar a exposição que pode afetar tais terceiros, uma avaliação muitas vezes subjetiva, particularmente no ambiente digital. Este constitui um dos desafios a serem enfrentados por clientes e corretores na análise da exposição cibernética (ORTEOUS; RAVINDRAN, 2015; HUBBARD, 2009).

O risco cibernético apresenta uma peculiaridade ao abranger tanto a perspectiva de primeira quanto de terceira parte. Sob tal escopo, uma série de cenários se desdobram, como, por exemplo, os danos suportados pelo próprio segurado e os danos provocados a terceiros em virtude de uma possível violação nos sistemas do mencionado segurado.

Antes da Lei 13.709/2018, para implementar controles e contratar a apólice observava-se pelos clientes uma consideração maior no próprio risco, não sendo observada grande preocupação com a responsabilidade civil nem com as consequências da exposição de dados.

Considerando a incerteza do limite de perdas possível em mercado, a precificação vem a se basear no que é mensurável, em conjunto com o apetite de risco da seguradora.

Kelliher *et al.* (2013) ressaltam que, para as seguradoras que operam no ramo de seguros de vida, o risco predominante está associado à frequência de ocorrência de sinistros, uma vez que a severidade (ou montante do sinistro) geralmente é conhecida. No entanto, para as seguradoras que atuam em outros ramos (não-vida), a situação é consideravelmente mais intrincada, dada a incerteza tanto em relação à frequência quanto à severidade dos sinistros, e o lapso temporal entre o acontecimento do sinistro, a notificação e o pagamento da indenização pode se estender significativamente. Com base nessas observações, os autores definem cinco variáveis que, de modo geral, influenciam o risco de subscrição:

a) Frequência de sinistros, de caráter prospectivo - relacionada à incerteza acerca do número de sinistros a ocorrer;

b) Frequência de sinistros, IBNR2 - diz respeito à incerteza quanto ao número de sinistros já ocorridos, porém ainda não notificados;

c) Severidade de sinistros, de natureza prospectiva - vinculada à incerteza acerca da magnitude dos sinistros a ocorrer;

d) Severidade de sinistros, sinistros reportados mas não liquidados - associada à incerteza sobre a magnitude dos sinistros já notificados, mas que ainda aguardam liquidação (o número deles é conhecido, mas não sua severidade final);

e) Severidade de sinistros, IBNR - refere-se à incerteza quanto à magnitude dos sinistros já ocorridos, mas ainda não notificados

Entende-se que pela observável falha de clara delimitação de coberturas observada pela Global Digital Trust Insights Survey (PWC, 2024), que reportou diferentemente de um seguro de vida, a indenização no caso dos seguros cibernéticos possui relação com o dano produzido pela ocorrência, uma vez que diferentemente de um seguro de carro, na qual é segurado um valor de um bem atualizado ao valor de mercado, a quantificação de um risco coberto, assim como em um seguro de vida, é bastante complexa de quantificar, visto que além da falta de experiencia nesse mercado, temos que as consequências de um evento podem causar tanto perdas financeiras quanto implicações em receita futura como riscos de relações públicas, juntamente com a dificuldade em classificar perdas em permanentes ou temporárias e a abrangência precisa na imagem do portifólio, por questões inerentes do seguro e por falta de maturidade do mercado para danos reputacionais.

À medida que as apostas aumentam e o mercado passa por evoluções, há uma ascensão perceptível na proeminência dos conceitos de gestão de riscos. Notavelmente, a detecção e a resiliência estão surgindo como elementos cruciais na navegação desse cenário. Essa mudança é atribuída às complexidades inerentes à transferência de riscos em cenários diversos, tornando necessárias práticas de gestão de riscos mais eficazes e essenciais.

