Marsh

Panorama de Mercado

Riscos Cibernéticos

31 de janeiro de 2024

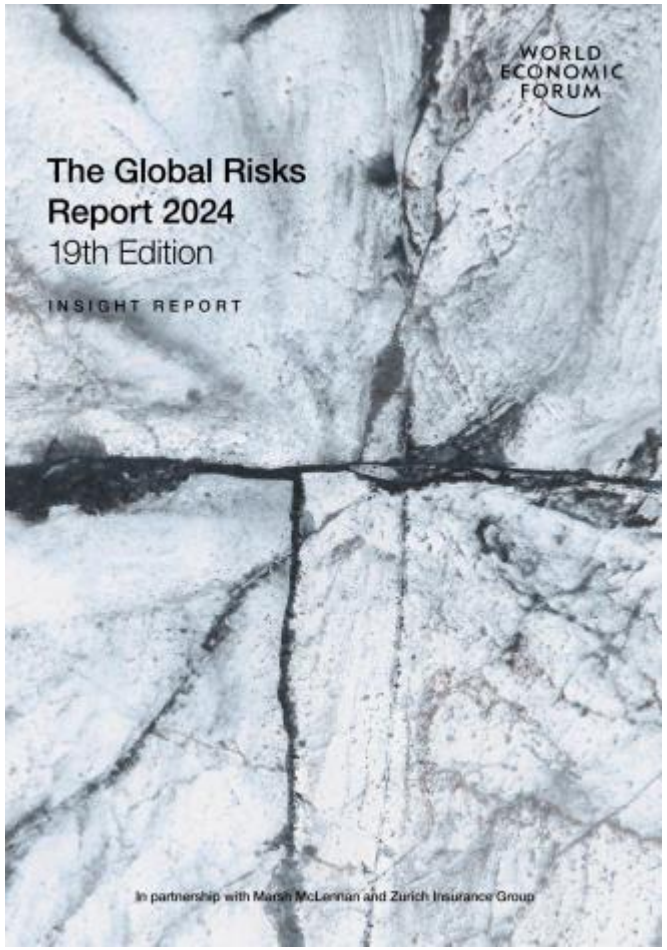
André Leão - Cyber Specialty Manager

Índice

Relatório de Riscos Globais - FEM

1

Relatório de Riscos Globais - FEM



Relatório de Riscos Globais

Elaborado anualmente pelo Fórum Econômico Mundial

Com base no **parecer de 1.490 especialistas globais** dos universos acadêmico, de negócios, governamental, comunidade internacional e sociedade civil, são mapeados e **quantificados os principais riscos que afetarão o mundo** no futuro.

O relatório é elaborado em parceria global com Marsh.

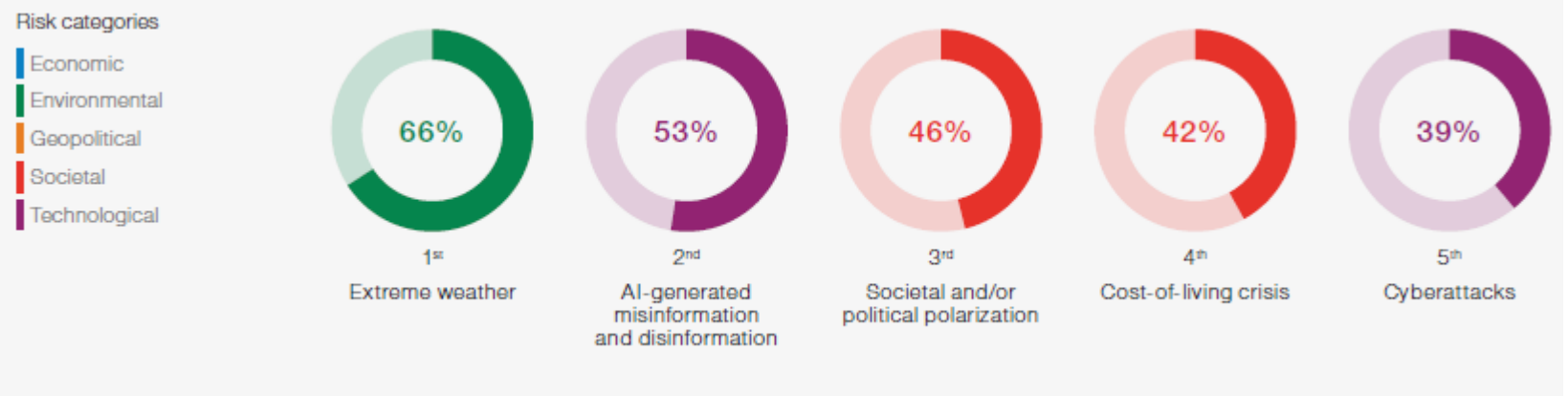
Apresenta os principais riscos globais divididos em 5 categorias:

- Econômico
- Ambiental
- Geopolítico
- Social
- Tecnológico

Relatório de Riscos Globais - FEM

Quais...

...são cinco riscos que você acredita serem os mais prováveis de apresentar uma crise material em escala global em 2024

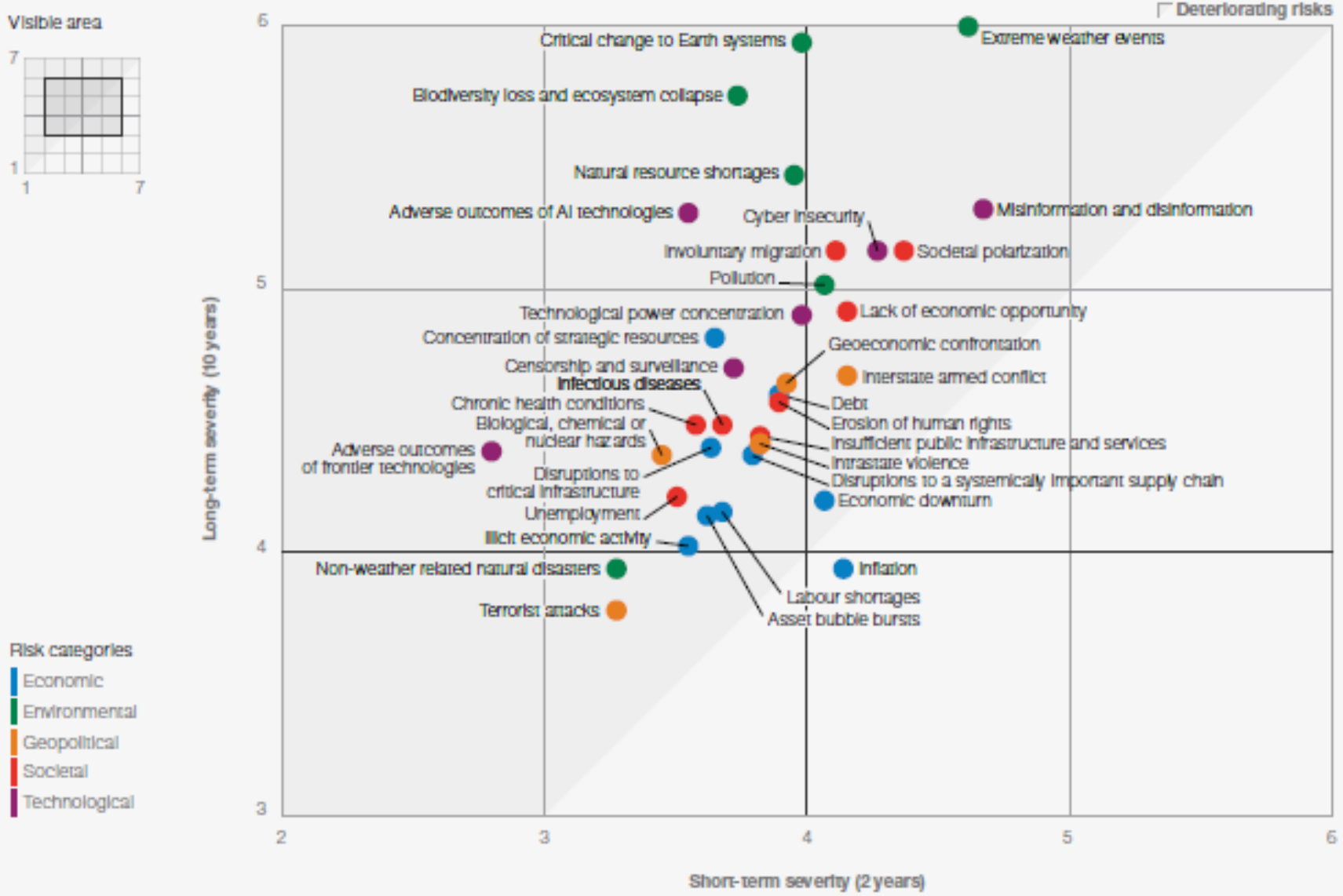


Estime...

