RELATÓRIO TÉCNICO 2025

PESQUISA DE MATURIDADE DA INDÚSTRIA EM CIBERSEGURANÇA, PROTEÇÃO DE DADOS E GOVERNANÇA DE IA

INTRODUÇÃO

O ambiente cibernético está se tornando cada vez mais complexo e desafiador, impulsionado por variáveis interconectadas como tensões geopolíticas, a rápida adoção de tecnologias emergentes por empresas e criminosos — especialmente a Inteligência Artificial (IA) — e cadeias de suprimento integradas. Esses fatores ampliam significativamente a superfície de ataque, tornando os riscos mais imprevisíveis e difíceis de gerenciar.

Empresas privadas e órgãos do Estado que não nasceram digitais, inevitavelmente estão em fase de digitalização e emprego de inovações. Elas são condicionantes para o desenvolvimento econômico e social no século 21.

Diante desse cenário, o risco cibernético deve ser compreendido como um componente estratégico do risco corporativo, e não apenas como uma responsabilidade isolada da equipe de segurança da informação.

Para a revolução tecnológica ser ainda mais potente, vibrante e melhorar a vida das pessoas, é preciso haver confiança digital, que se sustenta no tripé cibersegurança, proteção de dados pessoais e inteligência artificial ética e responsável.

Enquanto organizações com maior capacidade de investimento conseguem se adaptar mais rapidamente, as micro, pequenas e médias empresas (PMEs) podem estar mais expostas, o que compromete a resiliência de toda a cadeia produtiva.

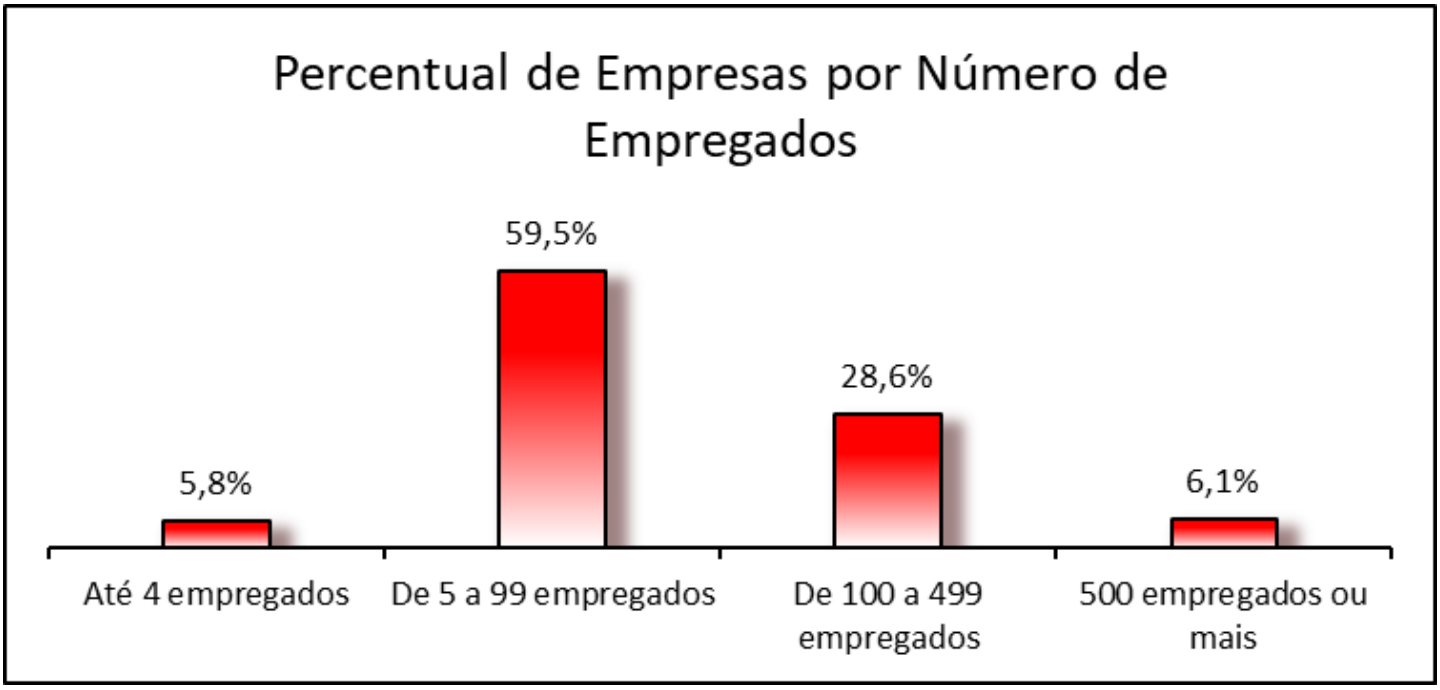
Assim, com o objetivo de avaliar o nível de maturidade em cibersegurança, proteção de dados e governança de Inteligência Artificial na indústria paulista, a Federação das Indústrias do Estado de São Paulo (FIESP), por meio do Departamento de Defesa e Segurança (DESEG), desenvolveu a **3ª edição da Pesquisa de Maturidade da Indústria em Cibersegurança**. A pesquisa será apresentada no VII Congresso de Cibersegurança, Proteção de Dados e Governança de Inteligência Artificial pelo Diretor Adjunto do DESEG e Diretor Técnico Responsável pelo Grupo de Trabalho de Segurança e Defesa Cibernética, Rony Vainzof.

Baseada em levantamento de dados realizado pelo Departamento de Economia (DEPECON) da FIESP junto a 294 empresas da indústria de São Paulo, a pesquisa tem como objetivo avaliar a maturidade da governança de cibersegurança sob três pilares: Segurança

Cibernética, Proteção de dados via Lei Geral de Proteção de Dados (LGPD) e Governança da Inteligência Artificial.

