MARSH | Microsoft

INSIGHTS | SETEMBRO

Estudo de Percepção do Risco Cibernético na América Latina 2019

MARSH & McLENNAN COMPANIES

INSIGHTS | SETEMBRO

Estudo de Percepção do Risco Cibernético na América Latina 2019

CONTEÚDO

Introdução

A tecnologia está transformando drasticamente os ambientes de negócios a nível global, com avanços contínuos em áreas que vão desde inteligência artificial e Internet das Coisas (IoT) até a disponibilidade sobre dados e blockchain. A velocidade com que as tecnologias digitais evoluem e rompem com os modelos tradicionais de negócios segue aumentando. Enquanto isso, os riscos cibernéticos parecem evoluir ainda mais rápido.

O risco cibernético passou de preocupação com roubo de dados e privacidade a esquemas mais sofisticados que podem interromper operações nas empresas, indústrias, cadeias de suprimento e nações, custando bilhões de dólares à economia nos mais diversos setores. A dura realidade que as organizações devem enfrentar é que o ciberrisco não pode ser eliminado. Portanto, ele deve ser gerenciado por meio de algumas ações, como identificação, mitigação e transferência.

O Global Cyber Risk Perception Survey Marsh-Microsoft 2019 investiga as percepções de ciberriscos e gestão de riscos em empresas de todo o mundo. A análise sobre a América Latina e o Brasil (partes da pesquisa global) reflete o status das percepções sobre o risco cibernético e seu gerenciamento nas organizações de nossa região, especialmente nesse contexto de um ambiente de negócios em rápida transformação. Nossas descobertas se concentram em cinco conceitos importantes que destacam o estado do risco cibernético no cenário empresarial atual:

1. Na América Latina e no Caribe (LAC), a preocupação das empresas com os ciberriscos e a confiança em suas próprias capacidades de geri-los aumentaram, em comparação com 2017.

2. Tanto a nível mundial quanto na América Latina, as empresas dão maior prioridade a tecnologia e prevenção que dedicar tempo, recursos e atividades necessárias para construir uma ciberresiliência.

3. Apesar de pouco mais de 1/3 dos respondentes afirmarem que o ciberrisco quase nunca seja um empecilho para a adoção de novas tecnologias, 29% responderam que seu nível de percepção de risco associado a essas tecnologias é muito alto.

4. A digitalização das cadeias de suprimentos traz benefícios, mas muitas empresas não dão a devida importância à interdependência de responsabilidades dentro da cadeia de suprimentos, principalmente as grandes corporações.

5. Existe uma incerteza sobre o valor tanto da legislação governamental como das normas da própria indústria acerca de cibersegurança. A maioria das empresas considera que ambas têm uma eficácia limitada. Ainda assim, as empresas demandam maior envolvimento e apoio do governo para combater as ciberameaças nacionais (internas e externas).

O Estudo de Percepção do Risco Cibernético na América Latina 2019 revela sinais animadores de uma melhora na percepção e gestão de riscos cibernéticos nas organizações. O ciberrisco é, agora, uma prioridade na pauta de riscos corporativos e podemos ver uma mudança positiva em direção à adoção de uma gestão mais rigorosa e abrangente em diferentes áreas. No entanto, várias organizações continuam empenhando-se, como podem, para articular, abordar e agir sobre o risco cibernético dentro de sua estrutura geral de riscos corporativos, mesmo quando a maré de mudanças tecnológicas traz preocupações novas e imprevistas.

Esperamos que este estudo ajude sua empresa a visualizar um panorama em constante evolução do risco cibernético. Incentivamos a todas as empresas a desenvolver estratégias de ciberresilência, abordando esse risco como uma ameaça crítica que, com monitoramento e aplicação das melhores práticas, pode ser gerida com confiança. Finalmente, agradecemos aos nossos clientes e, em geral, àqueles que compartilharam seus pontos de vista sobre este tema de grande importância.

Destaques do estudo

O Estudo de Percepção do Risco Cibernético na América Latina 2019 analisa como as empresas lidam com a ameaça crescente do ciberrisco, dentro de um ambiente de negócios altamente dinâmico, com transformações nos âmbitos de inovação tecnológica e interdependência. Os resultados mostram uma melhora, em comparação com 2017, em várias áreas relacionadas com a sensibilidade e as táticas para abordar os riscos cibernéticos.

Prioridade vs. confiança

O risco cibernético se fortaleceu como uma prioridade das empresas da América Latina, com 73% das organizações colocando essa ameaça entre as 5 principais preocupações. Além disso, a confiança das empresas em sua resiliência ao ciberrisco aumentou desde 2017. No entanto, um terço das organizações diz que não confia na sua resiliência cibernética.

- **73%** dos respondentes na América Latina classificaram o risco cibernético como uma das cinco principais preocupações para sua empresa, contra **47%** em 2017.
- O nível de confiança das empresas latino-americanas em sua própria capacidade para enfrentar o risco cibernético também aumentou em comparação com 2017, em cada uma das três áreas críticas de ciberresiliência.
  - De **16%** para **22%**, para compreender, avaliar e quantificar ciberameaças.
  - De **12%** para **20%**, para prevenir e mitigar ataques cibernéticos.
  - De **7%** para **18%**, para responder e recuperar-se de ciberataques.
- No entanto, **30%** das empresas disseram não confiar na resiliência em nenhuma das três áreas.
- No Brasil, **40%** dos respondentes disseram confiar amplamente em sua capacidade de gerir seus riscos cibernéticos.

Novas tecnologias

A inovação tecnológica é vital para a maioria das empresas. Mas isso inclui ainda mais complexidade ao ambiente tecnológico de uma organização, como o ciberrisco.

- **79%** das empresas pesquisadas disseram ter adotado ou estão pensando em usar uma nova tecnologia.
- **49%** mencionaram que o risco cibernético quase nunca é um empecilho para a adoção de novas tecnologias.
- **28%** consideram que os benefícios das novas tecnologias superam os potenciais riscos para o negócio.
- **75%** avaliam os riscos cibernéticos antes de adotar novas tecnologias, enquanto 25% dizem que avaliam riscos após sofrer um ataque cibernético.

Cadeia de suprimentos

A crescente interdependência e digitalização das cadeias de suprimentos resultam em um maior risco cibernético para todas as partes. Porém, muitas empresas não se percebem como ameaças à cadeia de suprimentos e, muitas vezes, pensam estarem expostas aos riscos por causa de seus fornecedores.

- **37%** das empresas brasileiras percebem os riscos de sua cadeia de suprimentos.
- Apenas **21%** pensam que sua própria organização representa risco à sua cadeia de suprimentos, no Brasil.
- Os entrevistados foram mais propensos a estabelecer padrões mais altos em suas organizações do que para com seus fornecedores.

Papel do governo

As empresas brasileiras acreditam que a regulamentação do governo e os padrões do setor têm eficácia limitada para ajudar a gerenciar o risco cibernético, com a exceção notável de ataques gerados pelo governo.

- **35%** acreditam que leis e regulamentações ajudam a melhorar o posicionamento da empresa em cibersegurança.
- **44%** se dizem muito preocupadas com ciberataques do estado.
- **44%** defendem que o governo deve fazer mais para proteger as empresas de ciberataques.

Cultura de segurança e resiliência cibernética

Muitas empresas estão concentrando seus investimentos em cibersegurança em ferramentas de proteção, deixando outras áreas de gerenciamento de riscos que criam resiliência cibernética desprotegidas, como a avaliação e transferência de riscos, assim como os planos de resposta a incidentes.

- Na América Latina:
  - **88%** dos respondentes dizem que a área de TI/segurança da informação é a principal responsável pelo gerenciamento de riscos cibernéticos.
  - A figura do gerente de riscos, como peça-chave na gestão de ciberriscos, passou de **17%** em 2017 para **46%** em 2019.
  - **33%** das empresas disseram usar métodos quantitativos para avaliar sua exposição ao risco, um aumento considerável em relação a 8% em 2017.
- No Brasil:
  - **70%** dos respondentes pretendem investir em tecnologia de cibersegurança nos próximos 3 anos.
  - **68%** disseram que um ataque cibernético em sua empresa seria o principal propulsor para aumentar investimentos na gestão de ciberriscos.
  - **41%** das organizações dizem que a adoção de novas tecnologias ajudará a gerar um maior investimento em segurança cibernética.
  - **65%** esperam investir mais nos próximos anos em capacitação de pessoal para lidar com riscos cibernéticos.

Seguro Cyber

A cobertura do seguro cyber está em expansão para enfrentar as ameaças em evolução e a percepção das empresas sobre ela.

- **29%** das empresas latinas, possuem seguro cyber, enquanto a média global é de **47%**.
- Na América Latina, a distribuição entre as empresas que compram seguro cibernético é a seguinte:
  - **40%** possuem renda superior a US$ 1 bilhão
  - **37%** com renda entre US$ 100 milhões e menos de US$ 1 bilhão
  - **22%** com renda inferior a US$ 100 milhões
- **52%** acreditam que o seguro cibernético cobre a totalidade ou grande parte das necessidades da empresa. Entretanto, **39%** dizem não saber se o seguro é uma ferramenta de proteção eficaz.
- **75%** das empresas que possuem seguro cyber confiam que suas apólices cobrirão o custo de um eventual incidente cibernético.

Risco cibernético: prioridade vs. confiança

Mais e mais empresas assumem o risco cibernético como prioridade. Tanto na América Latina como no Brasil, a confiança na ciberresiliência aumentou, mas, ainda assim, uma em cada três empresas não confia na resiliência.

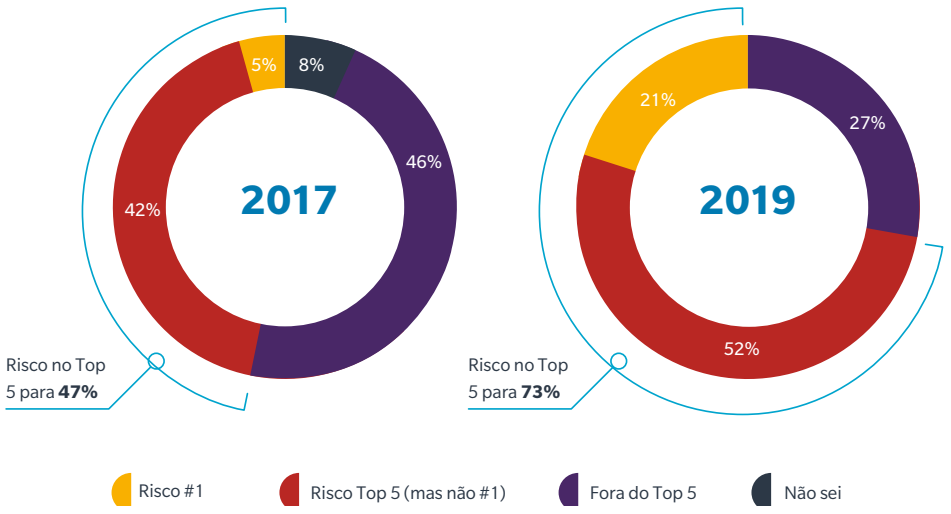
Aumenta a consciência sobre o risco cibernético

Impulsionados pela frequência e gravidade de incidentes, como WannaCry e NotPetya em 2017, os riscos e ameaças cibernéticos aumentaram significativamente entre as principais prioridades das organizações pesquisadas em 2019 (gráfico 1). No Brasil, **57%** das empresas classificaram o risco cibernético como uma das cinco principais preocupações de sua organização. O número de empresas latino-americanas que citam o risco cibernético como sua preocupação número 1 quadruplicou em dois anos, de **5%** a **21%**.