... o impacto provável (gravidade) dos seguintes riscos ao longo de um período de 2 anos e 10 anos.

Fonte: World Economic Forum Risk Report 2023

Relatório de Riscos Globais - FEM



Fonte: World Economic Forum Risk Report 2023

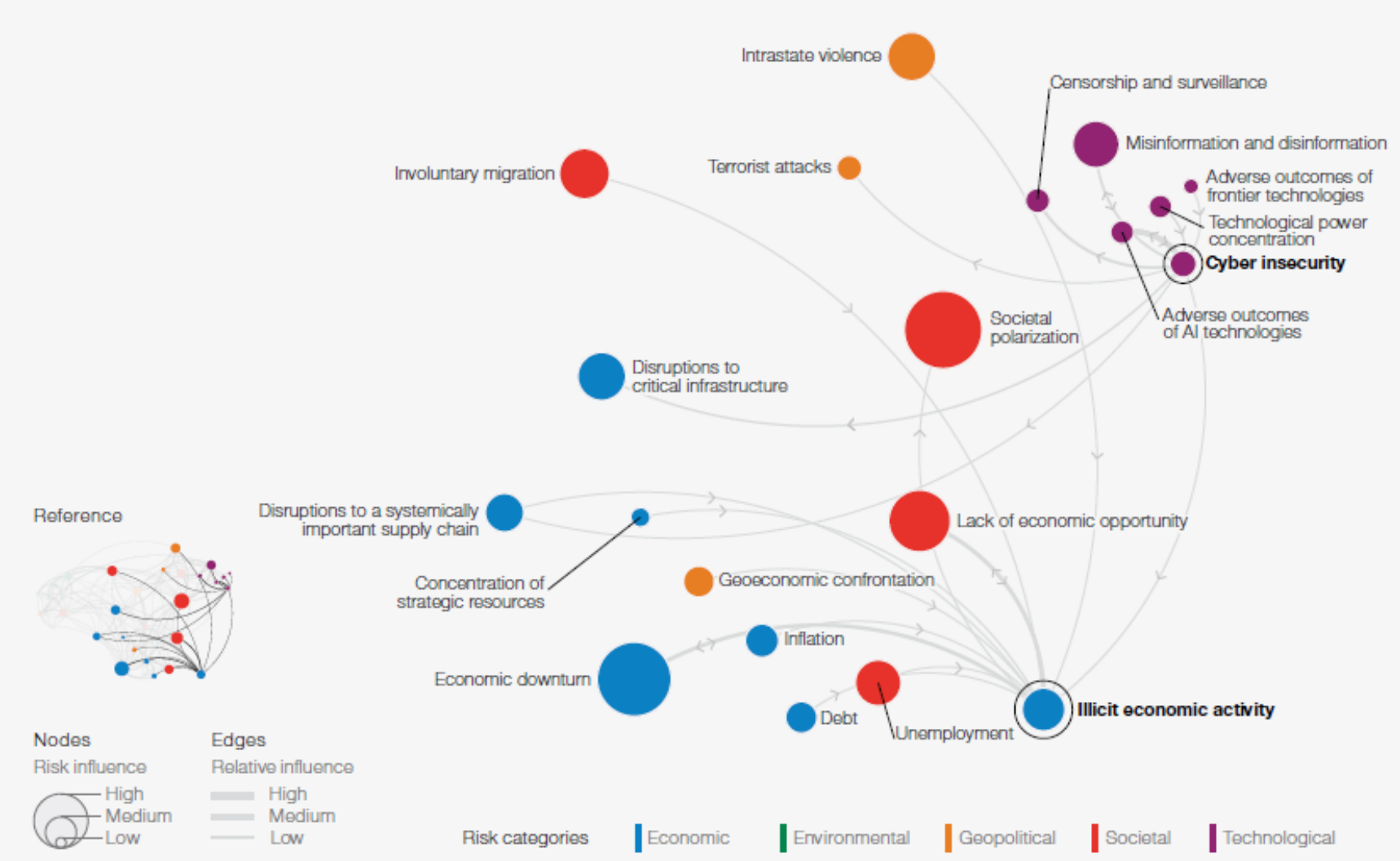
Cybercrimes e Desinformação

Foram considerados globalmente riscos que podem causar impactos globais tanto no curto prazo, como no longo prazo.

Marsh

Relatório de Riscos Globais - FEM

Ramificações da Insegurança Cibernética



Além dos efeitos tecnológicos,

Cybercrimes

possuem ramificações econômicas, sociais e geopolíticas.

Características de um Ataque Cibernético

2

Poder Destrutivo

	M16	F-16	G 16
Poder de fogo	20-30 tiros Calibre .556 Nato	511 tiros M61A1 Vulcan 20mm; 2 mísseis *wingtip;* 6 mísseis *underwing;* 1 míssil *under fuselage*.	Capaz de causar prejuízos bilionários a toda infraestrutura.
Alcance	500 m	860 Km	Ilimitado, basta uma conexão
Disponibilidade do Equipamento	Forças armadas, forças policiais, civis após checagem de antecedentes	Forças armadas dos EUA e seus aliados	Qualquer um
Custo (aprox.)	US$ 700,00	US$ 30.000.000,00	US$ 500,00

Poder Destrutivo de um Cyberataque

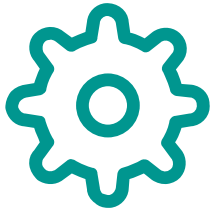
Um cyberataque não possui limitações....

Territoriais/Logísticas

No mundo físico, para cometer um crime, quase sempre você precisa **estar** no local do crime. Essa limitação não existe no mundo virtual

De Forma/Aparência

No mundo físico, um ataque tem **aparência** de ataque. Você pode **ver** o assalto. Em uma guerra, você vê as tropas e tanques inimigos.



Físicas/Operacionais

No mundo físico, você está **limitados a característica física** dos objetos. Por exemplo, você não pode usar um tanque para abrir uma caixa forte subterrânea. Ele não chega até lá.

De Repetição/Escala

No mundo físico, após um assalto fracassado, você não pode, imediatamente perpetrar o **mesmo assalto** em outro lugar. Após um assalto bem-sucedido, as vítimas não se tornam cúmplices do assaltante.