5 CONSIDERAÇÕES FINAIS

A Gestão de Riscos é praticada em diversas organizações. Compreender o conceito de risco e a possibilidade de transferência através do Seguro seria de suma importância para o desenvolvimento profissional de qualquer administrador, ainda mais se considerarmos a Gestão de Riscos como parte do planejamento estratégico da organização e a possibilidade de transferência do risco como um recurso no desenvolvimento dessa estratégia.

Apesar disso, como o conceito de "Gestão de Riscos" é amplo e pode ser aplicado em diferentes vertentes e abordado através das mais variadas ferramentas, o seu entendimento encontra-se num campo nebuloso. Somando-se a isso, grande parte dos administradores carece de conhecimento do mercado segurador e as referências encontradas sobre esse tema são, normalmente, fornecidas pelas próprias seguradoras, faltando uma avaliação mais crítica. Quando se trata de *Cyber Risks*, das novas legislações e responsabilidades com as quais os administradores terão de lidar como gestores, a criticidade de aprofundamento no tema torna-se ainda maior.

Diretores de Segurança da Informação (CISO) destacaram o monitoramento de rede e a gestão de identidade como prioridades. Da mesma forma, o investimento em medidas básicas para remediar sistemas legados foi identificado como uma área que tem se mostrado benéfica especialmente para os profissionais do setor bancário, enquanto outros setores foram menos consistentes, mencionando talento, consolidação de aplicativos ou proteção de dados como áreas de alto retorno para suas instituições específicas.

Corroborando com o apresentado por autores acadêmicos e vozes do mercado como Brasiliano e KPMG, as organizações devem criar estratégias para detectar e reduzir possíveis ciberataques, determinando com precisão o que deve ser protegido (seus ativos mais críticos) e praticando respostas adequadas para diferentes cenários de ataques ou incidentes. Isso requer uma maturidade de inteligência cibernética, uma metodologia robusta de avaliação de riscos, um sistema de resposta a incidentes experiente e uma organização bem-instruída.

Assim, as organizações ganham confiança na capacidade de enfrentar ameaças previsíveis e ataques inesperados, efetivamente "prevenindo" a ocorrência de ciberataques. Para alcançar o estágio de Antecipação, é crucial incorporar segurança cibernética voltada para o futuro, manter um foco tanto no ambiente atual quanto no futuro e adotar uma abordagem proativa, que inclua testes regulares da capacidade de resposta a incidentes. Isso significa oferecer respostas eficazes e rápidas para conter o dano.

Observa-se uma clara tendência de continuidade nos atuais índices de ataques cibernéticos, a menos que os gestores de segurança cibernética adotem uma postura diferente. É fundamental que esses gestores transmitam à alta administração as consequências significativas para o negócio, destacando o potencial impacto financeiro, de reputação, operacional e legal que a empresa poderá suportar. Uma mudança essencial nas atitudes e abordagens dos responsáveis pela segurança cibernética se mostra crucial para enfrentar eficazmente os desafios em evolução no cenário digital e garantir a resiliência da organização diante das ameaças cibernéticas.

Quanto a estudos futuros, é desejado considerar a aplicação de métodos quantitativos na análise de sinistros cibernéticos. Explorar abordagens que incorporem análises estatísticas e modelagem matemática pode proporcionar uma compreensão mais precisa e preditiva dos padrões de ataques cibernéticos, permitindo uma melhor antecipação e mitigação de riscos. O emprego de métodos quantitativos pode contribuir significativamente para o desenvolvimento de estratégias mais eficazes de segurança cibernética, possibilitando uma resposta proativa diante das ameaças emergentes no ambiente digital.

No entanto, é crucial exercer cautela em futuras pesquisas, dada a falta de disponibilidade de dados abrangentes sobre ataques cibernéticos e os montantes das perdas associadas, o que pode impactar a precisão e abrangência das análises. Uma vez que os negócios e as regulamentações evoluem mais rapidamente do que sistemas e processos, os ativos de dados geralmente não são organizados adequadamente para suportar o uso de diferentes formas. Além disso, a qualidade dos dados raramente é considerada desde a fase de design do projeto, e os controles são normalmente detectivos, em vez de preventivos. Da ausência da incorporação da qualidade dos dados na fase de design, pode-se inferir que corrigir a qualidade dos dados pode ser difícil. Uma mudança cultural em direção à qualidade de dados por design é benéfica.

