PESQUISA INÉDITA

Riscos cibernéticos

A percepção das lideranças brasileiras e práticas adotadas



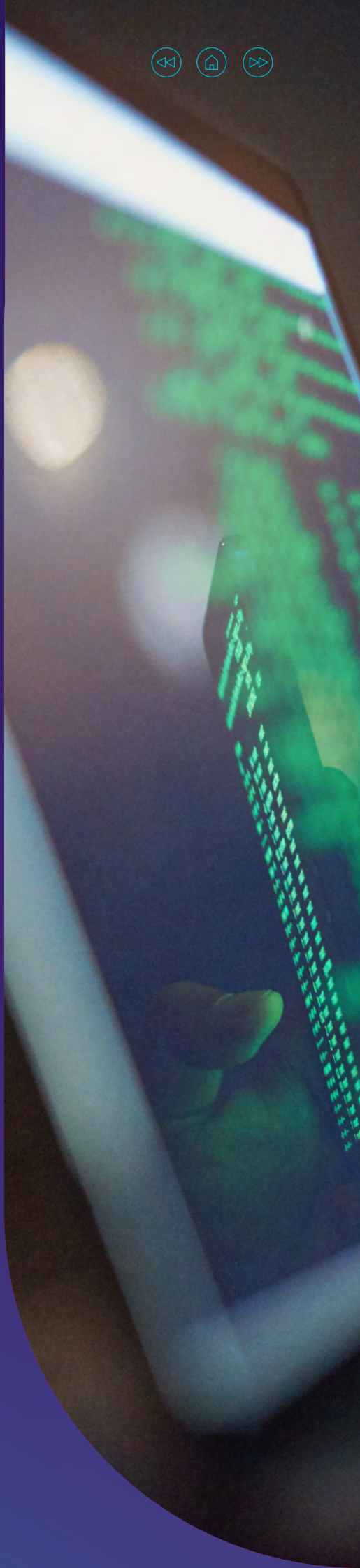
Realização:

Grant Thornton

Opice Blum

Conteúdo

Introdução	03
Resumo Executivo	04
Perfil dos respondentes	05
Risco cibernético entre as maiores preocupações	07
Avaliação de riscos para minimizar impactos	12
Medidas de prevenção de ataques cibernéticos	18
Resiliência Cibernética	21
Conclusão	32
Sobre a Grant Thornton	34
Sobre a Opice Blum Advogados	35
Autores	36



Introdução

A crescente digitalização das empresas trouxe novas oportunidades, mas também ampliou os riscos cibernéticos. Com ataques cada vez mais sofisticados e frequentes, a segurança digital se tornou um dos principais desafios das organizações.

Para entender como as empresas brasileiras percebem esses riscos e estão se preparando para enfrentá-los, a **Grant Thornton Brasil** e a **Opice Blum Advogados** realizaram esta pesquisa. Neste material é revelado como diferentes setores e portes de empresas compreendem a segurança cibernética, destacando principais ameaças, medidas adotadas e pontos de atenção.

Os dados apresentados servem como referência para que organizações avaliem suas estratégias e fortaleçam sua proteção contra incidentes digitais.

Realização:

Grant Thornton

Opice Blum

Resumo Executivo

A pesquisa contou com a participação de **248 profissionais de empresas brasileiras** e analisou a percepção dos riscos cibernéticos em diferentes setores e tamanhos de negócios. **Os principais destaques incluem:**

79%

das empresas acreditam estar **mais expostas a ataques cibernéticos** do que em anos anteriores

67%

possuem um plano de resposta a incidentes, enquanto 25% ainda não adotaram essa medida

66,5%

consideram os **riscos cibernéticos entre os cinco maiores desafios da empresa,** e 10,1% os consideram a principal preocupação

49,6%

das empresas afirmam que **consultariam especialistas antes de decidir pagar um resgate,** enquanto 14,5% considerariam o pagamento caso não houvesse alternativa

75%

das grandes empresas veem a **cibersegurança como um risco prioritário,** enquanto entre microempresas essa taxa cai para 55%

Principais ameaças:

Phishing (69%), vazamento de dados (68%) e *ransomware* (67%) são os ataques mais temidos pelas empresas

Engajamento da alta gestão:

Empresas com liderança envolvida apresentam controles mais consistentes e melhores práticas de segurança

Seguro cibernético:

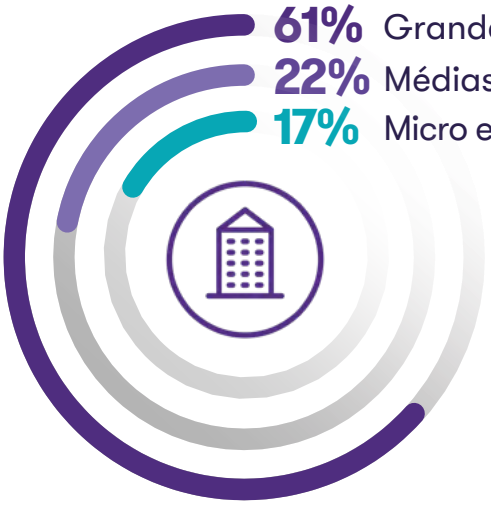
Apenas 25% das empresas possuem esse tipo de seguro, apesar do aumento das ameaças digitais

Perfil dos respondentes

A pesquisa foi conduzida entre **março e dezembro de 2024,** com a participação de **248 empresas nacionais.**

Tamanho

(em número de funcionários no Brasil)

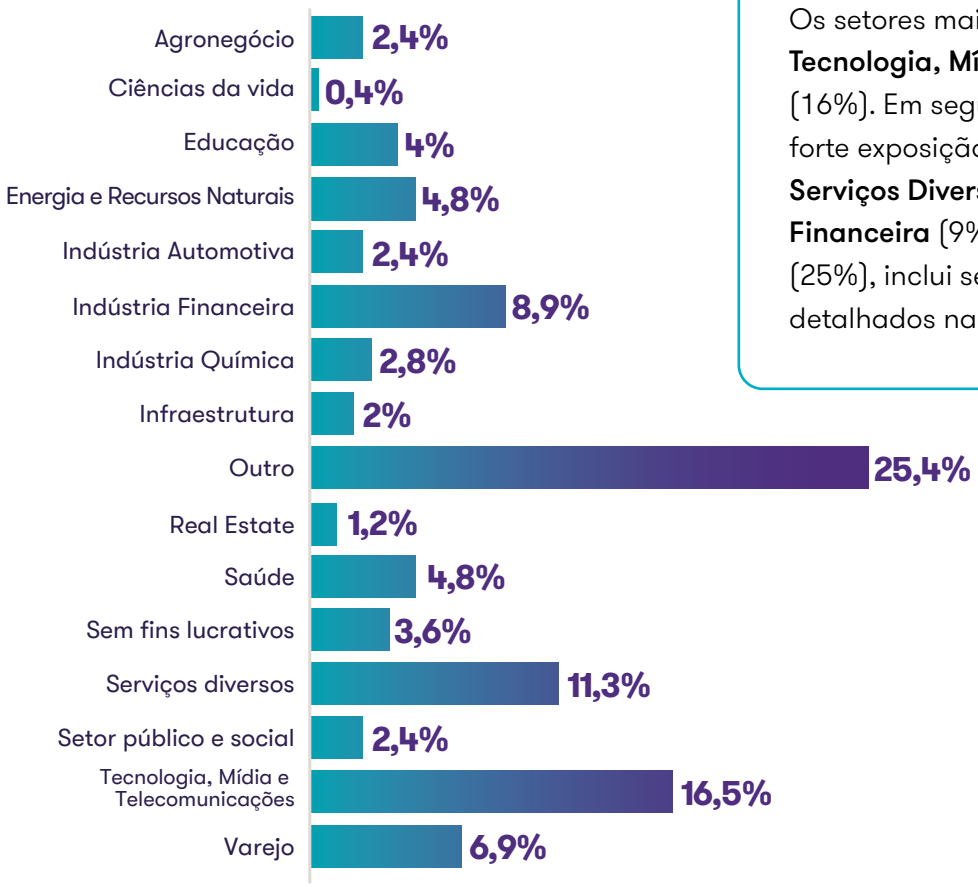


61% Grandes (mais de 250)
22% Médias (de 50 a 249)
17% Micro e Pequenas (até 49)

A maioria dos participantes são profissionais **de empresas de grande porte (61%).** As empresas de **médio porte** correspondem a 22%, enquanto as micro e pequenas representam juntas 17%.

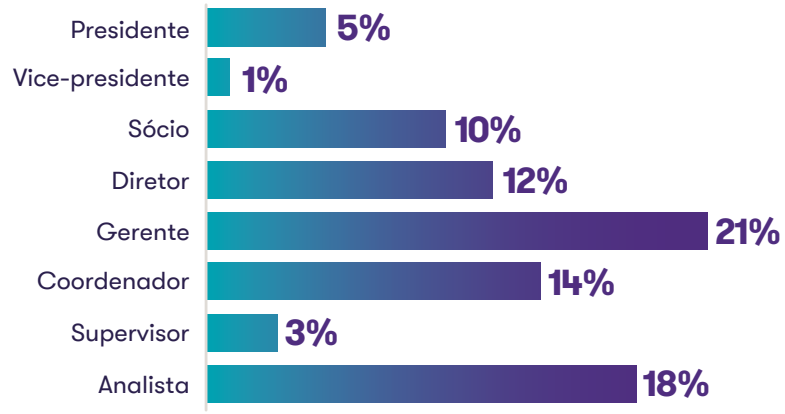
Essa predominância de grandes empresas é significativa, pois elas normalmente enfrentam maior exposição ao risco cibernético devido à complexidade tecnológica e ao volume de dados tratados e nos ajudam a ter um retrato sobre ações de enfrentamento diante desses riscos.

Distribuição por setor



Os setores mais representativos foram **Tecnologia, Mídia e Telecomunicações** (16%). Em seguida, estão setores com forte exposição a riscos digitais como **Serviços Diversos** (11%) e **Indústria Financeira** (9%). A categoria **"Outro"** (25%), inclui setores diversos não detalhados na pesquisa.

Cargo dos respondentes



A pesquisa alcançou principalmente profissionais em **cargos de gestão intermediária e executiva,** destacando-se **gerentes** (21%), **analistas** (18%), **coordenadores** (14%) e **diretores** (12%). Essa variedade de cargos indica uma percepção equilibrada, contemplando desde a visão estratégica até a operacional.

Risco cibernético está entre as 5 maiores preocupações

79% dos respondentes acreditam que suas empresas estão mais expostas a riscos cibernéticos agora do que em anos anteriores, indicando uma preocupação crescente com esse tema.

