Relatório

As PMEs na era da IA: navegar pela complexidade cibernética e criar resiliência

Com investigação e análise por

Sage

IDC

Metodologia e contexto do inquérito

Joel Stradling
Diretor Sénior de Investigação, Segurança Europeia, IDC

Este relatório baseia-se nos resultados de um estudo global realizado pela IDC, encomendado pela Sage, que inquiriu 2.210 pequenas empresas em oito mercados.

A investigação, publicada no relatório IDC InfoBrief "SMBs in the Age of AI: Navigating Cyber Complexity and Building Resilience" (março de 2026; IDC #EUR254487126) e da autoria do analista da IDC, Joel Stradling, avalia a forma como as PMEs estão a responder aos desafios atuais e emergentes da cibersegurança.

Explora as suas principais preocupações e posturas de segurança em relação à IA e às soluções de fornecedores externos, e identifica as mudanças estratégicas necessárias para migrar de uma defesa reativa para uma segurança proativa e uma resiliência cibernética sustentável e alinhada com os riscos.

O estudo abrangeu os seguintes setores: serviços financeiros, saúde, telecomunicações, energia, manufatura, recursos naturais, retalho, software e serviços de informação, transportes e viagens, serviços empresariais e pessoais, educação, governo, organizações sem fins lucrativos, auditoria e impostos, construção civil e hotelaria e lazer.

Fonte: IDC InfoBrief, "SMBs in the Age of AI: Navigating Cyber Complexity and Building Resilience", patrocinado pela Sage, abril de 2026, IDC Doc #EUR254487126.

Países incluídos no inquérito

- Canadá
- Espanha
- Estados Unidos
- Portugal
- França
- Reino Unido
- Alemanha
- África do Sul

Dimensão da empresa

1 - 9
Microempresa

10 - 99
Pequena empresa

100 - 499
Média empresa

"A IA deve ser uma oportunidade de crescimento para todas as PMEs, e não apenas para as que dispõem dos recursos de segurança mais fortes. As empresas mais pequenas continuam a ser mais cautelosas, uma vez que a adoção segura ainda é difícil na prática. Se queremos que mais PMEs beneficiem da IA, temos de tornar a cibersegurança mais simples de adotar através de salvaguardas incorporadas, orientações mais claras e apoio prático."

Gustavo Zeidan
Diretor de Segurança da Informação, Sage

Sage

Índice

Página 4
Resumo executivo

Página 5
A cibersegurança é agora uma prioridade central das PMEs - mas as exigências concorrentes em matéria de TI estão a esticar os orçamentos

Página 7
A governação da segurança continua a ser informal para a maioria das PMEs - limitando o impacto do aumento do investimento

Página 8
A maioria das PMEs tem as ferramentas de segurança certas, mas tem dificuldade em aplicá-las de forma consistente

Página 9
Quando a segurança continua a ser informal, os incidentes tornam-se perturbadores

Página 10
As ameaças em rápida evolução e a visibilidade limitada estão a aumentar a exposição das PMEs ao ciberespaço

Página 11
As ameaças impulsionadas pela IA estão a evoluir mais rapidamente do que as práticas de segurança das PMEs

Página 12
As PMEs procuram oportunidades na IA - mesmo quando o risco de segurança aumenta

Página 14
As PMEs já estão a lançar as bases para a conformidade regulamentar da IA

Página 15
Os desafios de segurança da IA para as PMEs centram-se nas lacunas de competências, na proteção de dados e nas ameaças em rápida evolução

Página 16
A monitorização limitada dos fornecedores de SaaS deixa muitas PMEs expostas

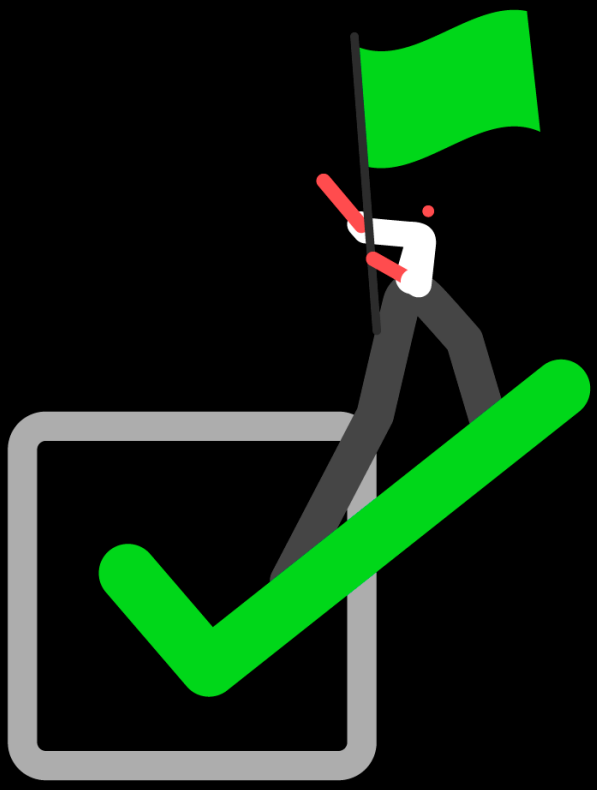
Página 17
As PMEs confiam em provas claras e verificáveis quando avaliam fornecedores externos

Página 18
Transformar a perceção em ação

Página 21
Mensagem da Sage

Página 22
Anexo: perceções do país

Resumo executivo



As PMEs estão a aumentar o investimento em cibersegurança e a acelerar a adoção da IA. Mas, para muitas delas, as práticas de segurança ainda estão a ficar para trás em relação ao ritmo das mudanças, deixando-as mais vulneráveis à medida que o risco aumenta mais rapidamente do que a resiliência.

Com base num inquérito a 2.210 PMEs em oito mercados, este relatório analisa a forma como as pequenas e médias empresas estão a responder à evolução dos desafios da cibersegurança, com especial destaque para a adoção da IA e o risco de fornecedores externos. A cibersegurança é agora uma prioridade de negócio fundamental para as pequenas e médias empresas.

Neste estudo, 52% das PMEs afirmam que garantir a cibersegurança e a proteção de dados é uma das suas principais prioridades para os próximos 12 meses, apenas atrás do crescimento do negócio, com 59%, e muito à frente da expansão da utilização da IA, com 33%. Ao mesmo tempo, 60% esperam aumentar as despesas com a cibersegurança, mostrando uma clara intenção de agir.

Mas, para muitas PMEs, a ação ainda não está a acompanhar o risco. Cerca de metade das empresas relatam ter sofrido um incidente cibernético todos os anos e as práticas de segurança proativas continuam a ser limitadas, especialmente entre as empresas mais pequenas. Apenas 13% das microempresas e 21% das pequenas empresas descrevem a sua abordagem como proativa, em comparação com 48% das organizações de média dimensão.

A IA está a aumentar a pressão. Não está a criar um conjunto de riscos totalmente novo, mas está a tornar as ameaças conhecidas mais rápidas, mais convincentes e mais difíceis de gerir. Muitas PMEs ainda estão na fase inicial de preparação para as ameaças relacionadas com a IA, em especial as empresas mais pequenas. 84% das microempresas e 65% das pequenas empresas afirmam que não estão preparadas ou estão apenas a dar os primeiros passos.

Ao mesmo tempo, 22% afirmam não ter medidas de segurança específicas em vigor para aplicações de IA, aumentando para 44% entre as microempresas.

Os riscos relacionados com SaaS de terceiros e com a cadeia de abastecimento representam um grande ponto cego. Embora as ferramentas SaaS estejam omnipresentes nos ecossistemas das PMEs, 43% das microempresas não realizam uma monitorização regular ou contínua dos fornecedores externos, confiando, em vez disso, em certificações estáticas ou verificações pontuais. Este facto limita a visibilidade em tempo real do risco dos fornecedores e aumenta a probabilidade de as falhas de segurança não serem detetadas até ocorrerem perturbações.

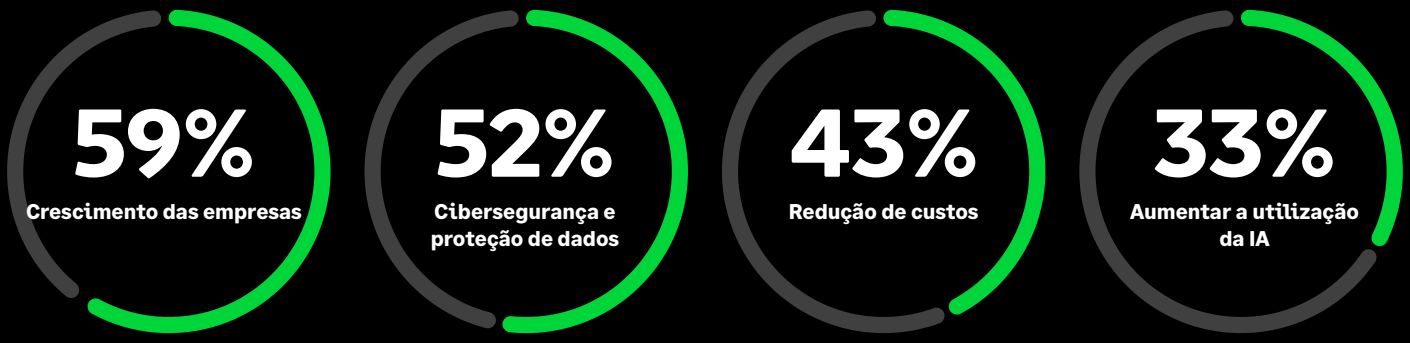
Os resultados apontam para um imperativo claro: as PMEs não precisam de mais complexidade. Precisam de formas mais simples e práticas de ultrapassar a segurança reativa e baseada em ferramentas e tornar a gestão do risco parte do quotidiano empresarial.

Isto significa integrar a segurança desde o início, reforçar a disciplina quotidiana e centrar-se numa propriedade clara, na monitorização regular e na sensibilização dos trabalhadores de forma a refletir a dimensão da empresa. Fazer isto corretamente é importante não só para as organizações individuais, mas também para a confiança dos clientes, para as cadeias de abastecimento e para a resiliência do ecossistema digital em geral.

A cibersegurança é agora uma prioridade central das PMEs, mas as exigências concorrentes em matéria de TI estão a esticar os orçamentos

Quando questionadas sobre as suas principais prioridades de negócio para os próximos 12 meses, mais de metade das PMEs (52%) citam a cibersegurança e a proteção de dados, colocando-as logo atrás do crescimento do negócio (59%) e à frente da redução de custos (43%). Este facto assinala uma clara mudança de mentalidade. O risco cibernético já não é visto como uma questão puramente técnica, mas como uma preocupação comercial importante.

Principais prioridades empresariais para o ano:



Planeamento do aumento do orçamento de segurança nos próximos 12 meses:

51% **1 - 9**
Microempresa

59% **10 - 99**
Pequena empresa

65% **100 - 499**
Média empresa

Sage

Esta intenção é reforçada pelo investimento planeado. Seis em cada dez PMEs (60%) afirmam que esperam aumentar as despesas com a cibersegurança nos próximos 12 meses, o que indica tanto o reconhecimento do problema como a vontade de agir. No entanto, as pressões concorrentes - incluindo o controlo dos custos e a aceleração da adoção da IA (33%) - significam que o progresso é desigual.

Como resultado, embora a cibersegurança esteja claramente a subir na lista de prioridades, o aumento das despesas nem sempre se traduz numa melhor preparação, ajudando a explicar por que razão persistem lacunas na confiança, governação e execução em todo o mercado das PMEs.

Os dados apontam para uma lacuna crescente entre intenção e execução. A cibersegurança é mais importante do que nunca, mas muitas PMEs têm dificuldade em operacionalizá-la de forma consistente.