REFERÊNCIAS

AIG SEGUROS BRASIL S.A. CyberEdge: Seguro de Proteção de Dados e Responsabilidade Cibernética. S. l., 2019. E-book (28 p.).

AIG SEGUROS BRASIL S.A. SEGURO CIBERNÉTICO: O QUE É E COMO SE PROTEGER DESSES RISCOS?
Disponível em: https://www.negocioseguroaig.com.br/industria/de-olho/seguro-cibernetico/
Acesso em: 15 de Dez. 2023

ALLIANZ, Global Corporate & Specialty (AGCS) , 2015 - A Guide to Cyber Risk Managing the Impact of Increasing Interconnectivity, pg 5. Disponível em: https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/AGCS-Cyberrisk-report.pdf. Acesso em: 01 de Ago. 2023

BAE Systems Applied Intelligence. Disponível em: https://www.baesystems.com/en/digital/feature/cyber-threat-landscape--the-inside-track. Acesso em: 01 de Ago. 2023

BASLE COMMITTEE ON BANKING SUPERVISION. International Convergence of Capital Measurement and Capital Standards. Basileia, 1988.

BRASIL, 2022 – Incidentes de segurança com dados pessoais, Disponível via : https://www.gov.br/anpd/pt-br/assuntos/semana-da-protecao-de-dados-2022/incidentes-de-seguranca-com-dados-pessoais#:~:text=Um%20incidente%20de%20seguran%C3%A7a%20com,dados%20inadequada%20ou%20il%C3%ADcita%2C%20os
Acesso em: 14 de dez. de 2023

BRASILIANO, Antônio Celso Ribeiro. Gestão e Análise de Riscos Corporativos: Método Brasiliano Avançado. 2ª ed. São Paulo: Sicurezza Editora, 2012.

BRASILIANO, Antônio Celso Ribeiro. CONHECENDO QUATRO RISCOS ESTRATÉGICOS CIBERNÉTICOS, 2016.
Disponível via : https://www.linkedin.com/pulse/conhecendo-quatro-riscos-estrat%C3%A9gicos-cibern%C3%A9ticos-antonio-brasiliano/?originalSubdomain=pt
Acesso em: 14 de dez. de 2023

BRASILIANO, Antonio Celso Ribeiro. Gestão de Riscos Cibernéticos | Foco nos negócios - Joias da coroa, abril de 2023.

BRASILIANO, Antônio Celso Ribeiro. GESTÃO DE RISCOS CIBERNÉTICOS, FOCO NOS NEGÓCIOS JOIAS DA COROA, 2023.

CAMPBELL, T. (2008). Risk management: Implementing an effective system. Accountancy Ireland, 40(6), 54–66.

Casa Civil. MANUAL DE GESTÃO DE RISCOS DO TCU – 2ª edição 2020. Brasília: CC/PR, 2020. Disponível em: https://portal.tcu.gov.br/data/files/46/B3/C6/F4/97D647109EB62737F18818A8/Manual_gesta

o_riscos_TCU_2_edicao.pdf.. Acesso em: 01 de Ago. 2023

CAVALCANTI, Carlos Diego. Gestão de Riscos: abordagem de conceitos e aplicações. 2009. Disponível em: http://www.valcann.com/publicacoes/riscos_conceitosaplicacoes.pdf Acesso em: 22 de mar. de 2023

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) , 2023 - Disponível via: https://stats.cert.br/incidentes/#tipos-incidente Acesso em: 14 de dez. de 2023

CHAMBON, C. (2003). Project risk management: Processes, techniques and insights. Chichester, England: John Wiley & Sons.
CIRCULAR SUSEP Nº 177, de 11 de dezembro de 2001

CNSEG, Seguro de riscos cibernéticos Edição 195 / Mesa-Redonda / Seguro de riscos cibernéticos, 2019. Disponível em: https://cadernosdeseguro.ens.edu.br/secao.php?materia=794. Acesso em: 01 de Ago. 2023

CONDAMIN, L., Louisot, J.-P., & Naïm, P. (2006). Risk quantification: Management, diagnosis and hedging.Chichester, England: John Wiley & Sons.