O aumento do risco cibernético pode ser atribuído a vários fatores:

Crescimento das tentativas de ataques:

em 2022, o Brasil registrou 31,5 bilhões de tentativas de ataques cibernéticos, um aumento de 94% em comparação com o ano anterior. Esse crescimento é impulsionado pela maior digitalização e conectividade das empresas e indivíduos[1].

Baixo investimento em cibersegurança:

historicamente, o Brasil tem investido menos em cibersegurança em comparação com outros países. Embora o cenário esteja mudando, ainda há um déficit significativo[1].

Sofisticação dos ataques:

os cibercriminosos estão utilizando técnicas cada vez mais avançadas, como inteligência artificial e aprendizado de máquina, para realizar ataques mais complexos e difíceis de detectar[2].

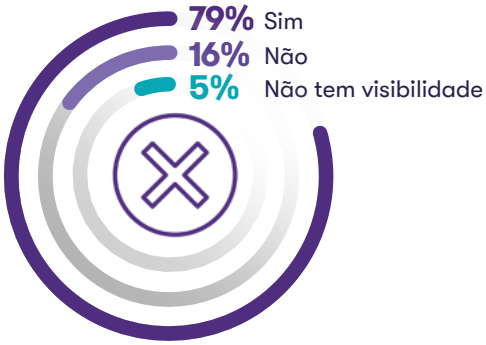
Superexposição a ciberataques:

o Brasil possui uma das maiores superfícies de ataque cibernético exposta no mundo, devido à implementação insuficiente de medidas de segurança em sistemas críticos[3].

Esses fatores contribuem para o aumento do risco cibernético no país, e essa percepção foi capturada em nossa pesquisa quando 79% dos participantes responderam que entendem que suas empresas estão mais expostas a riscos cibernéticos agora em relação a anos anteriores. Esses números refletem um cenário de crescente preocupação com ataques cibernéticos entre as empresas brasileiras.

Em linha com essa preocupação, 66,5% das empresas que participaram da pesquisa declaram que os riscos cibernéticos estão entre os cinco maiores riscos e 10,1% os classificam como a maior preocupação. Isto deixa evidente que a segurança digital é uma prioridade significativa.

Gráfico 1
Percepção das empresas sobre maior exposição atualmente do que em anos anteriores



[1]CNN Brasil - Levantamento mostra que ataques cibernéticos no brasil cresceram 94%
https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/

[2]Security Leaders - Ataques cibernéticos crescem cerca de 70% no brasil em um ano
https://securityleaders.com.br/ataques-ciberneticos-crescem-cerca-de-70-no-brasil-em-um-ano/

[3]Convergencia Digital - TCU alerta para superexposicao do brasil a ciberataques em nova lista de alto risco
https://convergenciadigital.com.br/governo/tcu-alerta-para-superexposicao-do-brasil-a-ciberataques-em-nova-lista-de-alto-risco/

Além disso, 21% das empresas veem o tema como preocupante, mas não prioritário, sugerindo que ainda há espaço para aumentar a conscientização e a urgência em adotar medidas preventivas robustas. Apenas 2,4% das empresas não consideram os riscos cibernéticos uma preocupação.

A percepção de riscos cibernéticos varia entre empresas de diferentes portes e setores:

75%

das grandes empresas consideram os riscos cibernéticos entre suas cinco maiores preocupações ou como a principal preocupação.

Enquanto apenas

55%

das microempresas têm o mesmo nível de preocupação, indicando que empresas menores ainda têm um longo caminho para amadurecer em segurança cibernética.

Essa diferença na percepção pode ser atribuída ao impacto potencialmente significativo que incidentes cibernéticos podem ter em grandes empresas, que geralmente possuem mais ativos digitais e dados sensíveis a proteger. Por outro lado, microempresas podem subestimar ou não compreender plenamente os riscos digitais que enfrentam, possivelmente devido a recursos limitados ou falta de conhecimento especializado em cibersegurança.

Gráfico 2
Preocupação das empresas com riscos cibernéticos

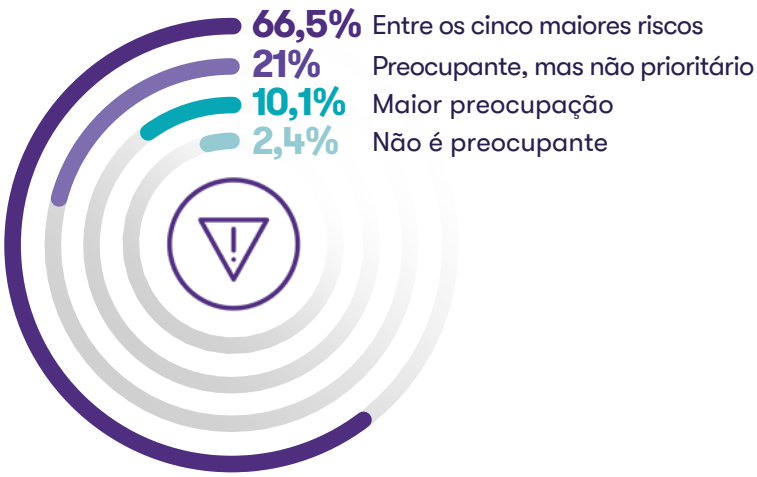
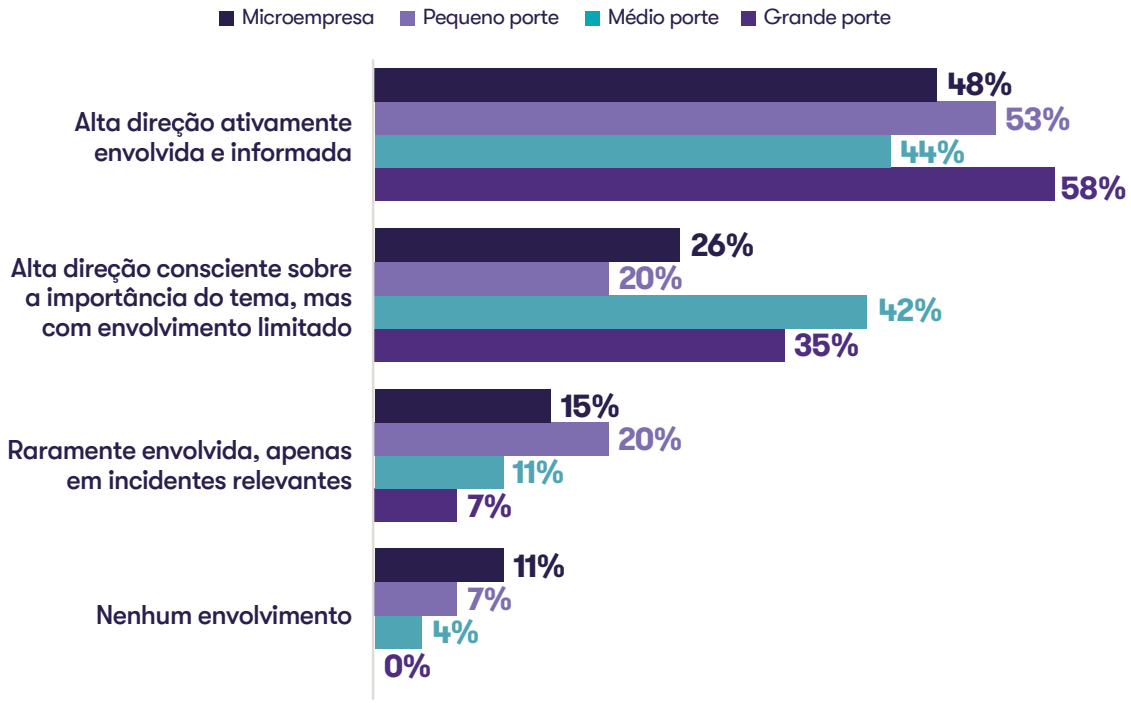




Gráfico 3
Envolvimento da liderança em cibersegurança de acordo com o porte da empresa



Os dados indicam, ainda, que o envolvimento da alta administração na gestão de riscos cibernéticos varia significativamente conforme o porte da empresa. Entre as grandes empresas, 58% têm a alta administração envolvida e informada, enquanto 35% têm a administração consciente, mas com envolvimento limitado, e nenhuma grande empresa relatou ausência total de envolvimento. Já nas médias empresas, 44% têm a alta administração ativamente envolvida e 42% com envolvimento limitado. As pequenas empresas mostram um alto nível de envolvimento, com 53% da alta administração ativamente engajada e 20% com envolvimento limitado. Já nas microempresas, 48% têm a alta administração ativamente envolvida e 26% com envolvimento limitado. Esses números destacam a importância do engajamento da alta administração na segurança cibernética, especialmente em empresas de maior porte, onde a complexidade e o volume de dados exigem uma abordagem mais robusta e informada.

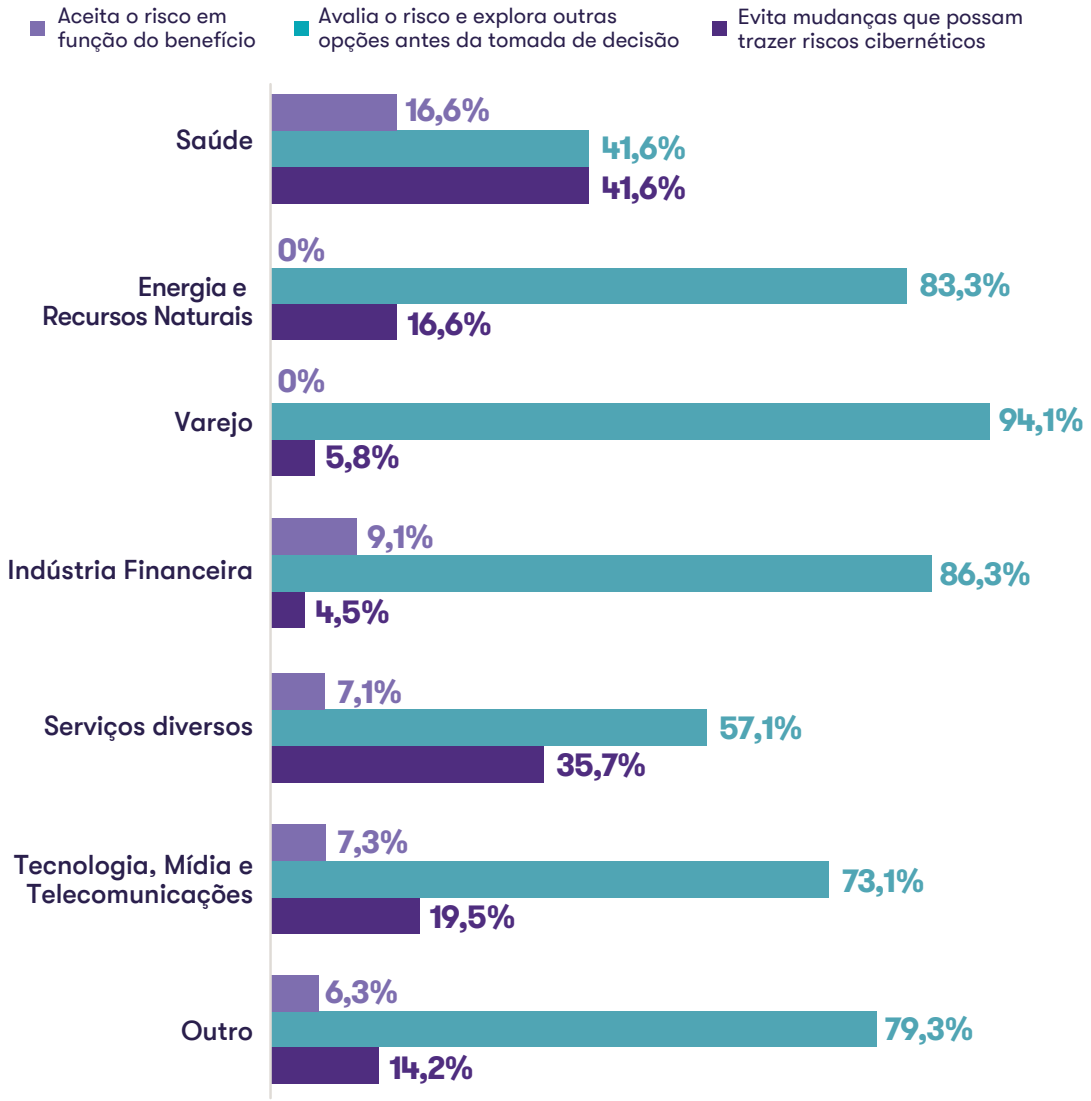
Também podemos observar uma variância em relação à preocupação com a análise de riscos cibernéticos, correlacionando-os com o setor econômico da empresa.