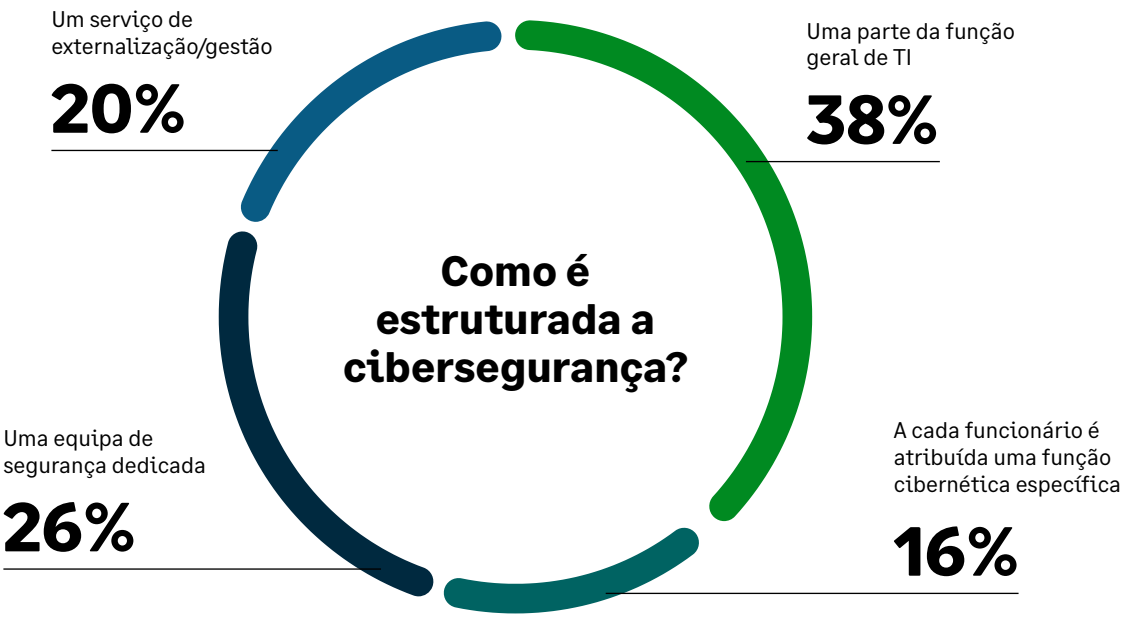
das PMEs afirmam que esperam aumentar as despesas com cibersegurança nos próximos 12 meses

A governação da segurança continua a ser informal para a maioria das PMEs, limitando o impacto do aumento do investimento

Para a maioria das PMEs (38%), as responsabilidades em matéria de cibersegurança continuam a ser definidas de forma vaga e integradas na função de TI mais alargada, em vez de serem apoiadas por uma propriedade clara, ciclos de revisão formais ou processos documentados.

Consequentemente, a atividade de segurança é muitas vezes reativa, desencadeada por incidentes, em vez de ser gerida como uma disciplina empresarial de rotina.

Esta lacuna de governação ajuda a explicar por que razão o aumento das despesas com a cibersegurança nem sempre resulta numa maior preparação. Sem uma responsabilização mais clara, uma supervisão de rotina e uma disciplina operacional, mesmo um investimento bem-intencionado tem dificuldade em proporcionar uma redução consistente dos riscos - especialmente à medida que a IA e as ferramentas de terceiros aumentam a exposição.



Para colmatar esta lacuna, **as PMEs precisam de tornar a segurança uma parte mais consistente do quotidiano empresarial**, com uma responsabilidade clara, uma revisão regular e processos práticos que possam ser escalados ao longo do tempo.

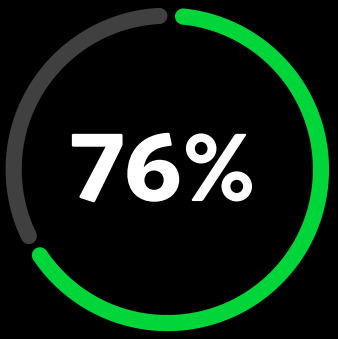
A maioria das PMEs tem as ferramentas de segurança corretas, mas tem dificuldade em aplicá-las de forma consistente

Os controlos técnicos essenciais são agora padrão na maioria das PMEs, mas continuam a existir desafios em áreas como a gestão de ferramentas, a formação do pessoal e o planeamento da resposta a incidentes.

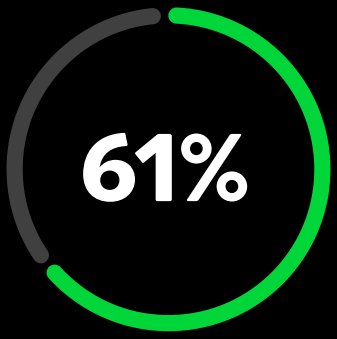
Como resultado, a maturidade em matéria de segurança depende menos da introdução de novos controlos e mais da incorporação da disciplina operacional necessária para manter as salvaguardas existentes eficazes à medida que o negócio evolui.

Para reforçar a postura de cibersegurança, as PMEs devem dar maior ênfase à governação dos dados, aos controlos de segurança e à transparência. À medida que crescem, isto exige ciclos de revisão mais formais, responsabilidades claramente definidas e processos consistentemente documentados em toda a organização.

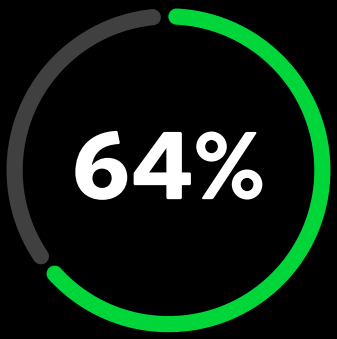
Indicadores de confiança operacional:



revêm regularmente a sua cibersegurança

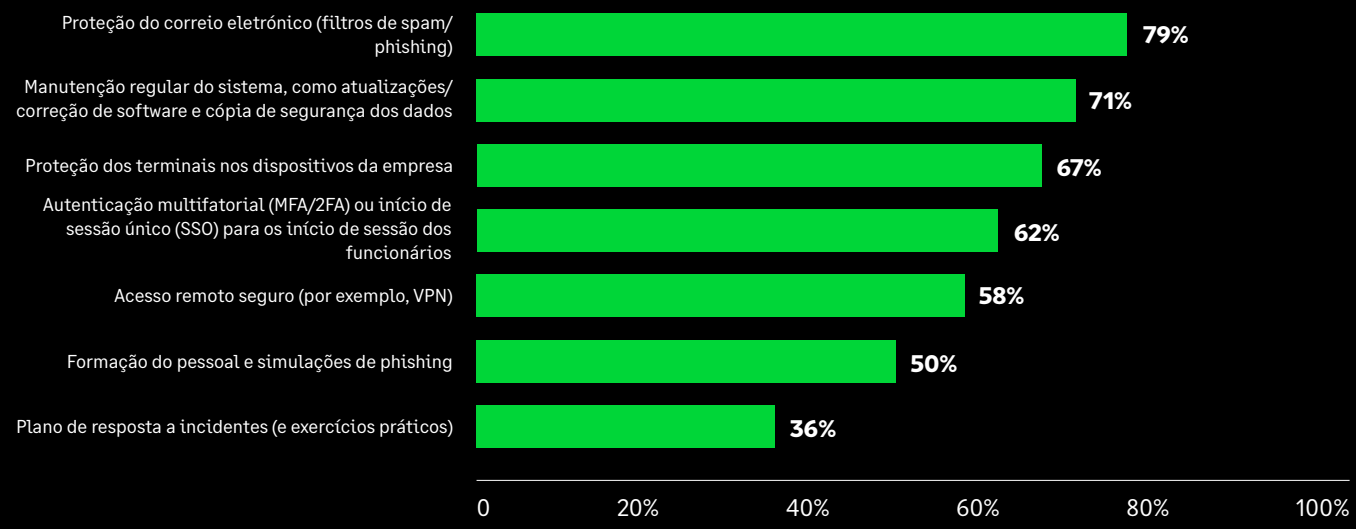


dizem que os funcionários recebem formação para identificar os riscos cibernéticos



analisam rigorosamente a segurança dos terceiros antes de os contratar

Que medidas de cibersegurança estão atualmente em vigor?



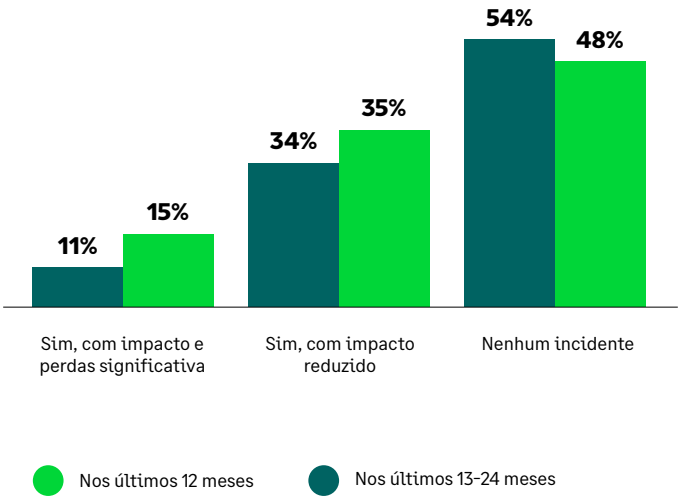
Quando a segurança continua a ser informal, os incidentes tornam-se perturbadores

Para as PMEs, o risco cibernético já não é uma perturbação ocasional. É um desafio comercial permanente, moldado por uma mistura de ameaças mais vasta e menos previsível, desde o phishing e a engenharia social ao risco interno, à exposição de terceiros e às vulnerabilidades da cadeia de abastecimento.

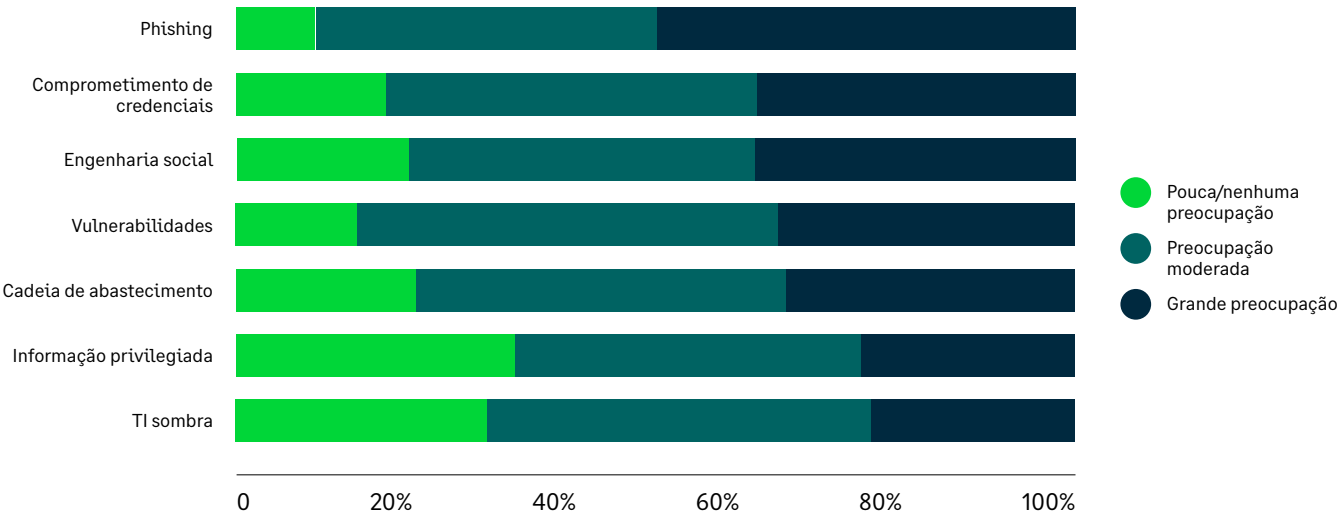
À medida que esta exposição aumenta, a resiliência passa a depender menos da tentativa de prevenir todos os incidentes e mais da capacidade de gerir bem as interrupções.