GRÁFICO 1

O risco cibernético aumentou consideravelmente entre as prioridades de riscos das empresas.

P. Entre as seguintes ameaças comerciais, classifique como o cyber aparece entre as 5 principais que mais preocupam a sua empresa.



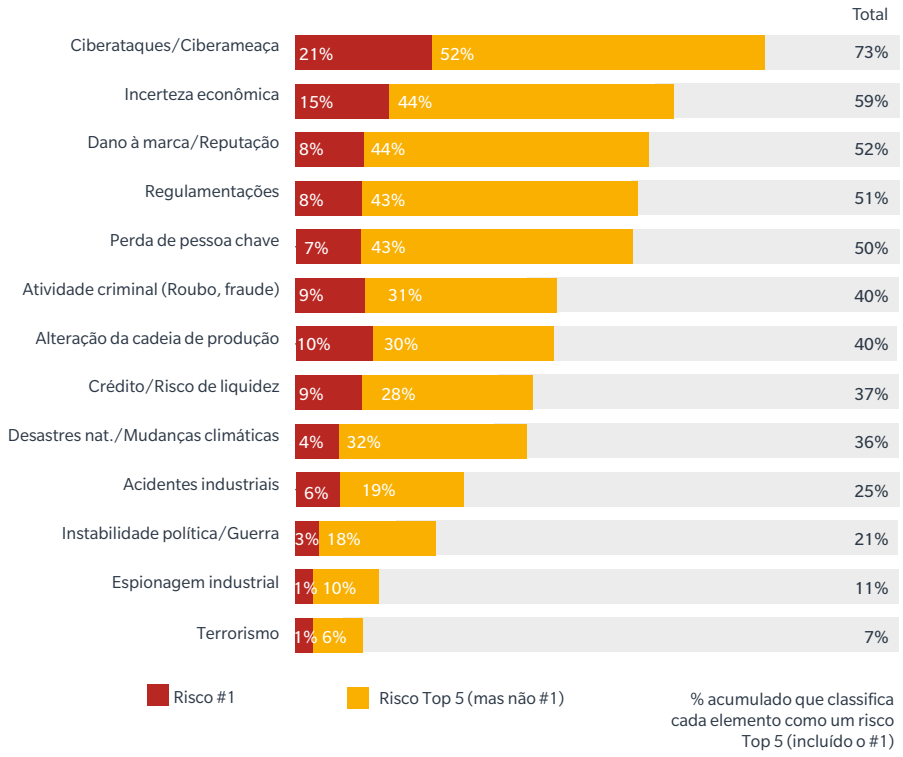
Em 2019, mais entrevistados classificaram o risco cibernético como uma de suas principais preocupações em comparação com outro importante risco comercial (gráfico 2). A incerteza econômica ficou em segundo lugar no Top 5, com **59%**, 14 pontos percentuais abaixo dos ataques e ameaças cibernéticos..

Esses resultados sugerem um aumento evidente da importância do risco cibernético e se correlacionam fortemente com outros estudos recentes. Por exemplo, o Relatório de Riscos Globais de 2019 do Fórum Econômico Mundial (WEF) classificou o roubo de dados e os ataques cibernéticos entre os cinco riscos mais frequentes a nível global.

GRÁFICO 2

O risco cibernético supera a outros riscos por uma ampla margem.

Entre as seguintes ameaças de negócio, classifique as 5 principais preocupações para sua organização.



A confiança cibernética aumentou

A pesquisa deste ano encontrou um aumento na confiança das empresas em cada área crítica da resiliência cibernética:

1. Entender, avaliar e medir os possíveis ciberriscos
   Identificando o tipo, a probabilidade e o impacto econômico potencial das ameaças às quais elas estão suscetíveis pelo uso de dados e tecnologias em suas operações.

2. Ser capaz de reduzir a probabilidade de ciberataques ou prevenir danos
   Compreende uma combinação de proteções técnicas e não-técnicas.

3. Administrar, recuperar e responder a incidentes cibernéticos
   Planos de contingência claros e bem ensaiados e recursos disponíveis facilmente para minimizar as consequências negativas e o tempo para recuperação de um incidente.

Em conjunto, estas áreas apresentam uma média geral da capacidade de recuperação de uma empresa: para superar um ciberataque, aplicar uma variedade de recursos de planejamento, avaliação, prevenção, mitigação e resposta para gerenciá-lo, além do retorno ao normal das operações com tempo de inatividade e perdas mínimos. Eles se alinham à amplamente utilizada estrutura de cibersegurança do Instituto Nacional de Padrões e Tecnologia (NIST) para detectar, impedir, responder e recuperar.

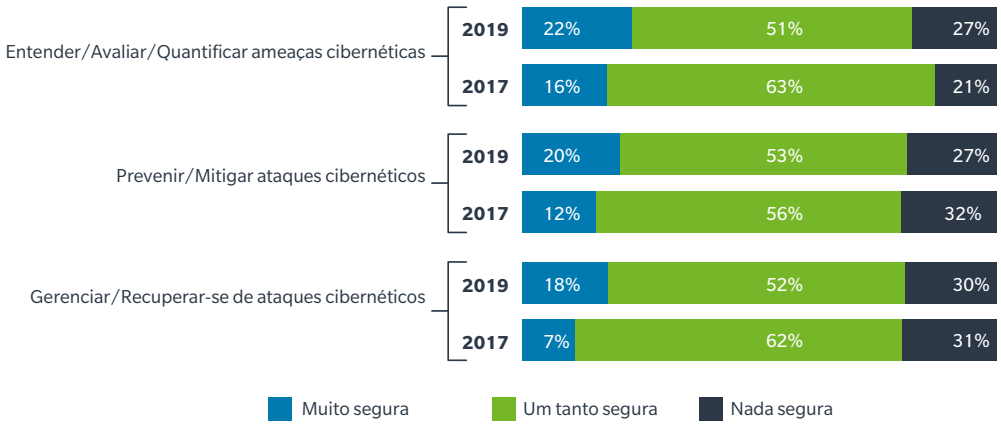
Em 2019, **40%** disseram confiar amplamente na sua capacidade atual de gerir os próprios riscos cibernéticos no Brasil. Já na América Latina, o aumento mais significativo foi relacionado à confiança no gerenciamento, resposta e recuperação de um incidente cibernético, de **7%** para **18%**, em relação a 2017.

No entanto, uma em cada três empresas disse que não confiava na resiliência em todas as três áreas críticas. Isso reflete a necessidade de continuar trabalhando na detecção, prevenção, resposta e recuperação de ameaças ou ciberataques.

Essa total falta de confiança pode ser devida, em parte, ao fato de as organizações ainda não serem capazes de tornar tangível o resultado de seus crescentes investimentos em tecnologia de cibersegurança: produtos e serviços destinados a prevenir ou mitigar ataques cibernéticos. Prevê-se que o mercado global de segurança cibernética ultrapasse US$ 124 bilhões em 2019, mas, apesar do aumento nos gastos com segurança cibernética, o custo anual de crimes cibernéticos é estimado em US$ 1 trilhão.

GRÁFICO 3

A confiança nas medidas de resiliência cibernética melhorou em geral de 2017 a 2019.



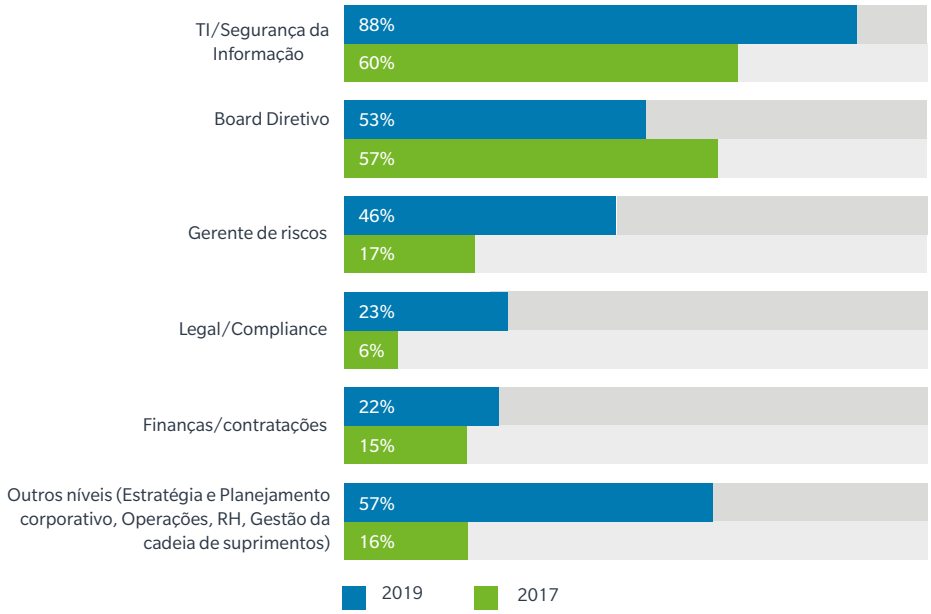
A governança cibernética ainda é delegada à área de TI e segurança da informação

A responsabilidade pelo gerenciamento do risco cibernético está principalmente na área de TI e segurança da informação e aumentou significativamente (28%) nos últimos dois anos: 9 em cada 10 empresas identificaram essa área como o principal responsável pelo risco cibernético em 2019 (gráfico 4). Outro dos papéis que também tiveram um aumento em seu nível de responsabilidade dentro da organização foi o de gestor de riscos, que passou de **17%** (2017) para **46%** (2019). Esse aumento indica uma tendência clara e positiva sobre um maior posicionamento dos gestores de riscos. No entanto, é surpreendente que, ao invés de aumentar a responsabilidade dos conselhos administrativos, tenha diminuído **4%** desde 2017.

GRÁFICO 4

A equipe de TI segue como principal responsável da gestão de risco cibernético na maioria das empresas.

P: Classifique as três áreas que sejam os principais responsáveis pela gestão do risco cibernético.



% que identifica cada função como um dos principais responsáveis

Novas tecnologias aumentam a exposição aos cyber risks

As empresas estão abraçando a inovação tecnológica e a maioria não considera que o risco cibernético seja uma barreira. Mas a avaliação do risco e das novas tecnologias não é tão rigorosa e consistente como deveria ser.

