Informe

Las pymes en la era de la IA: cómo afrontar la complejidad de la ciberseguridad y reforzar la resiliencia

Con investigación y análisis realizados por

Sage

IDC

Metodología y contexto de la encuesta

Joel Stradling
Director sénior de Investigación, Seguridad en Europa, IDC

Este informe se basa en los resultados de un estudio mundial realizado por IDC por encargo de Sage, en el que se encuestó a 2210 pequeñas empresas de ocho mercados.

La investigación, publicada en el IDC InfoBrief Las pymes en la era de la IA: cómo afrontar la complejidad de la ciberseguridad y reforzar la resiliencia (marzo de 2026; Documento de IDC N.º EUR254487126) y elaborada por el analista de IDC Joel Stradling, evalúa cómo están respondiendo las pymes a los retos actuales y emergentes en materia de ciberseguridad.

Analiza sus principales inquietudes y su nivel de madurez en seguridad en relación con la IA y con las soluciones de terceros, e identifica los cambios estratégicos necesarios para pasar de una defensa reactiva a una seguridad proactiva y a una ciberresiliencia sostenible y alineada con el riesgo.

El estudio abarcó los siguientes sectores: servicios financieros, sanidad, telecomunicaciones, energía, industria manufacturera, recursos, comercio minorista, software y servicios de información, transporte y viajes, servicios empresariales y personales, educación, sector público, entidades sin ánimo de lucro, auditoría y fiscalidad, construcción, y hostelería y ocio.

Fuente: IDC InfoBrief, «Las pymes en la era de la IA: cómo afrontar la complejidad de la ciberseguridad y reforzar la resiliencia», patrocinado por Sage, abril de 2026, doc. IDC n.º EUR254487126.

Países incluidos en la encuesta

- Canadá
- España
- Estados Unidos
- Portugal
- Francia
- Reino Unido
- Alemania
- Sudáfrica

åla empresa

1 - 9
Microempresa

10 - 99
Pequeña empresa

100 - 499
Mediana empresa

> “La IA debería ser una oportunidad de crecimiento para todas las pymes, no solo para las que cuentan con más recursos en materia de seguridad. Las empresas más pequeñas siguen actuando con más cautela, ya que en la práctica sigue siendo difícil adoptar la IA de forma segura. Si queremos que más pymes se beneficien de la IA, debemos facilitar la adopción de la ciberseguridad mediante salvaguardas integradas, orientaciones más claras y apoyo práctico.»

Gustavo Zeidan
Director de Seguridad de la Información, Sage

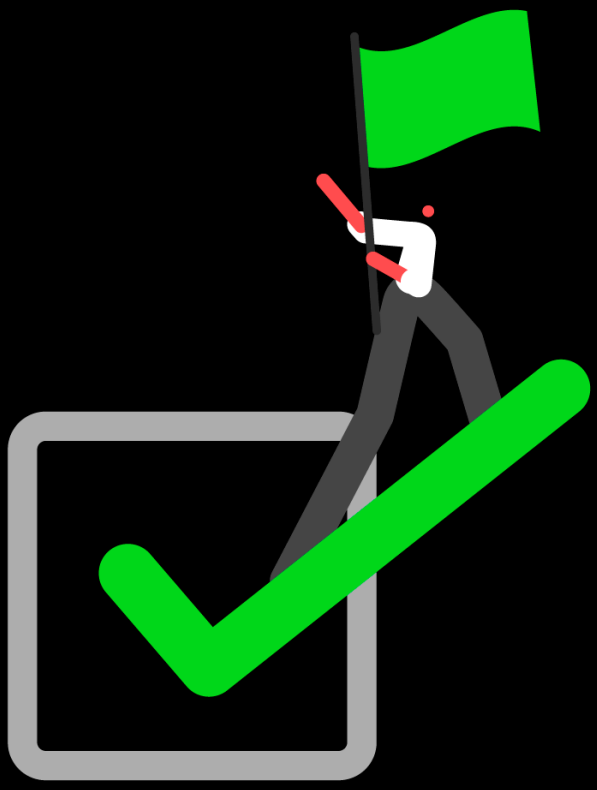
Sage

Índice

Sage

Resumen ejecutivo

Las pymes están incrementando su inversión en ciberseguridad y acelerando la adopción de la IA. Sin embargo, en muchas de ellas las prácticas de seguridad siguen sin avanzar al ritmo del cambio, lo que las deja más expuestas a medida que el riesgo crece más rápido que su resiliencia.