Motivações e Efeitos de um Cyberataque

Autor	Descrição	Motivação	Alvo	Efeito
Cyber-terroristas	Grupos extremistas.	Aliciar apoio à própria causa, dissuadir causa oposta.	Conforme ideologia (religiosa, étnica)	Danos materiais; Compro-metimento de infraestrutura crítica; apagar/alterar dados médicos
Hacktivistas	Grupos com ideologias políticas, econômicas, sociais específicas.	Trazer conhecimento de uma causa, exercitar o direito de expressão	Conforme ideologia (indústria, setor econômico, partido político)	Publicação de dados indesejados, vulnerabilida-des, indisponibilidade de sistemas.
Cyberataques patrocinados por Estados	Grupos altamente sofisticados que recebem apoio técnico e financeiro de um Estado/Nação	Fazer valer os interesses do Estado/Nação a qual pertencem / o qual representam,	Outros estados, fornecedores na área da defesa e infraestrutura crítica.	Espionagem, Danos materiais; Compro-metimento de infraestrutura crítica e de defesa.
Cyber-criminosos	Criminosos “comuns”, sem motivação ideológica.	Ganho Financeiro, Poder	Repositório de dados, bancos, empresas, hospitais.	Acessar dados e/ou comprometer sistemas para monetizar sua devolução/recuperação.
Oportunistas	Pessoas comuns que encontraram uma vulnerabilidade	Vingança pessoal, atenção, reconhecimentos	Ex-empregadores, ex-namorado(a)s	Apagamento e divulgação de informações confidenciais,

Tipos de Ataque

Malware

Inserir códigos maliciosos no sistema da vítima.
Tipos mais comuns: Virus, Worms, Ransomware, Spyware.

DoS

Sobrecarregar os sistemas da vítima prejudicando sua operação.
Tipos mais comuns: DoS; DDoS

Phishing

Induzir a vítima a executar uma operação ou inserir dados.
Timos mais comuns: Spear Fishing, Whaling, SMiShing, Vishing

Spoofing

Passar-se por uma fonte confiável para ganhar acesso a um sistema
Timos mais comuns: Domain Spoofing, E-mail Spoofing, ARP Spoofing

Ataques de Identidade

Usuário malicioso “se mascara” de usuário legitimo. De posse de credenciais da vítima, tentar acessar seus sistemas.
Tipos mais comuns: Man in the Middle, Pass the Hash, Password Spraying, Brute Force.

Na maioria dos casos, o mesmo incidente combina 2 ou mais tipos de ataque

Marsh

Cyber Segurança e Incidentes

3

Incidentes Cibernéticos seguem em alta mundialmente

Principais tendências para 2024/2025

Aumento de ataques de ransomware

- Estudos indicam que os ataques de ransomware continuarão a crescer em 2024, com maior sofisticação e direcionamento a empresas de todos os tamanhos.

Fonte: Relatório de Tendências de Segurança Cibernética da CrowdStrike.

Ameaças à Internet das Coisas (IoT):

- Com o aumento da adoção de dispositivos IoT, espera-se um aumento nas vulnerabilidades e nos ataques direcionados a esses dispositivos.

Fonte: Relatório de Ameaças Cibernéticas da Symantec.

Aumento de ataques de engenharia social:

- Os ataques de engenharia social, como phishing e spear phishing, continuarão a ser uma ameaça significativa em 2024, com hackers cada vez mais habilidosos em manipular as pessoas para obter acesso a informações confidenciais.

Fonte: Relatório de Ameaças Cibernéticas da Verizon.

Incidentes Cibernéticos seguem em alta mundialmente

Principais tendências para 2024/2025

Aumento de ataques a cadeias de suprimentos:

- Os ataques a cadeias de suprimentos, nos quais os hackers comprometem fornecedores para obter acesso a empresas-alvo, estão se tornando mais comuns e representam um risco significativo para as organizações.

Fonte: Relatório de Ameaças Cibernéticas da FireEye.

Preocupações com a privacidade de dados:

- Com a implementação de regulamentações de privacidade de dados, como a LGPD no Brasil e o GDPR na União Europeia, as empresas enfrentarão desafios crescentes para proteger os dados pessoais dos clientes e cumprir as exigências regulatórias.

Fonte: Relatório de Tendências de Segurança Cibernética da McAfee.

E o que fazer para responder à estas ameaças?

Principais tendências para 2024/2025

Implementar medidas de segurança robustas contra ransomware

- Realizar backups regulares de dados e armazená-los em locais seguros.
- Manter sistemas e softwares atualizados com as últimas correções de segurança.
- Implementar soluções de segurança avançadas, como firewalls e sistemas de detecção de intrusões.

Fonte: Guia de Prevenção de Ransomware da ANPD (Autoridade Nacional de Proteção de Dados).

Fortalecer a conscientização e treinamento em segurança cibernética

- Realizar treinamentos regulares para funcionários sobre práticas seguras de navegação na internet, identificação de phishing e proteção de informações confidenciais.
- Promover uma cultura de segurança cibernética, incentivando os funcionários a relatarem incidentes e suspeitas de atividades maliciosas.

Fonte: Guia de Boas Práticas em Segurança Cibernética do CERT.br.

E o que fazer para responder à estas ameaças?

Principais tendências para 2024/2025

Adotar medidas de proteção específicas para setores-chave

- Implementar soluções de segurança especializadas para setores como financeiro, saúde e energia, levando em consideração as ameaças específicas enfrentadas por esses setores.
- Realizar avaliações regulares de risco e vulnerabilidade para identificar e mitigar possíveis brechas de segurança.

Fonte: Guia de Segurança Cibernética para o Setor Financeiro do Banco Central do Brasil.

Adquirir uma apólice de seguros para riscos cibernéticos

- Considerar a contratação de uma apólice de seguro específica para riscos cibernéticos, que possa cobrir as despesas relacionadas a incidentes cibernéticos, como recuperação de dados, notificação de violação de dados, responsabilidade cibernética e interrupção de negócios.

Fonte: Guia de Segurança Cibernética para Empresas do Instituto Nacional de Tecnologia da Informação - ITI.

E o que fazer para responder à estas ameaças?

Principais tendências para 2024/2025

Estabelecer uma estratégia de resposta a incidentes cibernéticos

- Desenvolver um plano de resposta a incidentes cibernéticos que inclua a identificação, contenção, investigação e recuperação de incidentes.
- Designar uma equipe de resposta a incidentes e estabelecer protocolos claros de comunicação e coordenação.

Fonte: Guia de Resposta a Incidentes Cibernéticos do CERT.br.

Estabelecer parcerias com especialistas em segurança cibernética

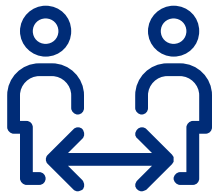
- Considerar a contratação de serviços de consultoria em segurança cibernética para realizar avaliações de risco, testes de penetração e auditorias de segurança.
- Trabalhar em conjunto com especialistas em segurança cibernética para desenvolver e implementar estratégias de segurança personalizadas para a empresa.

Fonte: Guia de Boas Práticas em Segurança Cibernética do CERT.br.

Seguro Cyber

4

Gerenciando os Riscos de um Cyberataque

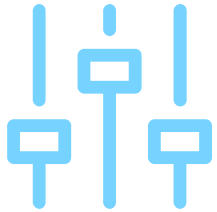


Evitar

Não incorrer no risco

Não utilizar conexões com a internet.

No mundo atual, esta alternativa é cada vez mais improvável



Mitigar

Reduzir o risco

Ferramentas e Processos: Aprimorar sistemas protecionais, de controle de acesso, backups, redundâncias.

Transferir

Transferir o risco

Contratação de apólice de seguros, que incorrerá com a parte majoritária dos custos de um ataque.

Aceitar

Estar preparado p/ o risco

Aceitar não é “conformar-se”. É ter conhecimento detalhado do risco e estar preparado para enfrenta-lo caso ele se manifeste.

Apólice de Seguro Cibernético

Objetivo

Proteger a **empresa e a PF** dos administradores, caso estas venham a sofrer danos ou ser responsabilizadas por **incidentes cibernéticos**.

Contratação

O seguro é contratado e pago pela empresa (**Tomador**). A cobertura estende-se ao próprio Tomador, suas subsidiárias e as PFs responsáveis por segurança da informação. (**Segurados**).

A base de Reclamações e Descobertas

Para que haja cobertura, é necessário que:

OU um terceiro apresente uma **Reclamação** contra um **Segurado.**

OU o Segurado **descubra um Incidente Cibernético**

Cobertura

Os custos necessários e razoáveis associados a:

Danos a empresa:

- Recuperação dos sistemas da empresa

Resp. por danos a 3os

- Defesa das Reclamações

O que está Coberto:

Danos ao próprio segurado

Em caso de descoberta de evento cibernético pelo segurado:.