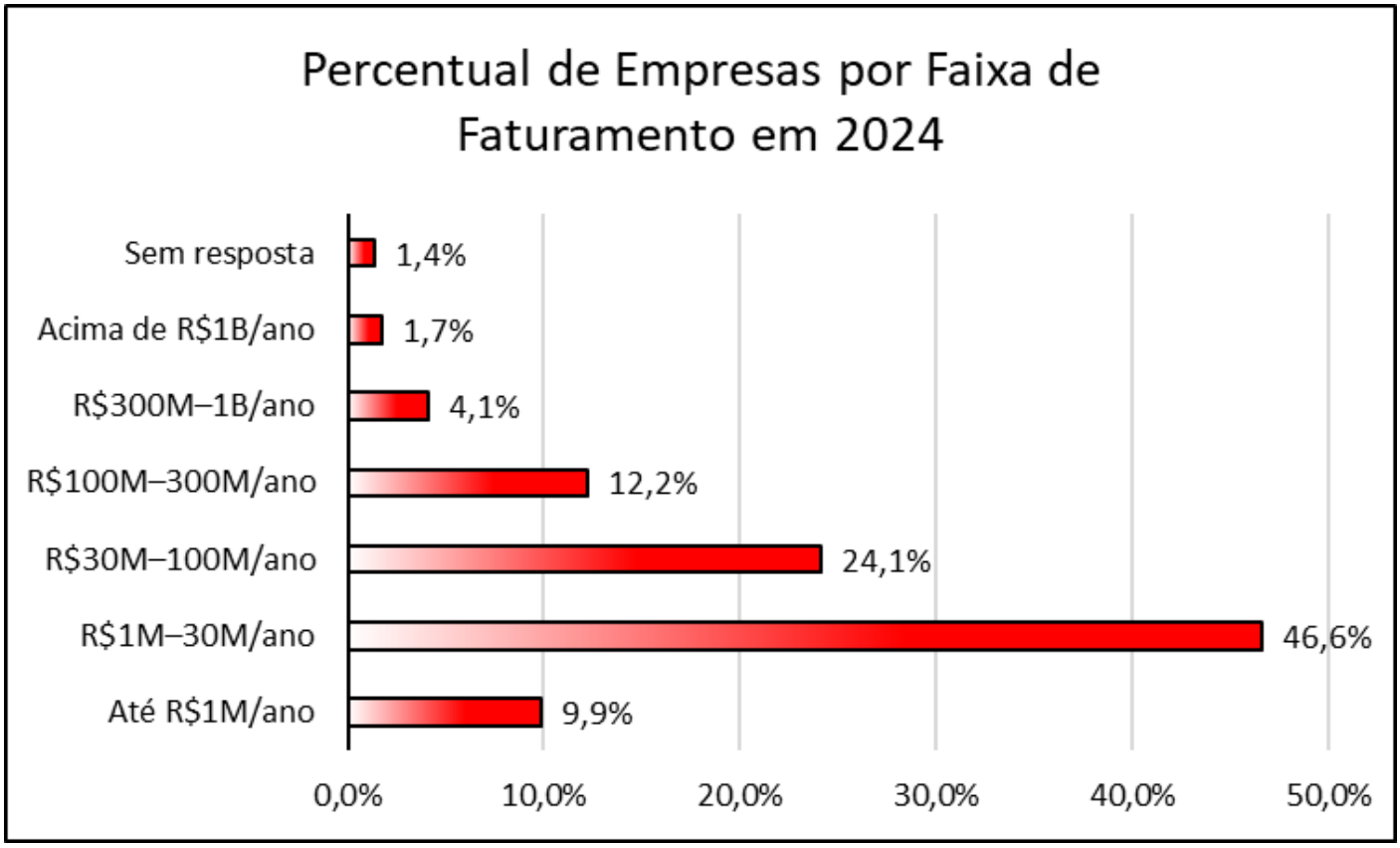
METODOLOGIA E PERFIL DE RESPONDENTES

A pesquisa foi conduzida por meio de um formulário, enviado à base de indústrias associadas à FIESP entre os dias 16 de abril e 31 de maio de 2025. O recorte cronológico adotado foi anual, tendo como referência o ano de 2024. Ao final do período, foram obtidas respostas de 294 empresas, cujo perfil é apresentado a seguir:

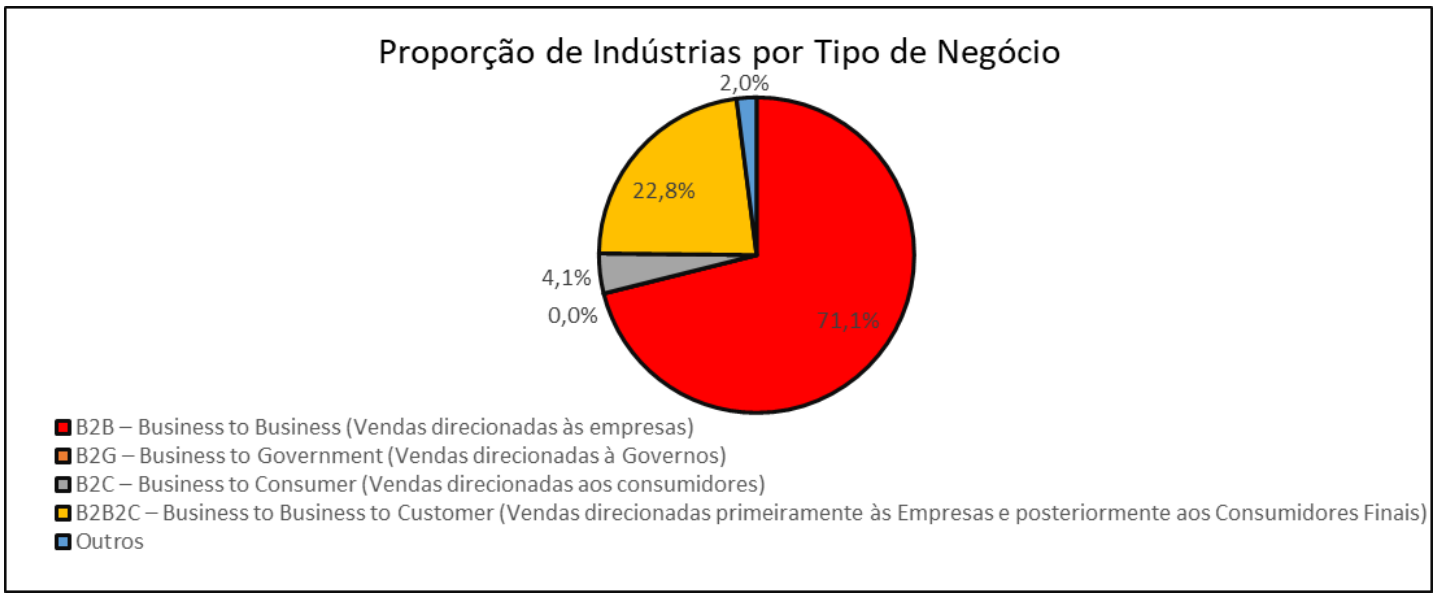


Com base no número de empregados, a pesquisa verificou que se mantém o padrão da série histórica, onde pequenas empresas representam a maior parte das indústrias respondentes, com 59,5%. Quando somadas aos microempreendimentos, correspondem a 65,3% das instituições. Já as médias e grandes empresas correspondem, respectivamente, a 28,6% e 6,1% dos respondentes da presente pesquisa.

O perfil da indústria, com base na faixa de faturamento, indicou um predomínio de 46,6% de pequenas e médias empresas com faturamento anual entre 1 milhão e 30 milhões de reais. Adicionalmente, outras faixas de faturamento foram analisadas, revelando a diversidade entre as empresas participantes, conforme o gráfico abaixo:



O modelo de vendas predominante entre as indústrias é o B2B (Business to Business), responsável por 71,1% das respostas, evidenciando um forte foco em transações entre empresas. Em seguida, aparece o modelo B2B2C (Business to Business to Consumer), com 22,8%, indicando que uma parcela significativa das vendas envolve uma cadeia intermediária antes de alcançar o consumidor final. Já o modelo B2C (Business to Consumer) representa apenas 4,1%, revelando uma atuação limitada no mercado consumidor direto. Não foram registrados casos de vendas no modelo B2G (Business to Government), o que evidência o recorte específico da pesquisa do setor privado.



Conclui-se, portanto, que o perfil predominante das indústrias respondentes é composto por empresas de menor porte, com estrutura enxuta e foco em relações comerciais entre empresas. Esse grupo representa um segmento dinâmico da indústria paulista, com atuação diversificada em termos de faturamento, mas com forte orientação ao mercado corporativo.

CIBERSEGURANÇA

Em um cenário industrial cada vez mais digitalizado, a cibersegurança consolidou-se como um pilar essencial para a continuidade dos negócios, competividade e a proteção de ativos críticos. A exposição a riscos digitais, aliada à crescente complexidade das ameaças, exige das organizações uma abordagem estruturada, preventiva e integrada à governança corporativa.

Esta seção apresenta um panorama da maturidade cibernética no setor industrial, destacando as práticas adotadas, as vulnerabilidades mais recorrentes, os impactos causados por incidentes e os principais desafios enfrentados na construção de um ambiente digital seguro, resiliente e sustentável.

Atualmente, se faz necessário tratar cibersegurança como estratégia integrada de riscos, contemplada desde os Conselhos de Administração[1], pois a agenda é de negócios e não apenas da área de Segurança da Informação.

[1] Para entender mais sobre o assunto acesse a Cartilha de Governança de Cibersegurança para Conselhos da Alta Administração, lançada pelo Departamento de Defesa e Segurança (DESEG) da FIESP.

Porém, a pesquisa de maturidade de cibersegurança na indústria identificou que 48,6% das organizações consideram a cibersegurança como "algo necessário, mas não prioritário". Enquanto 29,7% das organizações a definem como uma prioridade estratégica, outros 23,5% a veem como uma obrigação que não traz grandes benefícios para o negócio.

Importante notar que, de acordo com o aumento do faturamento, o tema ganha "prioridade estratégica":

- Até R$ 1 milhão, 17,2%;
- Entre R$ 1 milhão e R$ 30 milhões, 22,6%;
- Entre R$ 30 milhões e R$ 100 milhões, 32,4%;
- Entre R$ 100 milhões e R$ 300 milhões, 41,7%;
- Entre R$ 300 milhões e R$ 1 bilhão, 75%;
- Acima de R$ 1 bilhão, 80%.