Basado en una encuesta a 2210 pymes de ocho mercados, este informe analiza cómo las pequeñas y medianas empresas están respondiendo a unos retos de ciberseguridad en constante evolución, con especial atención a la adopción de la IA y al riesgo asociado a terceros proveedores. La ciberseguridad es ya una prioridad empresarial clave para las pymes.

En este estudio, el 52 % de las pymes afirma que garantizar la ciberseguridad y la protección de los datos es una de sus principales prioridades para los próximos doce meses, solo por detrás del crecimiento del negocio (59 %) y muy por delante de la ampliación del uso de la IA (33 %). Al mismo tiempo, el 60 % prevé aumentar su gasto en ciberseguridad, lo que muestra una clara voluntad de actuar.

Sin embargo, para muchas pymes la respuesta todavía no está a la altura del riesgo. Aproximadamente la mitad declara haber sufrido un incidente de ciberseguridad cada año, y las prácticas de seguridad proactiva siguen siendo limitadas, especialmente entre las empresas de menor tamaño. Solo el 13 % de las microempresas y el 21 % de las pequeñas empresas describen su enfoque como proactivo, frente al 48 % de las empresas medianas.

La IA está intensificando la presión. No crea un conjunto completamente nuevo de riesgos, pero sí hace que amenazas ya conocidas sean más rápidas, más convincentes y más difíciles de gestionar. Muchas pymes siguen en fases muy tempranas de preparación frente a amenazas relacionadas con la IA, sobre todo las más pequeñas. El 84 % de las microempresas y el 65 % de las pequeñas empresas afirman no estar preparadas o encontrarse solo en los primeros pasos.

Al mismo tiempo, el 22 % declara no contar con medidas de seguridad específicas para aplicaciones de IA, porcentaje que asciende al 44 % entre las microempresas.

Los riesgos asociados a proveedores SaaS y a la cadena de suministro constituyen un importante punto ciego. Aunque las herramientas SaaS están ampliamente implantadas en los entornos de las pymes, el 43 % de las microempresas no realiza una supervisión periódica o continua de los proveedores externos y se limita a certificaciones estáticas o comprobaciones puntuales. Esto reduce la visibilidad en tiempo real sobre el riesgo de los proveedores y aumenta la probabilidad de que las brechas de seguridad pasen inadvertidas hasta que se produzca una interrupción.

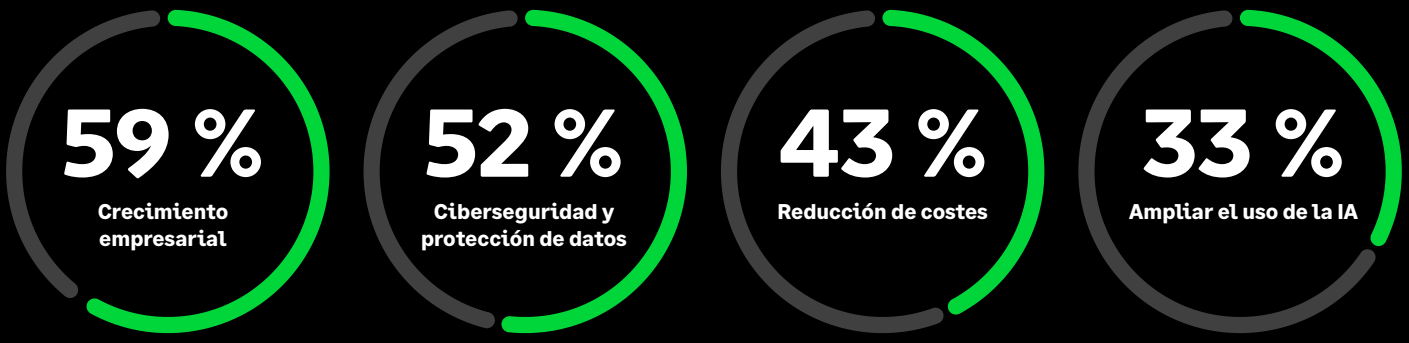
Las conclusiones apuntan a una necesidad clara: las pymes no necesitan más complejidad. Necesitan formas más sencillas y prácticas de superar una seguridad reactiva centrada en herramientas y de integrar la gestión del riesgo en la operativa diaria del negocio.