Isto muda o foco dos incidentes em si para a qualidade da resposta: a rapidez com que os problemas são identificados, a eficácia com que são contidos e a consistência com que a empresa consegue recuperar, protegendo a confiança, o fluxo de caixa e a continuidade do negócio.

Incidentes de cibersegurança ou violações de dados



Preocupação com cada um dos seguintes riscos



Para as PMEs, isto significa pôr em prática **formas simples e repetíveis de detetar problemas atempadamente**, responder rapidamente, conter o impacto e manter a empresa a funcionar quando ocorrem perturbações.

A rápida evolução das ameaças e a visibilidade limitada estão a aumentar a exposição das PMEs ao ciberespaço

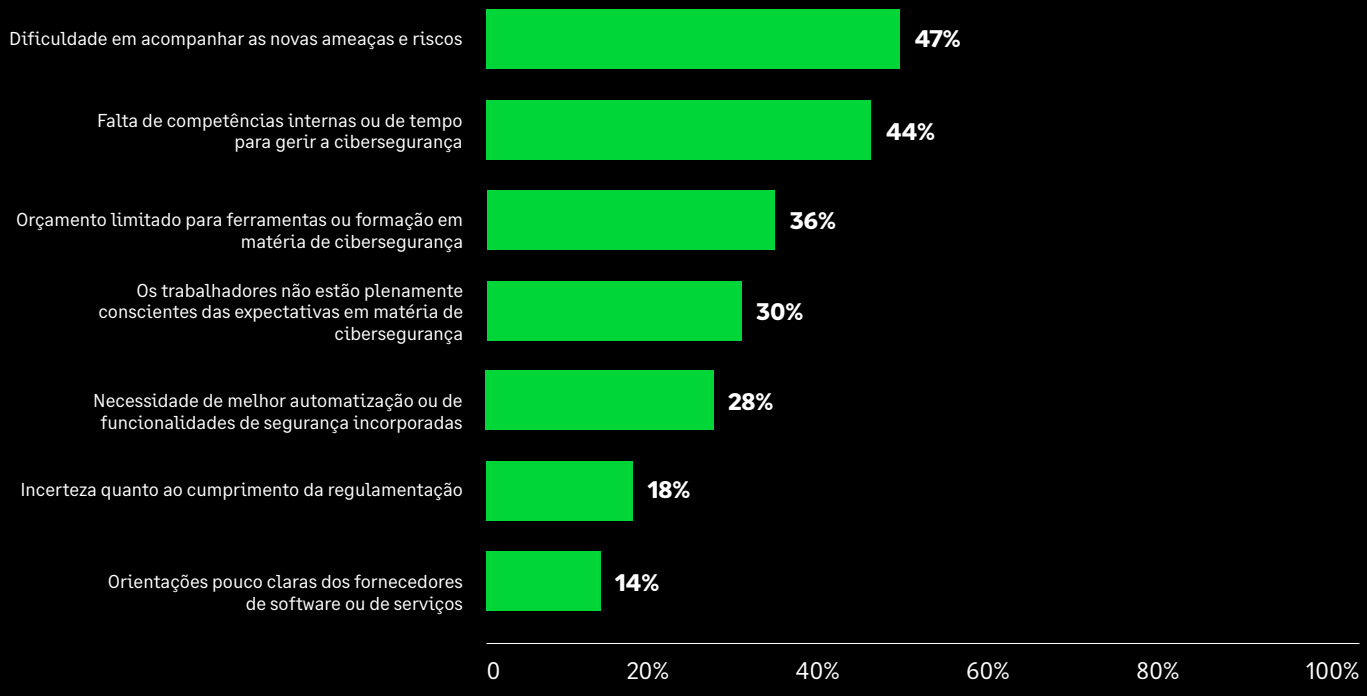
Quase metade das PMEs (47%) considera que acompanhar as novas ameaças e riscos é o seu principal desafio em matéria de cibersegurança.

Os ataques com IA, o phishing mais sofisticado e a crescente utilização de serviços de nuvem e SaaS estão a aumentar tanto a velocidade como a complexidade do risco cibernético — muitas vezes mais rápido do que a capacidade de adaptação interna. Ao mesmo tempo, muitas PMEs carecem de uma visibilidade clara e contínua sobre onde residem as suas maiores vulnerabilidades.

As competências especializadas limitadas, as prioridades operacionais concorrentes e as restrições orçamentais dificultam a manutenção da monitorização contínua ou da avaliação estruturada dos riscos. Como resultado, o risco cibernético é frequentemente compreendido em termos gerais, mas não gerido ativamente no dia-a-dia.

Esta combinação — ameaças em rápida evolução e visibilidade incompleta — aumenta significativamente a probabilidade de os problemas serem detetados tardiamente, priorizados de forma inconsistente ou resolvidos apenas após a ocorrência de uma interrupção. Para as PMEs com uma governação informal e uma disciplina operacional inconsistente, isto cria um fosso persistente entre o risco percebido e a exposição real.

Qual das seguintes opções descreve melhor os principais desafios que a sua organização enfrenta na gestão da cibersegurança?



Para acelerar o progresso, as PMEs devem dar prioridade a soluções que reduzam os encargos operacionais, incluindo a automatização, as salvaguardas incorporadas e o apoio externo adaptado às suas limitações de recursos.

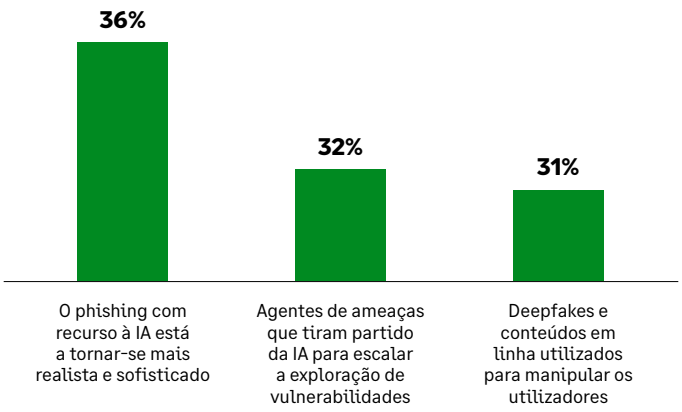
As ameaças impulsionadas pela IA estão a evoluir mais rapidamente do que as práticas de segurança das PMEs

A IA está a aumentar a pressão num cenário cibernético já de si desafiante, e as empresas mais pequenas são as menos preparadas para o acompanhar.

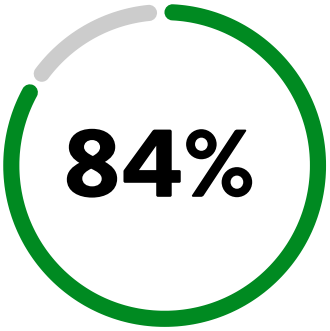
As micro e pequenas organizações enfrentam as maiores lacunas, com uma supervisão diária mais fraca, uma monitorização menos consistente e uma menor sensibilização do pessoal, deixando-as mais expostas à medida que a IA aumenta a velocidade e a escala dos ataques. As práticas de segurança que podem ter sido suficientes no passado estão a tornar-se menos eficazes à medida que as ameaças evoluem mais rapidamente.

Para as PMEs, a resposta deve começar pelo básico: maior sensibilização, salvaguardas práticas e formas mais claras de detetar e gerir os riscos numa fase precoce. Mas isso é apenas parte da resposta. À medida que as ameaças relacionadas com a IA evoluem, as empresas também precisarão de formas mais simples de automatizar as tarefas de segurança de rotina, reduzir o esforço manual e libertar a capacidade limitada de TI e segurança para se concentrarem nas áreas de maior risco.

As 3 principais preocupações sobre os riscos emergentes da IA

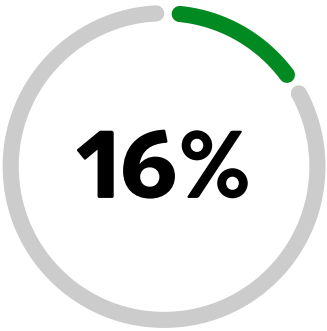


Não estão preparadas ou estão numa fase inicial de preparação para ameaças relacionadas com a IA:



Microempresa

Pequenas empresas



Média empresa

Para as **PMEs menos maduras, em particular, a educação e a sensibilização continuam a ser fundamentais.** Os líderes de segurança devem dar prioridade a medidas práticas e fáceis de adotar que ajudem as equipas a reconhecer e reduzir os riscos relacionados com a IA sem acrescentar complexidade desnecessária.

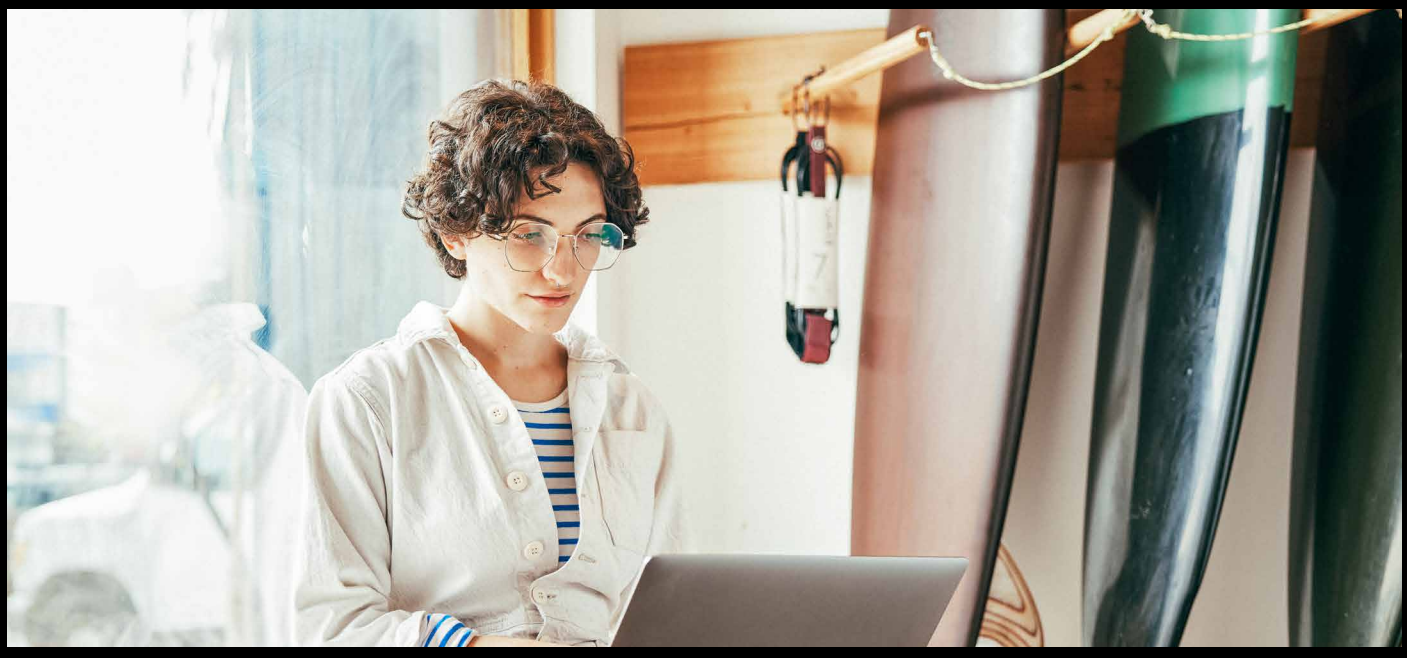
Sage

As PMEs procuram oportunidades na IA, mesmo com o aumento do risco de segurança

Uma parte significativa das PMEs vê uma oportunidade na IA, mas uma percentagem maior acredita que a IA aumenta o risco cibernético. Uma parte significativa das PMEs vê uma oportunidade na IA, enquanto uma proporção maior acredita que a IA aumenta o risco cibernético. A perceção varia consoante a dimensão. As médias empresas têm maior probabilidade de ver a IA como uma oportunidade.