- **Custos de Recuperação de Dados**
- **Custo de Gestão de Incidente Cibernético**
- **Custos de Monitoramento de Crédito**
- **Custos de Extorsão Cibernética**
- **Lucros Cessantes**
- **Multas e Sanções**

Responsabilidade por Danos à Terceiros

Em caso de Reclamações de Terceiros, Alegando a responsabilidade cibernética do segurado:

- **Responsabilidade sobre dados em poder da empresa**
- **Responsabilidade sobre dados em poder empresas terceirizadas**
- **Custos de Defesa**
- **Indenizações por Danos Morais**

Relação das Coberturas

Danos ao próprio segurado (1st Party)

	DESCRIÇÃO
Restauração de Dados	Custos para restaurar, recriar ou recuperar seus dados e outros ativos intangíveis que são corrompidos ou destruídos por um ataque cibernético
Cyber Extorsão	Ameaça de comprometer a rede ou os dados se o resgate não for pago.
Gerenciamento de eventos/ Breach Response	Custos resultantes de uma violação de segurança ou privacidade da rede.
Network Business Interruption - Lucros Cessantes	Interrupção ou suspensão de sistemas de computador devido a uma violação de segurança de rede.
Dependent Business Interruption - Lucros Cessates Dependentes	Interrupção ou suspensão de sistemas de computador devido a uma violação de segurança de rede de Fornecedores.
Custos de Restituição de Imagem para Sociedade	Custos e despesas para mitigar os danos à reputação da sociedade em consequência Violação de Segurança de Dados
Custos de Restituição de Imagem para Imagem Pessoal	Custos e despesas para mitigar os danos à reputação pessoal em consequência Violação de Segurança de Dados (ex.: DPO)
Serviço de Informática Forense	Custos incorridos para a contratação de um Perito Forense a fim de investigar uma Violação de Informação Pessoal ou Corporativa, ou uma Violação de Segurança aos sistemas de computadores do Segurado
Custos de Hardware ("Bricking")	Custos razoáveis e necessários incorridos para reparar ou substituir hardware ou equipamento de computador danificado ou inoperante.
Custos de Melhoria de Hardware	Aumento da capacidade de memória ou a velocidade de processamento necessária para instalar uma versão mais segura e eficiente do Sistema de Computador do Segurado dentre as definições descritas na apólice
Despesas Emergenciais	Custos e despesas para mitigar valores incorridos em conexão com violação de informação (pessoal ou corporativa) com a principal intenção de evitar e/ou minorar uma Reclamação coberta pela Apólice

Relação das Coberturas

Responsabilidade por danos a terceiros (3rd Party)

	DESCRIÇÃO
Responsabilidade pela Privacidade	Falha em impedir o acesso não autorizado, a divulgação ou a coleta de informações pessoais; Contaminação de Dados de Terceiros por software não autorizado ou código malicioso; Destruição, modificação, corrupção ou eliminação de Dados armazenados em qualquer Sistema de Computador;
Custos de Defesa	Custos jurídicos resultantes de um vazamento de informações em que o segurado é acionado frente a violação da privacidade
Danos Regulatórios e custos Defesa	Ações regulatórias, e multas relacionadas avaliadas pelos órgãos reguladores.
Multas e Penalizações	Multas e penalizações decorrentes de uma ação regulatória
Responsabilidade por empresas Tercerizadas	Falha de empresas terceirizadas a quem você confiou os seus dados, por não notificar adequadamente uma violação de privacidade.
Media Liability - Responsabilidade de Mídia	Defesa e responsabilidade por difamação online, calúnia, depreciação, apropriação indébita de nome ou semelhança, plágio, violação de direitos autorais, negligência no conteúdo daqueles que confiaram no conteúdo.

Principais Exclusões

Conduta / Má Fé

O cometimento de atos dolosos, fraudulentos, ou violação intencional de leis e/ou normas. Está assegurado o direito aos custos de defesa até a confissão de culpa ou trânsito em julgado.

Não inerente a Responsabilidade Cibernética

Reclamações cuja responsabilidade não derive de ou não esteja relacionada ao vazamento de dados e/ou responsabilidade cibernética.

SLAs / Obrigações Contratuais

Qualquer Reclamação relacionada ao não cumprimento de SLAs e/ou obrigações contratuais. Está assegurado o direito de defesa em caso de responsabilidade que prevaleceria na ausência do contrato ou SLA

Falha na Transferência de Fundos

Qualquer transferência de fundos indevida, fraudulenta, assim como quaisquer ordens de pagamento, compra, venda ou movimentação financeira ou de valores mobiliários

Engenharia Social

Perdas decorrentes de ações inadequadas tomadas por indivíduos dentro da organização como resultado de engano e manipulação.

Fatos ou Atos Anteriores

Quaisquer: Fatos Geradores e/ou Reclamações:
(i) anteriores a Data de Retroatividade;
(ii) já existentes antes da primeira Reclamações
(iii) anteriores a uma empresa ser uma subsidiária.

Danos Materiais / Corporais

Quaisquer danos à propriedade tangível (máquinas, equipamentos, construções) e/ou danos corporais, ainda que em consequência de um evento cibernético

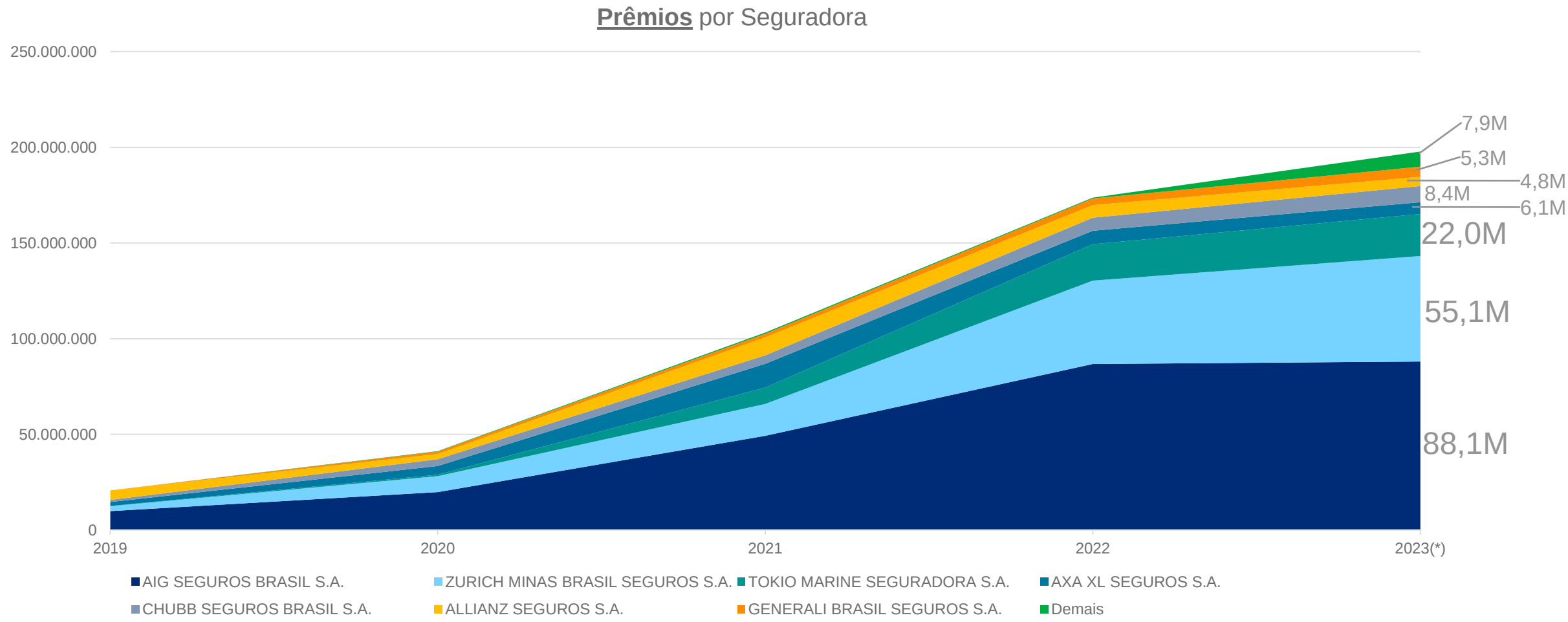
Falência / Insolvência

Reclamações originadas por, decorrentes de, ou associadas a condição de Recuperação Judicial, Falência ou Insolvência do Tomador ou suas Subsidiárias