Eso implica incorporar la seguridad desde el principio, reforzar la disciplina del día a día y centrarse en una asignación clara de responsabilidades, una supervisión periódica y una mayor concienciación del personal, de un modo acorde con el tamaño de la empresa. Hacerlo bien es importante no solo para cada organización, sino también para la confianza de los clientes, las cadenas de suministro y la resiliencia del ecosistema digital en su conjunto.

La ciberseguridad es ya una prioridad clave para las pymes, pero otras exigencias de TI están tensionando los presupuestos

Cuando se les pregunta por sus principales prioridades empresariales para los próximos doce meses, más de la mitad de las pymes (52 %) menciona la ciberseguridad y la protección de los datos, situándolas justo por detrás del crecimiento del negocio (59 %) y por delante de la reducción de costes (43 %). Esto refleja un claro cambio de mentalidad. El ciber riesgo ya no se percibe como una cuestión puramente técnica, sino como un asunto empresarial de primer orden.

Principales prioridades empresariales para este año:



Empresas que prevén aumentar el presupuesto de seguridad en los próximos 12 meses:

51 % — **1 - 9** Microempresa

59 % — **10 - 99** Pequeña empresa

65 % — **100 - 499** Mediana empresa

Sage

Esta intención se ve reforzada por las inversiones previstas. Seis de cada diez pymes (60 %) afirman que esperan aumentar el gasto en ciberseguridad durante los próximos doce meses, lo que refleja tanto el reconocimiento del problema como la voluntad de actuar. Sin embargo, las presiones concurrentes, entre ellas el control de costes y la aceleración de la adopción de la IA (33 %), hacen que los avances sean desiguales.

Como resultado, aunque la ciberseguridad está escalando claramente en la lista de prioridades, un mayor gasto no siempre se traduce en una mejor preparación, lo que ayuda a explicar por qué persisten carencias en materia de confianza, gobernanza y ejecución en el mercado de las pymes.

Los datos apuntan a una brecha cada vez mayor entre intención y ejecución. La ciberseguridad importa más que nunca, pero muchas pymes siguen teniendo dificultades para integrarla de forma sistemática en su operativa.

de las pymes afirman que prevén aumentar el gasto en ciberseguridad en los próximos doce meses

La gobernanza de la seguridad sigue siendo informal en la mayoría de las pymes, lo que limita el impacto del aumento de la inversión

Para la mayoría de las pymes (38 %), las responsabilidades en materia de ciberseguridad siguen estando poco definidas e integradas en la función general de TI, en lugar de sustentarse en una asignación clara de responsabilidades, ciclos formales de revisión o procesos documentados.

Como consecuencia, la actividad relacionada con la seguridad suele ser reactiva y estar motivada por incidentes, en lugar de gestionarse como una disciplina empresarial habitual.

Esta brecha de gobernanza ayuda a explicar por qué el aumento del gasto en ciberseguridad no siempre se traduce en una mayor preparación. Sin una atribución más clara de responsabilidades, una supervisión periódica y una disciplina operativa sólida, incluso las inversiones bienintencionadas tienen dificultades para traducirse en una reducción constante del riesgo, especialmente a medida que la IA y las herramientas de terceros aumentan la exposición.

Para cerrar esta brecha, **las pymes deben integrar la seguridad de forma más sistemática en la actividad diaria**, con una asignación clara de responsabilidades, revisiones periódicas y procesos prácticos que puedan ampliarse con el tiempo.