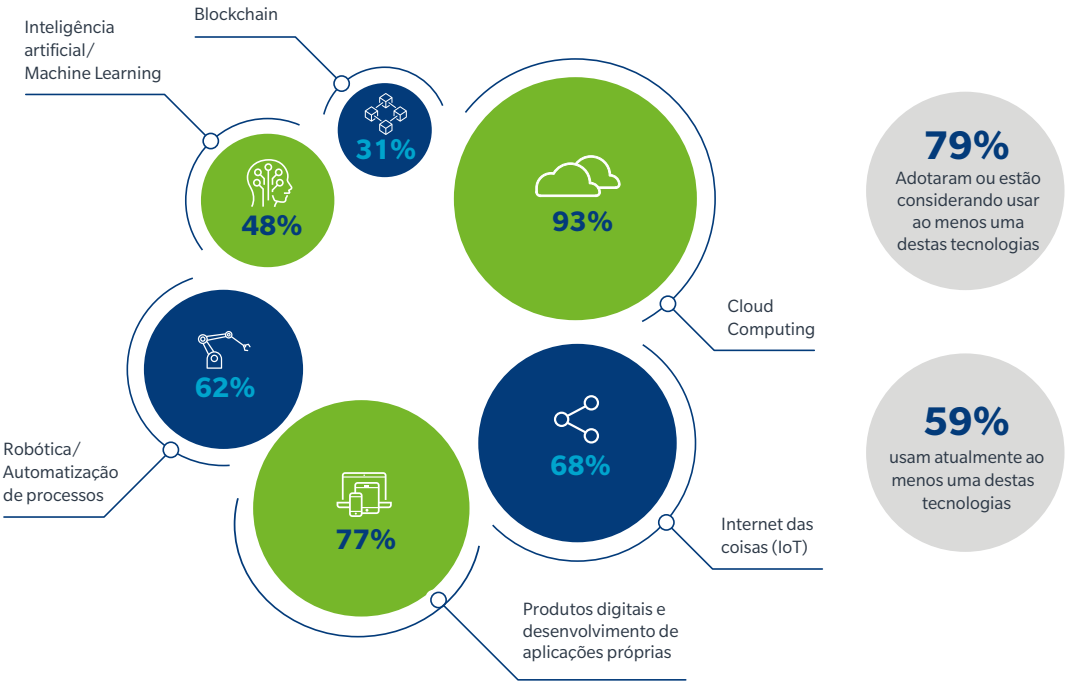
Estima-se que até 2025 a quantidade de dispositivos conectados à internet em todo o mundo seja de 75 bilhões. A medida que o mundo se aproxima de uma "internet de tudo", aumenta a quantidade e variedade de dados digitais armazenados, processados e compartilhados pelas empresas. Setores tradicionais da indústria, como a manufatureira, esperam que cerca de 50% dos produtos desenvolvidos sejam "inteligentes" ou "conectados" de alguma maneira até 2020, o que resultaria em novas fontes de receita em serviços baseados em dados.

Quase 80% dos entrevistados em 2019 citaram pelo menos uma tecnologia emergente (como nuvem, produtos digitais e dispositivos conectados/IoT) que eles adotaram ou estão considerando adotar (gráfico 5).

GRÁFICO 5

Uma boa parte das empresas usam ou estão considerando usar novas tecnologias.

P: Para cada uma das seguintes tecnologias, indique em que cenário considera o uso se aplica melhor a sua organização.



% de empresas que tem adotado ou estão provando/considerando cada tecnologia.

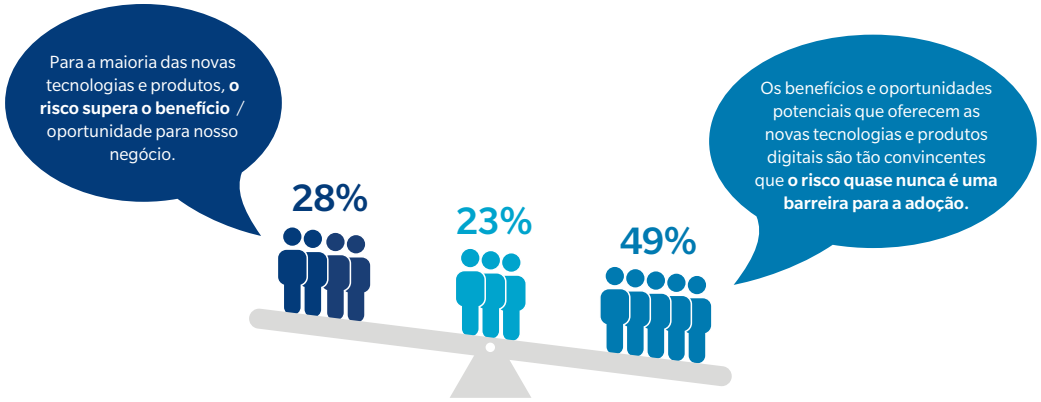
Os desafios para a segurança podem ser percebidos cada vez que uma nova tecnologia passa a fazer parte da infraestrutura corporativa, representando uma nova e adicional preocupação ao marco tecnológico. Riscos e exposições oferecidos pelas novas tecnologias devem ser pesados diante dos possíveis benefícios para o negócio e a tolerância ao risco varia de acordo com a indústria e a própria empresa. A metade dos entrevistados (49%) respondeu que o ciberrisco quase nunca é um empecilho à adoção de novas tecnologias (gráfico 6).

Apesar disso, 29% dos entrevistados mencionaram que a maioria das novas tecnologias apresenta riscos que superam os possíveis benefícios e oportunidades. Essa tendência ocorreu principalmente em pequenas empresas (aquelas com faturamento anual inferior a US$ 100 milhões), independentemente do setor.

GRÁFICO 6

Em geral, se considera que os possíveis benefícios das novas tecnologias superam os potenciais riscos.

P: Indique qual das seguintes declarações reflete melhor a atitude de sua organização.



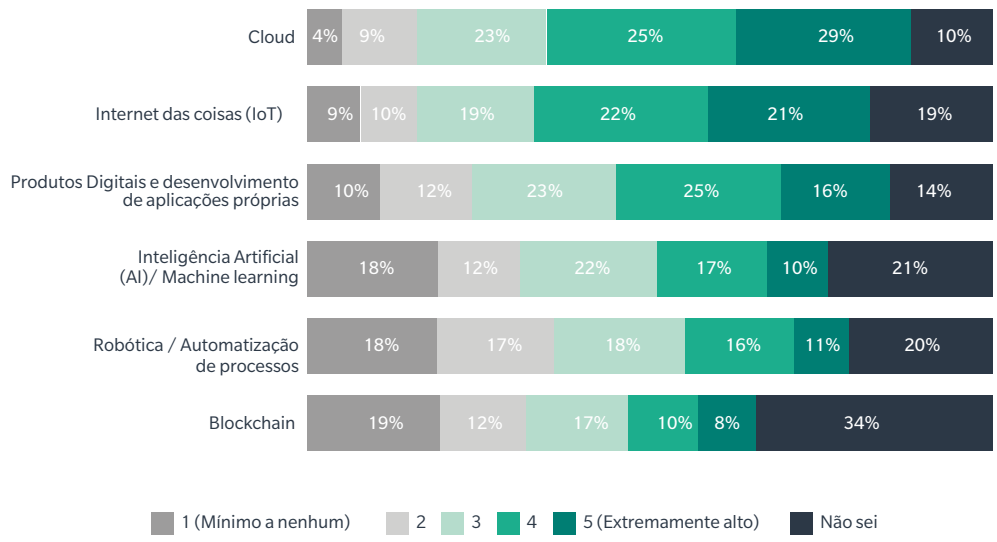
% de organizações que estão de acordo com alguma das declarações.

Apesar da predisposição para novas e emergentes tecnologias, há incerteza sobre o nível de risco associado a essas tecnologias (gráfico 7). Com relação ao nível de risco cibernético associado, a computação em nuvem teve a menor quantidade de respostas relacionadas à opção "não sei" (10%), enquanto que blockchain obteve a maior (34%). No caso de novos produtos ou aplicativos digitais em desenvolvimento, as opiniões foram divididas igualmente: aqueles que perceberam um alto nível de risco e aqueles que viram um nível mais baixo. O nível mais alto de incerteza foi relacionado às novas tecnologias blockchain (34%) e inteligência artificial (20%).

GRÁFICO 7

Muitos responsáveis pela tomada de decisões nas empresas não estão seguros do grau de risco que representam as novas tecnologias.

P: Qualifique o nível de ciberrisco associado com cada tecnologia, em uma escala de 5 pontos.



A maioria das empresas (75%) realiza avaliações de risco cibernético nos estágios iniciais de exploração e teste das novas tecnologias que serão implementadas em sua organização ou no final da compra dessa tecnologia. 60% realizam essa avaliação após a implementação da nova tecnologia ou quando ocorre um ataque/incidente cibernético (25%) (gráfico 8).

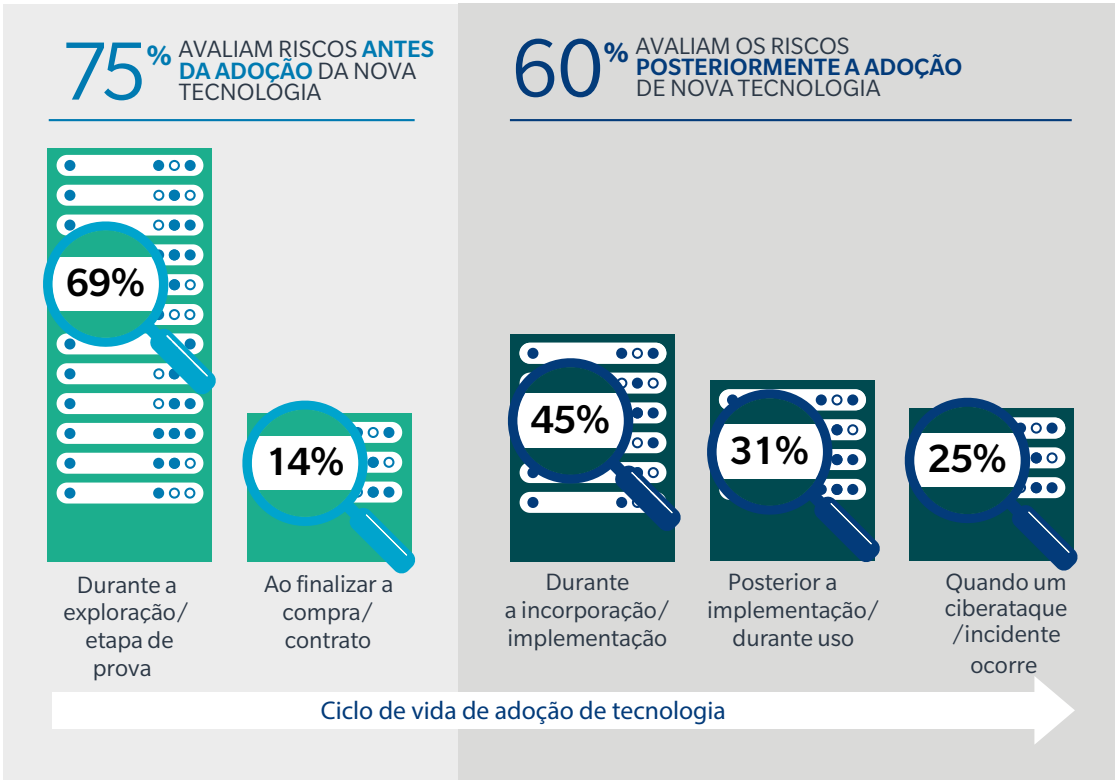
Quase metade das empresas da América Latina (42%) examina os riscos potenciais de uma nova tecnologia antes e depois de sua implementação. No entanto, apenas 2% avaliam o ciberrisco ao longo do ciclo de vida da tecnologia, o que inclui revisões periódicas além do estágio de adoção. É preocupante que 12% garantam que eles não realizem nenhum tipo de avaliação de risco cibernético, antes, durante ou após a implementação de uma nova tecnologia.

evaluación del ciber riesgo, antes, durante o después de implementar una nueva tecnología.

GRÁFICO 8

O risco cibernético se avalia mais durante as etapas de exploração ou provas da nova tecnologia.

P: Quando adota e implementa novas tecnologias, como as que acaba de identificar, em qual das seguintes etapas avalia o risco cibernético?



Apenas **42%** avaliam os riscos antes e depois da adoção

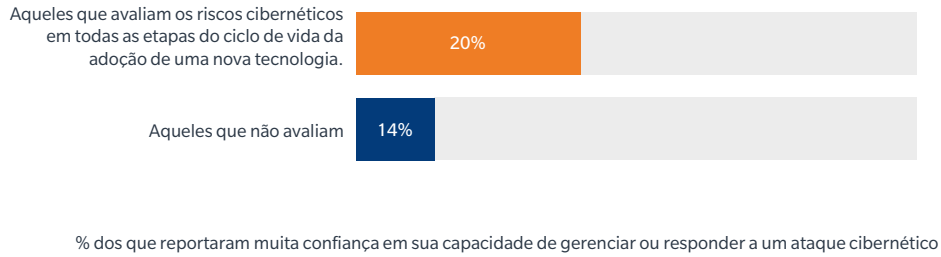
Apenas **2%** avaliam os riscos em todas as etapas do ciclo de vida

12% não avaliam em absoluto nenhuma etapa

O seleto grupo de empresas que avaliam riscos cibernéticos continuamente ao longo da implementação de novas tecnologias confiam mais em seus próprios recursos para gerenciar ou responder a ataques cibernéticos (gráfico 9).