Gráfico 4

Como a empresa lida com novas tecnologias que trazem risco cibernético, de acordo com o porte da empresa

*apenas os setores com maior representatividade nas respostas



A preocupação com riscos cibernéticos é mais evidente em empresas reguladas, como Tecnologia, Midia e Telecomunicações, Serviços financeiros ou setores de Energia e Recursos Naturais e Saúde. Os setores de Serviços e Varejo também se destacam, principalmente devido à forte dependência de recursos de tecnologia para suas operações, vendas, divulgação, entre outros aspectos.

44%

das empresas de médio porte têm a alta administração ativamente envolvida no tema

Os dados da pesquisa refletem, ainda, uma correlação entre a crescente preocupação das empresas com riscos cibernéticos e sua estruturação para enfrentar esses desafios. Com 66,1% das empresas declarando que estão estruturadas contra ataques cibernéticos, é evidente que a maioria reconhece a importância de se preparar adequadamente.

No entanto, 25,8% das empresas afirmam que não estão estruturadas, o que indica que ainda há um número significativo de organizações vulneráveis. Além disso, 8,1% das empresas não sabem se estão preparadas, sugerindo uma necessidade de maior conscientização e clareza sobre as medidas de segurança adotadas. Esses dados destacam a urgência de fortalecer a resiliência cibernética e implementar estratégias eficazes para proteger os ativos digitais.

Gráfico 5
Estruturação das empresas contra ataques cibernéticos





Avaliação de riscos para minimizar impactos

Ainda no contexto da percepção de aumento do risco cibernético pelas empresas, quando questionados sobre a preocupação com avaliação de novas tecnologias para identificação de mitigação de riscos antes de sua implementação, a maioria dos profissionais afirma realizar este procedimento.

A avaliação de riscos de novas tecnologias é um passo importante na proteção cibernética das empresas. O fato de 66,5% das empresas afirmarem que realizam essa avaliação para identificar e mitigar riscos antes de implantar novas soluções demonstra um compromisso proativo com a segurança cibernética. No entanto, a existência de 18,5% das empresas que não fazem esse tipo de avaliação e 14,9% que não souberam responder indica que ainda há um caminho a percorrer para alcançar uma preparação uniforme e abrangente.

Os dados sobre a avaliação de riscos cibernéticos de novas tecnologias refletem uma abordagem predominantemente cautelosa. Com 74,6% das empresas afirmando que avaliam o risco e exploram outras opções antes da tomada de decisão sobre a utilização, evidenciando que a maioria das organizações está comprometida em identificar e mitigar possíveis ameaças antes de implementar novas soluções. Por outro lado, 19% das empresas evitam mudanças que possam trazer riscos cibernéticos, demonstrando uma postura conservadora em relação à adoção de novas tecnologias. Apenas 6,5% das empresas aceitam o risco em função do benefício, indicando que uma pequena parcela está disposta a assumir riscos cibernéticos em troca de vantagens potenciais. Esses dados destacam a importância da avaliação de riscos como uma prática essencial para garantir a segurança e a integridade das operações empresariais.

Gráfico 6
Avaliação de riscos de novas tecnologias pelas empresas

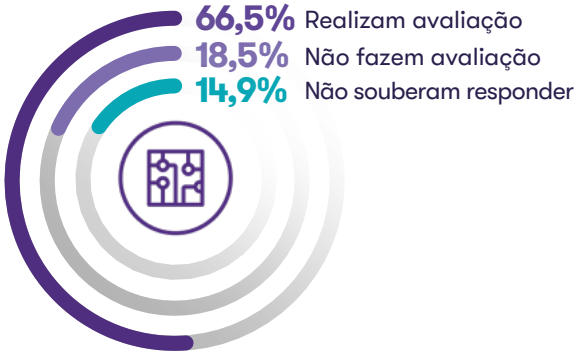


Gráfico 7
Avaliação de riscos cibernéticos de novas tecnologias pelas empresas



Envolvimento da liderança e mapeamento de riscos

O envolvimento ativo da alta administração é importante para a eficácia da proteção do ambiente cibernético. Empresas onde a alta direção está ativamente envolvida apresentam uma maior consistência em seus controles. Esse engajamento da liderança garante que a cibersegurança seja uma prioridade estratégica, facilitando a alocação de recursos adequados e a implementação de políticas robustas de segurança.

Por outro lado, empresas com liderança menos envolvida mostram controles menos frequentes ou eficazes.

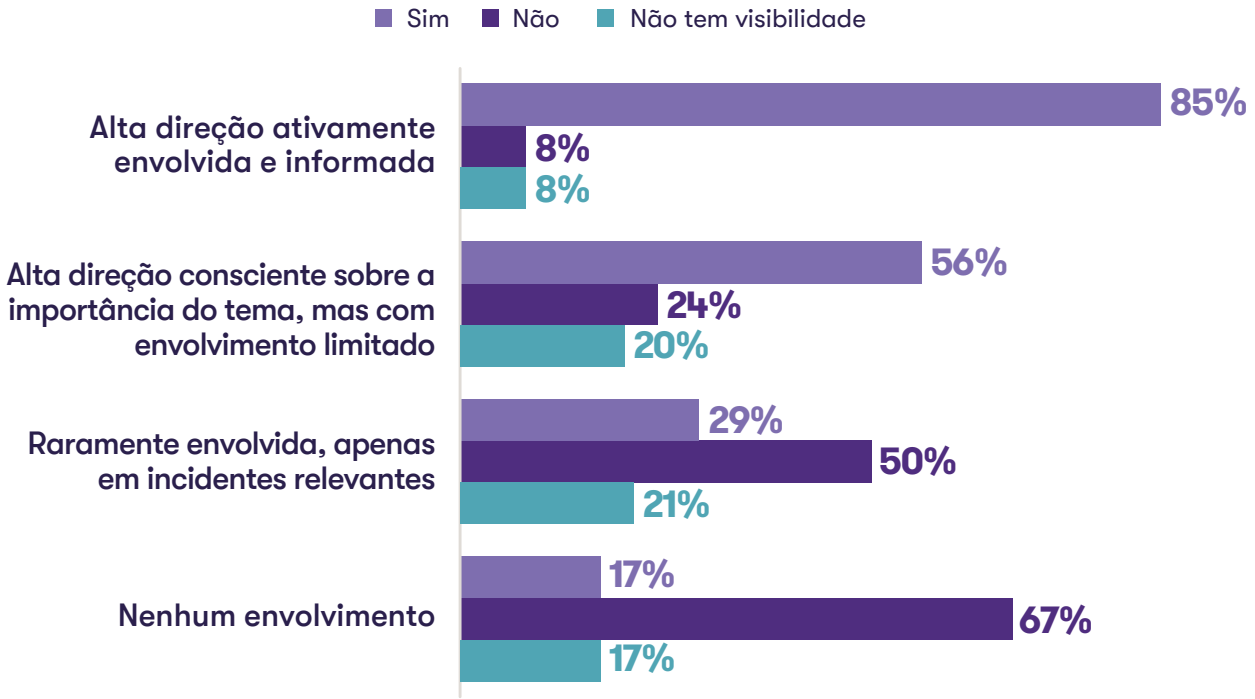
A falta de engajamento da alta administração pode resultar em uma abordagem fragmentada e insuficiente à cibersegurança, deixando a empresa vulnerável a ataques. A liderança ativa é, portanto, um fator determinante para a maturidade em cibersegurança, reforçando a necessidade de engajamento contínuo da alta administração para garantir a proteção eficaz do ambiente cibernético e a resiliência contra ameaças digitais.



85%

das empresas que realizam mapeamento e controle de riscos cibernéticos apresentam a alta direção ativamente envolvida

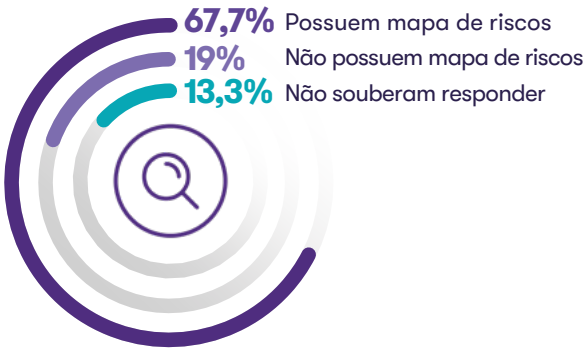
Gráfico 8
Realização de mapeamento de riscos cibernéticos e envolvimento da liderança



Os dados indicam, ainda, que a maioria das empresas brasileiras (67,7%) possui um mapa de riscos cibernéticos, enquanto uma quantidade menor (19%) não possui e outras (13,3%) não souberam responder. Isso demonstra uma conscientização crescente sobre a importância do mapeamento de riscos cibernéticos.