Ainda, na média, em comparação com a edição anterior da Pesquisa de Maturidade em Cibersegurança, houve um crescimento de 2.7 pontos percentuais na percepção de que a cibersegurança é uma prioridade estratégica. Em relação à visão de que a cibersegurança é necessária, mas não prioritária, houve uma redução de 5.6 pontos percentuais. Além disso, com um aumento de 8.5 pontos percentuais, mais empresas passaram a definir a cibersegurança como uma obrigação que não traz grandes benefícios para o negócio.

De todas as empresas respondentes, pouco mais da metade (54,8%) das organizações possui uma estrutura organizacional de segurança cibernética e/ou segurança da informação. Enquanto 41,2% das indústrias não possuem essa estrutura, outros 4,1% não souberam responder. Além disso, 58,2% das organizações possuem reporte direto à alta gestão ou supervisão dos conselhos da alta administração, em comparação com 36,7% que não possuem e outros 5,1% que não souberam responder.

Ademais, 72,4% dos conselhos de administração não possuem membros com experiência em segurança cibernética, enquanto 20,1% dos conselhos possuem esse profissional. 7,5% dos entrevistados não souberam responder. Porém, para empresas com faturamento entre R$ 300 milhões e R$ 1 bilhão anuais, a realidade é outra. Mais de 40% possuem membros com experiência em cibersegurança.

Outro dado alarmante é que 58,2% das organizações não discutem segurança cibernética de forma regular ou contínua, enquanto apenas 35,4% tratam do tema periodicamente. Além disso, 6,5% dos respondentes não souberam informar a frequência

---

Disponível em: https://www.fiesp.com.br/indices-pesquisas-e-publicacoes/1a-cartilha-sobre-ciberseguranca-para-os-conselhos-de-administracao/

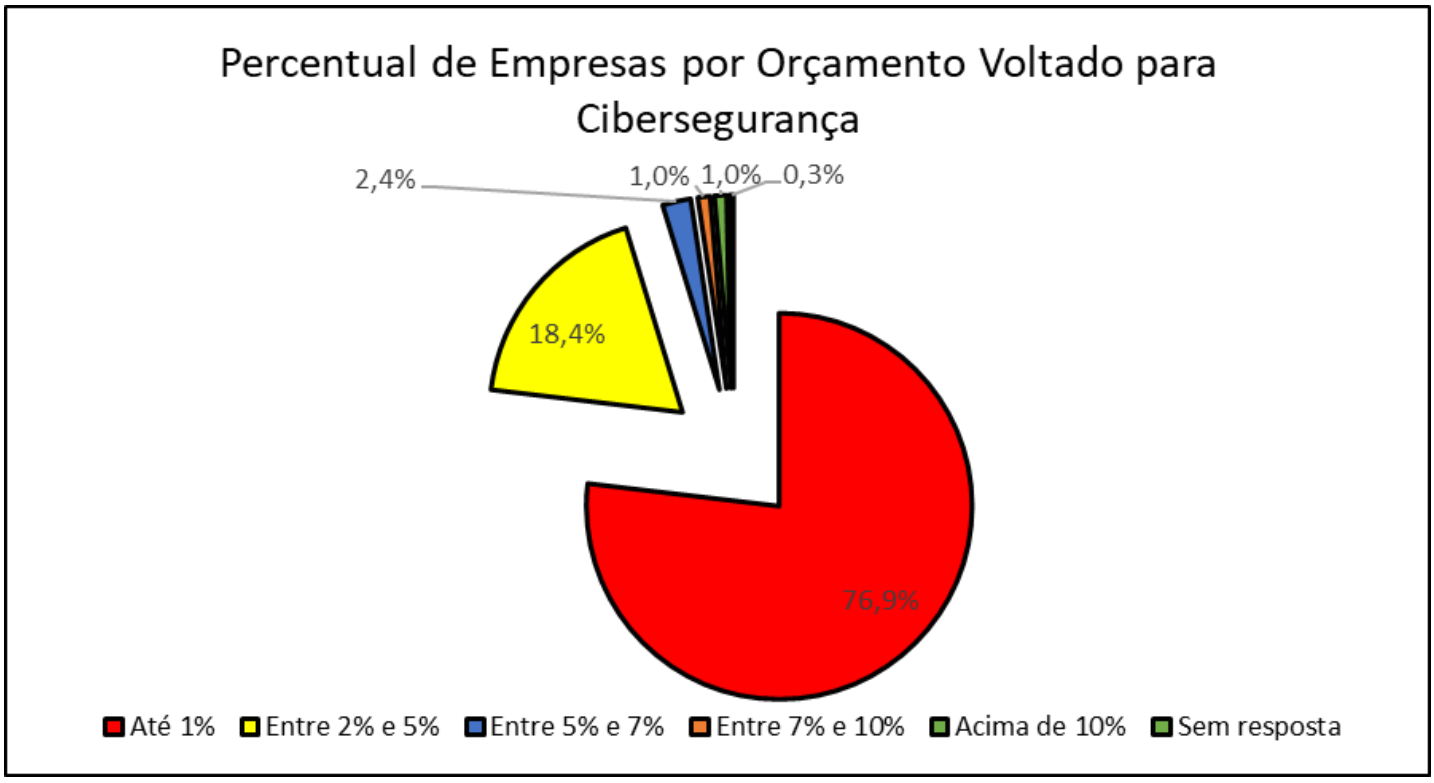
dessas discussões. Esse cenário é reforçado por outro indicador preocupante: 67,3% das empresas não consideram a segurança cibernética como uma de suas principais prioridades, e somente 25,7% a tratam como pauta estratégica no conselho de administração. Outros 7,5% não souberam responder. Esses dados evidenciam uma lacuna significativa na governança da cibersegurança, indicando a necessidade urgente de maior engajamento da alta liderança na gestão dos riscos digitais.

Por outro lado, a diferença significativa de maturidade em segurança cibernética entre grandes empresas e pequenas empresas, se torna evidente ao observar que enquanto apenas 22,6% das PMEs (R$1M-30M/ano) classificam cibersegurança como prioridade estratégica e 26,3% declaram ser "uma obrigação, que não reflete em grandes benefícios ao negócio", 75% das grandes empresas (R$300M-1B/ano) tratam cibersegurança como prioridade estratégica e nenhuma grande empresa considera a cibersegurança apenas uma obrigação sem benefícios ao negócio.

Conforme ilustrado no quadro abaixo, é necessário assumir um ponto de vista sensível às diferenças de porte entre as empresas. Pois não há heterogeneidade da indústria quanto à formalidade de estrutura de governança de cibersegurança, indicando que as fragilidades são diferentes quando se observa de empresas de pequeno, médio e grande porte.

Empresas:	**Total**			**PMEs (R$1M-30M/ano)**			**Grandes Empresas (R$300M-1B/ano)**		
Pergunta:	**Sim**	**Não**	**Não sei**	**Sim**	**Não**	**Não sei**	**Sim**	**Não**	**Não sei**
A instituição possui estrutura organizacional de Segurança Cibernética e/ou Segurança da Informação?	54,8%	41,2%	4,1%	43,1%	52,6%	4,4%	75%	25%	0%
Na sua organização o risco cibernético possui reporte direto à alta gestão, incluindo algum tipo de supervisão pelo Conselho Administrativo?	58,2%	36,7%	5,1%	50,4%	43,8%	5,8%	75%	25%	0%
Na sua organização o Conselho Administrativo discute segurança cibernética de forma regular ou constante?	35,4%	58,2%	6,5%	29,9%	65,7%	4,4%	66,7%	25%	8,3%
Na sua organização a Segurança Cibernética é uma das principais prioridades do Conselho de Administração?	25,2%	67,3%	7,5%	20,4%	74,5%	5,1%	50%	41,7%	8,3%
A sua organização possui algum membro do Conselho de Administração com experiência em Segurança Cibernética?	20,1%	72,4%	7,5%	18,2%	77,4%	4,4%	41,7%	41,7%	16,7%

Além da dificuldade de priorização da segurança cibernética na estrutura de governança organizacional, 77,1% das indústrias possuem um orçamento inferior a 1% da receita total destinado para cibersegurança, conforme demonstrado no gráfico abaixo:



À luz desse contexto, evidencia-se um descompasso entre a crescente conscientização sobre a importância da cibersegurança e sua efetiva priorização nas estruturas de governança. A ausência de conhecimento ou de especialistas nos conselhos de administração, a baixa frequência de discussões sobre o tema e os orçamentos limitados revelam desafios estruturais significativos. Esses fatores precisam ser superados para que a segurança cibernética seja tratada com a urgência e a relevância que o atual ambiente digital exige, como parte integrante da estratégia corporativa e da resiliência organizacional.