GRÁFICO 9

As organizações que avaliam continuamente o risco cibernético das novas tecnologias temem mais confiança em sua cibersegurança geral.



As empresas que testam os riscos da tecnologia em vários estágios de implementação podem se sentir melhor informadas porque a avaliação contínua dos riscos fornece visibilidade em tempo real dos riscos e vulnerabilidades emergentes. Preparadas com o conhecimento oportuno de possíveis fraquezas ou exposições de segurança, elas estão prontas para implementar melhorias rapidamente e desenvolver planos de contingência para gerenciar os riscos envolvidos nesses sistemas.

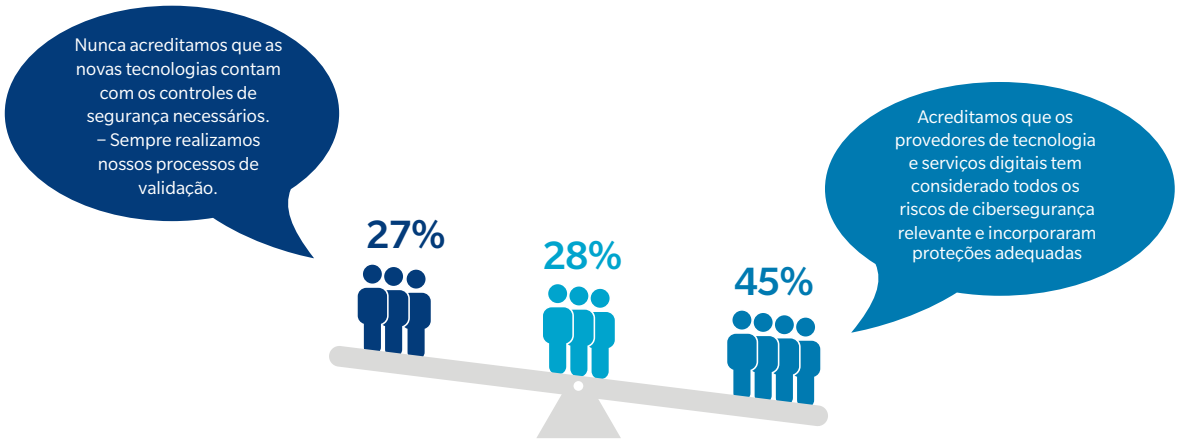
A avaliação de riscos cibernéticos de novas tecnologias está intimamente associada à confiança que as organizações têm, ou não, nos fornecedores que fornecem as tecnologias. Elas não devem representar necessariamente maior exposição se gerenciadas adequadamente. Algumas tecnologias podem adicionar novos riscos se não forem implementadas de acordo com os padrões de segurança ideais, mas em muitos casos, a segurança é integrada desde o início.

45% das empresas na América Latina assumem que seus fornecedores de tecnologia consideraram todos os riscos cibernéticos relevantes e que nenhuma verificação adicional é necessária. Apenas **27%** asseguram que "sempre realizam seu próprio procedimento" para verificar se as necessidades de segurança e as proteções integradas que os fornecedores de novas tecnologias estão completas (gráfico 10).

GRÁFICO
10

Quase a metade das empresas assume que os provedores de tecnologia tem considerado todos os riscos cibernéticos relevantes.

P: Indique qual das seguintes afirmações reflete melhor a atitude de sua organização.



% de empresas que estão de acordo com alguma das afirmações.

Cada empresa deposita um certo nível de confiança em seus relacionamentos com fornecedores e contratados. No entanto, dada a importância de plataformas e serviços tecnológicos para ativos e operações centrais, uma posição rigorosa de confiança e verificação deve ser assumida para ajudar a garantir a validade e adequação das proteções prometidas por terceiros. Essa maior vigilância é especialmente importante quando novos processos digitais são inerentes aos modelos de negócios das empresas.

37%

das empresas brasileiras percebem os riscos de sua cadeia de suprimentos

Risco no supply chain: rumo a uma responsabilidade social tecnológica

Nas cadeias de suprimentos digitais cada vez mais interdependentes, o risco cibernético deve ser uma responsabilidade coletiva.

Em um mundo de cadeias de suprimentos hiperconectadas, há uma necessidade crítica de confiança entre parceiros, já que a falta de confiança pode levar ao prejuízo do desempenho e da inovação dos negócios. Toda organização precisa entender, confiar e desempenhar um papel de igual importância na segurança dos componentes e softwares de suas cadeias de suprimentos digitais. O conceito de "responsabilidade social tecnológica" (o conhecimento e o reconhecimento de cada organização de seu papel e obrigações de segurança cibernética na cadeia de suprimentos) está na agenda de muitos líderes do setor.

No entanto, embora muitas organizações reconheçam os riscos potenciais que seus parceiros da cadeia de suprimentos podem representar para si, a maioria não vê. Há uma discrepância notável na visão de muitas organizações em relação ao risco cibernético: maior para os parceiros em comparação com o nível de risco que sua organização representa para eles.

Cerca de 1 em cada 3 entrevistados (34%) considera que a cadeia de suprimentos representa um risco alto para sua organização (gráfico 11). Enquanto que eles acreditam que há duas vezes mais chances de estarem vulneráveis aos riscos de seus parceiros do que em suas próprias cadeias de suprimentos.

GRÁFICO 11

Muitas organizações estão mais preocupadas de que se materialize um risco na cadeia de suprimentos por terceiros que por eles mesmos.

P: Que nível de risco cibernético representa para sua organização terceiros na cadeia de suprimentos? E ao contrário: que nível de risco representa sua organização para a cadeia de suprimentos?

% com respeito a cada risco como "alto" ou "muito alto"

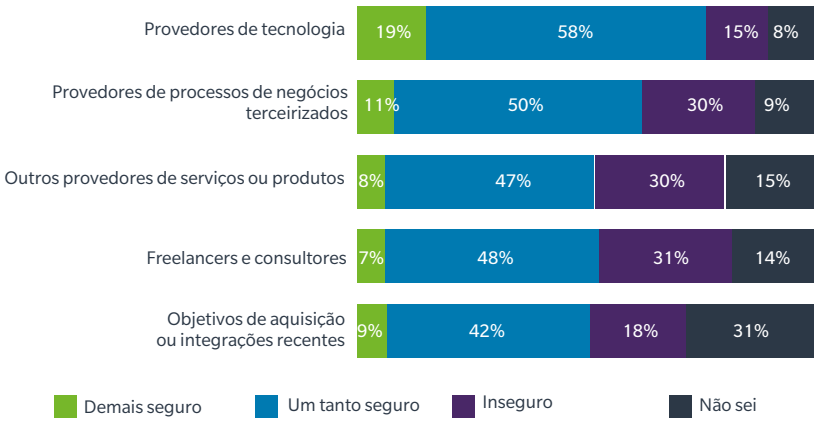
Em geral, **25%** *das empresas na América Latina disseram não confiar nem um pouco em sua capacidade de impedir ameaças cibernéticas de pelo menos um de seus parceiros*

A desconexão pode ser gerada pela baixa confiança das organizações em suas habilidades para prevenir ou mitigar os riscos cibernéticos derivados de seus stakeholders. A porcentagem de organizações que disseram ter "alta confiança" na mitigação das ameaças cibernéticas de seus parceiros da cadeia de suprimentos variou entre 8% e 19%, dependendo do tipo de fornecedor (gráfico 12). No geral, 25% disseram que "não confiavam em nada" em sua capacidade de impedir ameaças cibernéticas de pelo menos um dos fornecedores.

GRÁFICO 12

Poucas empresas confiam muito em sua capacidade para gerenciar o risco cibernético de terceiros.

P: O quão seguro está da capacidade de sua organização para prevenir/mitigar o risco cibernético dos seguintes:



% de empresas que reportam diferentes níveis de confiança

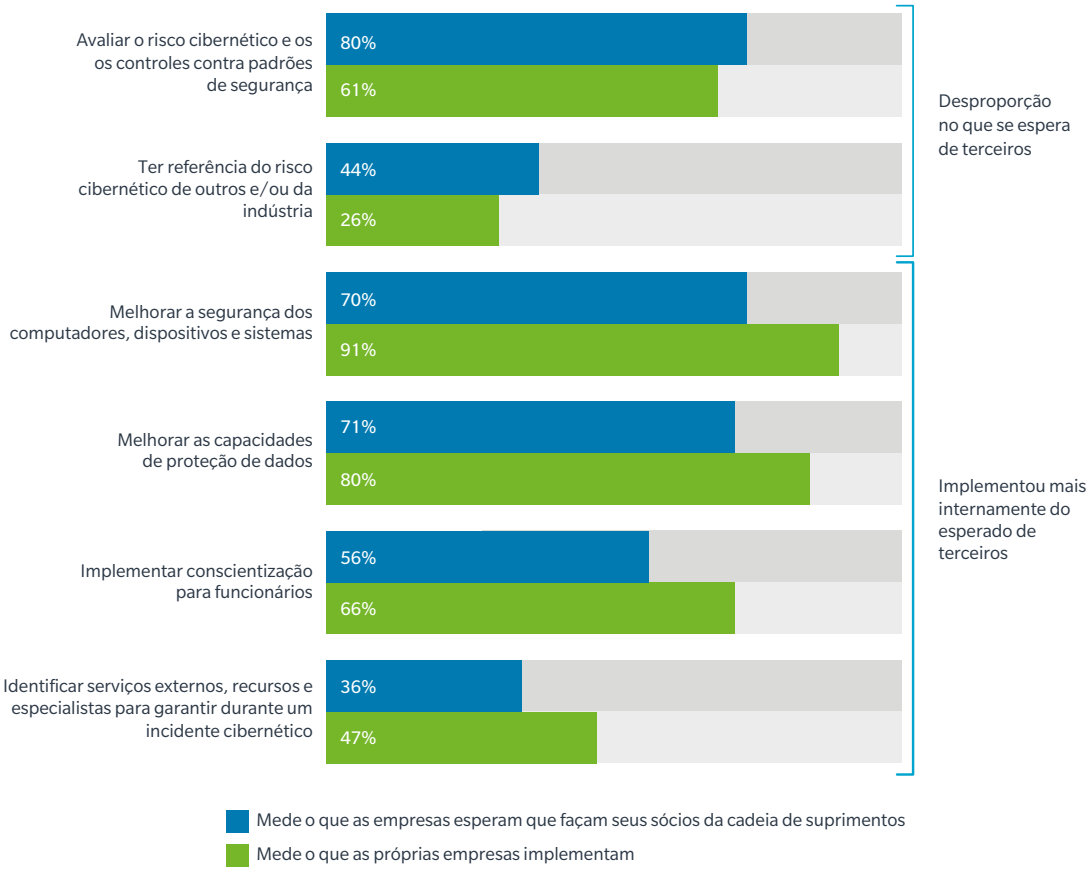
Há também uma disparidade entre medidas e padrões de cibersegurança que as organizações aplicam a si mesmas, em comparação com o que elas esperam dos seus fornecedores (gráfico 13). No geral, os entrevistados foram mais propensos a estabelecer medidas mais exigentes de gerenciamento de riscos cibernéticos em sua própria organização do que em seus fornecedores.