Corporate Finance Institute (CFI), Risk, The probability that actual results will differ from expected results, 2023. Disponível em: https://corporatefinanceinstitute.com/resources/career-map/sell-side/risk-management/risk/. Acesso em: 01 de Ago. 2023

COSO, erm – Gerenciamento de Riscos Corporativos Integrado com Estratégia e Performance, 2017.

CRO Forum, Cyber resilience, The cyber risk challenge and the role of insurance, 2014. Disponível em: https://www.thecroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-version-24-1.pdf. Acesso em: 01 de Ago. 2023.

CRO Forum, Ransomware Threats, Countermeasures and Trends within the Insurance Industry. Disponível em: https://www.thecroforum.org/wp-content/uploads/2023/03/Ransomware-Threats-Countermeasures-and-Trends-within-the-Insurance-Industry-1.pdf
Acesso em: 15 de Dez. 2023

DAMODARM, A. (2007). Strategic risk taking: a framework for risk management. Pearson Prentice Hall.

SLYWOTZKY, Adrian. Do risco à oportunidade. (2007).

DORFMAN, Mark S. Introduction to Risk Management and Insurance. 6. ed. Arkansas: Prentice Hal, Inc., 1998. 567 p

EDWARDS, C., Ham, W., & Tittel, E. (2017). CISSP For Dummies. John Wiley & Sons.
EIOPA, 2018 - Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), 2017. Commonality of risk assessment language in cyber insurance Recommendations on Cyber Insurance. ISBN 978-92-9204-228-8, DOI 10.2824/691163

FERMA,2003 – NORMA DE GESTÃO DE RISCOS © AIRMIC, ALARM, IRM: 2002, translation copyright FERMA: 2003. Disponível em: https://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-portuguese-version.pdf. Acesso em: 01 de Ago. 2023

GREGORIOU, G. N. (2006). Advances in risk management. New York, NY: Palgrave Macmillan.
HESTER, R. E., & Harrison, R. M. (1998). Risk assessment and risk management. Cambridge, England: Royal Society of Chemistry.

HORCHER, K. A. (2005). Essentials of financial risk management.

HUBBARD, D. (2009). The Failure of Risk Management: Why It's Broken and How to Fix It. John Wiley & Sons.

IBGC – INSTITUTO BRASILEIRO DE GESTÃO DE RISCOS CORPORATIVOS. Guia de Orientação para Gerenciamento de Riscos Corporativos (www.ibgc.org.br).

IBM, Cost of a Data Breach Report, 2023. Disponível em: https://www.ibm.com/downloads/cas/E3G5JMBP 2023. Acesso em: 18 de Ago. 2023

ISACA. Pagina de glossários ISACA. Disponível em: https://www.isaca.org/resources/glossary, Acesso em: 09/09/2023.

KAPLAN, R., & Mikes, A. (2012). Managing Risks: A New Framework. Harvard Business Review, 90, 48-60.

KEEGAN, M. (2004). The orange book: Management of risk—Principles and concepts. Norwich, England: HM Treasury.

KELLIHER, P. et al. A common risk classification system for the Actuarial Profession. British Actuarial Journal, v. 18, n. 01, p. 91-121, 2013. Disponível em: http://dx.doi.org/10.1017/S1357321712000293. Acesso em: 01 de Ago. 2023

KPMG - 2016 TAKING THE OFFENSIVE Working together to disrupt digital crime. Disponível em: https://home.kpmg.com/uk/en/home/insights/2016/07/taking-the-offensive-working-together-to-disrupt-digital-crime.html. Acesso em: 01 de Ago. 2023

KUERBIS, B.; BADIEI, F. Mapping the cybersecurity institutional landscape. Australian Catholic University, v. 19, p. 466-492, 2017.