La mayoría de las pymes cuentan con las herramientas de seguridad adecuadas, pero tienen dificultades para aplicarlas de manera sistemática

Los controles técnicos básicos ya son habituales en la mayoría de las pymes, pero siguen existiendo retos en ámbitos como la gestión de las herramientas, la formación del personal y la planificación de la respuesta ante incidentes.

Como resultado, la madurez en materia de seguridad depende menos de incorporar nuevos controles y más de implantar la disciplina operativa necesaria para que las salvaguardas existentes sigan siendo eficaces a medida que evoluciona la empresa.

Para reforzar su postura de ciberseguridad, las pymes deberían prestar más atención a la gobernanza de los datos, los controles de seguridad y la transparencia. A medida que crecen, esto exige ciclos de revisión más formalizados, una atribución clara de responsabilidades y procesos documentados de forma coherente en toda la organización.

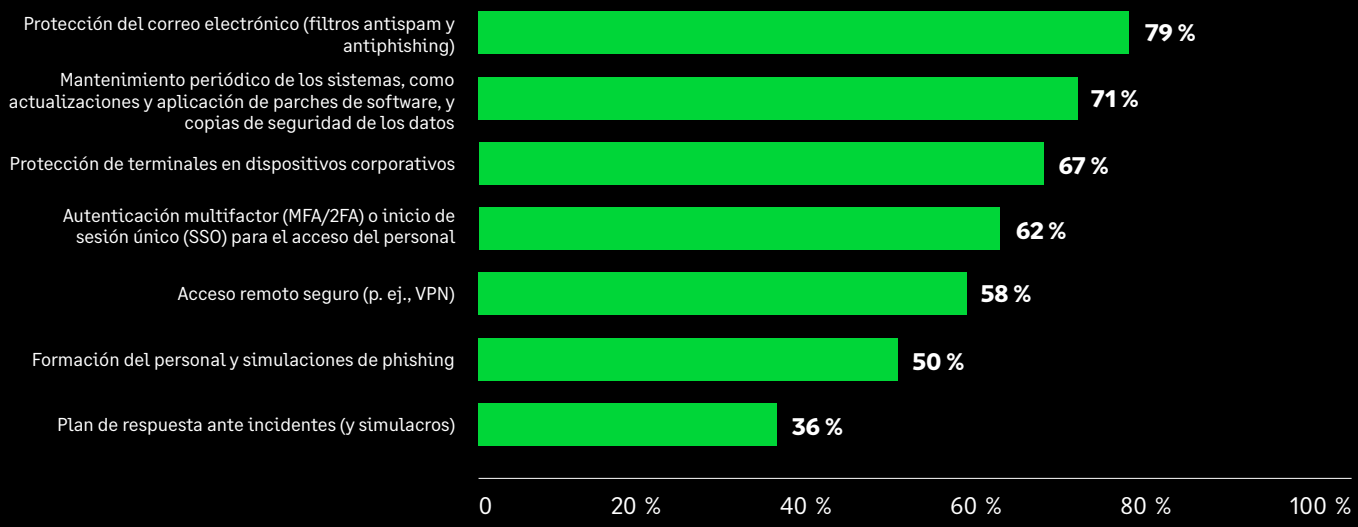
Indicadores de confianza operativa:

revisa periódicamente su ciberseguridad

afirma que el personal está formado para identificar ciber riesgos

evalúa rigurosamente la seguridad de terceros antes de contratarlos

¿Qué medidas de ciberseguridad tienen actualmente implantadas?