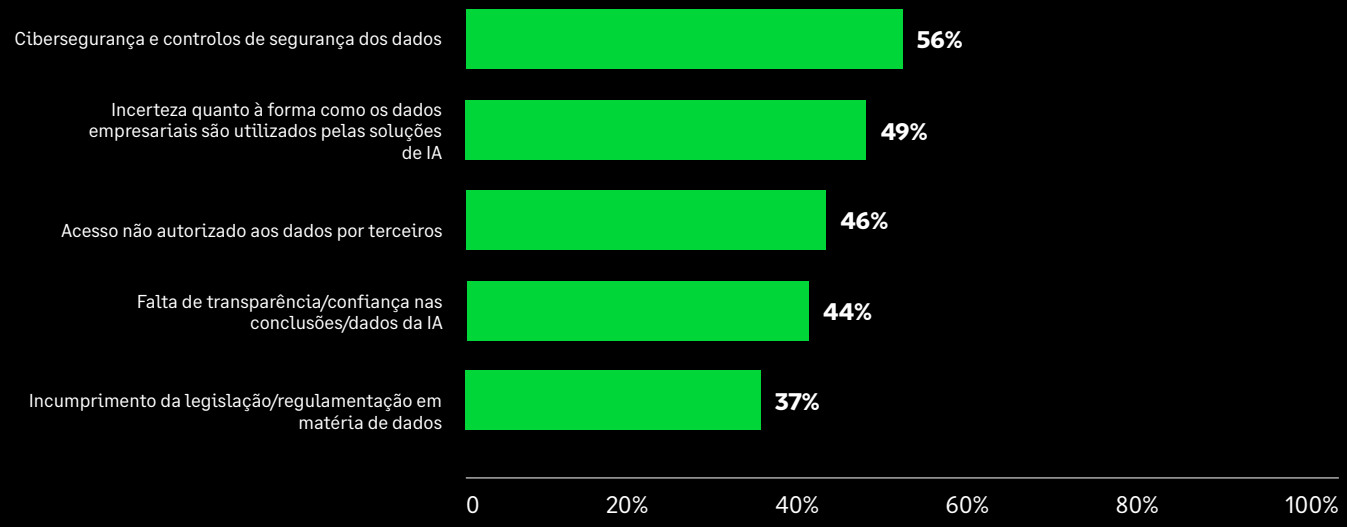
As micro e pequenas empresas abordam a IA com mais cautela. Isto reflete diferenças na confiança nos controlos de segurança e na governação, e não na ambição.

A IA é vista como uma oportunidade de negócio:



Existem preocupações em torno da segurança dos dados, da governação e da transparência na adoção da IA. Sem uma visibilidade clara de como os dados são usados e protegidos, muitas PMEs permanecem cautelosas quanto ao dimensionamento da IA.

Qual das seguintes opções melhor descreve as suas principais preocupações quanto à adoção ou utilização da IA na sua empresa?



À medida que a IA se torna mais integrada nas operações diárias, as PMEs precisam de uma visibilidade clara sobre onde e como está a ser utilizada, juntamente com uma governação definida para gerir os riscos associados. Isto inclui a identificação de ferramentas e sistemas de IA em toda a empresa e o estabelecimento de supervisão, políticas e responsabilidade adequadas a nível de liderança. Sem isso, o ritmo de adoção da IA pode ultrapassar a capacidade de uma organização para gerir o risco, aumentando a exposição em vez de proporcionar valor.

As PMEs já estão a lançar as bases para a conformidade regulamentar da IA

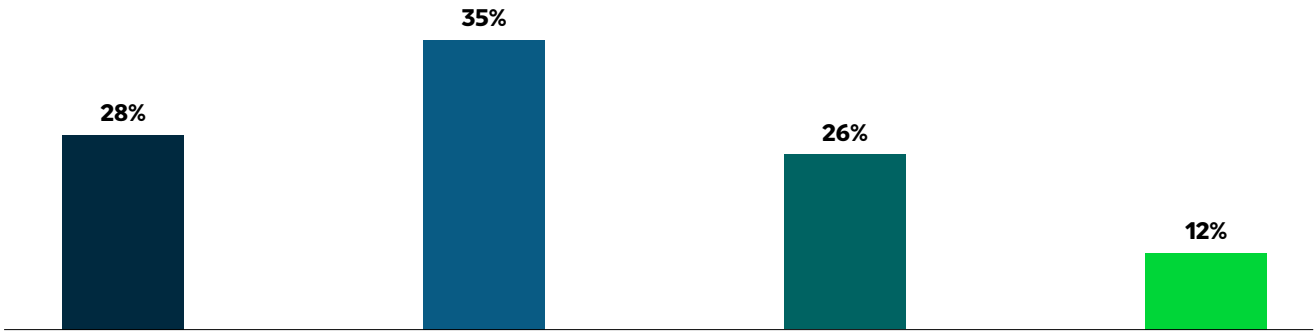
À medida que os regulamentos e normas de IA continuam a surgir, muitas PMEs estão a começar a lançar as bases para a conformidade.

Quadros como os regulamentos nacionais em matéria de IA e os códigos de conduta voluntários destinam-se a ajudar as organizações a traduzir políticas de alto nível em medidas práticas e quotidianas de segurança e governação. Um número crescente de governos está a reconhecer que o software de base e as práticas de segurança da IA têm de ser amplamente adotados em toda a cadeia de abastecimento, e não apenas pelas grandes empresas. Países como o Reino Unido estão a concentrar-se em abordagens práticas e proporcionais.

Um exemplo é o Código de Práticas de Segurança do Software e o Esquema de Embaixadores de Segurança do Software associado, lançado como parte do Plano de Ação Cibernética do Governo do Reino Unido. O esquema reúne organizações dos setores público e privado - incluindo a Sage - para defender a adoção de princípios fundamentais de segurança de software, partilhar experiências práticas de implementação e apoiar uma maior resiliência em toda a economia.

> “As PMEs são a espinha dorsal da economia britânica, mas sabemos que muitas têm dificuldades em investir em cibersegurança numa altura em que as ciberameaças estão a aumentar. Melhorar a resiliência cibernética em todo o Reino Unido é uma prioridade para o governo, razão pela qual o nosso Centro Nacional de Cibersegurança desenvolveu o Kit de Ferramentas de Ação Cibernética para ajudar as PMEs a reforçar as suas defesas cibernéticas. Recomendamos que todas as empresas adotem o nosso programa Cyber Essentials, altamente eficaz, que ajuda a proteger contra ameaças online comuns e reduz as probabilidades de se tornarem vítimas de um ciberataque dispendioso e disruptivo.”
>
> **A Deputada Liz Kendall, Secretária de Estado da Ciência, Inovação e Tecnologia do Reino Unido**

Preparação das PMEs para cumprirem os regulamentos e as normas de garantia da IA



Não preparadas
Pouca ou nenhuma sensibilização ou planeamento para os regulamentos ou normas da IA

A dar os primeiros passos
Consciente dos requisitos futuros; discussões iniciais ou planeamento em curso

Em curso
Desenvolvimento ativo de políticas, controlo e governação para cumprir

Bem preparadas
Processos e salvaguardas já em vigor para cumprir os novos requisitos

Para as PMEs, iniciativas como esta destacam um caminho pragmático: alinhar-se com quadros reconhecidos, escolher parceiros comprometidos com o desenvolvimento seguro e incorporar práticas básicas de segurança desde o início, à medida que a adoção da IA acelera.

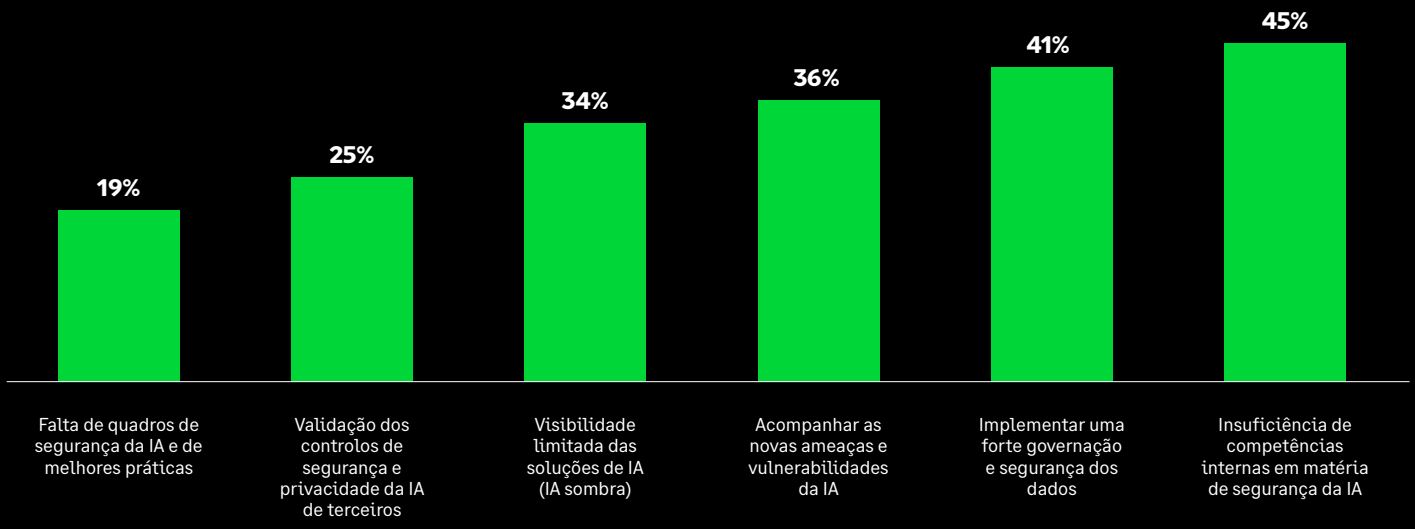
Os desafios de segurança da IA para as PMEs centram-se em lacunas de competências, proteção de dados e ameaças em rápida evolução

A IA está a expor uma lacuna de capacidade para as PMEs, e não apenas uma lacuna tecnológica. Muitas organizações estão a adotar a IA mais rapidamente do que conseguem compreender os riscos, avaliar a exposição ou julgar a segurança dos fornecedores externos.

Isto é especialmente difícil para as pequenas empresas, onde a responsabilidade recai frequentemente sobre um único especialista em TI ou uma equipa generalista.

A proteção de dados e as ameaças em rápida evolução aumentam o desafio. Uma vez que as ferramentas de IA dependem do acesso a dados comerciais e de clientes, uma visibilidade fraca e uma supervisão pouco rigorosa podem aumentar rapidamente a exposição. Ao mesmo tempo, a IA está a tornar os ataques familiares mais rápidos, mais convincentes e mais difíceis de gerir, deixando muitas PMEs com dificuldades em acompanhar o ritmo.

Maiores desafios na proteção de aplicações e infra-estruturas de IA e GenAI



Para as PMEs com recursos especializados limitados, a prioridade é manter a praticidade: limitar a utilização da IA a ferramentas aprovadas, definir regras simples para os dados que podem ou não ser introduzidos, rever regularmente a utilização da IA e apoiar-se em fornecedores de confiança ou parceiros externos quando os conhecimentos internos são limitados. Isto contribuirá mais para reduzir o risco do que aumentar a complexidade.