Incidentes Cibernéticos

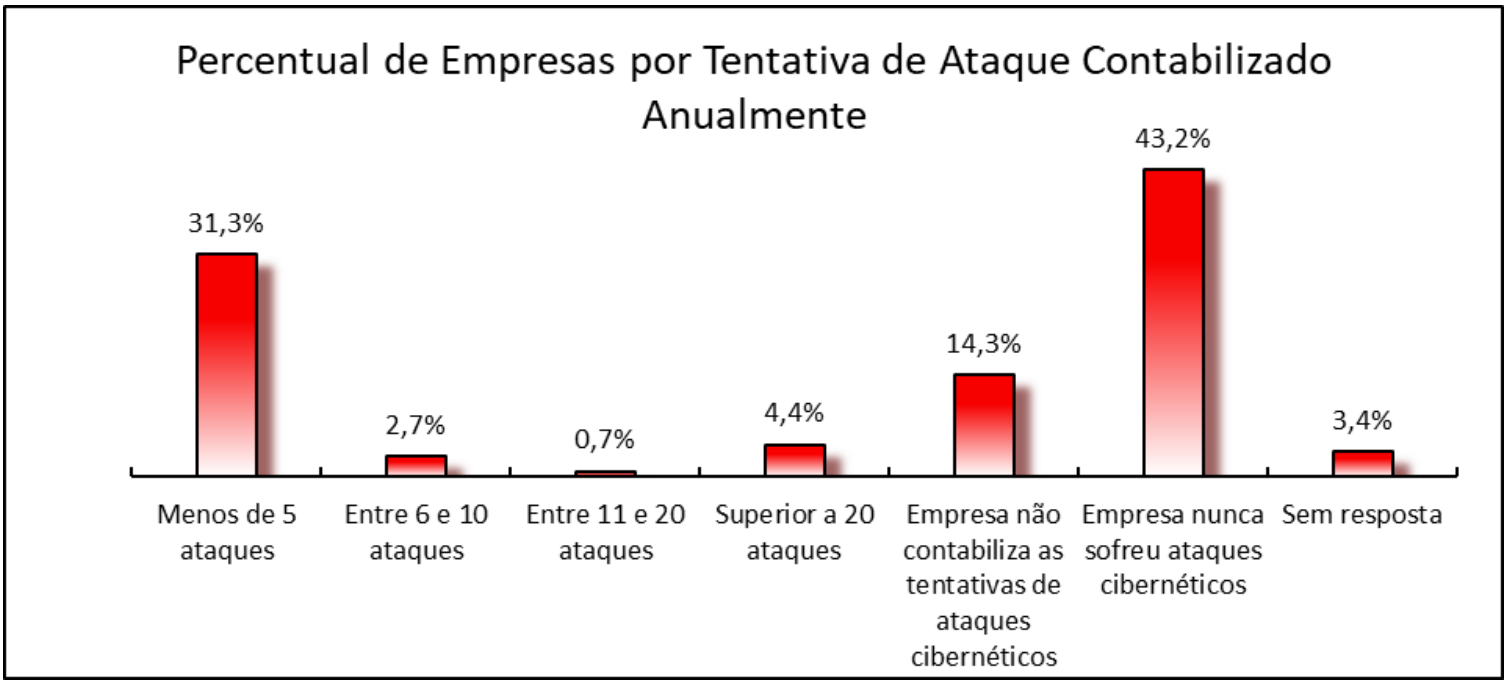
Conforme apresentado no Manual de Resposta a Incidentes Cibernéticos[2], lançado em 2024, pelo Departamento de Defesa e Segurança da FIESP, dentre as muitas complexidades que envolvem a cibersegurança, uma delas está no fato de existirem vários tipos de ataques, cada um com suas características e métodos específicos, mas que em comum, possuem efeitos que agem nos quatro princípios da segurança da informação: confidencialidade, integridade, disponibilidade e autenticidade.

No último ano, 34,7% das empresas afirmaram já ter sofrido algum ataque cibernético. Destes ataques, 42,2% foram exitosos, cujos principais objetivos foram: indisponibilizar a operação da empresa ou de produtos e serviços (65,1%), acessar ou extrair segredos de negócio (4,7%), e acessar ou extrair dados pessoais de clientes ou colaboradores (9,3%).

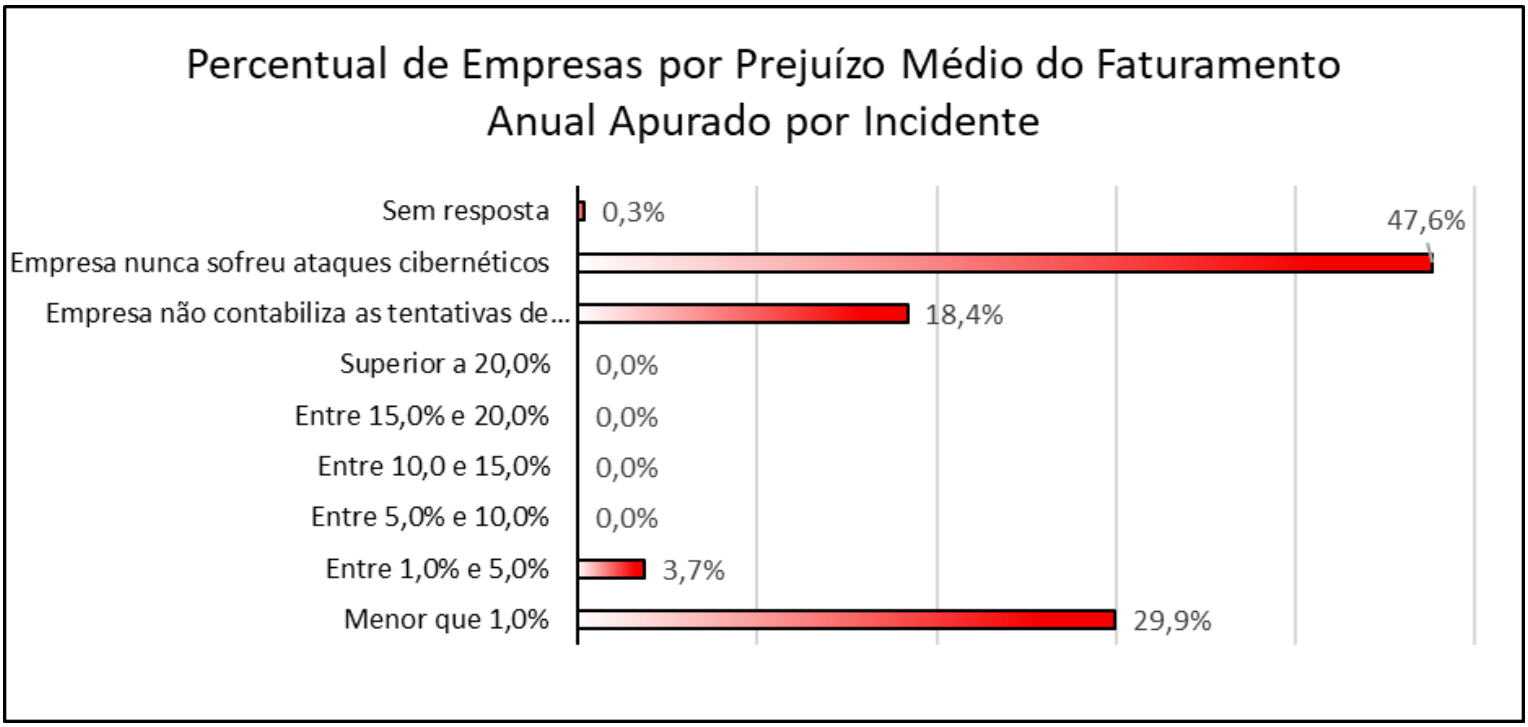
67,4% dos ataques cibernéticos declarados exitosos foram seguidos de tentativa de extorsão, entre eles, 34,5% das empresas atacadas pagaram o pedido financeiro de resgate e 65,5% não pagaram. As empresas que pagaram o pedido de resgate financeiro dos criminosos tiveram o reestabelecimento das operações ou a disponibilização dos dados exfiltrados. Entretanto, **o pagamento da extorsão é, na verdade, o que torna o delito comercialmente atrativo, sendo crucial reforçar a contraindicação a qualquer tipo de negociação com os responsáveis pelo ataque cibernético**.