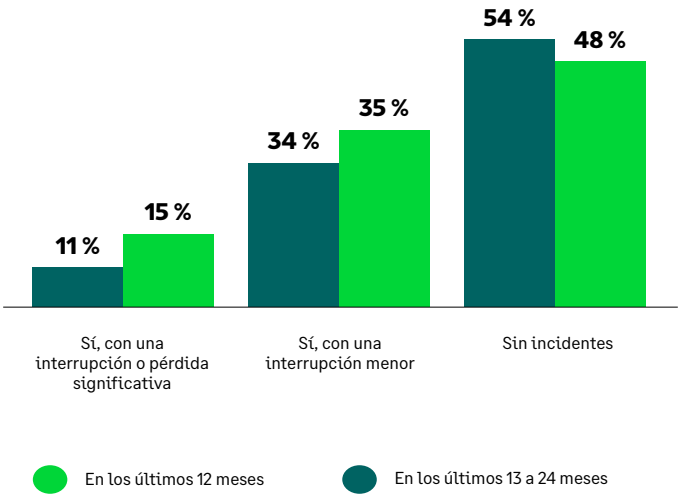
Cuando la seguridad sigue gestionándose de forma informal, los incidentes se vuelven disruptivos

Para las pymes, el ciber riesgo ya no es una disrupción ocasional. Es un reto empresarial permanente, configurado por una combinación cada vez más amplia y menos predecible de amenazas, desde el phishing y la ingeniería social hasta los riesgos internos, la exposición a terceros y las vulnerabilidades de la cadena de suministro.

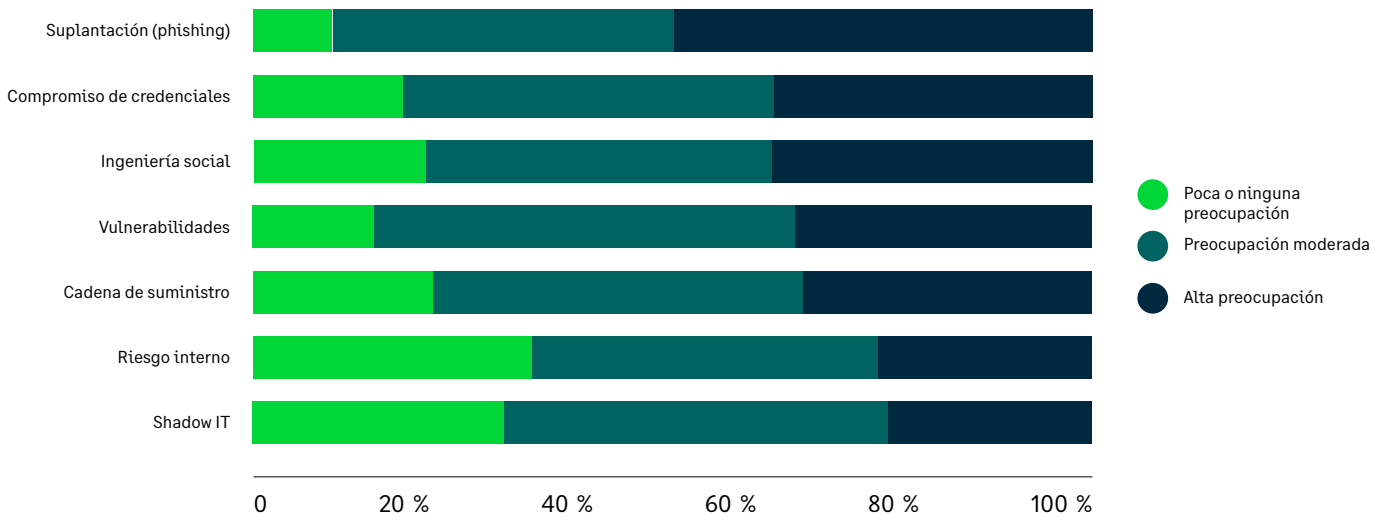
A medida que aumenta esa exposición, la resiliencia depende menos de intentar evitar todos los incidentes y más de la capacidad para gestionar bien las disrupciones.

Esto desplaza el foco desde los incidentes en sí hacia la calidad de la respuesta: la rapidez con la que se detectan los problemas, la eficacia con que se contienen y la solidez con la que la empresa puede recuperarse protegiendo al mismo tiempo la confianza, el flujo de caja y la continuidad de la actividad.