Mercado de Cyber: Brasil

Relatórios SUSEP

A Concentração começa a diluir

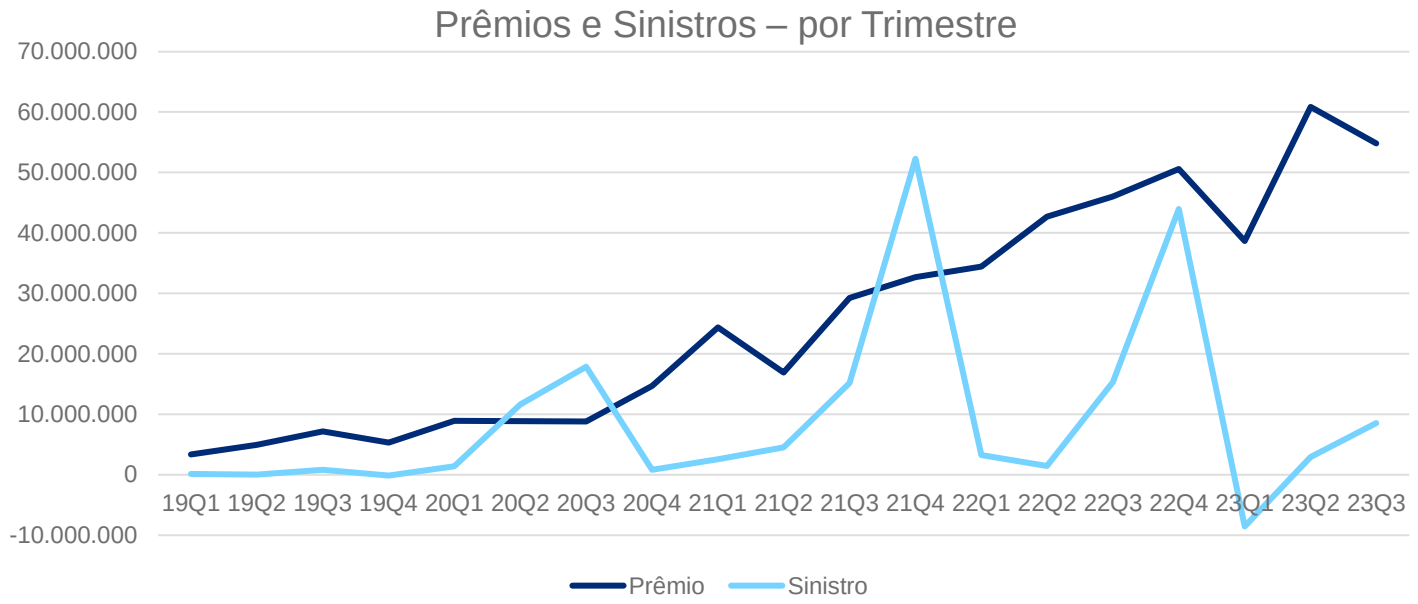


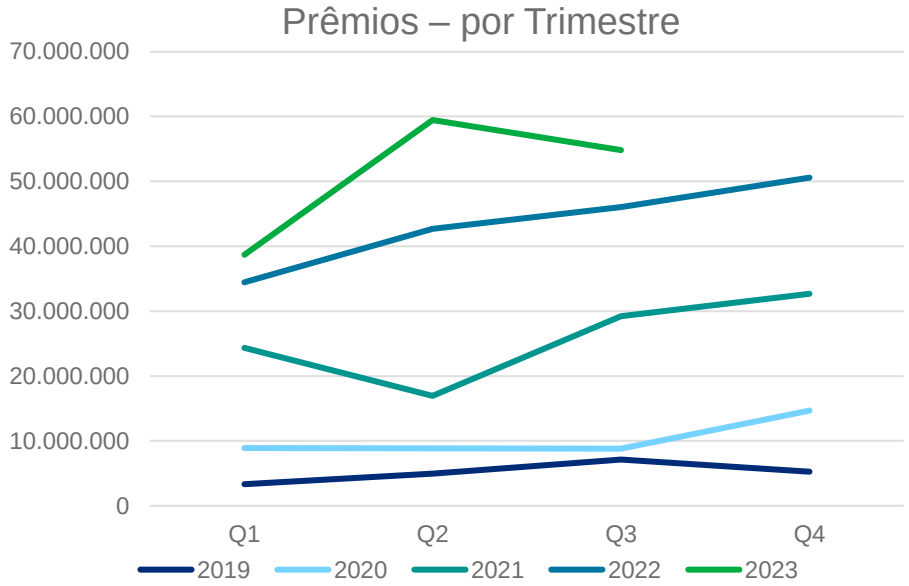
Fonte: SUSEP. Compilado por Marsh

(*) Estimativa para o ano de 2023 com valores até Out/23 anualizados para 12 meses

Relatórios SUSEP

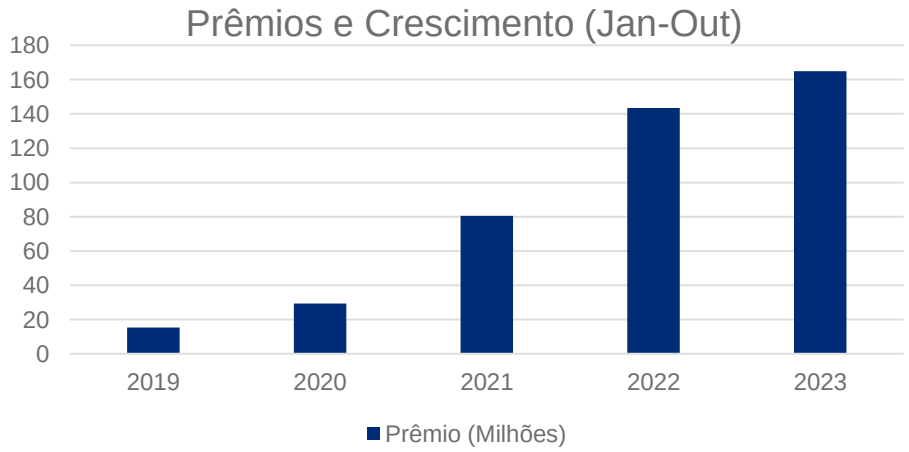
O crescimento continua a passos moderados





CYBER: Prêmios e Sinistros - ano a ano

	2019	2020	2021	2022	2023 (OUT)
Prêmios:	20.703.699	41.285.725	103.166.857	173.709.432	164.864.405
Sinistros:	811.476	31.617.316	74.513.760	63.941.061	11.651.207



Marsh

Fonte: RELATÓRIOS SES-SUSEP. Compilado por Marsh

Mercado de Cyber: LatAm e Mundo

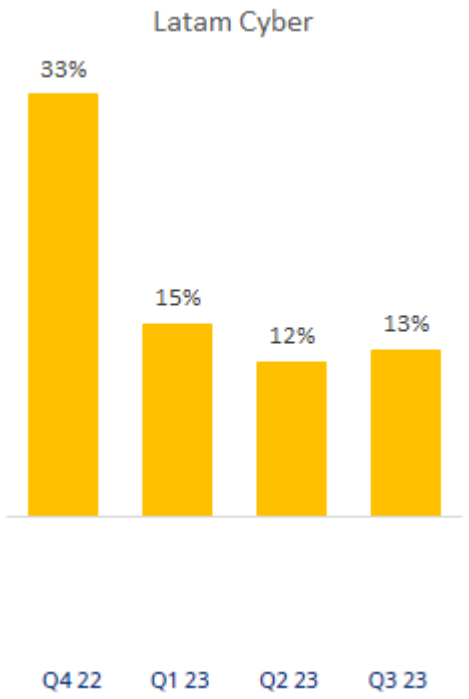
6

Principais Tendências – América Latina

Principais Tendências

- O preço do seguro cibernético aumentou 13% no terceiro trimestre, em comparação com 12% no trimestre anterior.
- O mercado de seguros cibernéticos mostrou sinais de estabilização.
- Novos entrantes no mercado, especialmente no cenário internacional, intensificaram a concorrência.
- Ao mesmo tempo, a região vivenciou vários eventos cibernéticos significativos que impulsionaram o aumento dos preços, especialmente no México.