Embora a maioria das empresas (62,2%) tenha declarado que nunca sofreu um ataque cibernético, no que diz respeito à contabilização anual do número de ataques, a imagem abaixo revela que uma parcela significativa (31,3%) relata até 5 ataques por ano, indicando que a experiência com ataques varia entre as organizações:

[2] Para mais informações sobre o Manual de Resposta a Incidentes Cibernéticos acesse: https://www.fiesp.com.br/indices-pesquisas-e-publicacoes/manual-de-resposta-a-incidentes-ciberneticos/



No tocante aos impactos financeiros dos incidentes cibernéticos, cerca de 30% das organizações afirmaram ter um prejuízo médio de até 1% do faturamento anual, que assumindo como parâmetro da faixa de faturamento que mais possuem respondentes na presente pesquisa, corresponderia a um valor entre 10.000 reais e 300.000 reais apurados por incidente. Detalhadamente:



A falha humana segue sendo a principal vulnerabilidade que motiva os ataques cibernéticos, representando 45,5% das declarações. Seguido de Serviços em nuvem ou softwares de terceiros (14,7%), atividade dolosa de colaboradores ou prestadores de serviços (12%), erro sistêmico (11,6%), credenciais comprometidas (7,2%). A dificuldade das próprias organizações em identificar as vulnerabilidades se tornou evidente com 8,9% das empresas declarando outras respostas, que, majoritariamente, não souberam responder.

O cenário descrito evidencia a crescente sofisticação e impacto dos ataques cibernéticos no setor industrial, revelando não apenas a frequência dos incidentes, mas também a vulnerabilidade estrutural das empresas diante dessas ameaças. A recorrência de falhas humanas como principal vetor de ataque, aliada à atratividade financeira das extorsões, reforça a urgência de investimentos em cultura organizacional, capacitação e medidas preventivas robustas para mitigar riscos e fortalecer a resiliência digital das organizações. Neste sentido, voltado para as empresas nacionais, o Departamento de Defesa e Segurança organizou os seguintes materiais:

- 1ª Cartilha sobre Cibersegurança para os Conselhos de Administração;
- Curso Online: Prevenção e Reação aos Incidentes Cibernéticos;
- Exercício de Simulação de Resposta a Incidente Cibernético;
- Manual de Resposta a Incidentes Cibernéticos.

Medidas preventivas

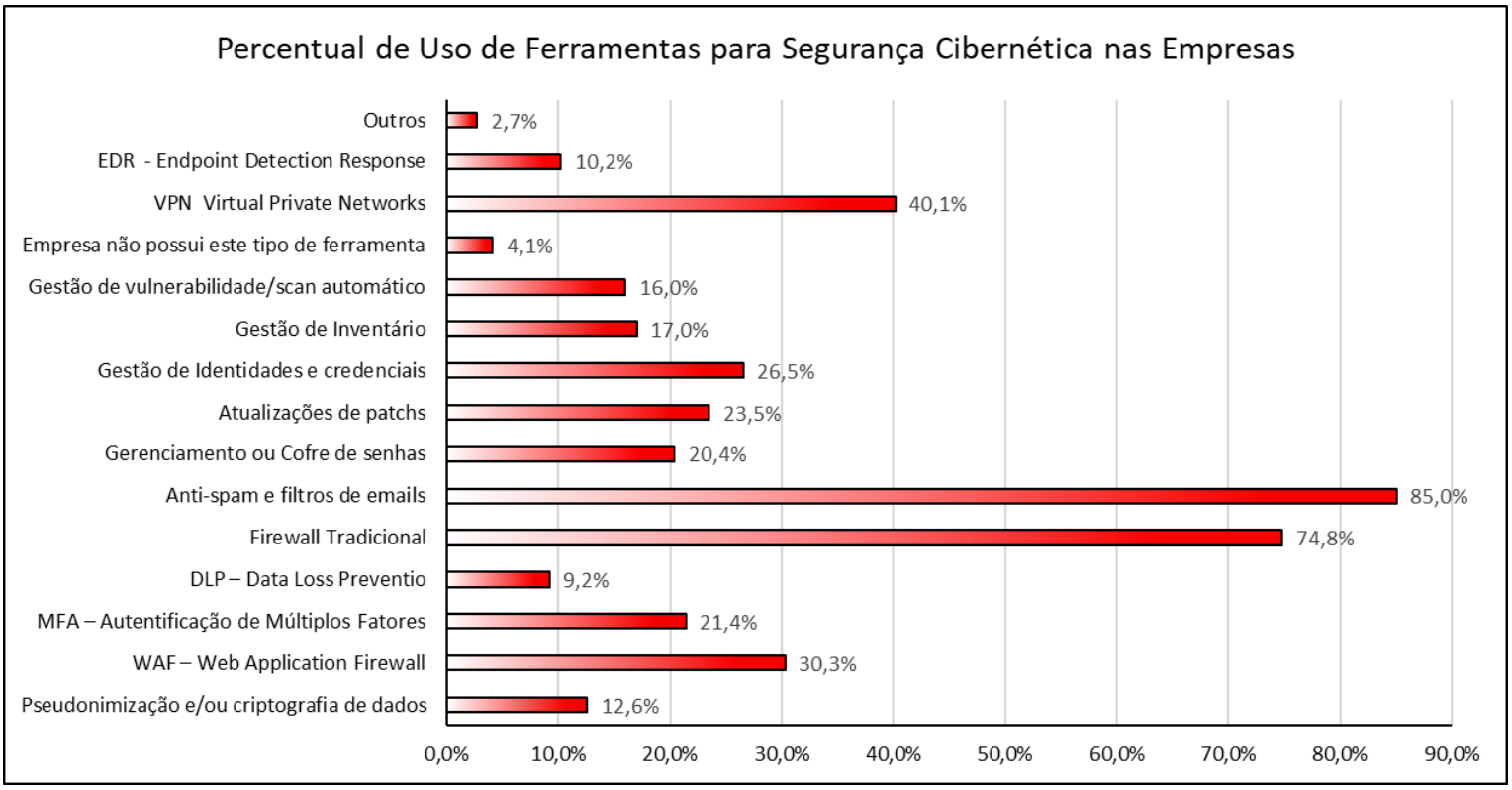
As medidas preventivas são fundamentais para mitigar a probabilidade e o impacto dos incidentes cibernéticos, além de impulsionar a capacidade de uma reposta rápida e adequada caso um incidente tenha êxito.

Como medidas básicas para segurança cibernética, 84% adotam e atualizam softwares de antivírus e antimalwares de acordo com recomendação da desenvolvedora selecionada e 13,3% adotam, mas atualiza esporadicamente. 1,7% das empresas não utilizam este tipo de software e 1% não souberam responder à pergunta. Por outro lado, a gestão de acesso de usuários autorizados aos sistemas é realizada em 85% das empresas, 11,9% não realizam e 3,1% não souberam responder. Já em relação à realização de PENTEST (Teste de Intrusão) indicou que 11,6% realizam com regularidade, 24,8% o fazem ocasionalmente, enquanto a maioria (63,3%), não realiza esse tipo de teste.

No que tange à existência de sistemas legados, 44,9% das empresas deixam estes sistemas isolados ou protegidos, enquanto 8,2% não isola ou os protege. 26,9% das empresas não possuem sistemas legados e outras 19,7% não souberam responder. Já em relação a medidas preventivas relacionadas à dependência de terceiros, 52,7% não faz nenhuma avaliação, 23,1% fazem um checklist no ato da contratação, 15% incluem no checklist pré-requisitos de segurança e faz parte do processo de compras avaliado anualmente. 9,2% das empresas utilizam ferramentas para fazer esta avaliação.

Entre as empresas respondentes, 56,8% não possuem o suporte de Centros de Operação de Segurança (SOC). Entre as que possuem, 18,4% adotam um SOC com funcionamento em horário comercial e 24,8% priorizaram uma adoção de um SOC 24 horas por dia durante os 7 dias da semana.