Incidentes de ciberseguridad o violaciones de datos



Preocupación por cada uno de los siguientes riesgos



Para las pymes, esto significa implantar **formas sencillas y repetibles de detectar problemas en una fase temprana**, responder con rapidez, contener el impacto y mantener la actividad operativa cuando se produzcan disrupciones.

La rápida evolución de las amenazas y la visibilidad limitada están aumentando la exposición de las pymes a los ciber riesgos

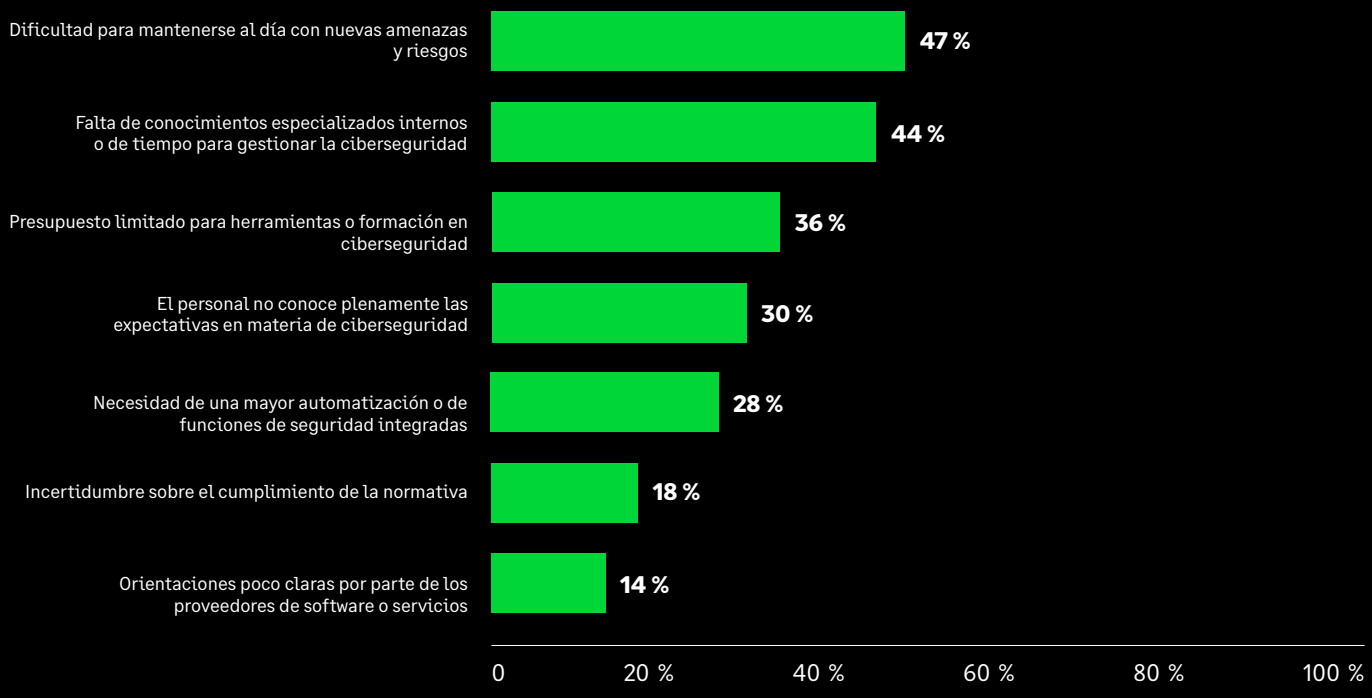
Casi la mitad de las pymes (47 %) identifica la dificultad para mantenerse al día con las nuevas amenazas y riesgos como su principal reto en materia de ciberseguridad.

Los ataques impulsados por la IA, un phishing cada vez más sofisticado y el uso creciente de servicios en la nube y SaaS están aumentando tanto la velocidad como la complejidad del ciber riesgo, a menudo más deprisa de lo que las capacidades internas pueden adaptarse.