Movimento Médio de Taxas



Capacidade

- Após 3 anos de redução, a capacidade está começando a retornar, tanto nos mercados de seguros quanto de resseguros. Chubb e AXA retomaram a oferta de capacidade em riscos selecionados. Uma classificação madura de cibersegurança continua sendo crucial para a aceitação.
- Mais capacidade significa limites mais altos disponíveis para os clientes. Após vários aumentos, as franquias estão caminhando para a estabilização.
- Embora em um ritmo mais moderado, a demanda por seguro cibernético continua aumentando no Brasil.

Preço

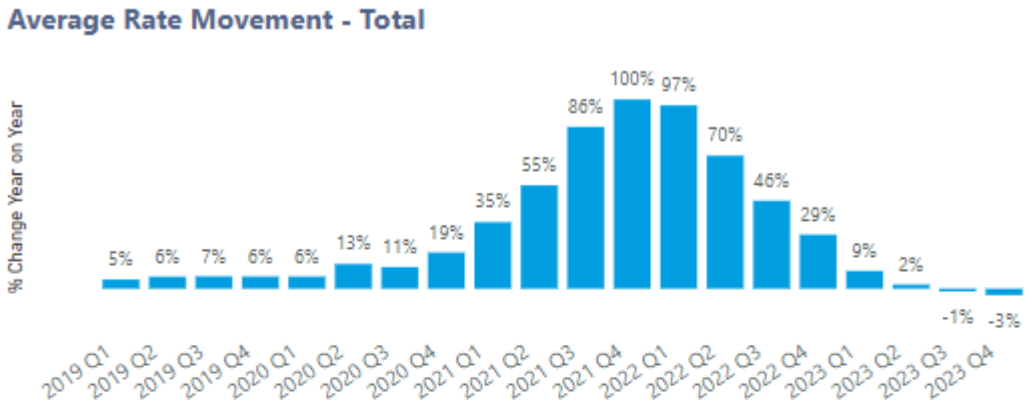
- Os aumentos de prêmio diminuíram significativamente. Ainda ocorrem aumentos, mas juntamente com renovações sem alteração e reduções.
- No geral, a taxa de sinistralidade tende a afetar menos os segurados com histórico de sinistros limpo. (Mais aumentos de taxa com base em riscos individuais e menos com base na indústria).
- Segurados com histórico significativo de sinistros e/ou sem melhoria na maturidade cibernética tendem a sofrer os maiores aumentos de taxa.

Cobertura

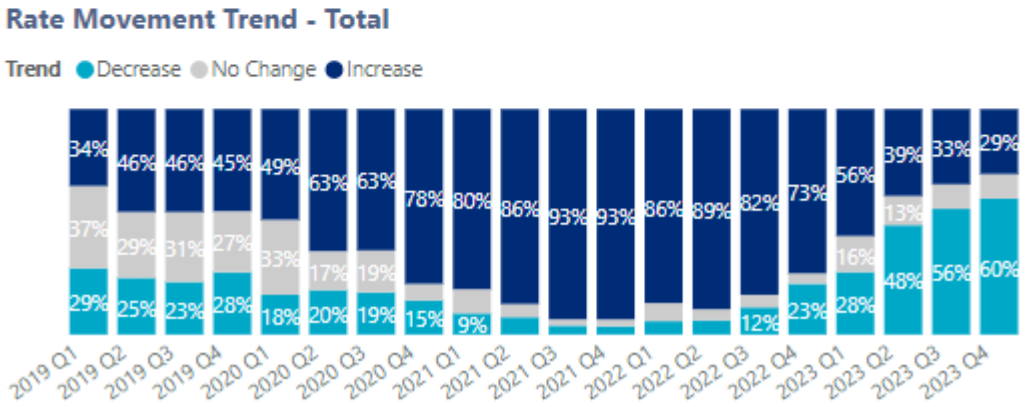
- Embora as cláusulas de ransomware ainda estejam presentes em muitas apólices, tem havido sucesso moderado em revogá-las para riscos com maior maturidade cibernética.
- Preocupações com exposições sistêmicas e risco de acumulação ainda existem, levando a recusas ou restrições de cobertura.
- O debate sobre exclusão de guerra permanece aberto e os conflitos na Ucrânia e, mais recentemente, em Israel continuam sendo observados de perto.

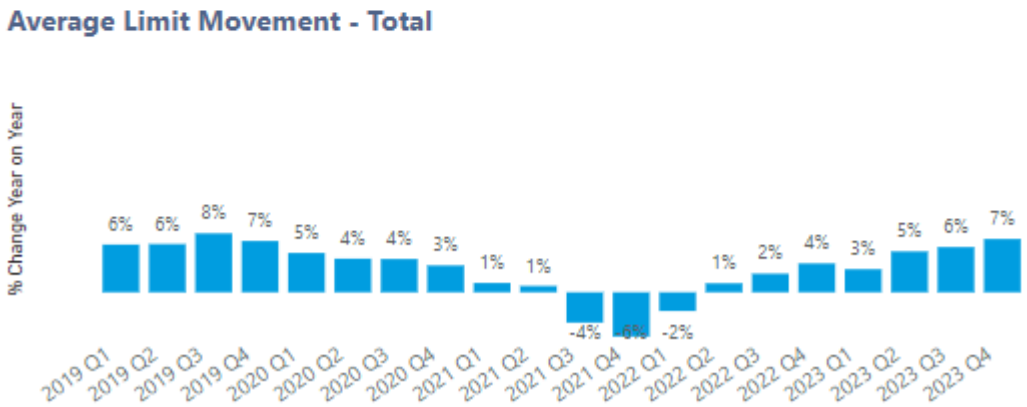
Movimentação de Prêmio - GLOBAL

GLOBAL



- Os preços **globais** dos seguros continuam a diminuir, impulsionados principalmente pelos mercados dos EUA e do Reino Unido..
- Custos de apólices de excesso continuam a reduzir preços totais de programas.
- Sinistros de *ransomware* continuam a aumentar. Melhorias nos controles de segurança cibernética levaram a uma maior proporção de segurados que não pagam resgates;Increased insurer competition led to clients generally being able to secure lower retentions without a premium increase.
- Com o aumento de sinistros em 2023, comparado a 2022 e os preços se estabilizando, os clientes geralmente buscaram limites mais altos.