É neste contexto que as tecnologias de segurança se apresentam como essenciais, pois existem diversas ferramentas que podem ser utilizadas para aumento da resiliência cibernética, entre diferentes níveis de proteção oferecida e complexidade de uso, as mais adotadas foram as ferramentas anti-spam e filtro de e-mails, com 85%. De acordo com o percentual de uso nas empresas, segue abaixo quais foram as principais ferramentas utilizadas:



No âmbito da cibersegurança corporativa, observa-se uma disparidade substancial na adoção de ferramentas de proteção entre pequenas e médias empresas e organizações de

grande porte. As PMEs, em sua maioria, restringem-se à implementação de soluções básicas — como antivírus, firewalls tradicionais e filtros de e-mail — apresentando baixa diversidade tecnológica e menor taxa de penetração de ferramentas avançadas, como sistemas de detecção e resposta a incidentes (EDR) ou Virtual Private Networks (VPN), por exemplo. Essa lacuna pode ser atribuída, em grande parte, a limitações orçamentárias, escassez de profissionais especializados e à subestimação dos riscos associados a ameaças cibernéticas complexas.

Como consequência, o nível de maturidade em segurança da informação nas PMEs permanece inferior às grandes empresas que ainda estão aquém do necessário para enfrentar o cenário atual de ameaças, caracterizado por ataques cada vez mais sofisticados e direcionados.

Ferramentas:	PMEs (R$1M-30M/ano)	Grandes Empresas (R$300M-1B/ano)
Pseudonimização e/ou criptografia de dados	7,3%	16,7%
WAF – Web Application Firewall	24,1%	58,3%
MFA – Autentificação de Múltiplos Fatores	10,9%	41,7%
DLP – Data Loss Prevention	7,3%	25,0%
Firewall Tradicional	72,3%	91,7%
Anti-spam e filtros de emails	85,4%	91,7%
Gerenciamento ou Cofre de senhas	11,7%	33,3%
Atualizações de patchs	16,1%	66,7%
Gestão de Identidades e credenciais	15,3%	50,0%
Gestão de Inventário	5,8%	50,0%
Gestão de vulnerabilidade/scan automático	8,0%	41,7%
Empresa não possui este tipo de ferramenta	3,6%	0,0%
VPN Virtual Private Networks	26,3%	91,7%
EDR - Endpoint Detection Response	2,2%	41,7%
Outros	4,4%	0,0%

Indo além de softwares, a cultura de cibersegurança é um esforço essencial para garantir a segurança cibernética. Atualmente, 62,6% das empresas conscientizam e treinam seus colaboradores e prestadores de serviços sobre segurança da informação, privacidade e proteção de dados. 31,6% não tomam medidas para conscientização e 5,8% não sabem responder se há algum esforço neste sentido. Entre estas empresas que treinam os funcionários, 39,1% realizam os treinamentos anualmente, com uma frequência semestral são 22,8%, além de outras que realizam treinamento trimestral (14,1%), bimestral (4,3%) e mensal (19,6%).

Em comparação, entre as PMEs (R$1M-30M/ano), cerca 59,9% das empresas conscientizam e treinam seus colaboradores e prestadores de serviços sobre segurança da informação, privacidade e proteção de dados e 36,6% não realizam esta atividade. Já entre as empresas de grande porte (R$300M-1B/Ano), apenas 8,3% não conscientizam e treinam seus

colaboradores e prestadores de serviço, e 83,3% possuem esta preocupação com os colabores em relação à segurança cibernética, privacidade e proteção de dados.

Os dados também indicaram para uma baixa adesão aos serviços de seguros cibernéticos por todas as empresas, das quais 84,7% não contratam este tipo de serviço e 11,8% não souberam responder. Visando garantia de segurança e capacidade de resposta à incidentes, apenas 5,2% possuem seguro cibernético, dos quais 13,3% precisaram utilizar e 80% não precisaram utilizar.

A maioria, 60,2% das empresas não têm um plano de resposta a incidentes cibernéticos e 11,6% não souberam responder. Em comparação, nas PMEs (R$1M-30M/ano) 12,4% possuem e 77,4% não possuem, já entre as grandes (R$300M-1B/Ano) 66,7% possuem e 25% não possuem o plano de respostas. Do total de empresas que possuem um plano de resposta a incidentes cibernéticos (28,2%), 53% realizam testes via simulações e 41% não realizam testes do plano de incidentes. 6% não souberam responder.

Os dados da pesquisa indicam que, embora muitas empresas adotem medidas básicas de proteção, como softwares antimalware e filtro de e-mails, ainda há lacunas significativas em práticas mais estruturadas e estratégicas de segurança cibernética. A ausência de avaliações de terceiros, a baixa adoção de SOCs e seguros cibernéticos, bem como a falta de planos de resposta a incidentes, indicam uma maturidade limitada na gestão preventiva e reativa frente a ameaças digitais. Isso reforça a necessidade de uma abordagem mais abrangente e proativa para fortalecer a resiliência cibernética nas organizações.

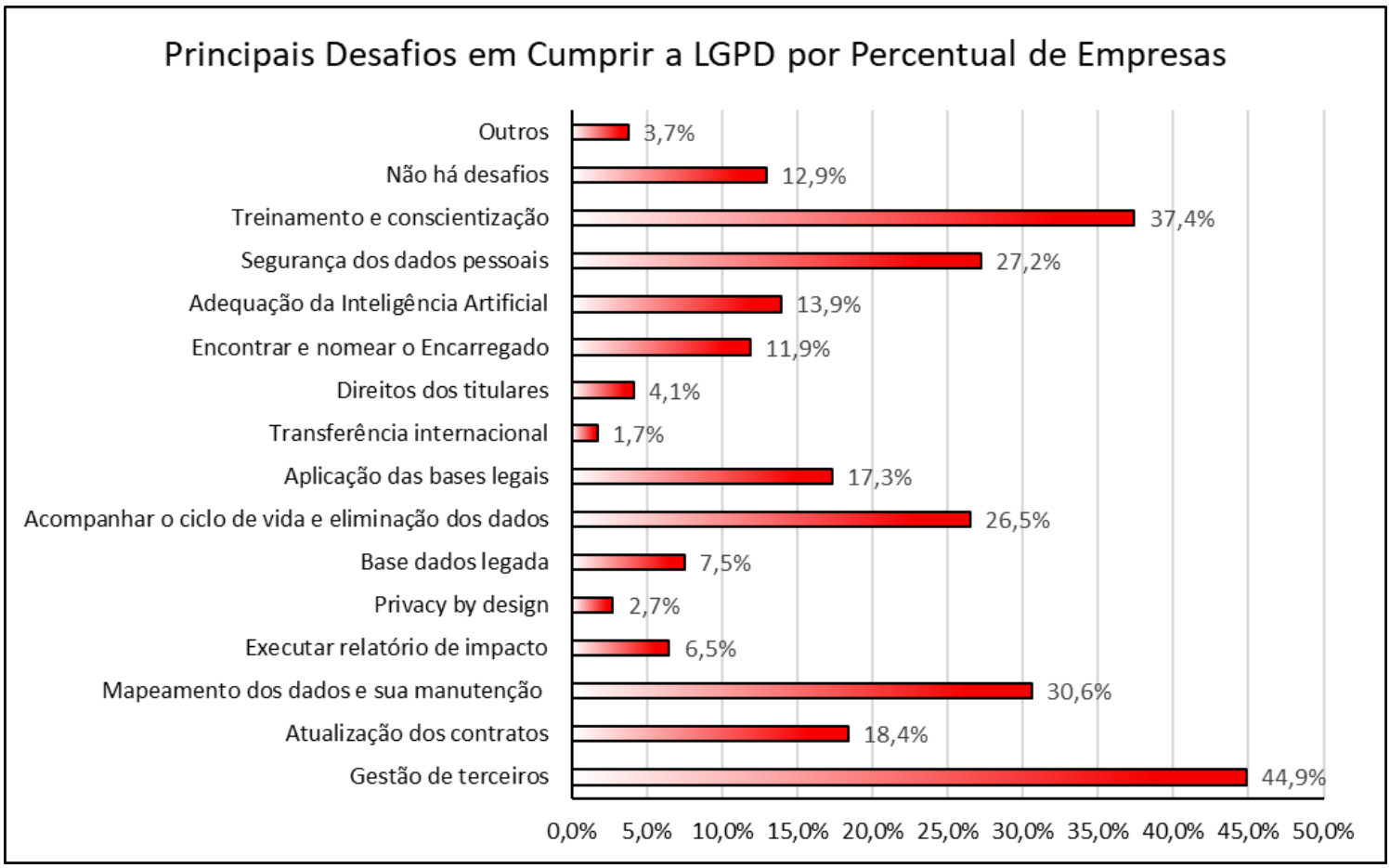
LEI GERAL DE PROTEÇÃO DE DADOS

A crescente digitalização das atividades empresariais e o uso intensivo de dados pessoais impõem às organizações o desafio de garantir a privacidade e a segurança das informações que tratam. Nesse contexto, a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD), estabelece regras para o tratamento de dados pessoais no Brasil. Esta seção aborda como as indústrias têm se adequado à LGPD, os principais desafios enfrentados na implementação de práticas de proteção de dados e a importância da governança e da responsabilidade no uso de informações pessoais em um ambiente cada vez mais conectado e regulado.