Por exemplo, 56% das organizações disseram esperar que os fornecedores de suas cadeias de suprimentos digitais implementem medidas de conscientização para seus funcionários. Por outro lado, 66% dos entrevistados disseram que sua organização implementou esse requisito internamente. Tais disparidades podem levar as organizações a pensar que seus fornecedores estão menos preparados para gerenciar riscos cibernéticos do que eles, o que diminui a confiança da empresa em sua cadeia de suprimentos.

GRÁFICO 13

Existe uma disparidade entre as medidas que as organizações esperam de si mesmas e as esperadas de terceiros.

P: Que medidas de cibersegurança espera que seus sócios tomem / terceiros da cadeia de suprimentos? Indique se sua organização tem tomado as ações específicas que se enumeram a seguir.



Opiniões divididas sobre o papel do governo

As empresas veem uma eficácia limitada da regulamentação governamental para ajudar a gerenciar o risco cibernético, mas desejam receber ajuda com desafios cibernéticos que não podem resolver sozinhas.

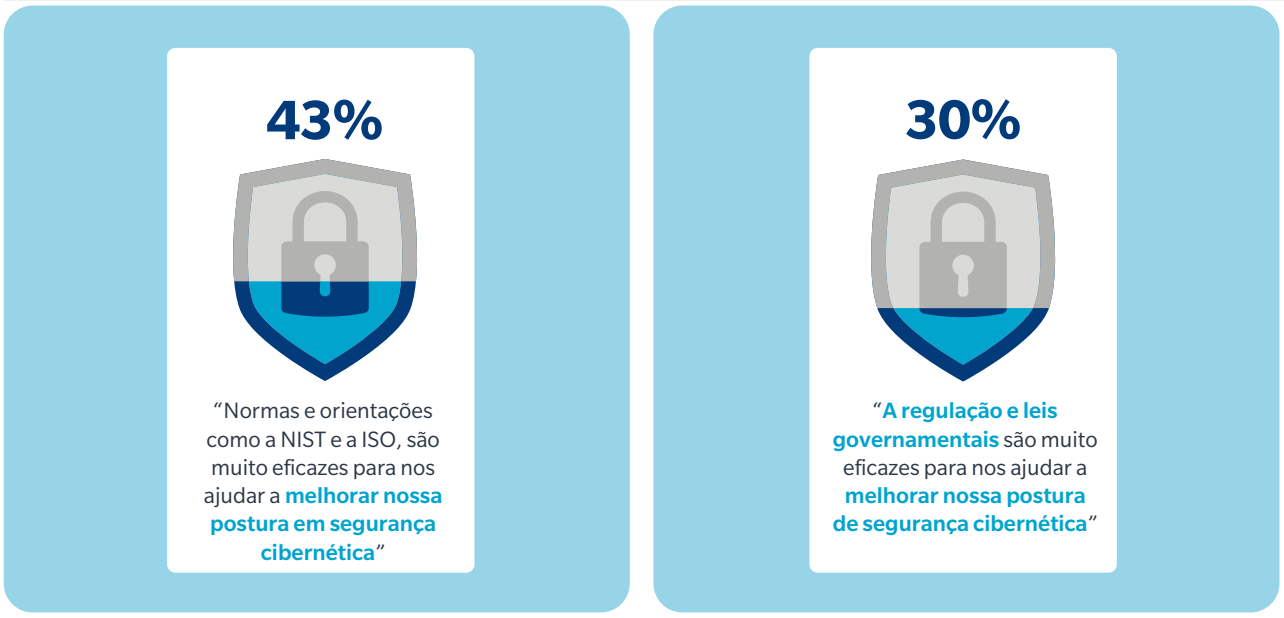
Nos últimos anos, os reguladores globais adotaram inúmeras medidas para tornar as empresas e os executivos mais diretamente responsáveis por uma segurança cibernética eficaz e manter os dados dos clientes em segurança. Muitos desses regulamentos e estruturas legais exigem um maior grau de transparência das organizações em todos os níveis de suas atividades de gerenciamento de dados e na preparação para o gerenciamento de riscos cibernéticos. O aumento de tais regulamentos complementa um conjunto de padrões para computadores e cibersegurança, estabelecidos por órgãos internacionais reconhecidos, como o NIST e a Organização Internacional para Padronização (ISO).

Em geral, as organizações latinas consideram que os padrões internacionais da indústria, que podem ser implementadas voluntariamente, são mais eficazes do que os regulamentos governamentais para ajudá-los a melhorar suas estratégias de segurança cibernética: 43% vs. 30% (gráfico 14).

GRÁFICO 14

Menos da metade das empresas na América Latina consideram que as leis governamentais ou as orientações da indústria são eficazes para melhorar a segurança cibernética.

P: Para cada uma das seguintes declarações, selecione uma ou mais opções que refletem na opinião de sua empresa.



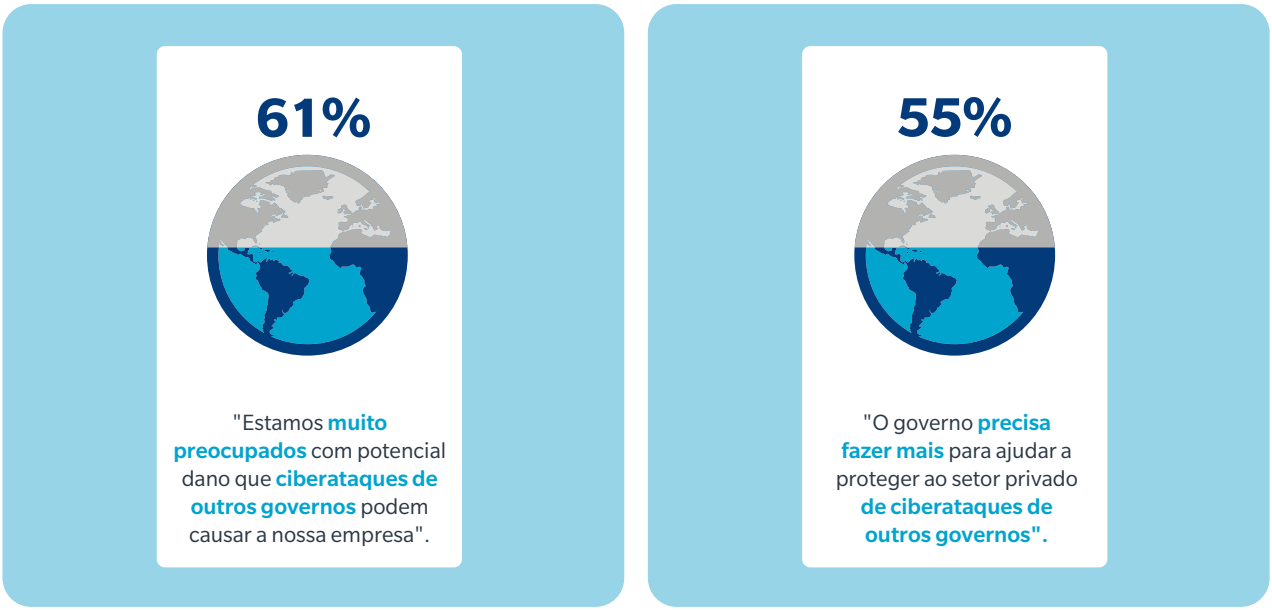
A principal diferença na atitude em relação à regulamentação cibernética está relacionada a ataques cibernéticos originados pelos próprios governos, sejam nacionais ou internacionais (gráfico 15). Nesse contexto, a maioria dos entrevistados (61%) disse estar muito preocupada com o impacto desse tipo de ataques cibernéticos.

De acordo com o exposto, 55% das organizações disseram que é necessário que os governos façam mais para proteger empresas privadas contra ataques cibernéticos originados por esses agentes, algo que acontece não apenas na América Latina, mas é uma constante no mundo inteiro. Esses resultados mostram que, embora as empresas geralmente prefiram uma abordagem independente para gerenciar seus problemas de segurança cibernética e de risco cibernético, em relação aos ataques governamentais, há uma clara exceção.

GRÁFICO 15

Empresas que buscam ajuda governamental para enfrentar ataques de outros governos.

P: Para cada uma das seguintes declarações, selecione uma ou mais opções que refletem na opinião de sua empresa.



Cultura de segurança e resiliência cibernética

O gerenciamento eficaz de riscos cibernéticos requer uma avaliação quantitativa de risco. Embora cada vez mais empresas latino-americanas meçam seus riscos cibernéticos economicamente, ainda há um longo caminho para todas as organizações adotarem essa prática e aplicarem essa quantificação para tomar decisões sólidas de investimento em ciberriscos.

Os investimentos em tecnologia de cibersegurança estão aumentando rapidamente e excedendo em muito os gastos com seguros cyber. Estima-se que o mercado global de seguros cibernéticos, medido pelo volume de prêmios emitidos, seja de aproximadamente US$ 8 bilhões em 2020, em comparação com um mercado global de segurança cibernética de US$ 124 bilhões.

Muitas organizações concentram sua estratégia de gerenciamento de ciberriscos na prevenção, investindo em defesa cibernética com tecnologia de ponta. Enquanto isso, os gastos com outras ferramentas e recursos para gerenciamento de riscos cibernéticos, como seguro ou treinamento em resposta a incidentes, continuam sendo uma fração do orçamento destinado à tecnologia. Isso sugere que muitas organizações continuam acreditando que podem eliminar ou mitigar seus riscos cibernéticos por meio da tecnologia e não mediante uma ampla gama de medidas de planejamento, transferência e resposta.

As melhores práticas não exigem a igualdade de gastos, mas uma estratégia de investimento que, refletindo o perfil de risco e as necessidades de uma organização, aproveite as funções complementares de tecnologia e seguro para impedir ataques cibernéticos sempre que possível e transferir riscos que não podem ser evitados. No entanto, a ênfase nos gastos em tecnologia de cibersegurança em detrimento de outras medidas revela que muitas empresas ainda não aceitaram essa verdade.