Marsh Cyber Specialty e Advisory

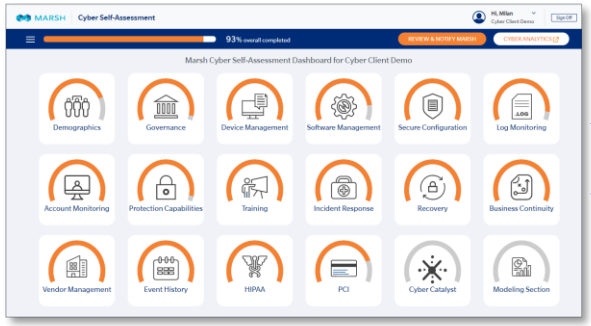
7

O Risco de Cyber precisa ser quantificado

A Marsh fornece uma visão de 360 graus da postura de segurança cibernética das organizações

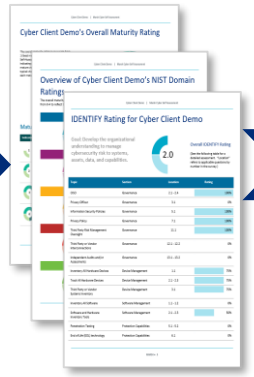
Único Documento compartilhado com as seguradoras

Client Dashboard



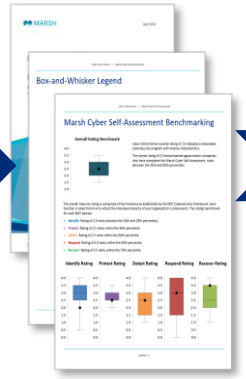
Cyber Self Assessment, a ferramenta de subscrição da Marsh que fornece uma visão 360º da postura de cybersegurança da sua organização.

NIST Report

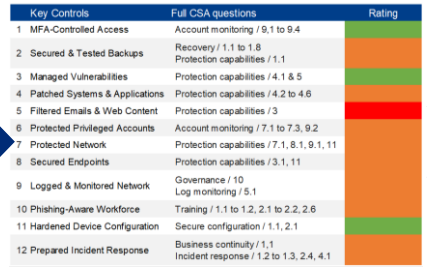


Relatórios produzidos com base na estrutura NIST.

Benchmark Report



12 Key controls Report



	Key Controls	Full CSA questions	Rating
1	MFA-Controlled Access	Account monitoring / 9,1 to 9.4	
2	Secured & Tested Backups	Recovery / 1.1 to 1.8 Protection capabilities / 1.1	
3	Managed Vulnerabilities	Protection capabilities / 4.1 & 5	
4	Patched Systems & Applications	Protection capabilities / 4.2 to 4.6	
5	Filtered Emails & Web Content	Protection capabilities / 3	
6	Protected Privileged Accounts	Account monitoring / 7.1 to 7.3, 9.2	
7	Protected Network	Protection capabilities / 7.1, 8.1, 9.1, 11	
8	Secured Endpoints	Protection capabilities / 3.1, 11	
9	Logged & Monitored Network	Governance / 10 Log monitoring / 5.1	
10	Phishing-Aware Workforce	Training / 1.1 to 1.2, 2.1 to 2.2, 2.6	
11	Hardened Device Configuration	Secure configuration / 1.1, 2.1	
12	Prepared Incident Response	Business continuity / 1,1 Incident response / 1.2 to 1.3, 2.4, 4.1	

Análise com base nos 12 principais controles da lente de um subscritor para avaliar aceitação

External Threat Analysis

SecurityScorecard
BITSIGHT®
The Standard in SECURITY RATINGS

Análise não intrusiva de ameaças externas das informações publicamente disponíveis.

Cyber Underwriting Report

Apenas as informações copiladas em um formato detalhado e já aceito pelos subscritores serão enviado ao mercado

Boa Maturi-dade?

Não

- **Efetuar Melhorias**
- **Aguardar Maior Nível Maturidade**

Sim

Ir à Mercado

Marsh

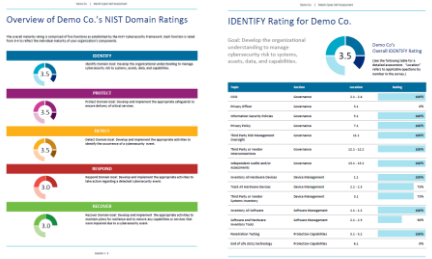
Expertise para Riscos Complexos

Muito mais do que a colocação do seguro, a Marsh oferece uma suíte de ferramentas exclusivas que fornecem uma visão do estado de segurança cibernética de qualquer tipo de organização

Conhecer o perfil de Risco

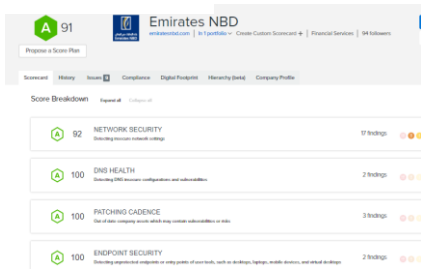
Propor Soluções Efetivas de Transferência de Risco

Marsh Cyber Self Assesment



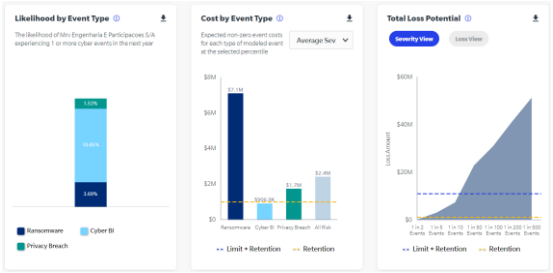
Cyber Threat Intelligence

SecurityScorecard

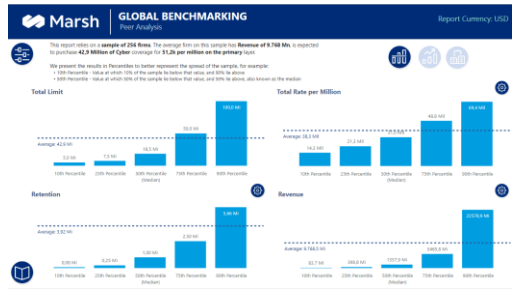


BITSIGHT
The Standard in SECURITY RATINGS

Ransomware Cost Analysis



Peer Benchmarking



Key Cyber Security Controls

	Key Controls	Full CSA questions	Rating
1	MFA-Controlled Access	Account monitoring / 9,1 to 9.4	
2	Secured & Tested Backups	Recovery / 1.1 to 1.8 Protection capabilities / 1.1	
3	Managed Vulnerabilities	Protection capabilities / 4.1 & 5	
4	Patched Systems & Applications	Protection capabilities / 4.2 to 4.6	
5	Filtered Emails & Web Content	Protection capabilities / 3	
6	Protected Privileged Accounts	Account monitoring / 7.1 to 7.3, 9.2	
7	Protected Network	Protection capabilities / 7.1, 8.1, 9.1, 11	
8	Secured Endpoints	Protection capabilities / 3.1, 11	
9	Logged & Monitored Network	Governance / 10 Log monitoring / 5.1	
10	Phishing-Aware Workforce	Training / 1.1 to 1.2, 2.1 to 2.2, 2.6	
11	Hardened Device Configuration	Secure configuration / 1.1, 2.1	
12	Prepared Incident Response	Business continuity / 1,1 Incident response / 1.2 to 1.3, 2.4, 4.1	

Business Interruption quantification

RETURN PERIOD	PERCENTILE	TOTAL EVENT COST	EXTORTION PAYMENT	BUSINESS INTERRUPTION	PRIVACY BREACH COSTS	RANSOMWARE RESPONSE & RECOVERY COSTS
Average	-	$7M	$2M	$3M	$325K	$2M
1 in 2 Events	50%	$4M	-	-	-	$1M
1 in 5 Events	80%	$10M	$2M	$4M	$158K	$3M
1 in 10 Events	90%	$18M	$5M	$10M	$261K	$5M
1 in 50 Events	98%	$40M	$18M	$30M	$4M	$7M
1 in 100 Events	99%	$48M	$30M	$39M	$9M	$7M
1 in 200 Events	99.5%	$55M	$42M	$49M	$17M	$8M
1 in 500 Events	99.8%	$62M	$48M	$55M	$22M	$8M

Privacy breach quantification

RETURN PERIOD	PERCENTILE	TOTAL EVENT COST	TOTAL IMPACTED DURATION (DAYS)	DISCOVERY	FULL OUTAGE	RECOVERY	RESTORATION
Average	-	$907K	7	$9K	$62K	$503K	$333K
1 in 2 Events	50%	$25K	2	$412	$3K	$16K	$6K
1 in 5 Events	80%	$72K	4	$1K	$6K	$48K	$17K
1 in 10 Eve...	90%	$2M	18	$36K	$143K	$1M	$609K
1 in 50 Eve...	98%	$12M	71	$92K	$830K	$6M	$5M
1 in 100 Ev...	99%	$18M	105	$138K	$1M	$9M	$7M
1 in 200 Ev...	99.5%	$23M	134	$176K	$2M	$12M	$9M
1 in 500 Ev...	99.8%	$32M	185	$242K	$2M	$17M	$13M

Marsh Cyber Specialty: Mundo

+ 25

Anos de Experiência

(Mundo)

A Marsh é pioneira na corretagem de riscos cibernéticos no Brasil e no mundo.