Além disso, das empresas onde os riscos cibernéticos estão entre as cinco maiores preocupações ou são a maior preocupação, 77% possuem um mapa de risco. Portanto, é possível inferir que a percepção de risco está diretamente ligada à implementação de medidas de controle. As empresas que reconhecem a gravidade dos riscos cibernéticos tendem a adotar práticas mais robustas de mapeamento e controle, evidenciando uma correlação entre a preocupação com a segurança cibernética e a ação preventiva. Isso sugere que aumentar a conscientização sobre os riscos cibernéticos pode incentivar mais empresas a desenvolverem e manterem mapas de risco eficazes.

Gráfico 9
Indicadores de mapeamento de riscos cibernéticos das empresas



Avaliação de riscos de terceiros

A avaliação de riscos de terceiros também foi considerada, pois ela é uma prática essencial para garantir a segurança e a integridade das operações empresariais. De acordo com os dados da pesquisa, 50% das empresas afirmam realizar avaliações, demonstrando um compromisso significativo com a mitigação de riscos e a proteção contra possíveis ameaças cibernéticas. Essa prática permite que as empresas identifiquem vulnerabilidades e adotem medidas preventivas antes de estabelecer parcerias, contribuindo para um ambiente de negócios mais seguro e confiável.

Por outro lado, 34,7% das empresas não realizam essa avaliação, o que pode representar uma exposição maior a riscos não identificados. Além disso, 15,3% das empresas não sabem informar se realizam ou não essa prática, indicando uma possível falta de conscientização ou clareza sobre os procedimentos adotados. Esses dados destacam a importância de promover a conscientização e a educação sobre a avaliação de riscos de parceiros, incentivando mais empresas a adotarem essa prática importante para a segurança e o sucesso das operações.

Um fato relevante revelado é que as empresas cuja alta administração está engajada com cibersegurança tendem a valorizar mais a gestão de riscos, incluindo avaliação de seus parceiros e fornecedores.

Gráfico 10
Avaliação de riscos de terceiros

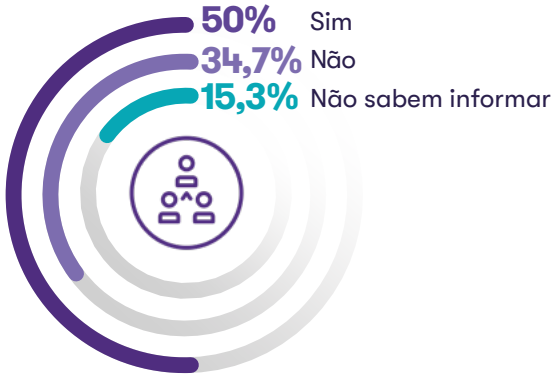
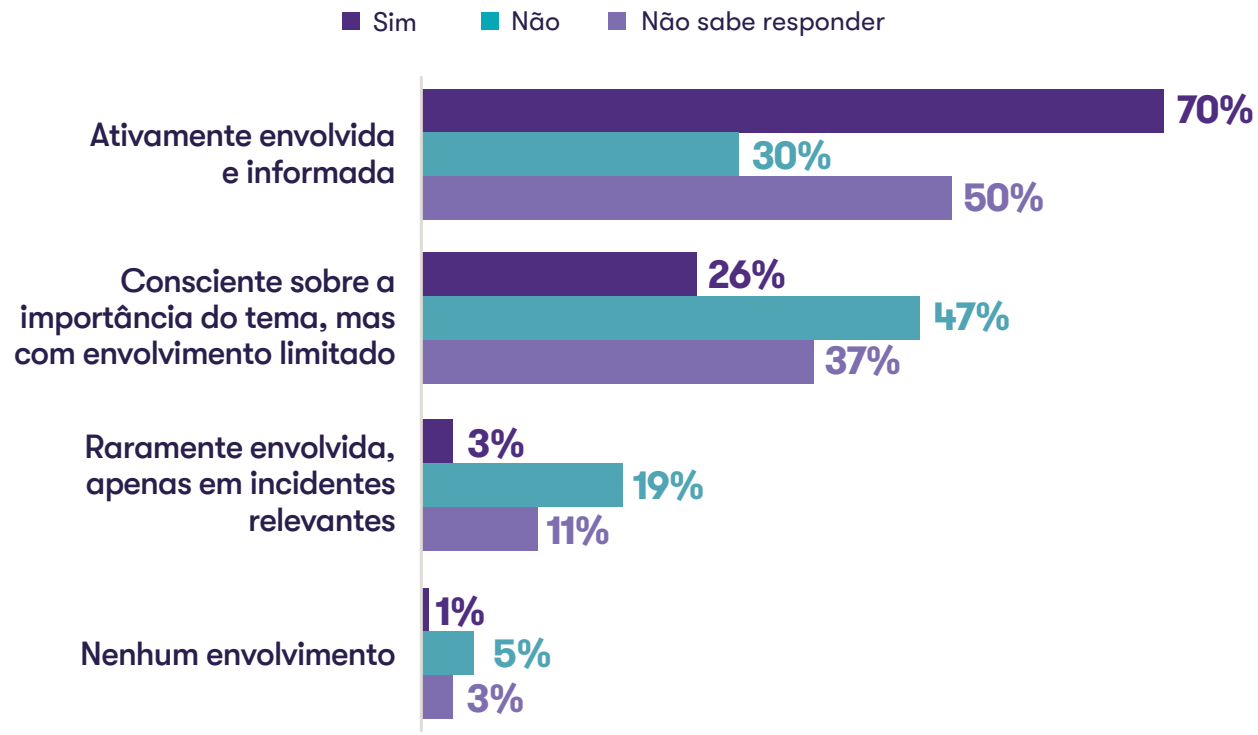


Gráfico 11
Nível de envolvimento da liderança na avaliação de riscos de terceiros

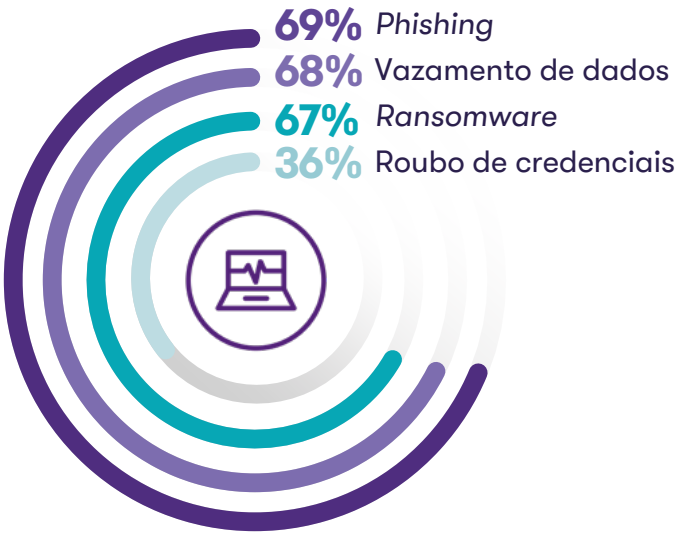




Principais ameaças identificadas pelas empresas

Compreender as principais ameaças cibernéticas, como *ransomware* e *phishing*, é essencial para identificar vulnerabilidades e implementar medidas preventivas eficazes. Esse conhecimento permite que as empresas desenvolvam estratégias de segurança robustas, protegendo dados sensíveis e garantindo a continuidade das operações.

Gráfico 12
Principais ameaças percebidas pelas empresas
*múltipla seleção



Entre as ameaças mais preocupantes indicadas pelas empresas estão:

***Phishing*:** mencionada por 69% dos respondentes, considerada a ameaça mais comum e preocupante atualmente.

Vazamento de dados: indicado por 68% dos respondentes, demonstrando preocupação com a segurança das informações para evitar consequências operacionais, legais, reputacionais e financeiras, além de regulatórias como o atendimento à LGPD.

***Ransomware*:** citado por 67% das empresas, mostrando grande relevância pela gravidade e impacto operacional.

Roubo de Credenciais: destacado por 36% das empresas, refletindo a preocupação crescente com fraudes internas e externas.



Estar ciente das ameaças cibernéticas ajuda as empresas no cumprimento das regulamentações específicas de segurança, evitando multas e penalidades. A conformidade regulatória é importante para manter a confiança dos clientes e parceiros de negócios, além de proteger a reputação da empresa no mercado.

A prevalência de ataques cibernéticos, como *phishing* e *ransomware*, em setores críticos como Tecnologia, Mídia e Telecomunicações e Indústria Financeira, destaca a vulnerabilidade dessas áreas a ameaças digitais.

De fato, o ataque *ransomware* tem crescido significativamente no Brasil, colocando o país na 7ª posição mundial em 2024, com 123 ataques registrados. Esse aumento é impulsionado pela sofisticação das estratégias de *ransomware* e pela vulnerabilidade das infraestruturas críticas[4]. O impacto para os negócios inclui perdas financeiras, interrupção operacional e danos à reputação, com o *ransomware* se tornando um negócio lucrativo para o crime organizado[5].

Além de combater o sofisticado *ransomware*, é preciso reconhecer e combater o *phishing*, pois ele continua sendo o principal vetor de entrada em incidentes cibernéticos, que incluem o ataque *ransomware*. O *phishing* envolve e-mails fraudulentos que enganam os usuários para clicarem em links maliciosos. A conscientização e o treinamento dos funcionários, juntamente com tecnologias de detecção e prevenção, são fundamentais para proteger as empresas contra essa ameaça iminente.

50%

das empresas não realizam e não sabem informar sobre avaliação de riscos de terceiros

[4] IT Show - Brasil foi o 7º país mais afetado por ransomware em 2024
https://itshow.com.br/brasil-7-lugar-ranking-ransomware-2024/

[5] Brasil em 7º lugar no ransomware em 2024
https://www.cisoadvisor.com.br/brasil-em-7o-lugar-no-ransomware-em-2024/



Medidas de prevenção aos ataques cibernéticos

A implementação de controles preventivos é essencial para minimizar os riscos cibernéticos e proteger as empresas contra ameaças. Esses controles ajudam a identificar, avaliar e mitigar vulnerabilidades antes que possam ser exploradas por atacantes.

Política e plano de resposta a incidentes

As organizações precisam de uma política e um plano de resposta a incidentes para garantir sua resiliência cibernética. Esses documentos fornecem um conjunto estruturado de procedimentos a serem seguidos em caso de um incidente de segurança, permitindo uma resposta rápida e eficaz, o que minimiza o impacto dos ataques, reduzindo o tempo de inatividade e os danos financeiros e reputacionais. Além disso, um plano bem elaborado garante que todos os funcionários saibam suas responsabilidades durante um incidente, promovendo uma coordenação eficiente e uma recuperação mais rápida das operações normais.



80%
possuem política de segurança da informação formalizada e divulgada.

67%
afirmam possuir um plano de resposta a incidentes estruturado.