A monitorização limitada dos fornecedores de SaaS deixa muitas PMEs expostas

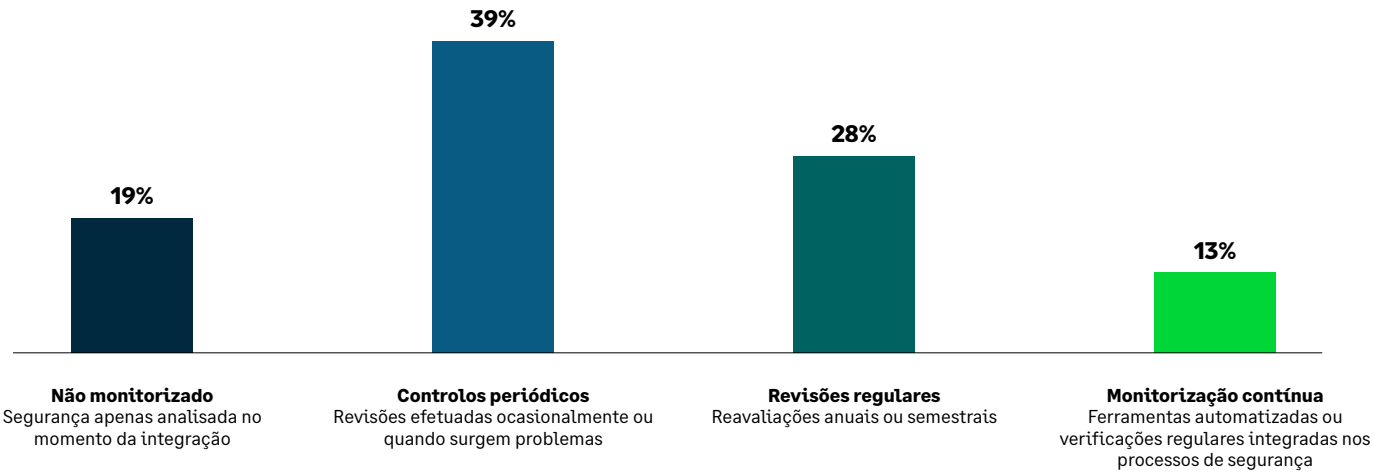
As aplicações SaaS e as plataformas de terceiros estão agora no centro das operações de muitas PMEs, mas a supervisão da segurança permanece frequentemente intermitente.

Para muitas empresas, o risco do fornecedor é revisto no início de uma relação ou quando um contrato é renovado, em vez de ser monitorizado continuamente. Este facto deixa lacunas na visibilidade, aumenta a exposição e aumenta a possibilidade de os problemas só serem identificados depois de já terem ocorrido perturbações.

As micro e pequenas empresas estão particularmente expostas, com uma percentagem significativa a referir pouca ou nenhuma monitorização regular dos serviços de terceiros. Consequentemente, os potenciais problemas podem passar despercebidos até que ocorra uma perturbação.

As PMEs mais maduras adotam controlos de acesso centralizados, uma gestão mais clara do ciclo de vida dos utilizadores e análises mais regulares dos fornecedores, o que melhora a sua capacidade de identificar anomalias e responder mais cedo. Os resultados sugerem que tratar a segurança de terceiros como um processo contínuo - em vez de uma verificação pontual - é cada vez mais crítico à medida que os ecossistemas SaaS se expandem e são introduzidas ferramentas com IA através de fornecedores externos.

Frequência com que as PMEs monitorizam a segurança dos fornecedores de software como serviço (SaaS) de terceiros?



Para as PMEs, a melhoria da segurança SaaS de terceiros começa com uma melhor disciplina diária: saber quais as ferramentas que estão a ser utilizadas, controlar quem lhes pode aceder, remover rapidamente as contas não utilizadas e estar atento a aplicações não autorizadas ou a atividades invulgares. Para as equipas mais pequenas, em particular, uma abordagem simples e consistente apoiada por fornecedores de confiança ou serviços geridos será mais eficaz do que tentar criar um modelo de monitorização complexo sozinho.

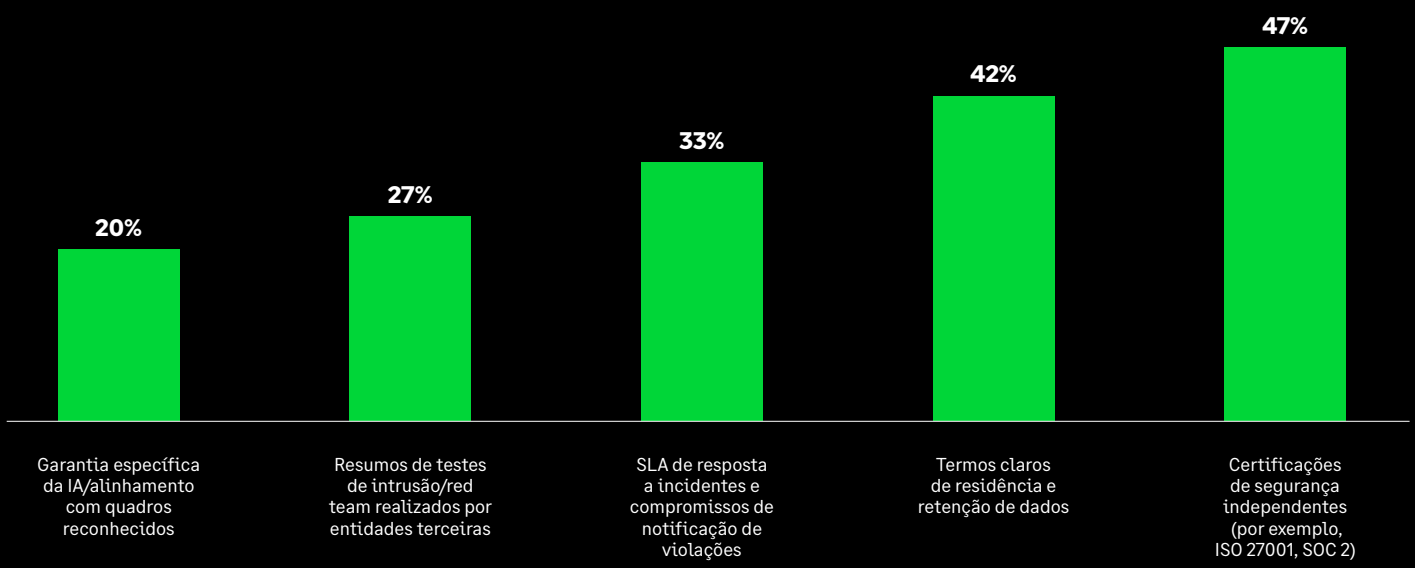
As PMEs confiam em provas claras e verificáveis quando avaliam fornecedores externos

À medida que os serviços SaaS e com IA integrada se tornam mais presentes nas operações das PMEs, a confiança nos fornecedores depende cada vez mais de provas que sejam claras, familiares e fáceis de verificar.

As PMEs valorizam mais as certificações independentes, o tratamento transparente dos dados e os compromissos claros de resposta a incidentes, uma vez que estes fornecem garantias práticas de que as principais medidas de segurança estão em vigor. As alegações mais técnicas específicas da IA podem parecer avançadas, mas são frequentemente mais difíceis de avaliar com confiança pelas organizações mais pequenas.

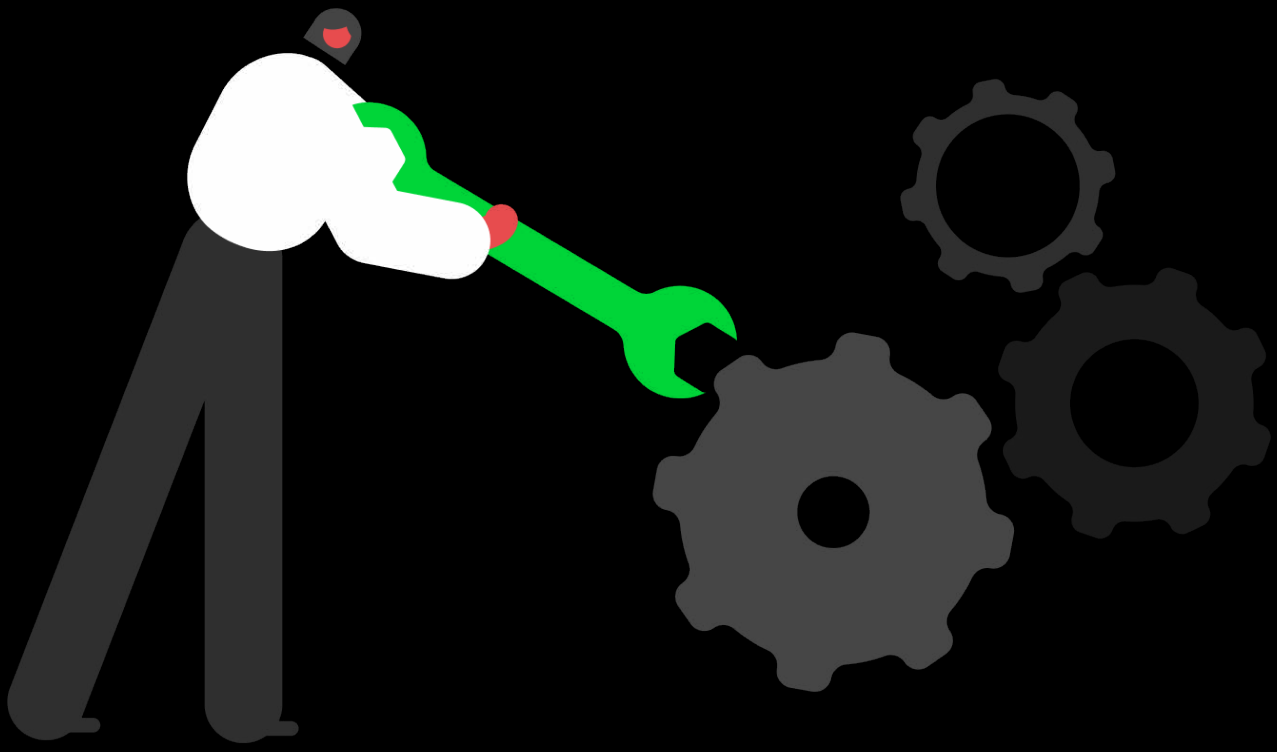
Isso faz com que a clareza seja uma vantagem competitiva. Os fornecedores que conseguem explicar, em termos simples, como os dados dos clientes são protegidos, onde são armazenados e o que acontece se algo correr mal, estão melhor posicionados para ganhar confiança.

Provas que reforçam a confiança na segurança da IA e nas práticas responsáveis de um fornecedor externo



As PMEs devem dar prioridade aos fornecedores que apresentem provas claras e auditáveis de como gerem a segurança e rever essa confiança regularmente, em vez de a tratarem como uma verificação pontual.

Transformar as perceções em ação



Sage

Microempresas: reforçar a resiliência através de medidas simples e escaláveis

Com a expansão da adoção da IA, o reforço da responsabilidade, dos ciclos de revisão e da governação básica torna-se crucial. As ações devem ser de baixo custo e fáceis de implementar, dando prioridade à simplicidade e à minimização da sobrecarga de gestão.

Ações a curto prazo

Postura de cibersegurança
Criar responsabilidade: Nomear um responsável pela segurança e documentar uma lista de verificação simples de resposta a incidentes que abranja o escalonamento, as cópias de segurança e o apoio externo.

Segurança da IAA
cesso seguro ao sistema de IA: Restringir o acesso aos sistemas de IA ao pessoal autorizado, permitir o registo simples de atividades e aplicar palavras-passe fortes para reduzir os riscos à medida que a utilização da IA cresce.

Planos a médio prazo

Postura de cibersegurança
Criar uma disciplina de rotina: Introduzir uma revisão regular da segurança que abranja os direitos de acesso e as atualizações de software. Cópias de segurança e ferramentas de terceiros.

Segurança da IA
Definir regras e formar o pessoal: Formalizar as regras de tratamento de dados e os protocolos de acesso, dar formação ao pessoal e criar as bases para uma segurança de IA escalável.

Considerações a longo prazo

Postura de cibersegurança
Reduzir a dependência do talento interno: Consolidar e normalizar os controlos, dando prioridade a serviços de baixo custo, agrupados ou geridos para reduzir as despesas gerais operacionais e financeiras.