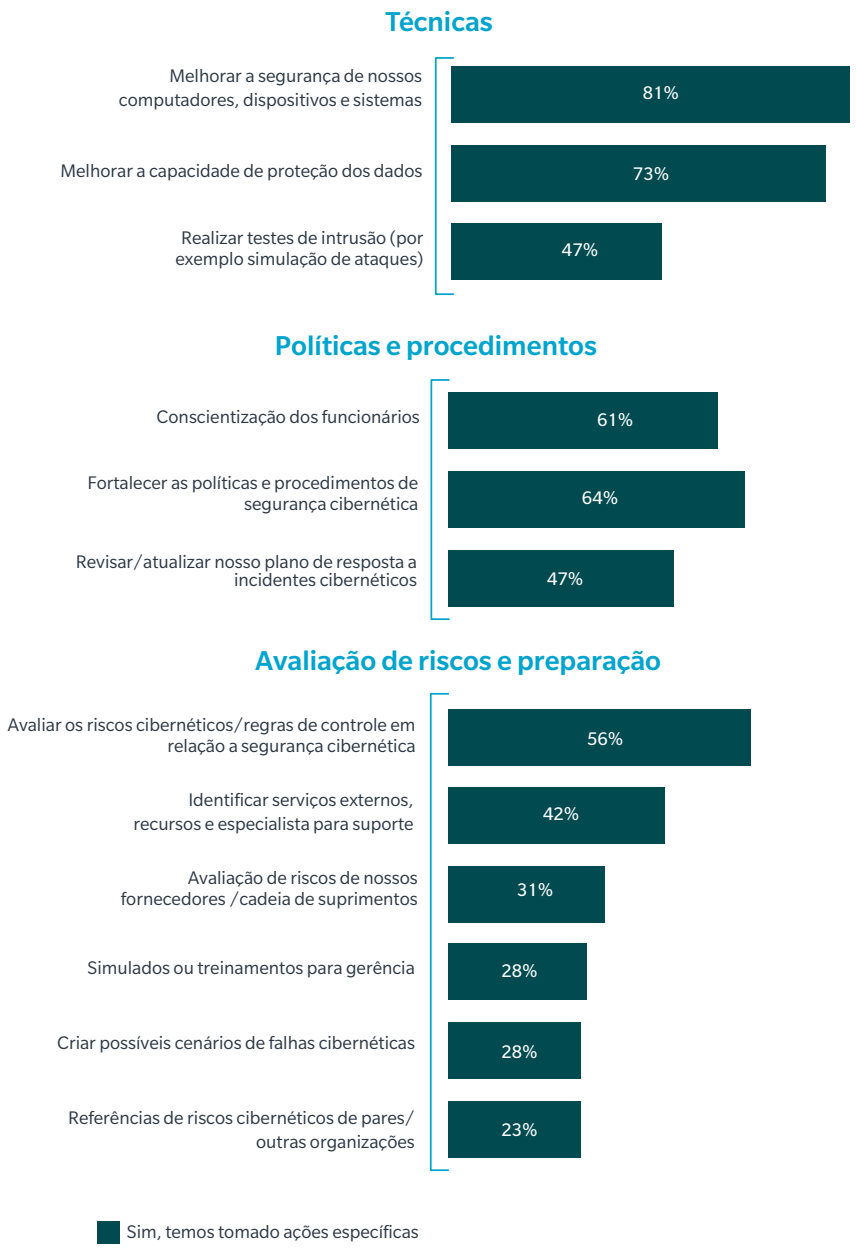
Por exemplo, a maioria dos entrevistados assegurou ter implementado uma ou mais melhorias técnicas nos últimos 12 ou 24 meses (gráfico 16). No entanto, foram tomadas menos iniciativas relacionadas a treinamento/conscientização dos funcionários ou a planos de resposta a incidentes cibernéticos.

Em geral, algumas das ações relatadas com menos frequência foram as que estão relacionadas à avaliação e modelagem de riscos cibernéticos. É preocupante que o fato de apenas 28% terem declarado ter trabalhado na modelagem de cenários de possíveis perdas antes de um ataque cibernético ou incidente ou no treinamento de seus líderes.

GRÁFICO 16

As ações de resiliência cibernética costumam focar em medidas técnicas.

P: Indique se sua organização realizou algumas das seguintes ações nos últimos 12/24 meses.

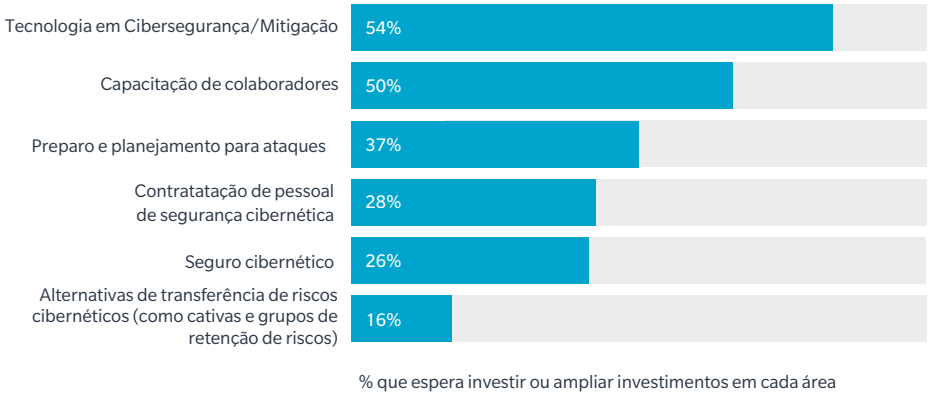


Olhando para o futuro, tudo indica que essas tendências continuarão. Entre as áreas em que as empresas planejam aumentar os gastos com gerenciamento de riscos nos próximos três anos, mais da metade citou a tecnologia / mitigação de segurança cibernética, muito mais do que em todas as outras áreas (gráfico 17). No entanto, é encorajador que o treinamento seja uma das áreas em que se planeja um maior investimento.

GRÁFICO 17

Os investimentos em gestão de riscos estão centrados em tecnologias de cibersegurança e mitigação.

P: Como espera que seja a evolução dos investimentos nas seguintes áreas de gestão de riscos nos próximos três anos?

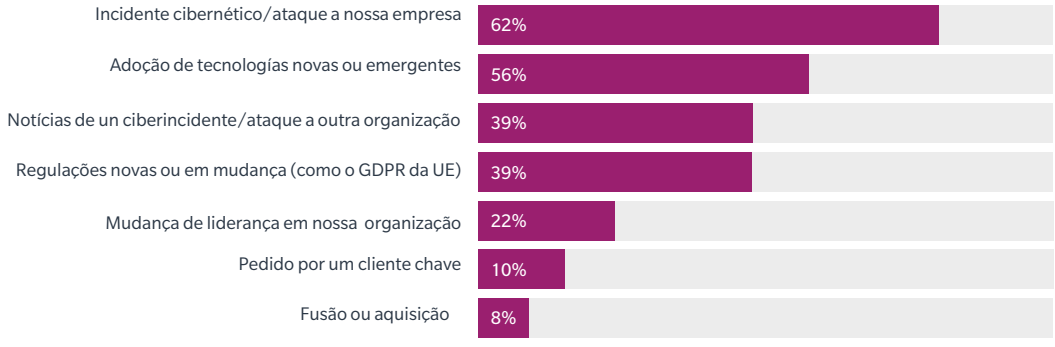


Embora o aumento do investimento em tecnologia seja uma boa notícia, é preocupante que essa despesa não seja acompanhada por um aumento correspondente no uso de estruturas econômicas (como a quantificação do risco cibernético) que permitem uma melhoria na tomada de decisões sobre investimento. É absolutamente crucial que as organizações possam medir a eficácia da redução de riscos ou permitam a comparação com outros investimentos em riscos corporativos. De fato, muitas organizações parecem ter uma postura reativa em relação ao risco cibernético, uma vez que o fator mais citado no aumento do investimento foi um incidente cibernético (gráfico 18). Muito menos comum de acontecer são os líderes das empresas proativamente investirem nisso.

GRÁFICO 18

Os incidentes cibernéticos são o principal estímulo para o aumento do investimento na gestão de risco cibernético.

P: Que fator terá maior impacto para que se amplie o orçamento dedicado às seguintes áreas de gestão do risco cibernético?

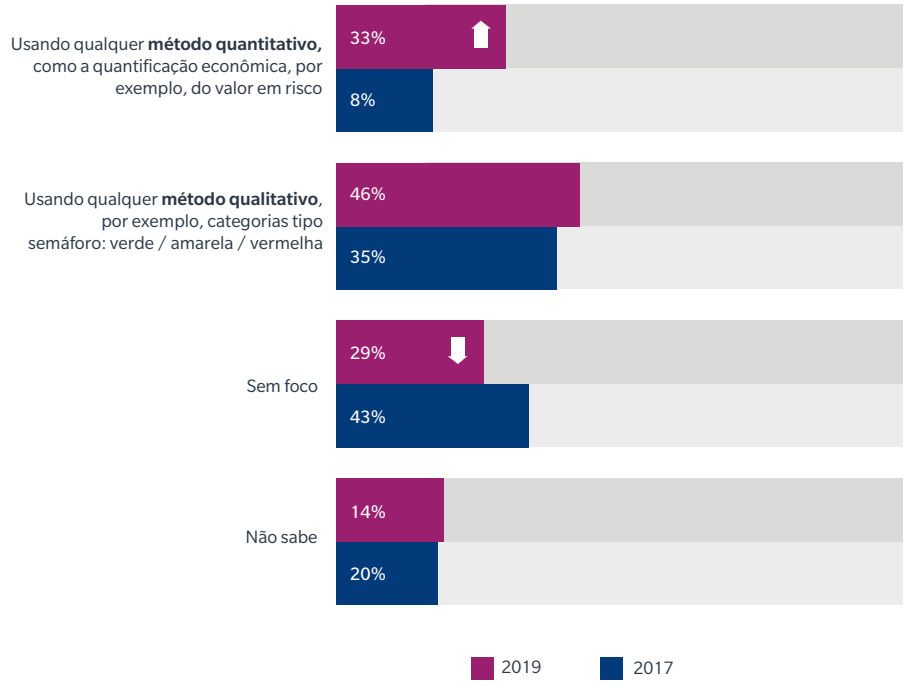


É animador comprovar o aumento no uso de métodos quantitativos para expressar exposições a riscos cibernéticos em nossa região (gráfico 19). A proporção de organizações latino-americanas que utilizaram esses métodos quadruplicou desde 2017, de 8% para 33%. No entanto, duas em cada três empresas (67%) não os utilizam. Por outro lado, a proporção de entrevistados que disseram não ter uma abordagem para avaliar formal ou sistematicamente sua exposição ao risco cibernético diminuiu: de 43% em 2017 para 29% 2019.

GRÁFICO 19

A medição quantitativa da exposição ao risco cibernético aumentou consideravelmente desde 2017, mas continuam baixas no geral.

P: A medição quantitativa da exposição ao risco cibernético aumentou consideravelmente desde 2017, mas continuam baixas no geral



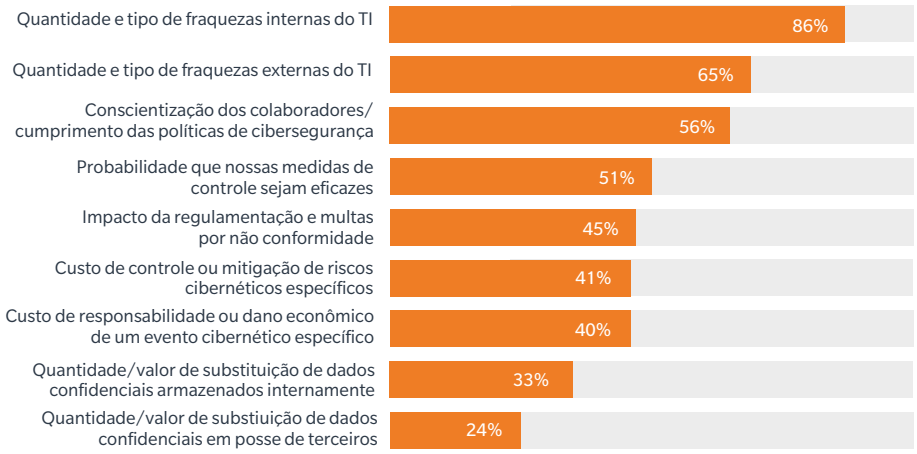
A maioria dos entrevistados em 2019 (67%) não expressou quantitativamente sua exposição a riscos cibernéticos ou usou dados quantitativos para orientar as decisões de investimento. Isso pode ser devido à falta de experiência organizacional em relação a essas metodologias, à falta de recursos (tempo e dinheiro) ou ao fato de muitas empresas continuarem a considerar as ameaças cibernéticas como um problema tecnológico mais que um risco econômico. Essa última posição é apoiada pelo fato de que mais do dobro das organizações avaliam o ciberrisco contando as vulnerabilidades dos sistemas em comparação com as que avaliam custos, multas e perdas em potencial (gráfico 20).