Al mismo tiempo, muchas pymes carecen de una visibilidad clara y continua sobre dónde se concentran sus mayores exposiciones. La escasez de perfiles especializados, las prioridades operativas concurrentes y las limitaciones presupuestarias dificultan mantener una supervisión continua o una evaluación estructurada del riesgo. Como resultado, el ciber riesgo suele entenderse en términos generales, pero no gestionarse activamente en el día a día.

Esta combinación, la rápida evolución de las amenazas y una visibilidad incompleta, aumenta de forma significativa la probabilidad de que los problemas se detecten tarde, se prioricen de forma incoherente o solo se aborden una vez producida la disrupción. Para las pymes con una gobernanza informal y una disciplina operativa desigual, esto genera una brecha persistente entre el riesgo percibido y la exposición real.

¿Cuál de las siguientes opciones describe mejor los principales retos a los que se enfrenta su organización para gestionar la ciberseguridad?



Para acelerar el progreso, las pymes deberían priorizar soluciones que reduzcan la carga operativa, incluida la automatización, las salvaguardas integradas y el soporte externo alineado con sus limitaciones de recursos.

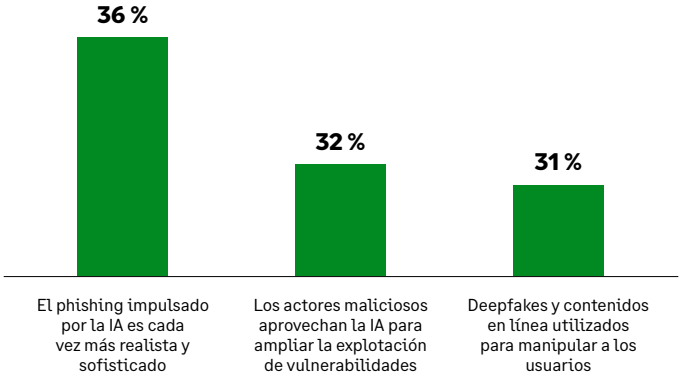
Las amenazas impulsadas por la IA evolucionan más rápido que las prácticas de seguridad de las pymes

La IA está añadiendo presión a un panorama de ciberseguridad ya complejo, y las empresas más pequeñas son las menos preparadas para seguir el ritmo.

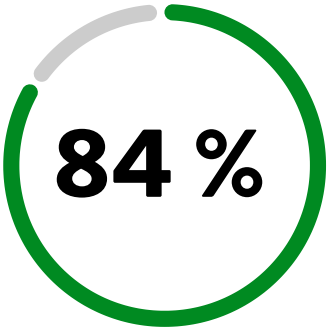
Las microempresas y las pequeñas empresas presentan las mayores carencias, con una supervisión diaria más débil, una monitorización menos sistemática y una menor concienciación del personal, lo que las deja más expuestas a medida que la IA aumenta tanto la velocidad como la escala de los ataques. Las prácticas de seguridad que podían haber sido suficientes en el pasado están dejando de ser eficaces a medida que las amenazas evolucionan con mayor rapidez.

Para las pymes, la respuesta debe empezar por lo básico: más concienciación, salvaguardas prácticas y formas más claras de detectar y gestionar el riesgo de manera temprana. Pero eso solo resuelve una parte del problema. A medida que evolucionan las amenazas relacionadas con la IA, las empresas también necesitarán formas más sencillas de automatizar tareas rutinarias de seguridad, reducir el esfuerzo manual y liberar la limitada capacidad de TI y seguridad para centrarse en las áreas de mayor riesgo.

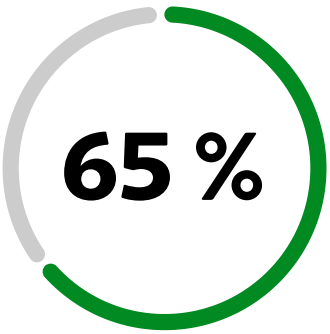
Tres principales preocupaciones en torno a los riesgos emergentes de la IA



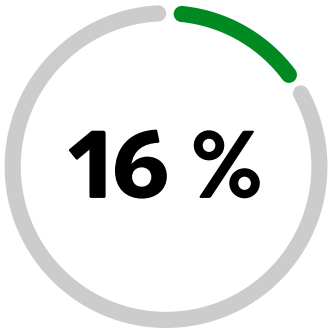
No están preparadas o se encuentran en fases iniciales de preparación frente a amenazas relacionadas con la IA:



Microempresa



Pequeña empresa



Mediana empresa

Para **las pymes con menor grado de madurez, en particular, la formación y la concienciación siguen siendo esenciales.** Los responsables de seguridad deberían priorizar medidas prácticas y fáciles de adoptar que ayuden a los equipos a reconocer y reducir el riesgo relacionado con la IA sin añadir complejidad innecesaria.