Segurança da IA
Implementar práticas de supervisão: Estabelecer uma monitorização contínua básica e efetuar verificações básicas da segurança da IA do fornecedor. Selecionar aplicações fiáveis e empenhadas na segurança.

Sage

Pequenas empresas: reforçar a segurança através da estrutura e da disciplina

As pequenas empresas precisam de estruturar os processos de segurança e a governação da IA. À medida que a adoção da IA se expande, a formalização e a aplicação consistente de práticas de segurança tornam-se críticas para reduzir o risco não gerido.

Ações a curto prazo

Postura em matéria de cibersegurança
Formalizar a visibilidade dos riscos: Tornar os relatórios de segurança regulares, confirmar quem é responsável pelas principais decisões e garantir que os incidentes e as análises de acesso são discutidos a nível da gestão.

Segurança da IA
Visibilidade dos ativos de IA: Manter um inventário atualizado dos modelos, agentes, conjuntos de dados e serviços de IA. Monitorizar a utilização não autorizada ou oculto de aplicações de IA.

Planos a médio prazo

Postura em matéria de cibersegurança
Profissionalizar as operações de segurança: Aplicar políticas de forma consistente em todas as equipas, introduzir verificações de risco de terceiros antes de contratar fornecedores e racionalizar as ferramentas existentes para reduzir a complexidade.

Segurança da IA
Interações seguras da IA: Validar as entradas e saídas para evitar a injeção imediata, desbloqueios e fuga de dados.

Considerações a longo prazo

Postura de cibersegurança
Integrar a segurança nas decisões empresariais: Integrar a segurança nas decisões de aquisição, nas iniciativas digitais e nos planos de expansão para que a gestão do risco evolua a par do crescimento do negócio.

Segurança da IA
Prontidão para incidentes de IA: Documentar e testar o plano de resposta a incidentes para falhas ou violações de IA. Introduzir uma gestão estruturada dos riscos dos fornecedores.

Médias empresas: escalar a segurança em toda a empresa de forma consistente

As médias empresas possuem uma segurança bem estruturada, com funções dedicadas, gestão proativa e supervisão formal por terceiros. O próximo passo é garantir que esta maturidade é consistentemente ampliada à medida que a exposição ao digital e à IA cresce.

Ações a curto prazo

Postura de cibersegurança
Reforçar os controlos existentes: Mapear ativos críticos e fornecedores-chave, rever os direitos de acesso entre equipas e identificar ferramentas de segurança sobrepostas ou subutilizadas.

Segurança da IA
Gestão do risco da IA: Formalizar um quadro de segurança da IA que incorpore a visibilidade da IA e dos dados, a monitorização contínua das anomalias do sistema e a gestão estruturada dos riscos dos fornecedores.

Planos a médio prazo

Postura em matéria de cibersegurança
Normalizar as práticas de segurança: Aplicar os mesmos controlos e regras em todos os departamentos, introduzir análises estruturadas dos fornecedores, comunicar regularmente os principais indicadores de risco à administração.

Segurança da IA
Alinhamento regulamentar: Assegurar que a utilização da IA está em conformidade com os regulamentos relativos à privacidade e à IA. Integrar considerações de IA nos quadros de garantia de segurança existentes.

Considerações a longo prazo

Postura de cibersegurança **Incorporar a segurança na governação da empresa:** Integrar a cibersegurança no aprovisionamento, na continuidade das atividades e no planeamento estratégico para que a proteção evolua de acordo com o crescimento da organização. **Segurança da IA** **Testes de adversários:** Testar a resiliência dos sistemas de IA contra ataques adversários ou de red teams.

Sage

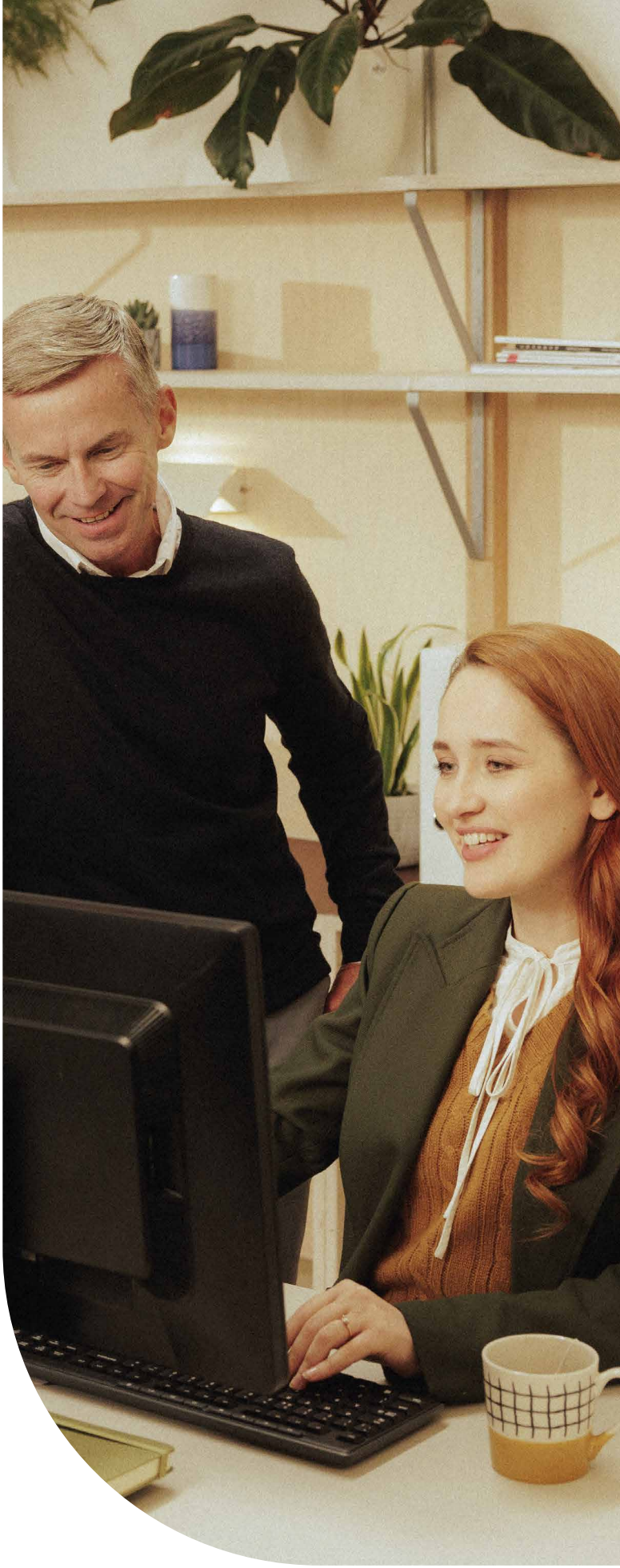
Mensagem da Sage

Há muito que a Sage defende as pequenas e médias empresas e compreende as oportunidades e as pressões que estas enfrentam. Este relatório mostra que a cibersegurança é agora uma prioridade empresarial fundamental para as PMEs. Situa-se logo a seguir ao crescimento na agenda empresarial, refletindo a forma como a ciber-resiliência está agora intimamente ligada à confiança, à continuidade e ao sucesso a longo prazo.

Muitas PMEs estão a enfrentar o aumento do risco cibernético com tempo, pessoal e orçamento limitados, à medida que a IA e a tecnologia de terceiros se tornam mais integradas no dia a dia das empresas. Não deveriam ter de gerir isso sozinhas.

Na Sage, estamos focados em ajudar as PMEs a pôr em prática uma boa segurança através de orientações claras, princípios de segurança desde a conceção e transparência sobre a forma como os dados são protegidos e como a IA é utilizada. O objetivo é permitir que as PMEs reduzam os riscos enquanto utilizam a tecnologia para impulsionar o crescimento.

Os governos, as entidades do setor, os fornecedores de software e os vendedores devem colaborar estreitamente para dar às PMEs orientações mais claras, salvaguardas mais simples e apoio prático que se adapte às realidades que enfrentam todos os dias.



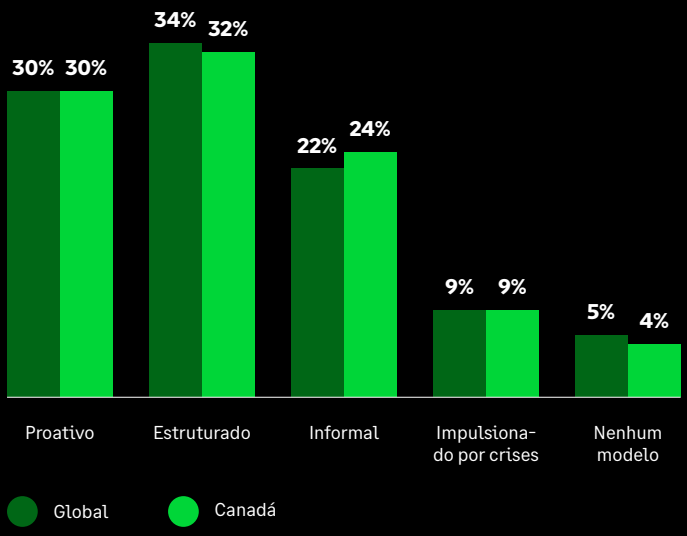
Anexo: perceções sobre os países

Canadá

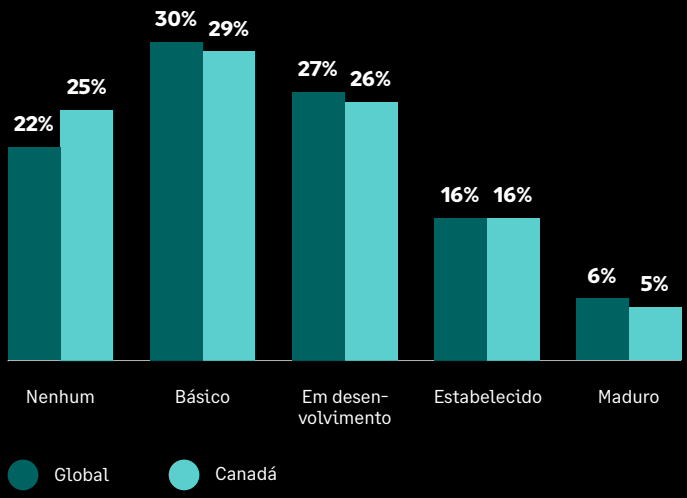
O Canadá está à frente da média mundial em matéria de medidas de segurança essenciais, o que lhe confere uma base sólida na proteção quotidiana e ajuda a manter os níveis de incidentes próximos da média mundial.

A lacuna abre-se em torno da preparação para a IA. O Canadá parece menos preparado para transformar essa base sólida numa segurança eficaz da IA, com uma adoção mais fraca de salvaguardas práticas, uma menor preparação para a conformidade e a maior escassez de conhecimentos especializados em segurança da IA. O foco precisa agora de mudar da manutenção do básico para o desenvolvimento das competências, da supervisão e das orientações práticas necessárias para gerir os riscos relacionados com a IA de forma mais eficaz.