Além de como o risco cibernético é expresso, as áreas consideradas ao realizar avaliações também variaram bastante. As organizações que realizam alguma forma de avaliação de riscos cibernéticos tendem a se concentrar na contagem de vulnerabilidades técnicas, em vez de focar em custos de reparação ou recuperação, multas ou outras responsabilidades.

GRÁFICO 20

Os métodos de avaliação de riscos se concentram nas fraquezas técnicas, mas não consideram adequadas os aspectos econômicos da exposição cibernética.

P: Sua empresa considera quais das seguintes opções na avaliação/medição do risco cibernético

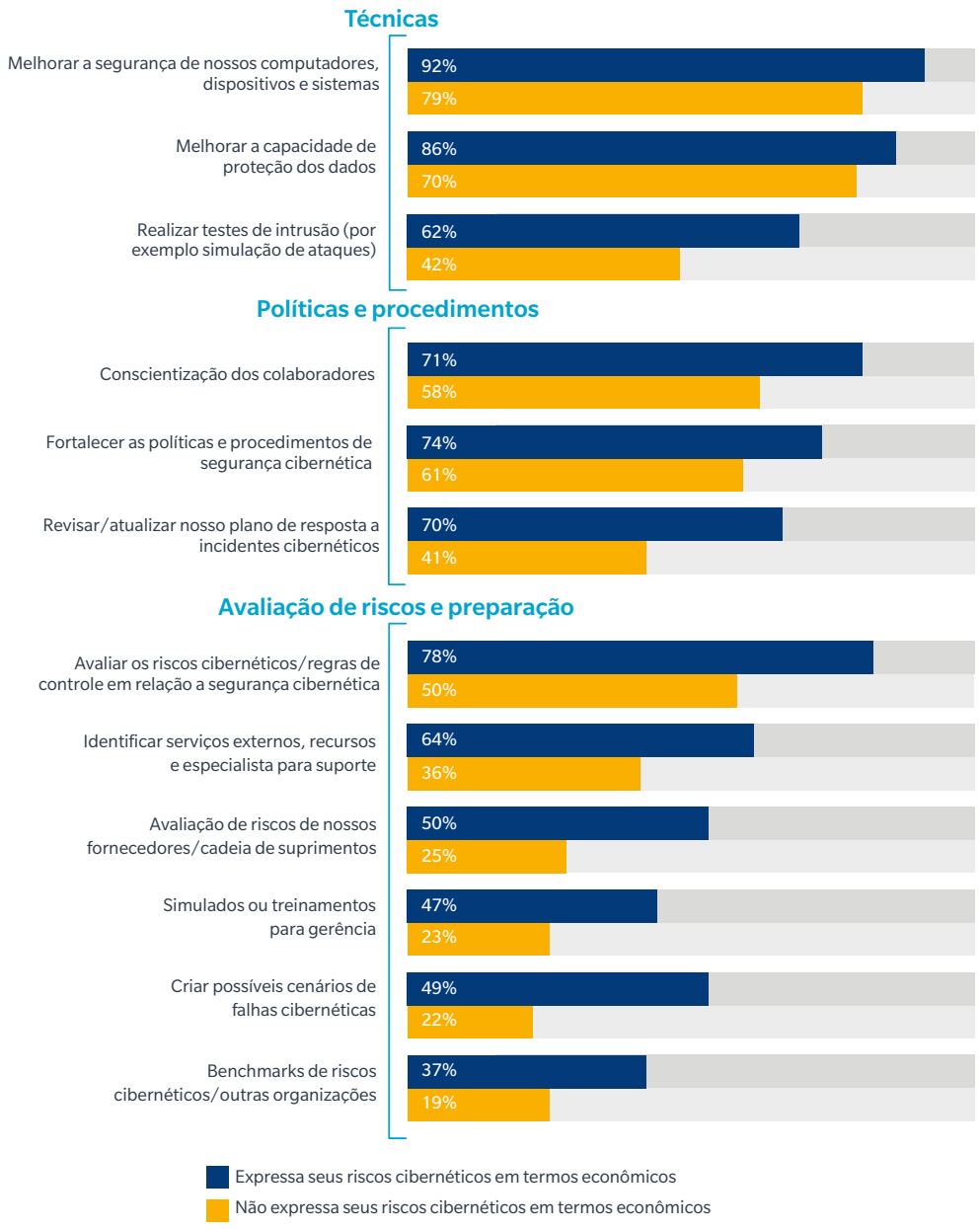


As organizações que expressam e relatam financeiramente os riscos cibernéticos tendem a implementar uma relação maior de atividades de avaliação, planejamento e treinamento que complementam medidas técnicas e são essenciais para o desenvolvimento de resiliência cibernética (gráfico 21). Isso envolve a transferência de riscos para o seguro, o estabelecimento de procedimentos e políticas e uma abordagem abrangente da avaliação desses riscos, incluindo de fornecedores e cadeias de suprimentos.

GRÁFICO 21

As empresas que realizam a quantificação econômica do risco cibernético tem mais probabilidade chances de equilibrar as ações técnicas e não técnicas.

P: Informe se sua empresa teve ações específicas nos últimos 12 a 24 meses, nas seguintes situações.



Seguro cibernético

Nem todos os riscos cibernéticos podem ser mitigados por meio de políticas corporativas ou tecnologia. Perdas de baixa frequência e alta intensidade podem impactar criticamente as finanças e operações de uma organização. Nesses casos, a transferência de risco por meio de seguro é essencial.

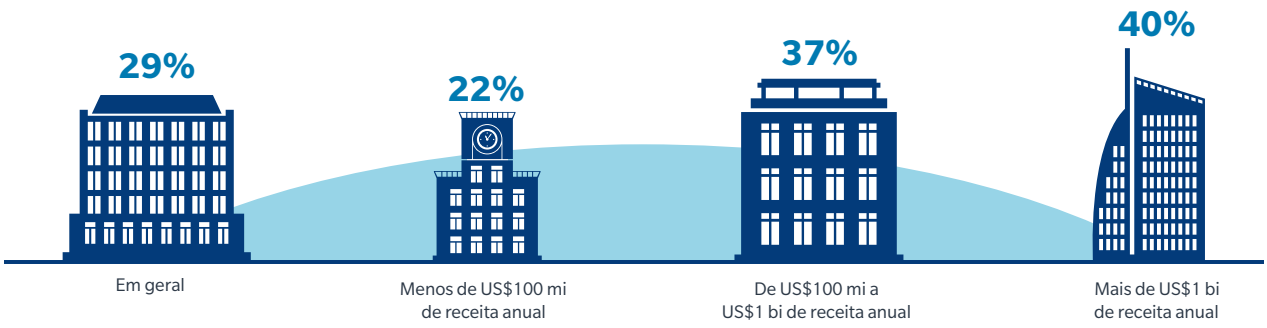
Na América Latina, 29% das empresas afirmam ter cobertura de seguro cyber (gráfico 22), em comparação com 47% da média global. No entanto, esse percentual varia de acordo com o tamanho da empresa: enquanto mais de um terço das organizações médias (37%) e grandes (40%) possui esse seguro, apenas 22% das pequenas empresas o compram. Da mesma forma, se compararmos esses números com os globais, nossa região ainda está longe dos níveis ideais de garantia.

Os investimentos em tecnologia de cibersegurança estão aumentando rapidamente e superando o gasto em seguro cyber. O mercado global desses seguros (medido em prêmios emitidos) é estimado em US$ 8 bilhões em 2020, em comparação com um mercado global de cibersegurança no valor de US$ 124 bilhões.

GRÁFICO 22

As médias e grandes empresas tem mais chances de possuir um ciberseguro

P: Como sua empresa se posiciona em relação ao seguro cibernético?

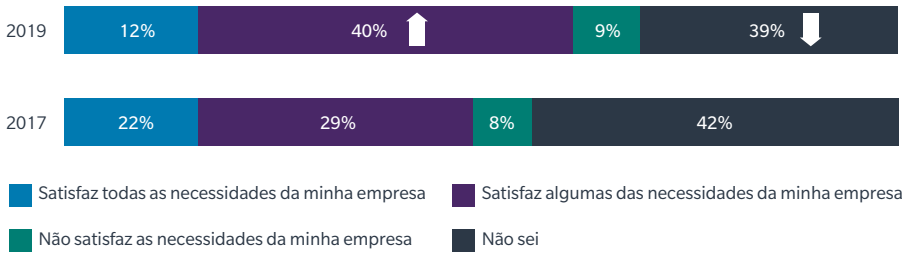


Desde 2017, a confiança das empresas na capacidade do seguro cibernético de protegê-las de alguma forma contra perdas de acidentes aumentou (40% vs. 29% em 2017). No entanto, se tomarmos o conjunto de empresas que garantem que sua cobertura atenda a todas ou algumas de suas necessidades de proteção cibernética, a confiança permanecerá estável (gráfico 23). O desafio para as seguradoras no futuro é aumentar a confiança de que o ciberseguro pode atender adequadamente todas as suas necessidades organizacionais, uma vez que esse percentual diminuiu em comparação com 2017 (12% vs. 22%).

GRÁFICO 23

A incerteza na capacidade de ciberseguro para satisfazer as necessidades de uma empresa diminuiu significativamente nos últimos anos.

P: Complete a sentença com uma das seguintes opções: O seguro cibernético disponível no mercado atual...

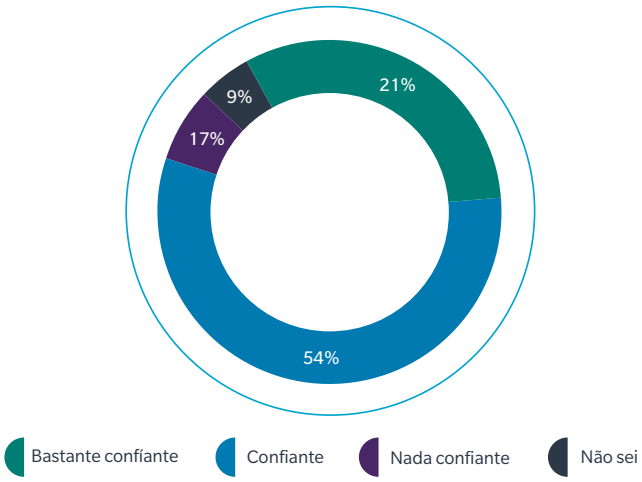


Uma em cada cinco empresas (21%) diz estar muito confiante na capacidade de resposta de suas apólices de seguro cibernético, o que, somado às que se sentem razoavelmente confiantes (54%), significa que podemos garantir que a maioria das organizações na América Latina se sente bem protegida com suas políticas atuais. No entanto, 17% disseram não confiar nessa capacidade de seguro (gráfico 24).

GRÁFICO 24

75% das empresas apresentam grande ou considerável confiança em que suas apólices de seguro cobririam todos os custos de um incidente cibernético.

P: Quão seguro está de que as coberturas do programa de seguros de sua empresa (apólices de riscos cibernéticos ou outras) cobrirão os custos em caso de um incidente cibernético?