La Fabrica de Pensamiento – Instituto de Auditores Internos de Espanã, Definición e Implantición de Apetito de Riesgo, 2013. Disponível em: https://auditoresinternos.es/uploads/media_items/apetito-de-riesgo-original.original.pdf. Acesso em: 15 dez. 2023.

LLOYD'S - Closing the gap : insuring your business against evolving cyber threats. In association with KPMG and DAC Beachcroft. S.l. : Lloyd's, 2017

MALEVERGNE, Y., & Sornette, D. (2005). Extreme financial risks: From dependence to risk management. New York, NY: Springer.

MARSH ; RIMS - Emerging risks : anticipating threats and opportunities around the corner. Report analysis and review Brian C. Elowe, Carol Fox. S.l. : MARSH; RIMS, 2016.

MENNY, Barzilay, A simple definition of Cybersecurity, May 2013. Disponível em: Disponível em http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296. Acesso em: 01 de Ago. 2023

MOLAK, V. (1997). Fundamentals of risk analysis and risk management. New York, NY: CRC Press.

NUNES, Ricardo Pereira. Análise do Fluxo de Caixa em Risco para uma Empresa Produtora de Derivados de Petróleo. Dissertação de Mestrado em Engenharia de Produção. Orientador: Carlos Patrício Samanez. Rio de Janeiro: Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio), 2009

Path to cyber resilience: Sense, resist, react EY's 19th Global Information Security Survey 2016-17. Disponível em: https://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2017/01/GISS-Report-to-reduce_Optimized4.pdf. Acesso em: 01 de Ago. 2023

PORTEOUS, T., & Ravindran, S. (2015). Risk Management in the Digital Era: An Exploration of the Impact of Cyber Risk in the Enterprise Context. Journal of Risk Research, 18(6), 621-634. Disponível em: http://www.accountancyireland.ie/. Acesso em: 01 de Ago. 2023

REFSDAL, Solhaug, & Stølen - Cyber-Risk Management, 2015

ROUSE, M. (2021). Malware (malicious software). SearchSecurity. Disponível em: https://searchsecurity.techtarget.com/definition/malware. Acesso em: 01 de Ago. 2023

The Law of Cyber-Attack - Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, 2012

VAUGHAN, EMMETT J.; VAUGHAN, THERESE M. Fundamentals of Risk and Insurance. 10th ed. New Jersey: John Wiley & Sons, Inc., 2008. 745 p

VERIZON. Data-breach-investigations-report-dbir, 2022.

VIEIRA, et al. Governança, gestão de riscos e integridade. 2019.

WARWICK, B. (2003). The handbook of risk. Chichester, England: John Wiley & Sons.

WILLIAMS, R., Bertsch, B., Dale, B., van der Wiele, T., van Iwaarden, J., Smith, M., &

Visser, R. (2006). Quality and risk management: What are the key issues. The TQM Magazine, 18, 67–87. doi:10.1108/09544780610637703

WORLD BANK, Financial Risk Assessment: A Handbook for Assessing and Managing Environmental and Social Risk in Financial Institutions, 2013. Disponível em: https://elibrary.worldbank.org/doi/abs/10.1596/17841. Acesso em: 01 de Ago. 2023

World Economic Forum, The Global Risks Report, 2018.
Disponível via : https://www3.weforum.org/docs/WEF_GRR18_Report.pdf
Acesso em: 14 de Dez. 2023.

ZARGAR, Saman Taghavi, James Joshi e David Tipper: A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. IEEE Communications Surveys Tutorials, 15(4):2046–2069, 2013.