Modelo de gestão da cibersegurança



Nível atual de segurança das aplicações baseadas em IA



Incidentes ou violações cibernéticas no último ano

Canadá	55% Nenhum incidente	33% Incidentes menores, rapidamente resolvidos	10% Incidentes que causam perturbações significativas
Global	54% Nenhum incidente	34% Incidentes menores, rapidamente resolvidos	11% Incidentes que causam perturbações significativas

Medidas de segurança de topo em vigor

Canadá	86%	82%	77%
Global	79%	71%	67%

Principais desafios na proteção das aplicações de IA

Canadá	48%	38%	41%
Global	45%	41%	36%

Principais salvaguardas para os riscos e ameaças da IA

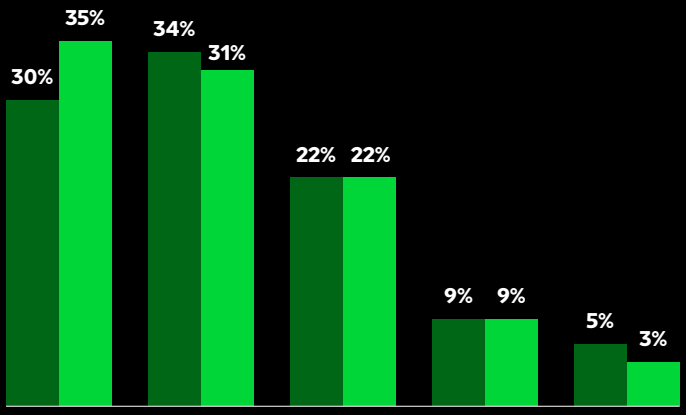
Canadá	35%	34%	32%
Global	41%	38%	33%

Estados Unidos

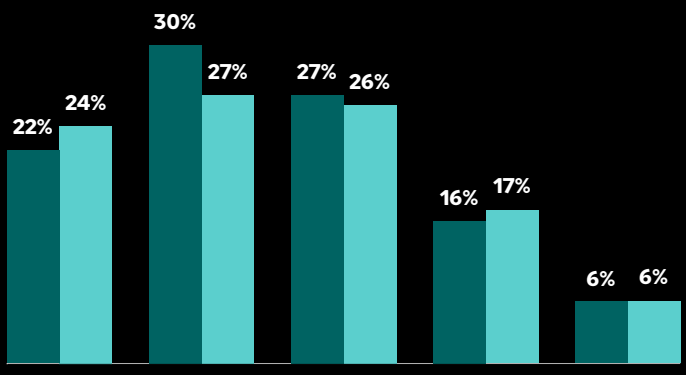
Os Estados Unidos estão à frente da média global na transição da sensibilização para a cibersegurança para práticas quotidianas mais estruturadas. Isto confere-lhes uma vantagem inicial em relação a muitos mercados, à medida que a IA se torna mais integrada nas operações comerciais.

A maior proporção de incidentes mais graves sugere que o foco precisa agora de mudar da construção de fundamentos para a melhoria da resiliência na prática, especialmente em relação à segurança dos dados, supervisão e capacidade de resposta à medida que as ameaças evoluem mais rapidamente.

Modelo de gestão da cibersegurança



Nível atual de segurança das aplicações baseadas em IA



Incidentes ou violações cibernéticas no último ano

Estados Unidos	55%	32%	13%
Global	54%	34%	11%

Medidas de segurança de topo em vigor

Estados Unidos	85%	71%	69%
Global	79%	71%	67%

Principais desafios na proteção das aplicações de IA

Estados Unidos	43%	38%	38%
Global	45%	41%	36%

Principais salvaguardas para os riscos e ameaças da IA

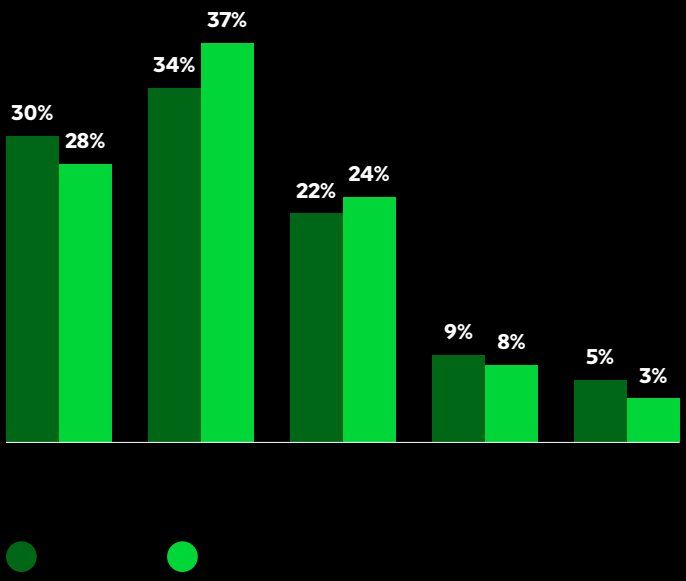
Estados Unidos	40%	39%	34%
Global	41%	38%	33%

França

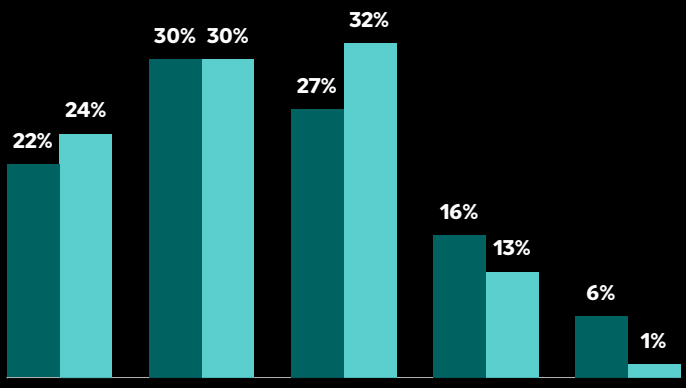
A França enfrenta um nível de pressão cibernética superior à média global. As principais medidas de segurança são menos adotadas, a proporção de empresas que relatam interrupções significativas é maior e a maturidade da segurança da IA continua mais fraca, com menos organizações no nível mais avançado. Isto aponta para um mercado onde os fundamentos da segurança são menos consistentes e onde o impacto do risco cibernético nos negócios é mais pronunciado.

O próximo passo é fortalecer tanto os fundamentos como a capacidade de gerir o risco relacionado com a IA na prática. Uma maior visibilidade, uma proteção de dados mais robusta e uma preparação de resposta mais estruturada serão cruciais, especialmente num mercado em que a confiança parece depender fortemente da capacidade das organizações para responder quando algo corre mal.

Modelo de gestão da cibersegurança



Nível atual de segurança das aplicações baseadas em IA



Incidentes ou violações cibernéticas no último ano

França	51%	33%	15%
Global	54%	34%	11%

Medidas de segurança de topo em vigor

França	77%	60%	69%
Global	79%	71%	67%

Principais desafios na proteção das aplicações de IA

França	48%	43%	35%
Global	45%	41%	36%

Principais salvaguardas para os riscos e ameaças da IA

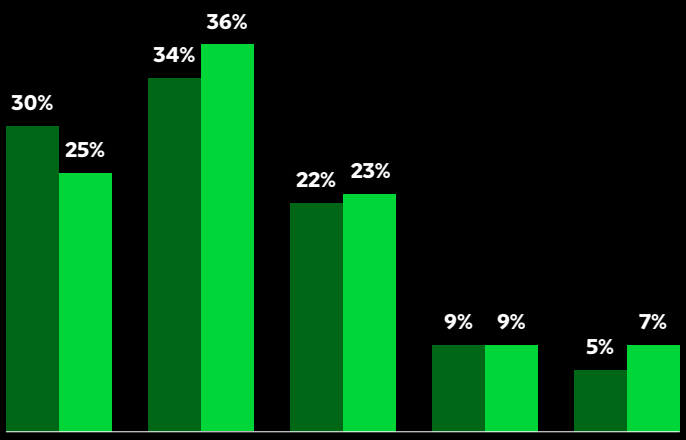
França	42%	38%	34%
Global	41%	38%	33%

Alemanha

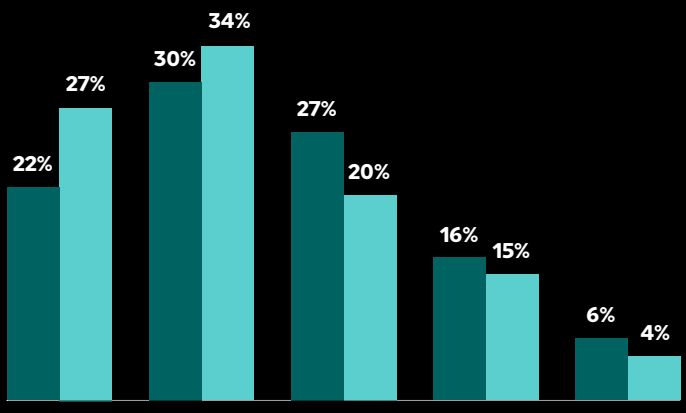
A Alemanha apresenta um perfil mais cauteloso e focado na conformidade do que a média global. As medidas essenciais são menos adotadas, a gestão proativa é menor e a maturidade em segurança da IA continua mais frágil, com mais organizações ainda em fases iniciais. Os níveis de incidentes estão próximos das normas globais, pelo que a pressão é menos visível hoje, mas as bases para a gestão de riscos relacionados com a IA ainda estão em desenvolvimento.

A prioridade da Alemanha é passar da cautela à prontidão prática. A forte preocupação com a utilização de dados e a visibilidade limitada das ferramentas de IA evidenciam um mercado focado no controlo e na conformidade. O próximo passo é reforçar as salvaguardas práticas, melhorar a visibilidade da utilização da IA e garantir que a cautela se traduz numa maior resiliência à medida que a adoção da IA cresce.

Modelo de gestão da cibersegurança



Nível atual de segurança das aplicações baseadas em IA



Incidentes ou violações cibernéticas no último ano

Alemanha	54%	36%	10%
Global	54%	34%	11%

Medidas de segurança de topo em vigor

Alemanha	77%	68%	61%
Global	79%	71%	67%

Principais desafios na proteção das aplicações de IA

Alemanha	43%	39%	37%
Global	45%	41%	36%

Principais salvaguardas para os riscos e ameaças da IA

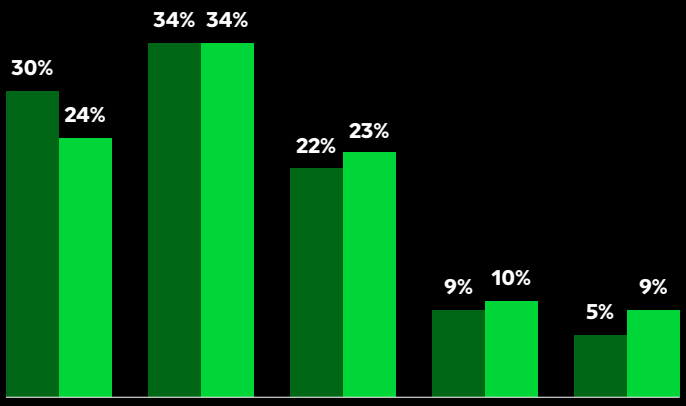
Alemanha	42%	32%	26%
Global	41%	38%	33%

Portugal

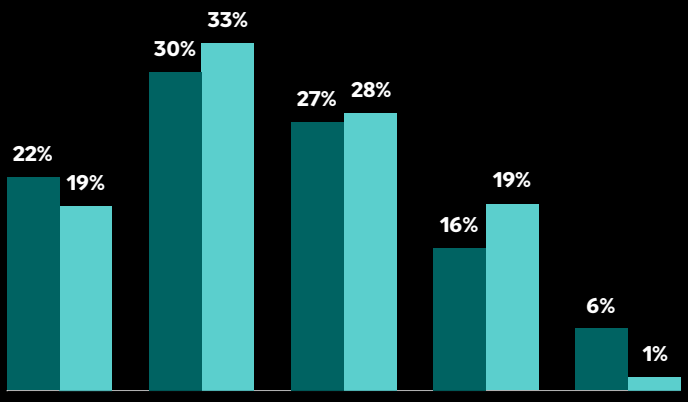
Portugal apresenta um perfil de segurança menos maduro do que a média global. As medidas de segurança essenciais são menos adotadas, os níveis de incidentes são mais elevados e as interrupções significativas são mais comuns. A maturidade da segurança da IA também permanece desigual, com mais organizações concentradas na fase básica e muito poucas a atingir a adoção madura.