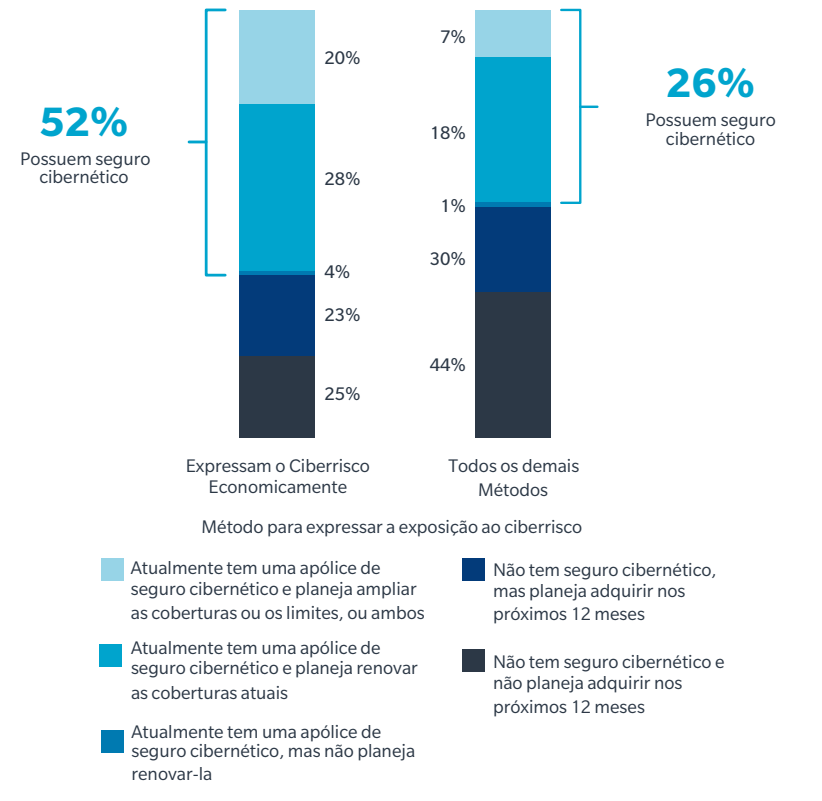
As empresas que usam métodos quantitativos de avaliação de riscos cibernéticos tendem a comprar mais seguro cibernético do que aquelas que usam apenas métodos qualitativos ou nenhum: 52% vs. 26% (gráfico 25). Isso acontece porque as primeiras estão mais informadas e dispostas a capitalizar o valor do seguro. Além disso, essas empresas garantem que planejam renovar (28%) ou expandir (20%) sua cobertura e/ou limites.

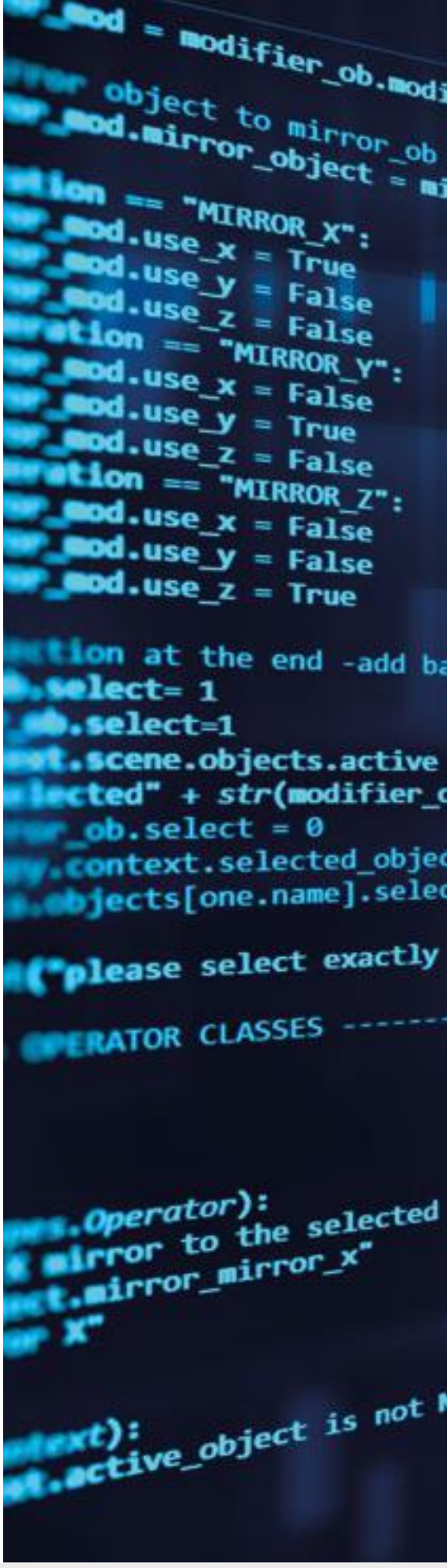
É preocupante que, em ambos os cenários, uma grande porcentagem de empresas ainda não tenha ou planeje comprar seguro: 25% entre as que quantificam economicamente o risco e 44% entre aquelas que utilizam outros métodos de avaliação.

GRÁFICO 25

As empresas que utilizam métodos econômicos de avaliação de riscos cibernéticos têm mais probabilidade de comprar seguro cyber e aumentar as coberturas atuais.

P: Como sua empresa se posiciona em relação ao seguro cibernético?





Conclusão

À medida que os riscos cibernéticos se tornam cada vez mais complexos e desafiadores, percebe-se que as empresas, lenta mas seguramente, estão começando a implementar as melhores práticas de gerenciamento ciberrisco. Quase todas as organizações pesquisadas reconhecem a magnitude do risco cibernético: muitas estão mudando aspectos de sua abordagem para enfrentar a ameaça e a maioria está fazendo um bom trabalho na segurança cibernética tradicional.

As organizações mais experientes estão desenvolvendo resiliência cibernética por meio de estratégias mais abrangentes e equilibradas para gerenciar os riscos, em vez de se concentrarem apenas na prevenção. Essas abordagens mais complexas explicam a necessidade de desenvolver recursos para entender, avaliar e quantificar os riscos cibernéticos em primeiro lugar, além de adicionar as ferramentas e os recursos para responder e se recuperar de incidentes cibernéticos quando eles ocorrem.

No entanto, a pesquisa deste ano mostra que permanece uma lacuna considerável entre a localização do risco cibernético na agenda corporativa e o nível geral de maturidade organizacional no gerenciamento de riscos. Muitas empresas em todo o mundo poderiam se beneficiar se aplicassem os princípios do gerenciamento estratégico de riscos à sua abordagem de ciberrisco, apoiadas por mais experiência, recursos e atenção dos membros da gerência à medida que desenvolvem resiliência cibernética.

Na era da Internet das Coisas (IoT), com cadeias de suprimentos digitalmente dependentes e tecnologia inovadora, as práticas e mentalidades de ontem não são suficientes e podem realmente inibir a inovação. Otimizar a segurança do "castelo" (a organização de mente fechada) para a comunidade em geral é mais difícil, mas inevitável. É fundamental uma mudança do foco exclusivo na segurança comercial para assumir a responsabilidade pela segurança em toda a cadeia de suprimentos.

Na prática, o estudo deste ano aponta para uma série de melhores práticas empregadas pelas empresas com maior resiliência cibernética e que todas as empresas devem considerar a adoção de:

- Criação de uma cultura de segurança cibernética organizacional forte, com padrões claros e compartilhados de governança, responsabilidade, recursos e ações.
- Quantificação do risco cibernético para tomar decisões de alocação de capital melhor embasadas, permitindo a medição do desempenho e enquadramento do risco nos mesmos termos econômicos que outros riscos comerciais.
- Avaliação das implicações do ciberrisco trazido pelas novas tecnologias como um processo contínuo e prospectivo ao longo de seu ciclo de vida.
- Gerenciamento do risco da cadeia de suprimentos como um problema coletivo, reconhecendo a necessidade de padrões de confiança e segurança compartilhados em toda a rede, incluindo o impacto cibernético da organização em seus parceiros.
- Procura e apoio a parcerias público-privadas em torno de problemas críticos de risco cibernético que possam fornecer proteções mais fortes e padrões básicos de boas práticas para todos.

Com o aumento da confiança organizacional na capacidade de gerenciar riscos cibernéticos, mais empresas reconhecem claramente a natureza crítica da ameaça e começam a buscar e adotar as melhores práticas. O gerenciamento eficaz de riscos cibernéticos requer uma abordagem abrangente que utilize avaliação, medição, mitigação, transferência e planejamento de riscos, e o programa ideal dependerá do perfil de risco exclusivo e da tolerância de cada empresa. Mesmo assim, essas recomendações abordam muitos dos aspectos comuns e mais urgentes do risco cibernético que as organizações enfrentam atualmente e devem ser vistas como sinais no caminho para a construção da verdadeira resiliência cibernética.

Metodologia

Este relatório é baseado em descobertas do Estudo de Percepção do Risco Cibernético na América Latina 2019 (como parte de um estudo global), realizada entre fevereiro e março de 2019.

No geral, 531 líderes de empresas latinas participaram da pesquisa, representando uma série de funções-chave, incluindo gerenciamento de riscos, tecnologia / segurança da informação, finanças, jurídico / compliance, diretores executivos e conselhos de administração.

Dados demográficos da pesquisa

Geografia

Onde os participantes da pesquisa estão	
Colômbia	34%
Brasil	18%
México	16%
Peru	12%
Argentina	8%
Outros	12%

Indústrias

Setores da indústria nos quais as empresas operam	
Manufatura/Automotiva	16%
Varejo/Atacado	11%
Instituições Financeiras	9%
Energy/Power	8%
Health Care/Life Science	7%
Transportes/Ferrovias/Marine	6%
Comunicações, Mídia and Tecnologia	5%
Professional Services	5%
Real Estate	4%
Química	4%
Infraestrutura	4%
Educação	4%
Entidades Públicas/Sem fins lucrativos	4%
Mineração/Metais/Minerais	2%
Aviação/Aerospacial	1%

SOBRE A MARSH

Marsh é a principal corretora de seguros e consultora de riscos do mundo. Com mais de 35.000 colaboradores operando em mais de 130 países, a Marsh atende clientes comerciais e individuais com soluções de risco orientadas a dados e serviços de consultoria. A Marsh é uma subsidiária integral da Marsh & McLennan Companies (NYSE: MMC), empresa líder global de serviços profissionais nas áreas de risco, estratégia e pessoas. Com receita anual superior a US$ 15 bilhões e 75.000 colaboradores em todo o mundo, a MMC ajuda os clientes a navegar em um ambiente cada vez mais dinâmico e complexo por meio de quatro empresas líderes de mercado: Marsh, Guy Carpenter, Mercer e Oliver Wyman. Siga a Marsh no Twitter @MarshGlobal, LinkedIn, Facebook e YouTube, ou assine *BRINK*.

SOBRE A MICROSOFT

A Microsoft (Nasdaq "MSFT" @microsoft) permite a transformação digital para a era de nuvem com vantagem inteligente. Sua missão é capacitar todas as pessoas e organizações do planeta para alcançar mais. A equipe de Diplomacia Digital da Microsoft, que fez parceria com Marsh neste estudo, combina conhecimento técnico e perspicácia em políticas públicas para desenvolver políticas que melhoram a segurança e a estabilidade do ciberespaço e possibilitam a transformação digital das sociedades em todo o mundo.

RECONHECIMENTOS

Marsh e Microsoft agradecem à B2B International por sua ajuda na criação, análise e relatório dos resultados desta pesquisa. A B2B International é a principal empresa de pesquisa de mercado business-to-business do mundo. É especializada no desenvolvimento de pesquisas de mercado personalizadas e programas de insight para algumas das principais marcas da indústria, financeiras e de tecnologia do mundo. A B2B International conta com 600 das 1.500 maiores empresas entre seus clientes. A B2B International faz parte da gyro, a agência criativa b2b dedicada à Dentsu Aegis Network.

Para mais informações sobre as soluções de gerenciamento de riscos cibernéticos da Marsh, acesse marsh.com.br ou entre em contato com seu representante Marsh Brasil:

Marta Helena Schuh (Líder de Riscos Cibernéticos)
+55 11 998 857 118
marta_schuh@jltbrasil.com

Para saber mais sobre as ofertas de segurança da Microsoft, visite www.microsoft.com/security.