No último ano, 58,5% das empresas afirmaram possuir um programa de governança de proteção de dados e 35% afirmaram não ter. Ademais, apenas 38,1% das empresas declaram possuir um encarregado para o cumprimento da LGPD, entre estes, 51% não nomeou um encarregado e 4,1% está em processo de recrutamento. Entre as empresas que possuem um

encarregado de proteção de dados, 80,4% possuem um encarregado interno e 19,6% possuem um encarregado externo. Além disso, em 88,9% dos casos o encarregado acumula outras funções na organização, em 5,6% o encarregado tem dedicação exclusiva e 5,6% dos respondentes não souberam responder.

Neste contexto, 12,8% das empresas já passaram por algum processo de auditoria ou certificação da Lei Geral de Proteção de Dados e 78,5% não passou por nenhuma. 8,7% não souberam responder. Adicionalmente, no gráfico abaixo são apresentados os principais desafios enfrentados pelas empresas ao cumprir a Lei Geral de Proteção de Dados (LGPD):



Ainda relacionado com a temática de proteção de dados apenas uma empresa afirma já ter reportado incidentes para a Autoridade Nacional de Proteção de Dados ou outros órgãos competentes, sendo reportada apenas uma vez no último ano. Neste caso, é importante ressaltar que 11,6% das empresas não reportaram pois não tinham conhecimento da agência e, a maioria das empresas (86,1%) declaram não ter reportado qualquer incidente para autoridades competentes, independente do motivo.

A análise da adequação das indústrias à LGPD revela alguns avanços, mas enfatiza as fragilidades como a ausência de encarregados formais e a baixa realização de auditorias ou

certificações. A maioria dos encarregados acumula outras funções, o que gera a necessidade de avaliação de conflito de interesse. Outro ponto é a possível subnotificação de incidentes à ANPD, mesmo diante de exigências legais quando um incidente ocasionar risco ou dano relevante. A conformidade com a LGPD deve ser encarada não apenas como uma obrigação legal, mas como uma oportunidade estratégica para fortalecer a confiança, mitigar riscos e consolidar uma cultura organizacional orientada à responsabilidade no uso de dados.

Por este motivo, o Departamento de Defesa e Segurança (DESEG) da FIESP produziu uma série de materiais sobre a Lei Geral de Proteção de Dados. Acesse:

- 5ª edição da Cartilha LGPD;
- 2ª edição do Guia LGPD aos Sindicatos;
- 2ª edição do Guia Orientativo às Empresas - LGPD;
- Curso Online: Regulamentação da LGPD e Atuação da ANPD;
- Curso Online: Privacidade e Proteção de Dados (LGPD).

INTELIGÊNCIA ARTIFICIAL

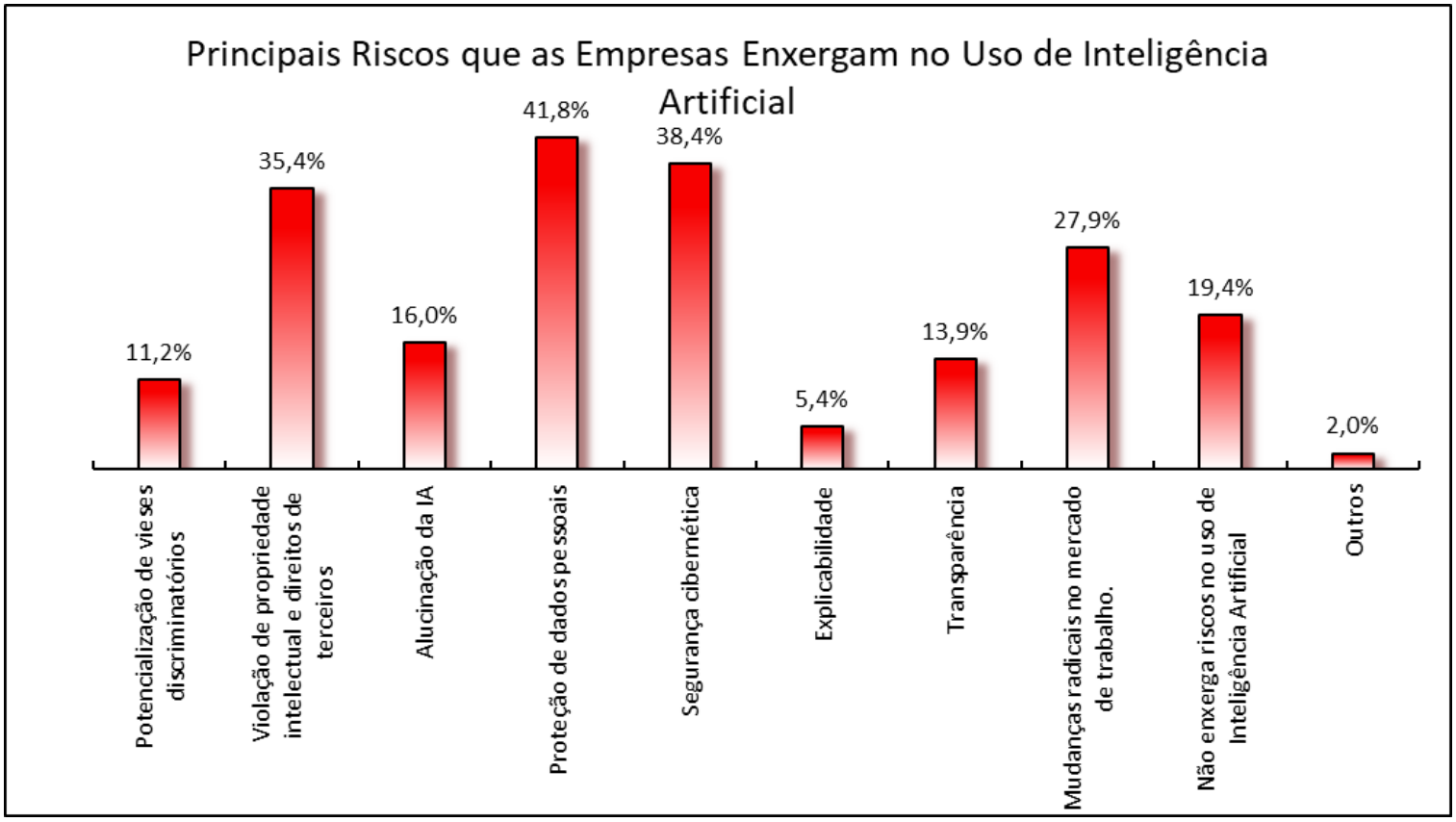
A Inteligência Artificial tem se tornado essencial para a sobrevivência, a competitividade e o desenvolvimento econômico e social de países e organizações — e o Brasil não é exceção.

Por outro lado, não podemos subestimar os desafios que a IA traz, como transformações abruptas no mercado de trabalho; explicabilidade, auditabilidade, supervisão e controle das decisões automatizadas; preservação de direitos autorais no treinamento de modelos em larga escala; cibersegurança; privacidade; discriminação algorítmica injusta; deepfakes e manipulações; dependência e confiança excessiva; e concentração de poder em poucos países e empresas.

Esta seção explora como a IA está sendo incorporada pelas indústrias, seus principais usos, desafios e oportunidades, considerando o cenário atual de maturidade e práticas de prevenção observadas no setor.