+ 10.000

Empresas Clientes

(150 delas no Brasil)

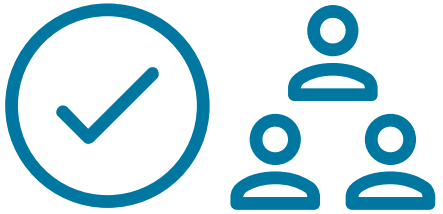
Mais empresas escolhem Marsh. A Marsh possui a maior carteira de seguros de riscos cibernéticos do mundo.

+ USD 1,5 Bi

Em prêmios Emitidos

(+ R$ 70 Mi no Brasil)

Experiência sem paralelo em riscos complexos: nenhuma outra corretora é responsável pela colocação de tantos riscos de cyber.



+ 250

Profissionais Especializados

(8 deles no Brasil)

A corretora com o maior e mais capacitado times de profissionais dedicados exclusivamente a seguros cibernéticos.

Marsh Cyber Specialty: Brasil

Da esq. p/ dir.: **André Leão** (Gerente Técnico); **Pedro Azevedo** (Analista); **Julia Olsak** (Analista Sr.); **Diego Pinto** (Gerente Comercial); **Daniel Lamboy** (Head); **Anderson Pereira** (Analista). Não estão na foto: **Fabiano Totino** (Cyber Claims Specialist) **Gabriella Lopes** (Analista Sr.)

A maior equipe dedicada do Brasil

8 pessoas dedicadas exclusivamente a cyber

Mais de **55** sinistros regulados ou em regulação.

Marsh

Marsh Cyber Advisory

Marsh Cyber Advisory

A Marsh possui uma linha de Cyber Risk voltada para apoiar nossos clientes na jornada de Segurança Cibernética.

Equipe formada por profissionais altamente capacitados

Conhecimento de casos reais de fraude e incidente de segurança cibernética

Capacidade de realizar a quantificação dos riscos cibernéticos

Equipe dedicada para suportar serviços de Segurança Cibernética em toda a América Latina.

Visão abrangente da gestão de riscos, não apenas focada na mitigação

Capacidade de atendimento regional através das equipes das diferentes equipes na América Latina

Geração de relatórios de Segurança Cibernética com informações regionais e globais

Centro de Excelencia em Segurança Cibernética focada em testes técnicos e resposta a Incidentes Cibernéticos

Cyber Risk Consulting

Nossos principais serviços

Cyber Strategy & Governance

- Avaliação de segurança cibernética
- Desenvolvimento de Estratégia de Cibersegurança
- Avaliação de segurança cibernética ICS/SCADA
- Avaliação de segurança cibernética para nuvem
- Avaliação de prevenção de fraudes digitais
- Desenvolvimento de políticas e procedimentos de segurança da informação e Cibersegurança
- Outsourcing de Segurança da Informação
- Desenvolvimento do painel executivo de segurança cibernética

Compliance

- Auditoria de controles gerais de TI
- Análise de lacunas de regulamentação de segurança cibernética
- Desenvolvimento de requisitos regulamentares de segurança cibernética
- Análise de lacunas do PCI DSS
- Desenvolvimento de Diagramas de Fluxo de Dados do Portador de Cartão (PCI DSS)
- Avaliação de privacidade de dados
- Implementação do Programa de Privacidade de Dados

Cybersecurity Culture

- Cyber Chimestry- Avaliação da Cultura de Segurança Cibernética
- Desenvolvimento do Programa de Conscientização sobre Segurança Cibernética
- Treinamento de segurança cibernética

Risk Management and Quantification

- Identificação e Classificação de Ativos de Informação
- Desenvolvimento da Metodologia Qualitativa e Quantitativa de Segurança da Informação e Gestão de Riscos Cibernéticos
- Segurança da Informação e Avaliação de Riscos Cibernéticos
- Quantificação de risco cibernético (CyberXQ, Cyber RFO, Marsh Blue[i] Cyber)

Third Party Risk Management

- Definição da estrutura de gerenciamento de risco cibernético de terceiros
- Segurança de informações de terceiros e avaliação de risco cibernético
- Cyber Due-Diligence para Fusões e Aquisições (M&A)

Cyber Insurance Policy

- Auto avaliação de segurança cibernética para o seguro cibernético*
- Cyber IDEAL – Estimativa de perdas de risco cibernético (violação de privacidade, Ransomware e perda de receita comercial)*
- Classificação de segurança cibernética (BitSight e SecurityScorecard)*
- Avaliação de risco de seguro cibernético
- Colocação de seguro cibernético*
- Reivindicações Cibernéticas e Orquestração de Crise

Secure Development Lifecycle

- Desenvolvimento da Metodologia de Ciclo de Vida de Desenvolvimento Seguro
- Treinamento de Desenvolvimento Seguro
- Revisão do código-fonte (teste de segurança de aplicativo estático)

Defensive and Offensive Security

- Cyber Inteligência (busca de informações vazadas na Internet)
- Gerenciamento de vulnerabilidades
- Revisão da configuração de segurança (proteção)
- Teste de penetração (Hacking Ético)
- Hackear aplicativos da Web e móveis
- Testes de engenharia social
- Operações Red Team

Cyber Incident Management

- Resposta a incidentes cibernéticos
- Desenvolvimento do Plano de Resposta a Incidentes Cibernéticos
- Desenvolvimento do Protocolo de Ransomware Organizacional
- Simulação de Crise Cibernética
- Desenvolvimento do Plano de Melhoria Pós-incidente

Cyber Risk Analytics

Specialized Tools

Conteúdos Marsh

9

Conteúdos Marsh

WEF Global Crisis Risks Report

A Marsh é uma das principais colaboradoras do relatório de riscos do Fórum Econômico Mundial. Ainda que este relatório trate de diversos tipos de riscos, ele trata de riscos cibernéticos em múltiplas ocasiões.

The State of Cyber Resilience Report

Anualmente, a Marsh, em parceria com a Microsoft, publica um relatório do estado de cyber-resiliência. Específico do universo cibernético, o relatório apresenta as principais tendências, com objetivo de auxiliar as empresas no planejamento de sua resiliência cibernética.

The Changing Face of Cyber Claims

Relatório que a Marsh publica anualmente sobre sinistros em apólices de Cyber. Ainda que este relatório reúna somente dados da Europa, ele pode proporcionar Insights e antecipar tendências do que podemos esperar no futuro por aqui.

Global Insurance Market Index

Trimestralmente a Marsh publica o “GIMI” – Global Market Insurance Index. É um relatório focado em preço de seguros. Ainda que não haja o monitoramento específico da linha de cyber, ela é uma das linhas que compõem o relatório. Aspectos específicos de cyber que afetam precificação e aceitação são mencionados neste relatório.

Marsh é a corretora de seguros com o

maior e mais completo

conteúdo de segurança cibernética do mundo