O desafio de Portugal é a execução. A prioridade agora é reforçar os fundamentos, reduzir a incerteza em torno do tratamento de dados relacionados com a IA e construir práticas de segurança diárias mais consistentes, para que o risco seja gerido com menos interrupções. A maior dependência de certificações independentes demonstra também um mercado que procura provas externas claras de confiança à medida que a adoção da IA cresce.

Modelo de gestão da cibersegurança



Nível atual de segurança das aplicações baseadas em IA



Incidentes ou violações cibernéticas no último ano

Portugal	43%	39%	16%
Global	54%	34%	11%

Medidas de segurança de topo em vigor

Portugal	65%	65%	61%
Global	79%	71%	67%

Principais desafios na proteção das aplicações de IA

Portugal	44%	40%	34%
Global	45%	41%	36%

Principais salvaguardas para os riscos e ameaças da IA

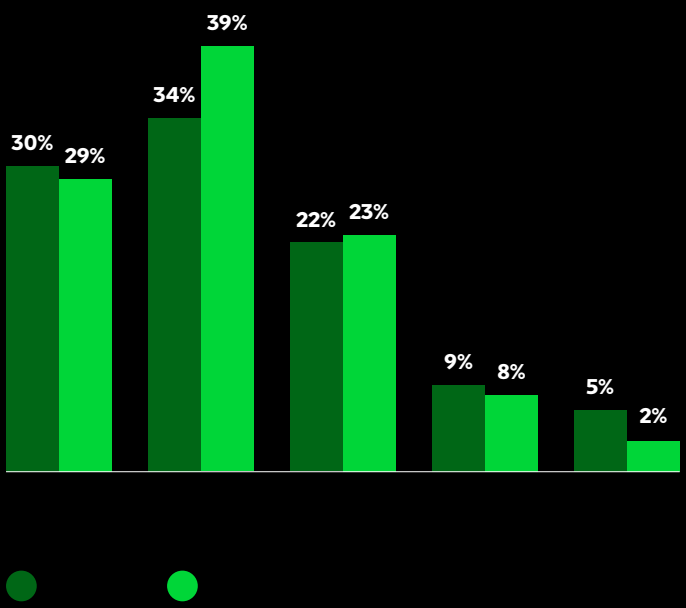
Portugal	43%	34%	33%
Global	41%	38%	33%

Espanha

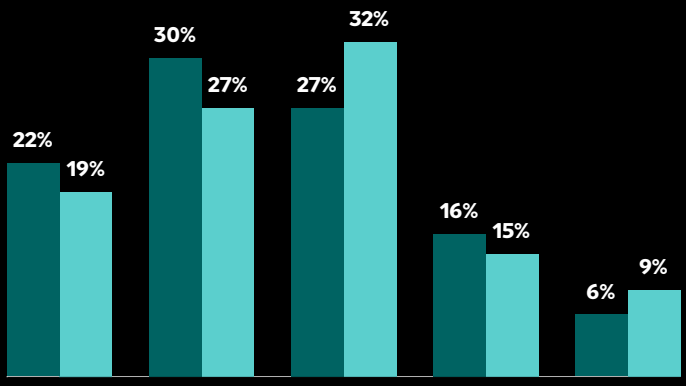
Espanha apresenta um perfil de segurança mais maduro do que a média global. Os níveis de incidentes são mais baixos, a gestão estruturada da segurança é mais comum e a maturidade da segurança da IA é maior, com mais organizações a ultrapassar as fases iniciais e a alcançar uma adoção madura.

O desafio de Espanha é manter esta posição à medida que a adoção da IA cresce. A prioridade é agora reforçar a proteção contra os riscos de fator humano, melhorar a visibilidade da utilização da IA e eliminar as lacunas na monitorização contínua por terceiros, para que um ponto de partida mais sólido não seja enfraquecido por pontos cegos à medida que as ameaças evoluem.

Modelo de gestão da cibersegurança



Nível atual de segurança das aplicações baseadas em IA



Incidentes ou violações cibernéticas no último ano

Espanha	60%	29%	10%
Global	54%	34%	11%

Medidas de segurança de topo em vigor

Espanha	75%	72%	62%
Global	79%	71%	67%

Principais desafios na proteção das aplicações de IA

Espanha	42%	36%	34%
Global	45%	41%	36%

Principais salvaguardas para os riscos e ameaças da IA

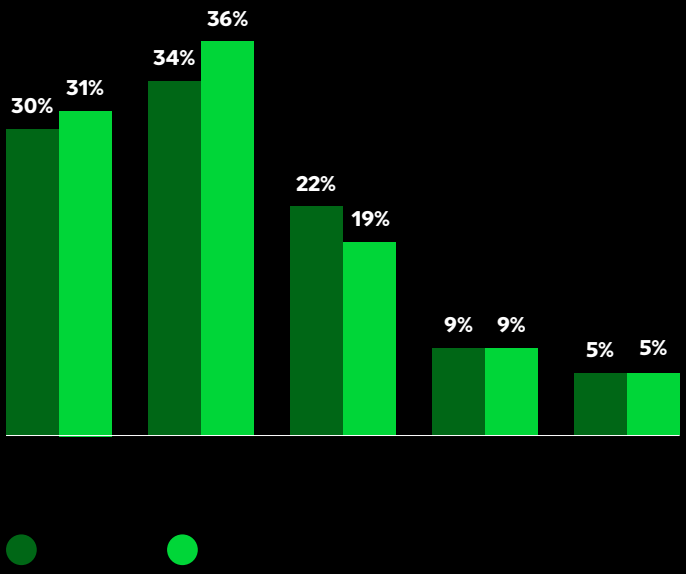
Espanha	43%	38%	32%
Global	41%	38%	33%

Reino Unido

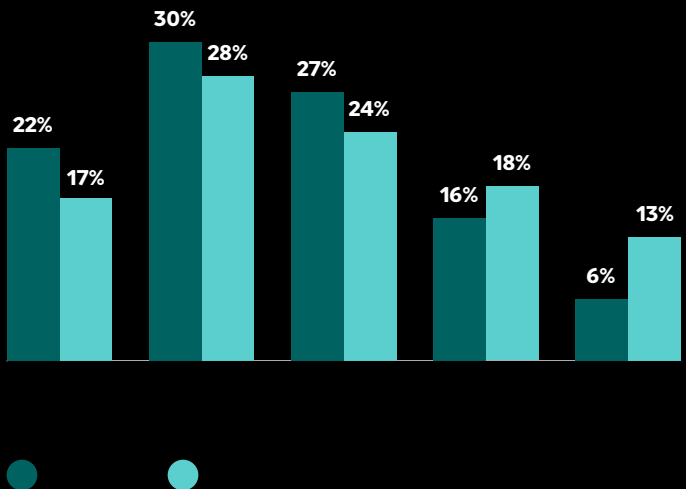
O Reino Unido destaca-se por avançar mais rápido e mais rapidamente na segurança da IA do que a média global. As organizações estão mais avançadas na implementação de salvaguardas práticas, são mais propensas a utilizar ferramentas aprovadas e políticas formais e estão mais avançadas na construção de uma postura de segurança de IA madura. Isto indica um mercado que não está à espera para reagir, mas adotando uma abordagem mais deliberada para se preparar para os riscos da IA à medida que a adoção cresce.

A prioridade é agora um controlo mais rigoroso à medida que a utilização da IA se expande, especialmente em relação à proteção de dados, às ameaças de rápida evolução e à capacidade de transformar uma postura de IA mais robusta em resiliência na prática. O nível ligeiramente mais elevado de interrupções significativas mostra também que o progresso na preparação ainda tem de ser acompanhado por uma execução consistente quando ocorrem incidentes.

Modelo de gestão da cibersegurança



Nível atual de segurança das aplicações baseadas em IA



Incidentes ou violações cibernéticas no último ano

Reino Unido	55%	32%	13%
Global	54%	34%	11%

Medidas de segurança de topo em vigor

Reino Unido	75%	79%	67%
Global	79%	71%	67%

Principais desafios na proteção das aplicações de IA

Reino Unido	44%	46%	37%
Global	45%	41%	36%

Principais salvaguardas para os riscos e ameaças da IA

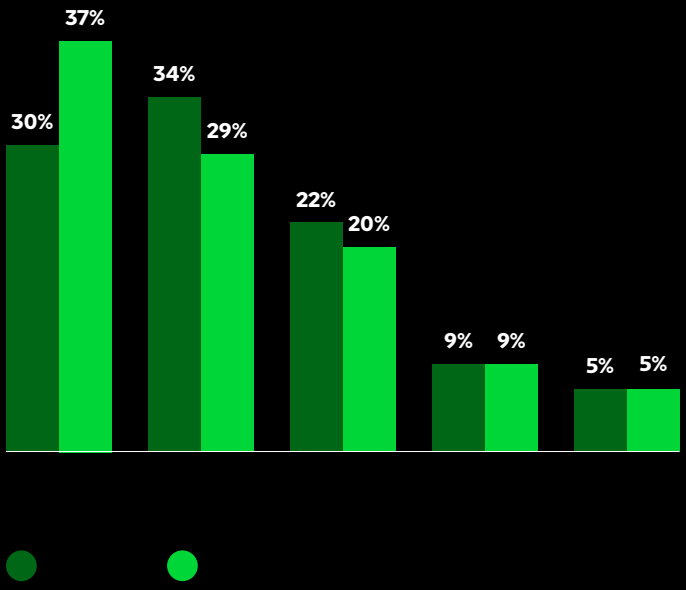
Reino Unido	43%	45%	38%
Global	41%	38%	33%

África do Sul

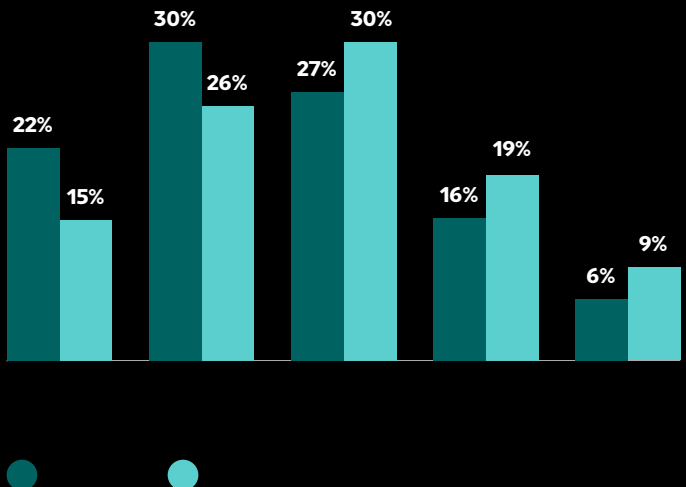
A África do Sul está à frente da média global em termos de maturidade da segurança da IA. As organizações são mais propensas a ter revisto a sua abordagem em resposta à IA, mais avançadas na sua postura de segurança para aplicações alimentadas por IA e mais fortes na monitorização contínua de terceiros. Isto aponta para um mercado que está a levar a sério o risco da IA e a implementar salvaguardas mais práticas à medida que a adoção cresce.

O desafio é transformar esse progresso numa consistência mais forte. As principais medidas de segurança ainda são mistas, e as preocupações com a proteção de dados e as ameaças em rápida evolução continuam elevadas. A prioridade agora é colmatar essas lacunas para que uma postura de IA mais forte seja acompanhada por uma prática de segurança quotidiana mais resiliente.

Modelo de gestão da cibersegurança



Nível atual de segurança das aplicações baseadas em IA



Incidentes ou violações cibernéticas no último ano

África do Sul	55%	35%	9%
Global	54%	34%	11%

Medidas de segurança de topo em vigor

África do Sul	75%	74%	70%
Global	79%	71%	67%

Principais desafios na proteção das aplicações de IA

África do Sul	45%	44%	37%
Global	45%	41%	36%

Principais salvaguardas para os riscos e ameaças da IA

África do Sul	45%	39%	36%
Global	41%	38%	33%

sage.com