O gráfico abaixo apresenta os principais riscos percebidos pelas empresas no uso de Inteligência Artificial. O risco mais citado é a proteção de dados pessoais, com 41,8% das respostas, seguido pela segurança cibernética (38,4%). A violação de propriedade intelectual e direitos de terceiros também é um risco significativo, mencionado por 35,4% das empresas. Mudanças radicais no mercado de trabalho foram apontadas por 27,9% dos respondentes, enquanto 19,4% afirmaram não enxergar riscos no uso de IA. Outros riscos incluem alucinação

da IA (16,0%), transparência (13,9%), potencialização de vieses discriminatórios (11,2%), explicabilidade (5,4%) e outros (2,0%).



Diante dos principais riscos associados ao uso de Inteligência Artificial, destaca-se um preocupante cenário que 57,3% das empresas não possuem qualquer tipo de governança ética e responsável para orientar a adoção e o uso desta tecnologia. Além disso, 35% das organizações ainda não utilizam IA, e entre aquelas que já adotam essas soluções, apenas 7,7% implementam algum tipo de medida voltada à governança. Esses dados evidenciam uma lacuna significativa entre a percepção dos riscos e a adoção de práticas concretas para mitigá-los, indicando a necessidade de avanços em políticas internas, capacitação e diretrizes éticas.

Apesar do avanço da Inteligência Artificial no ambiente corporativo, a adoção de práticas de governança ética e responsável ainda é extremamente limitada. Apenas 4,5% das PMEs (R$1M-30M/ano) implementam algum tipo de medida para orientar o uso ético da IA. Em contraste, 54,9% sequer possuem qualquer política de governança, e 40,6% ainda não utilizam IA em suas operações. Nas empresas de grande porte (R$300M-1B/ano), o cenário é um pouco mais avançado em termos de adoção tecnológica, mas ainda preocupante do ponto de vista

ético: 16,7% não utilizam IA, e entre as que utilizam, 58,3% não adotam nenhuma medida de governança ética. Apenas 25% dessas empresas contam com diretrizes formais para o uso responsável da tecnologia.

CONSIDERAÇÕES FINAIS

Os dados da pesquisa revelam fragilidades que podem comprometer a resiliência digital das organizações brasileiras. A cibersegurança, embora cada vez mais reconhecida como um tema estratégico, ainda não ocupa posição prioritária na maioria das empresas, especialmente as de pequeno porte. A ausência de estruturas organizacionais dedicadas, a baixa frequência de discussões nos conselhos de administração e o nível insuficiente de conscientização apontam uma maturidade ainda limitada. Soma-se a isso, o orçamento restrito: 77,1% das empresas investem menos de 1% da receita anual em segurança cibernética.

No campo da proteção de dados, observa-se um avanço na preocupação com privacidade e conformidade com a LGPD. Contudo, ainda há desafios expressivos na implementação de uma governança estruturada, especialmente na gestão de dados por terceiros, no acompanhamento do ciclo de vida dos dados e na sua eliminação adequada, bem como na capacitação contínua de colaboradores.

No que tange à Inteligência Artificial, o uso corporativo está em expansão, mas a governança ética e responsável permanece incipiente. Apenas 7,7% das empresas que utilizam IA adotam medidas concretas de controle, apesar do reconhecimento de riscos relevantes associados à tecnologia, como: proteção de dados pessoais (41,8%), segurança cibernética (38,4%) e violação de propriedade intelectual (35,4%).

A ausência de diretrizes claras e a falta de preparo para lidar com os impactos sociais e operacionais da IA, indicam a necessidade de uma abordagem mais estratégica e preventiva.

Para avançar rumo a uma cultura digital mais segura, ética e sustentável, as organizações devem adotar uma abordagem holística e baseada em risco, que integre tecnologia, governança, pessoas e processos. O ponto de partida é um diagnóstico honesto do grau de maturidade digital, seguido de um planejamento estratégico que considere os riscos mais relevantes ao modelo de negócio.

Essa abordagem permite priorizar ações conforme a criticidade dos ativos, a exposição a ameaças e o impacto potencial de incidentes — promovendo eficiência na alocação de recursos e melhor proteção do valor empresarial.

No caso das pequenas e médias empresas (PMEs), os dados reforçam que fazer o básico bem feito pode trazer resultados concretos. Medidas simples, de baixo custo e alta efetividade, como configurações de segurança dos softwares existentes, controles de acessos, cópias de segurança, atualização de sistemas, políticas claras e treinamentos regulares, são essenciais para reduzir riscos e aumentar a resiliência.

Entre as prioridades para empresas de todos os portes, destacam-se:

- Governança digital estruturada, com conexão entre inovação, segurança da informação, proteção de dados, governança de IA e liderança executiva;
- Investimentos proporcionais ao risco, com foco em ativos críticos e medidas de maior impacto;
- Capacitação contínua, para construir uma cultura organizacional de cibersegurança e letramento em Inteligência Artificial;
- Políticas claras e atualizadas, como planos de resposta a incidentes, critérios para avaliação de fornecedores e orientações internas simples e aplicáveis;
- Ciclo de melhoria contínua, com indicadores, auditorias e participação em redes de troca de experiências.

Ao adotar uma abordagem pragmática, proporcional e orientada a risco, mesmo empresas com recursos limitados podem elevar significativamente sua maturidade digital — transformando segurança e governança em aliadas da inovação, da confiança do cliente e da perenidade dos negócios.

Para mais informações, acesse os nossos materiais e cursos gratuitos:

- **Cartilha LGPD – 5ª edição**: https://www.fiesp.com.br/indices-pesquisas-e-publicacoes/cartilha-lgpd-5a-edicao-setembro-2024/
- **2ª Edição do Guia LGPD aos Sindicatos**: https://www.fiesp.com.br/indices-pesquisas-e-publicacoes/guia-lgpd-aos-sindicatos-2a-edicao-julho-de-2024/
- **Cartilha sobre Cibersegurança para os Conselhos de Administração**: https://www.fiesp.com.br/indices-pesquisas-e-publicacoes/1a-cartilha-sobre-ciberseguranca-para-os-conselhos-de-administracao/
- **2ª edição do Guia Orientativo às Empresas – LGPD**: https://www.fiesp.com.br/indices-pesquisas-e-publicacoes/guia-orientativo-as-empresas-lgpd/
- **Manual de Resposta a Incidentes Cibernéticos**: https://www.fiesp.com.br/indices-pesquisas-e-publicacoes/manual-de-resposta-a-incidentes-ciberneticos/
- **Curso Online: Regulamentação da LGPD e Atuação da ANPD**: https://sp.senai.br/curso/regulamentacao-lgpd-obrigatorios/105192?unidade=150
- **Curso Online: Prevenção e Reação aos Incidentes Cibernéticos**: https://sp.senai.br/curso/prevencao-ciberneticos-obrigatorios/105191?unidade=150
- **Curso Online: Ética na Inteligência Artificial**: https://sp.senai.br/curso/eitcanaia/103483?unidade=150
- **Curso Online: Privacidade e Proteção de Dados (LGPD)**: https://www.sp.senai.br/curso/privacidade-e-protecao-de-dados-lgpd/94075?unidade=150

FICHA TÉCNICA

Realização

FEDERAÇÃO DAS INDÚSTRIAS DO ESTADO DE SÃO PAULO – FIESP
DEPARTAMENTO DE DEFESA E SEGURANÇA – DESEG

Carlos Erane de Aguiar
Diretor Titular do Departamento de Defesa e Segurança da FIESP

Dagmar Cupaiolo
Diretor Titular Adjunto do Departamento de Defesa e Segurança da FIESP

Rony Vainzof
Diretor Adjunto do Departamento de Defesa e Segurança da FIESP

Clara Martinolli
Gerente do Departamento de Defesa e Segurança da FIESP

Elaboração

Rony Vainzof
Diretor do DESEG e Responsável pelo Grupo de Trabalho de Segurança e Defesa Cibernética

Murilo Cesar Ançolim Nazareth
Analista do Departamento de Defesa e Segurança da FIESP

Rafael de Morais Lima
Analista do Departamento de Defesa e Segurança da FIESP

Coordenação Técnica

Juliana Mota
Coordenadora do Departamento de Defesa e Segurança da FIESP