Esses números são positivos, porém é importante garantir que a eficácia real dessas políticas e planos sejam avaliadas e monitoradas continuamente para atualização e adequação. Um plano estruturado é essencial para minimizar impactos no caso de um incidente cibernético, mas um plano desatualizado ou inefetivo pode gerar o resultado oposto.

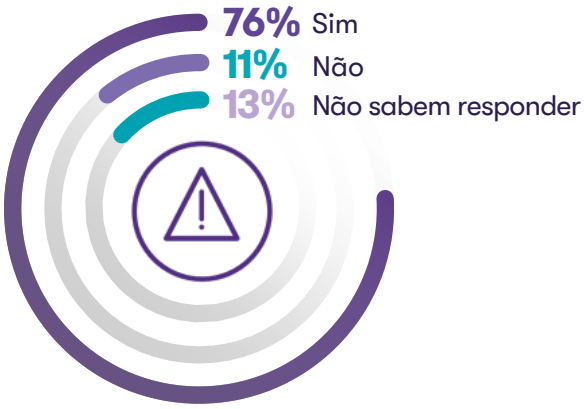
Utilização de ferramenta para detecção de vulnerabilidades

Para estruturar um programa de segurança cibernética eficaz, as empresas podem recorrer a *frameworks* reconhecidos, como a ISO 27001, que fornece um sistema de gestão de segurança da informação; o NIST Cybersecurity Framework (CSF) 2.0, que oferece diretrizes para melhorar a resiliência cibernética; e os CIS Controls, que são um conjunto de práticas recomendadas para proteger sistemas e dados contra ataques.

Esses *frameworks* fornecem uma base sólida para a criação de políticas, procedimentos e controles que ajudam a garantir a segurança cibernética de forma abrangente e contínua.

Os dados indicam que 76% das empresas afirmam utilizar ferramentas para detecção de vulnerabilidades, demonstrando uma conscientização significativa sobre a importância de identificar e corrigir pontos fracos antes que possam ser explorados por atacantes.

Gráfico 13
Utilização de ferramenta para detecção de vulnerabilidades



No entanto, 11% das empresas não utilizam essas ferramentas, o que pode deixá-las mais vulneráveis a ataques cibernéticos. Além disso, 13% das empresas não souberam responder, o que pode indicar uma falta de conhecimento ou de processos estabelecidos para a detecção de vulnerabilidades.

Embora a maioria das empresas afirmem estar no caminho certo, utilizando ferramentas de proteção, ainda há uma parcela relevante que não se possui tais infraestruturas, destacando a necessidade de aumentar a adoção e a compreensão das ferramentas de detecção de vulnerabilidades para fortalecer a segurança cibernética.

Estrutura técnica e organizacional para manutenção do nível de segurança

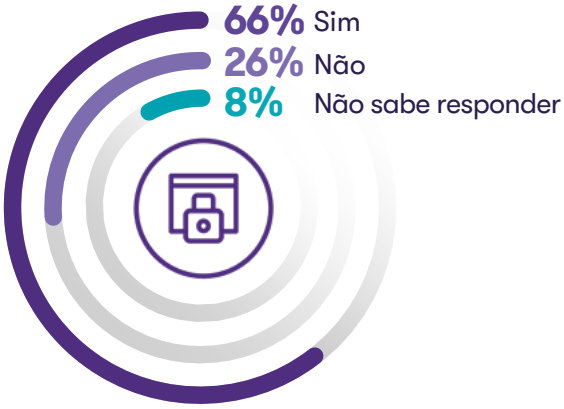
A estrutura técnica e organizacional de uma empresa é fundamental para a proteção do ambiente cibernético. A ISO 27001 destaca a relevância dos pilares de liderança e comprometimento, papéis e responsabilidades, bem como o devido planejamento da estrutura de segurança, apoio (que inclui recursos e competências) e operação. Esses elementos são essenciais para garantir que a segurança cibernética seja integrada em todos os níveis da organização, promovendo uma cultura de segurança e resiliência.

O *framework* NIST CSF 2.0 também inova ao trazer no centro de seus domínios de segurança o pilar de governança, buscando endereçar justamente a necessidade das empresas terem uma estrutura adequada.

Os dados da pesquisa mostram que **66% das empresas afirmam ter uma estrutura técnica e organizacional adequada** para manter um alto nível de segurança cibernética. Isso indica que a maioria das empresas reconhece a importância de uma estrutura bem definida para proteger seus ativos digitais. No entanto, **26% das empresas afirmam que não possuem essa estrutura, o que pode deixá-las mais vulneráveis a ataques cibernéticos.** Além disso, 8% das empresas não souberam responder, o que pode indicar uma falta de clareza ou de comunicação interna sobre as práticas de segurança cibernética. Esses números ressaltam a necessidade de fortalecer a estrutura técnica e organizacional em todas as empresas para garantir uma proteção eficaz contra ameaças.

A implementação de uma estrutura técnica e organizacional robusta é importante para a proteção do ambiente cibernético. As empresas devem investir em liderança, planejamento, recursos e competências para garantir que a segurança cibernética seja uma prioridade em todos os níveis. Isso não apenas ajuda a prevenir ataques, mas também a responder de forma eficaz a incidentes, minimizando os impactos e garantindo a continuidade dos negócios.

Gráfico 14
Considera a empresa estruturada tecnicamente e organizacionalmente para manter um alto nível de segurança



Resiliência Cibernética

As empresas precisam de resiliência cibernética para assegurar sua segurança no ambiente digital atual. Isso envolve a capacidade de se preparar, responder e se recuperar de incidentes cibernéticos. O processo inclui etapas essenciais como a identificação e avaliação de riscos, monitoramento e prevenção, além da resposta e recuperação.

Identificar e avaliar riscos permite que as empresas compreendam suas vulnerabilidades e priorizem ações de segurança, enquanto o monitoramento contínuo e a prevenção ajudam a detectar e impedir ataques antes que causem danos significativos.

Além disso, as etapas de resposta e recuperação garantem que as empresas possam lidar de maneira eficaz com incidentes cibernéticos, minimizando os impactos e restaurando rapidamente as operações normais. Juntas, essas etapas permitem que as organizações protejam seus ativos digitais, mantenham a confiança dos clientes e parceiros, e assegurem a continuidade dos negócios em um cenário de ameaças cibernéticas crescentes.



Nível de confiança das empresas nas etapas:

- Identificação e Avaliação de Riscos (45%)
- Monitoramento e Prevenção (45%)
- Resposta e Recuperação (45%)

Os dados demonstram que a confiança das empresas foi classificada majoritariamente como **média,** demonstrando um cenário onde as lacunas e pontos de melhoria em todas as fases de resiliência cibernética são reconhecidas pelas empresas.

Plano de resposta e histórico de incidentes cibernéticos

A importância de um plano estruturado de resposta a incidentes não pode ser subestimada, pois permite que as empresas ajam rapidamente para minimizar os danos potenciais causados por um ataque. Isso inclui a redução do tempo de inatividade, a proteção da integridade e confidencialidade dos dados, e a manutenção da continuidade dos negócios. Além disso, um plano eficaz ajuda a preservar a reputação da empresa e a evitar penalidades legais associadas a falhas de segurança.

De acordo com os dados da pesquisa, **67% das empresas participantes possuem um plano de resposta a incidente cibernético,** demostrando investimento em prevenção e controle de riscos. Por outro lado, 25% não possuem e 8% não souberam informar. Estes dois últimos indicadores são preocupantes, a medida que um plano de resposta a incidente predefinido e testado pode ser o fator determinante para aumentar ou reduzir os danos em caso de um incidente cibernético.

Entre as empresas participantes, 40% relataram já ter sofrido um incidente cibernético. Desses casos, apenas 64% possuem planos estruturados de resposta, um percentual ainda menor em comparação ao número anterior. Isso mostra que, embora o plano de resposta a incidentes cibernéticos seja um instrumento preventivo, muitas vezes ele é criado a partir da uma situação real de incidente.

Gráfico 15
Possui plano de resposta a incidente cibernético

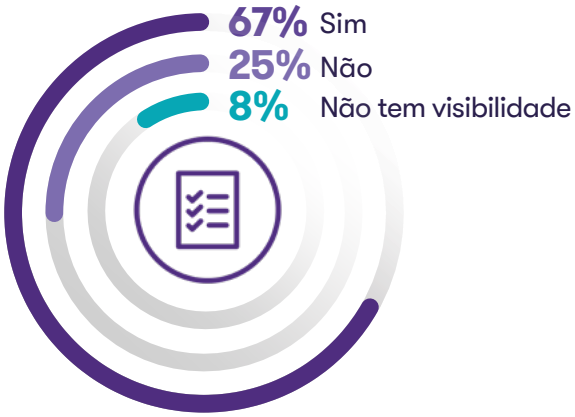
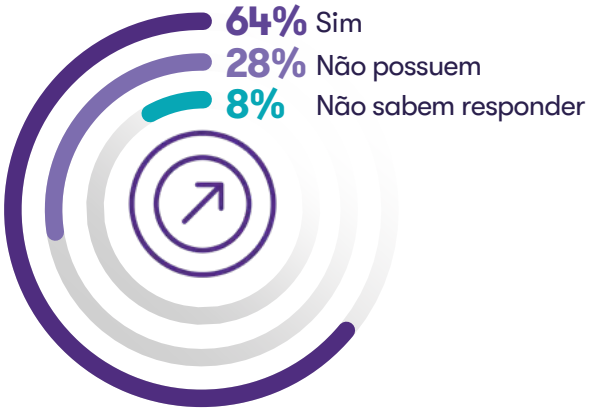


Gráfico 16
Empresas que sofreram incidente cibernético e possuem plano de resposta

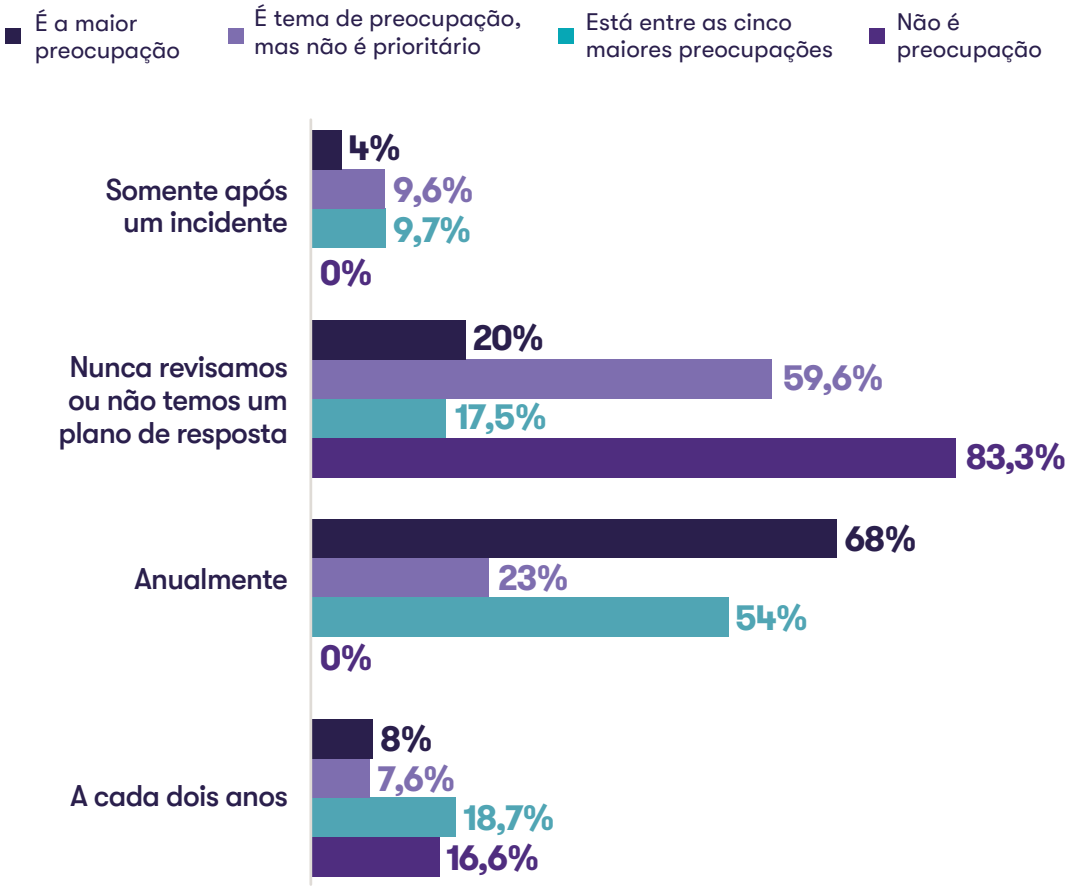


Empresas que já passaram por ataques cibernéticos tendem a reconhecer a importância de estar preparadas para futuras ameaças e, portanto, desenvolvem e implementam planos de resposta mais completos, ou melhoraram planos ineficientes. Essa experiência prévia reforça a necessidade de uma abordagem proativa e estruturada para lidar com incidentes, garantindo que a empresa esteja mais bem equipada para responder rapidamente e mitigar os impactos de qualquer nova ameaça cibernética.

Além disso, empresas que revisam seus planos de resposta a incidentes anualmente ou a cada dois anos representam uma parcela significativa das empresas onde risco cibernético é uma das maiores preocupações, ou está entre as cinco maiores preocupações, 76% e 72,7%, respectivamente . Este indicador cai drasticamente quando focamos em empresas que não tem preocupação com riscos cibernéticos ou o tema não é prioritário.



Gráfico 17
Relação entre riscos cibernéticos como preocupação e a frequência de revisão do plano de respostas a incidentes



Importância da conscientização e treinamento

Diante das evoluções tecnológicas e de seus riscos e vulnerabilidades iminentes, é imperativo que as empresas invistam em conscientização e treinamento em segurança cibernética para fortalecer sua resiliência. Funcionários bem treinados são a primeira linha de defesa contra ameaças cibernéticas, atuando como agentes de proteção. Quando entendem os riscos e sabem como responder a incidentes, eles ajudam a prevenir ataques e minimizar danos. Adicionalmente, os programas contínuos de conscientização e treinamento reforçam a segurança da empresa, promovendo uma cultura de vigilância e responsabilidade compartilhada.

Os dados mostram que **69,7% das empresas realizam treinamentos de conscientização e segurança cibernética para todos os colaboradores,** enquanto 13,3% fazem isso para um grupo determinado, totalizando 83% que realizam algum tipo de treinamento. No entanto, 15% das empresas afirmam não possuir treinamentos. Isso indica que, embora a maioria das empresas reconheça a importância da capacitação em segurança cibernética, ainda há uma parcela significativa que não investe nessa área. A falta de treinamento pode deixar essas empresas mais vulneráveis, destacando a necessidade de ampliar esses programas.

Porém, os dados indicam que apenas **21,4% das empresas consideram seus treinamentos altamente eficazes,** com avaliações regulares. A maioria, 51,2%, acredita que os treinamentos são moderadamente eficazes, com algumas lacunas identificadas. Além disso, 27,4% afirmam que não realizam treinamentos ou que eles não são eficazes. Esses resultados mostram que, embora a maioria das empresas realize treinamentos, há uma necessidade de melhorar a qualidade e a eficácia desses programas.

Gráfico 18
Planos de conscientização e treinamentos realizados pelas empresas

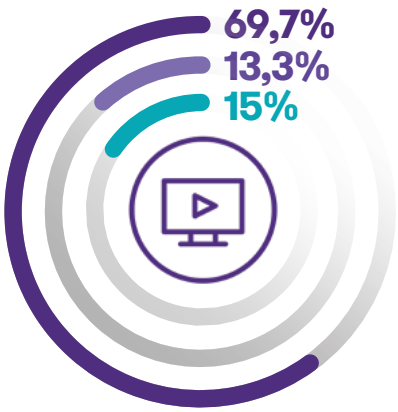
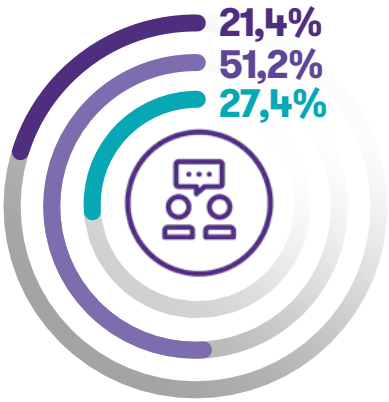


Gráfico 19
Eficácia dos treinamentos de conscientização e segurança cibernética



A correlação com o gráfico anterior revela que, mesmo entre as empresas que realizam treinamentos, muitas ainda enfrentam desafios para garantir que esses programas sejam realmente eficazes. Melhorar a avaliação e a adaptação dos treinamentos pode aumentar a resiliência cibernética das empresas.

Os resultados da pesquisa mostram, ainda, que **70,5% das empresas que realizam treinamentos para todos os colaboradores são de grande porte.** Essa predominância também é observada nas empresas que fazem treinamentos para grupos específicos de colaboradores, onde 52,6% são grandes empresas.

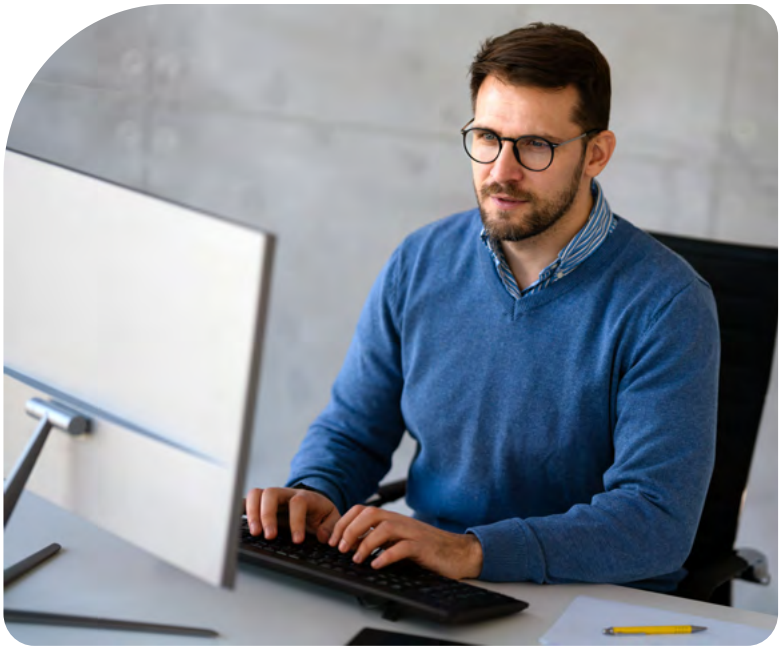
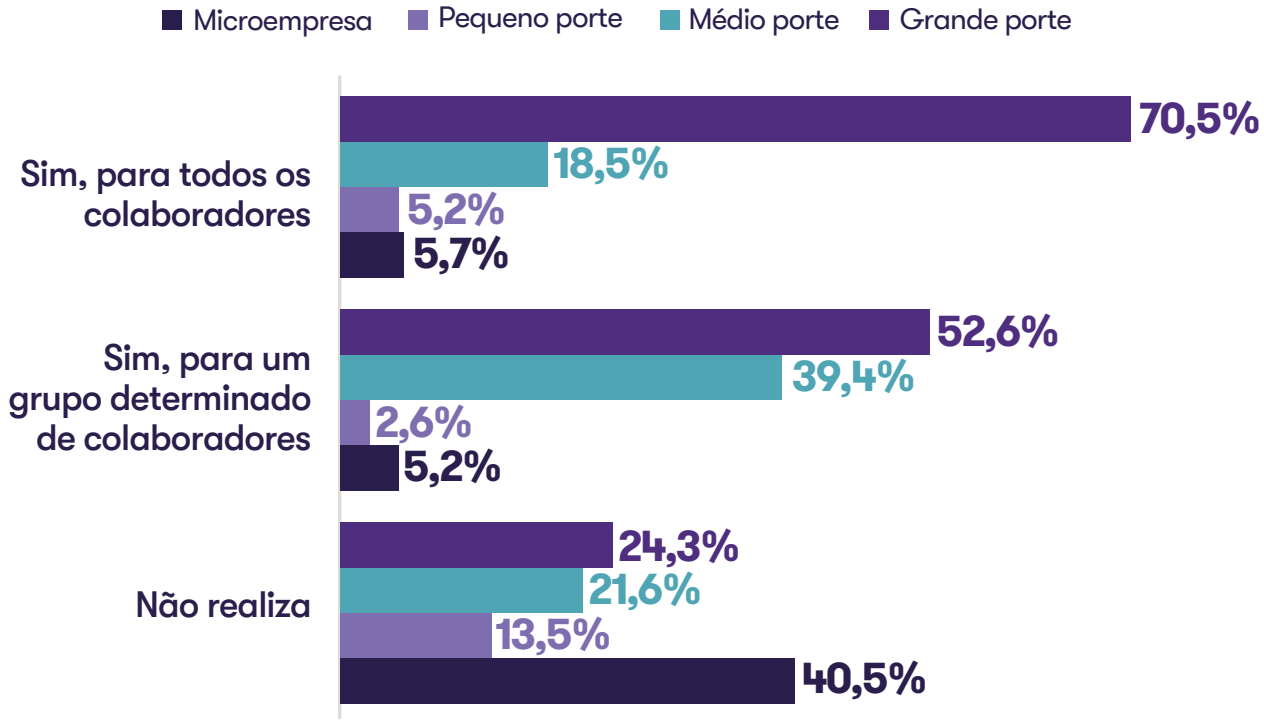


Gráfico 20
Processos de conscientização e treinamentos aos colaboradores (por porte de empresa)



Já as empresas de médio porte representam 18,5% das que realizam treinamentos regulares para todos os colaboradores, enquanto 39,4% fazem treinamentos para grupos específicos. Por outro lado, as **empresas que não possuem processos de conscientização e treinamento têm uma participação significativa de pequenas e médias empresas, representando 54%.** Esses números indicam que as grandes empresas estão mais atentas à importância da conscientização e treinamento em segurança cibernética, enquanto as pequenas e médias empresas ainda enfrentam desafios para implementar esses processos.

Embora a maioria das empresas reconheça a importância da conscientização e treinamento em segurança cibernética, há variações significativas na implementação e na qualidade desses programas. Grandes empresas lideram na realização de treinamentos para todos os colaboradores, enquanto pequenas e médias empresas ainda têm uma participação significativa na ausência de processos de conscientização e treinamento. Apenas 21,3% das empresas consideram seus treinamentos altamente eficazes. Esses dados destacam a necessidade de melhorar a qualidade e abrangência dos programas de treinamento, especialmente nas pequenas e médias empresas, para fortalecer a resiliência cibernética e preparar todos os colaboradores para atuar como a primeira linha de defesa contra ameaças.



69,7%

realizam treinamentos de conscientização e segurança cibernética para todos os colaboradores

21,4%

consideram seus treinamentos altamente eficazes

Notificação de incidentes às autoridades

As empresas devem estar cientes de suas obrigações de notificação de incidentes cibernéticos às autoridades reguladoras, como a Autoridade Nacional de Proteção de Dados (ANPD), o Banco Central do Brasil (BACEN) e outras entidades. A notificação adequada é importante para garantir a transparência, a conformidade com as regulamentações e a proteção dos dados dos diversos stakeholders. Além disso, comunicar incidentes às autoridades pode ajudar a mitigar os impactos negativos e a melhorar as práticas de segurança cibernética.

Os dados mostram que 40% empresas relataram ter sofrido incidentes cibernéticos, enquanto 36% apontam que não sofreram e 23% não podem afirmar. Isso indica que uma parte significativa das empresas já enfrentou desafios relacionados à segurança cibernética, destacando a necessidade de medidas preventivas e reativas eficazes.

Os setores mais impactados por ataques cibernéticos são:

Varejo
47%

Indústria Financeira
45%

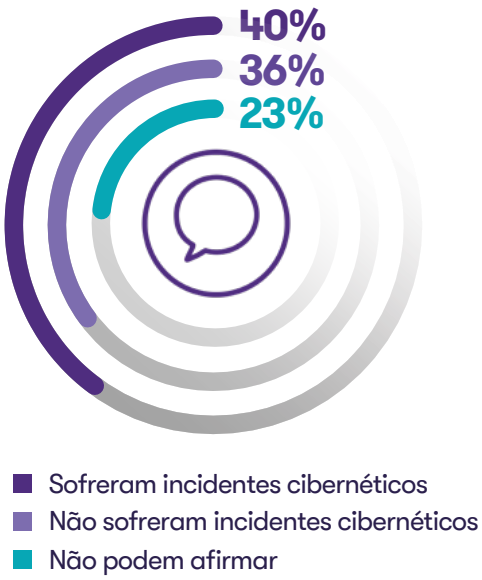
Serviços
43%

Saúde
42%

Tecnologia, Mídia e Telecomunicações
32%

Além disso, 32% das empresas não se classificaram nos setores perguntados e estão indicadas como “Outros”. Esses dados sugerem que setores com alta dependência de tecnologia e dados sensíveis são mais visados por atacantes cibernéticos.

Gráfico 21
Empresas que relatam ter sofrido incidentes cibernéticos



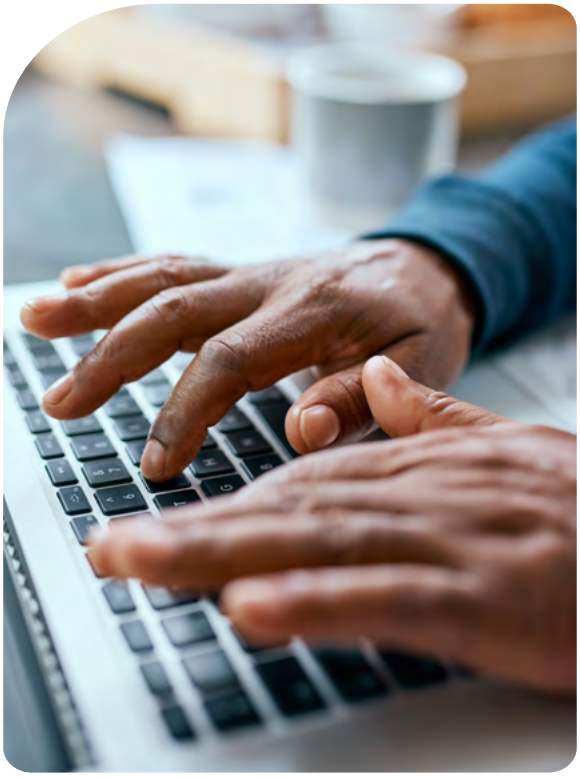
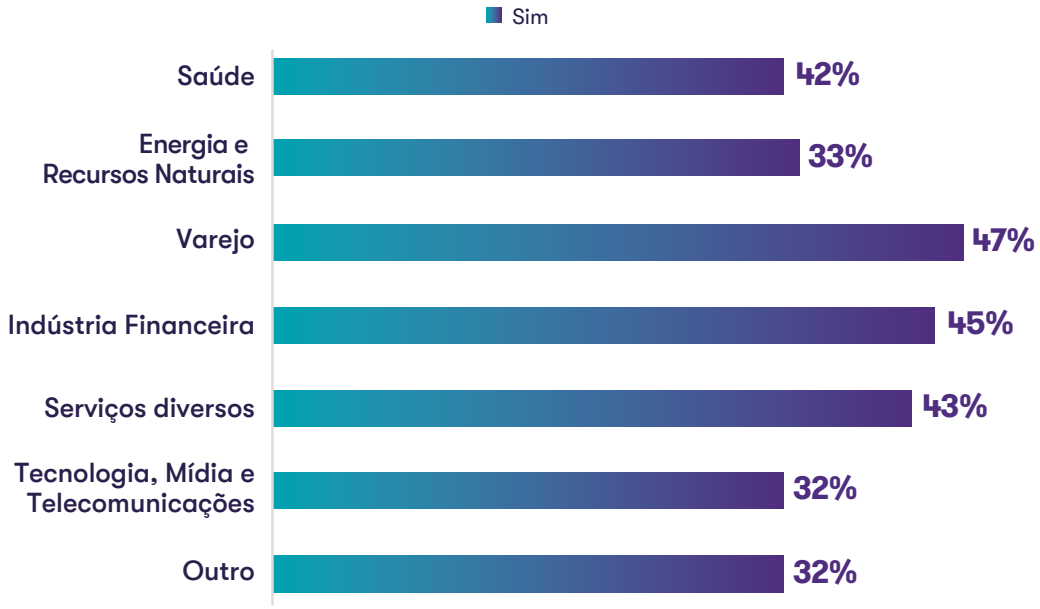


Gráfico 22

Sua empresa já sofreu incidentes cibernéticos?

*7 setores com maior representação na pesquisa

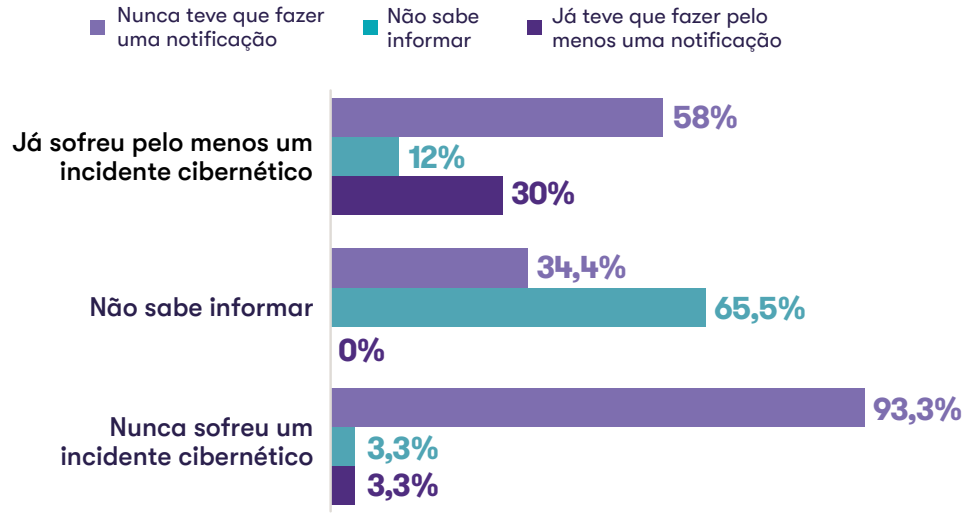


Os setores de Tecnologia, Mídia e Telecomunicações, Serviços e Indústria Financeira são alvos frequentes, possivelmente, devido à sua alta regulamentação, grande porte e a quantidade de dados sensíveis que manipulam. Esses setores são alvos atraentes para cibercriminosos, que buscam explorar vulnerabilidades para obter ganhos financeiros ou informações valiosas. A concentração de ataques nesses setores destaca a necessidade de investimentos contínuos em segurança cibernética e treinamento.

Ainda nesse contexto, é importante destacar que as empresas devem notificar incidentes cibernéticos às autoridades competentes dentro de prazos específicos. Por exemplo, a ANPD exige notificação em até 72 horas em caso de incidente com dano relevante ao titular de dados. O BACEN também possui regulamentações específicas para comunicação de incidentes, conforme a Circular no 3.909. Empresas de capital aberto nos Estados Unidos devem notificar a SEC (Securities and Exchange Commission) sobre incidentes cibernéticos relevantes, e outros.

Os dados da pesquisa mostram que 58% das empresas que sofreram incidentes cibernéticos não notificaram as autoridades, 12% não sabem responder e apenas 30% realizaram a notificação. Isso indica uma lacuna significativa na conformidade com as obrigações de notificação, o que pode resultar em penalidades e danos à reputação. Isso destaca a necessidade de maior conscientização e conformidade com as obrigações regulatórias para mitigar riscos e proteger dados sensíveis.

Gráfico 23
Volume de empresas que sofreram incidente cibernético e notificaram autoridades

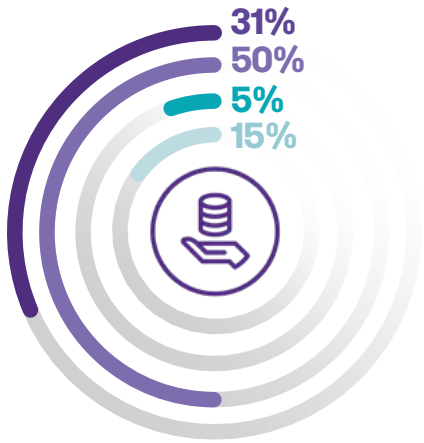


Pagamento de resgate em caso de *ransomware*

Entre as maiores ameaças ao negócio, o *ransomware* é apontado por 66% das empresas respondentes. *Ransomware* é um tipo de *malware* que criptografa os dados da vítima e exige um pagamento de resgate para restaurar o acesso. Os atacantes geralmente pedem o pagamento em criptomoedas para dificultar o rastreamento. A decisão de pagar o resgate envolve várias considerações legais, éticas e práticas.

Os dados mostram que **50% das empresas consultariam especialistas antes de tomar a decisão de pagar o resgate.** Isso indica uma abordagem cautelosa e informada, buscando orientação legal e técnica para avaliar as implicações do pagamento. Por outro lado, **31% afirmam que não pagariam por falta de respaldo legal,** destacando a importância de conformidade com as regulamentações e a preocupação com possíveis consequências legais.

Gráfico 24
Consideração de pagamento por resgate em caso de ataque aos ativos críticos



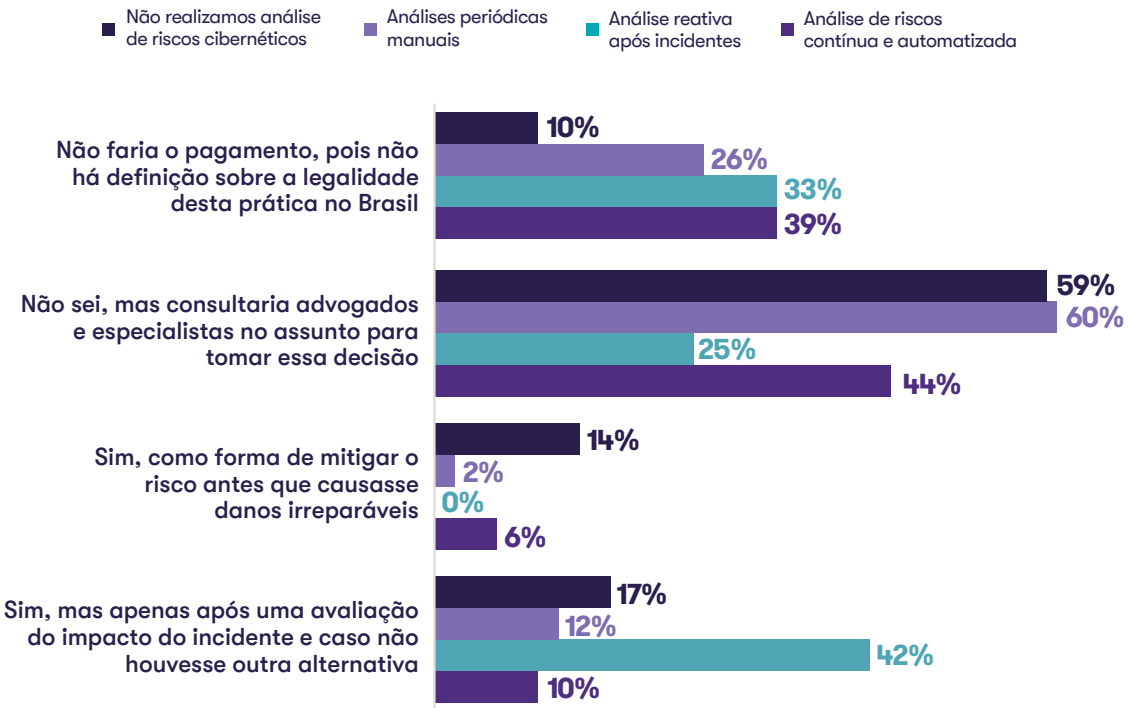
- Não faria o pagamento, pois não há definição sobre a legalidade desta prática no Brasil
- Não sabe, mas consultaria advogados e especialistas no assunto para tomar essa
- Sim, como forma de mitigar o risco antes que causasse danos irreparáveis
- Sim, mas apenas após uma avaliação do impacto do incidente e caso não houvesse outra alternativa

Além disso, **15% pagariam apenas após uma avaliação do impacto do incidente** e não havendo outra opção, enquanto **5% pagariam para mitigar riscos antes que causasse danos irreversíveis.** Esses resultados refletem a complexidade da decisão de pagamento de resgate, onde as empresas ponderam entre minimizar danos e cumprir obrigações legais.

A comparação dos indicadores revela que **empresas com análise contínua e automatizada de riscos cibernéticos tendem a não realizar o pagamento (39%) ou consultar especialistas antes de tomar a decisão (44%),** o que demonstra confiança na maturidade dos processos de resposta a incidentes. Empresas que fazem análise periódica manual seguem a mesma linha, com 26% não realizando o pagamento e 60% consultando especialistas. Já empresas que realizam análise reativa de risco após um incidente, afirmam que pagariam resgate após a avaliação de impacto (42%), 25% consultariam especialistas e 33% não pagariam. Isso representa um aumento significativo na probabilidade de pagamento de resgate, destacando a importância de uma abordagem proativa e contínua na análise de riscos cibernéticos.



Gráfico 25
Frequência das análises de riscos e pagamento de resgate



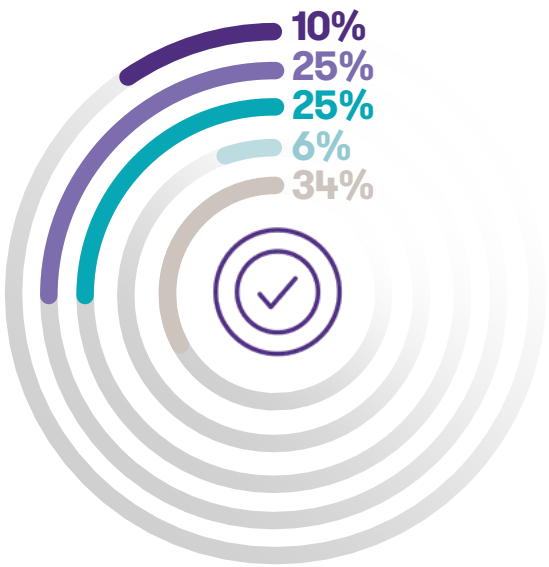
Seguro cibernético

O seguro cibernético tem se tornado uma medida de controle de risco cada vez mais procurada. Sua importância é destacada pela capacidade de oferecer proteção financeira contra os impactos de incidentes cibernéticos, como violações de dados, ataques de *ransomware* e outras ameaças. As vantagens de possuir um seguro cibernético incluem a cobertura de custos de recuperação, assistência jurídica e suporte técnico especializado, além de ajudar a mitigar perdas financeiras e danos à reputação. Com o aumento das ameaças, o seguro cibernético se torna uma ferramenta essencial para garantir a resiliência e continuidade dos negócios.

Os dados mostram que apenas **25% das empresas entendem a relevância do seguro cibernético e já possuem essa proteção.** Outros 25% também reconhecem sua importância, mas não têm intenção de adquirir o seguro. Além disso, **10% das empresas afirmam entender a relevância e estão no processo de aquisição.** Esses indicadores revelam que, embora haja uma conscientização crescente sobre a importância do seguro cibernético, ainda existe uma resistência significativa à sua adoção. As razões para essa resistência podem incluir custos, falta de informação detalhada sobre os benefícios, ou a percepção de que outras medidas de segurança são suficientes.

No entanto, esse é um investimento que pode proporcionar uma camada adicional de proteção, integrando ao programa de gestão de riscos para aumentar as garantias de preparação no enfrentamento e superação dos desafios impostos pelo cenário cibernético atual.

Gráfico 26
Entendimento das empresas em relação a seguro cibernético



- É relevante e está em processo de cotação do seguro (primeira vez)
- É relevante e possui seguro
- É relevante, mas não possui seguro e não tem intenção de contratar
- Não entende como relevante
- Não sabe responder

Conclusão

A pesquisa evidencia que, embora muitas empresas tenham avançado em segurança digital, ainda há desafios a serem superados. O baixo investimento e a falta de estrutura em algumas organizações aumentam a exposição a ataques.

A conscientização, a implementação de medidas preventivas e o envolvimento da alta gestão são fatores essenciais para a construção de um ambiente corporativo mais seguro.



Realização:

Grant Thornton

Opice Blum



Sobre a Grant Thornton

Exceder as expectativas é o que nos move e nos diferencia no mercado

A Grant Thornton é uma das maiores empresas globais de auditoria, consultoria e tributos. Está presente em 156 países e conta com mais de 76.000 colaboradores. No Brasil, está posicionada nos 16 principais centros de negócios do país, com mais de 1.800 pessoas que colaboram para a excelência no atendimento e prestação de serviços aos clientes e parceiros, contribuindo para ampliar o nosso reconhecimento pelo mercado como especialistas em middle market.

Nossos especialistas são focados em desenvolver soluções customizadas a todos os tipos de empresas e segmentos, desde startups, empresas privadas, familiares, a empresas de capital aberto e organizações públicas nacionais e internacionais. Temos como objetivo manter uma economia vibrante, baseada na confiança e na integridade dos mercados, além de promover crescimento sustentável em empresas e gerar impacto positivo na sociedade. Para isso, reforçamos em nossos valores o compromisso com as pessoas, inovação, sustentabilidade, excelência, foco no cliente e senso de dono para direcionar seus esforços para a constante construção de uma cultura organizacional mais diversa e inclusiva.

Acesse grantthornton.com.br para descobrir mais sobre nós

Grant Thornton

Sobre a Opice Blum Advogados

Opice Blum Advogados é sinônimo de inovação digital.

Desde 1997, o escritório é parceiro de seus clientes, redefinindo os limites do possível e trazendo novas estratégias para novas necessidades. Com um time de advogados especialistas, o escritório está onde a transformação acontece e se destaca pela excelência em áreas capazes de impactar positivamente os setores em que atua, como Proteção de Dados, Segurança da Informação, Contencioso Digital e Legal Innovation, entre outras.

Acesse opiceblum.com.br

Autores



Everson Probst
Sócio de Cybersecurity
E everson.probst@br.gt.com



Tiago Neves Furtado
Sócio das áreas de Resposta a Incidentes & Cibersegurança e proteção de Dados do Opice Blum Advogados
E tiago.furtado@opiceblum.com.br

Realização:

Grant Thornton

Opice BLUM