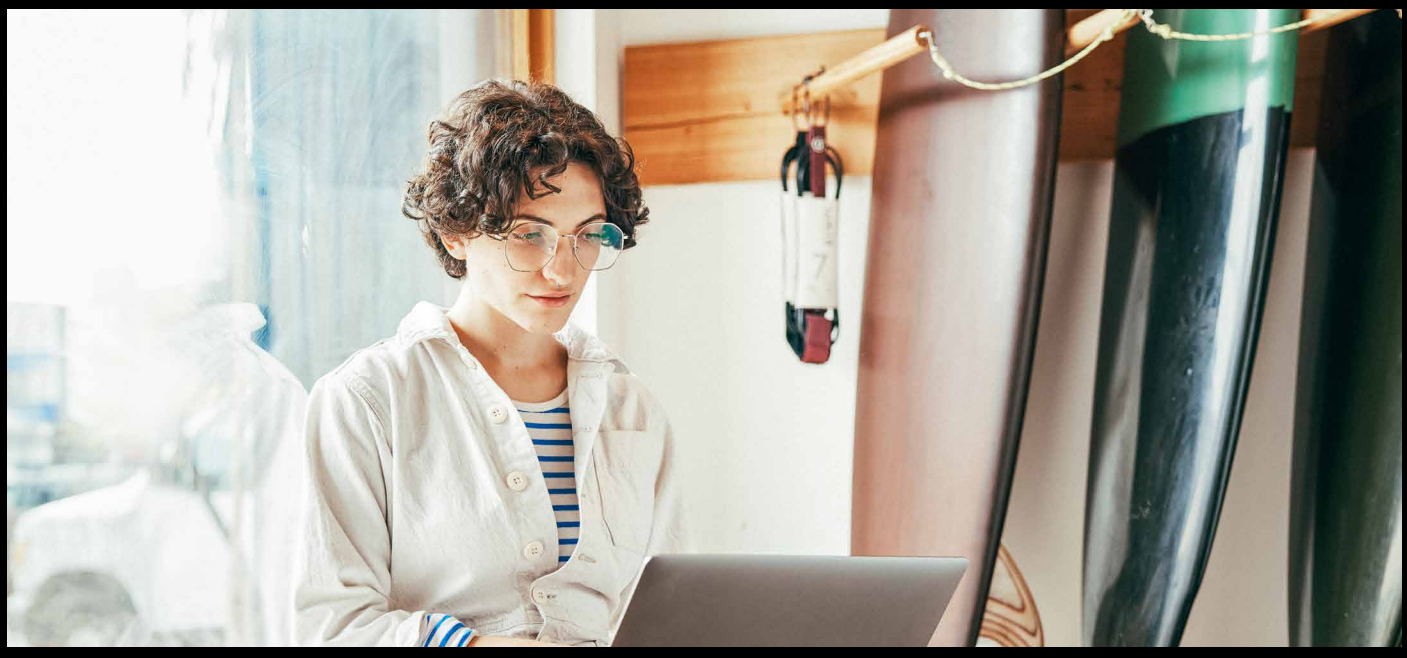
Sage

Las pymes ven en la IA una oportunidad, aun cuando aumenta el riesgo de seguridad

Una proporción significativa de pymes ve oportunidades en la IA, aunque una proporción aún mayor considera que la IA incrementa el ciber riesgo. La percepción varía en función del tamaño: las empresas medianas son más propensas a ver la IA como una oportunidad.

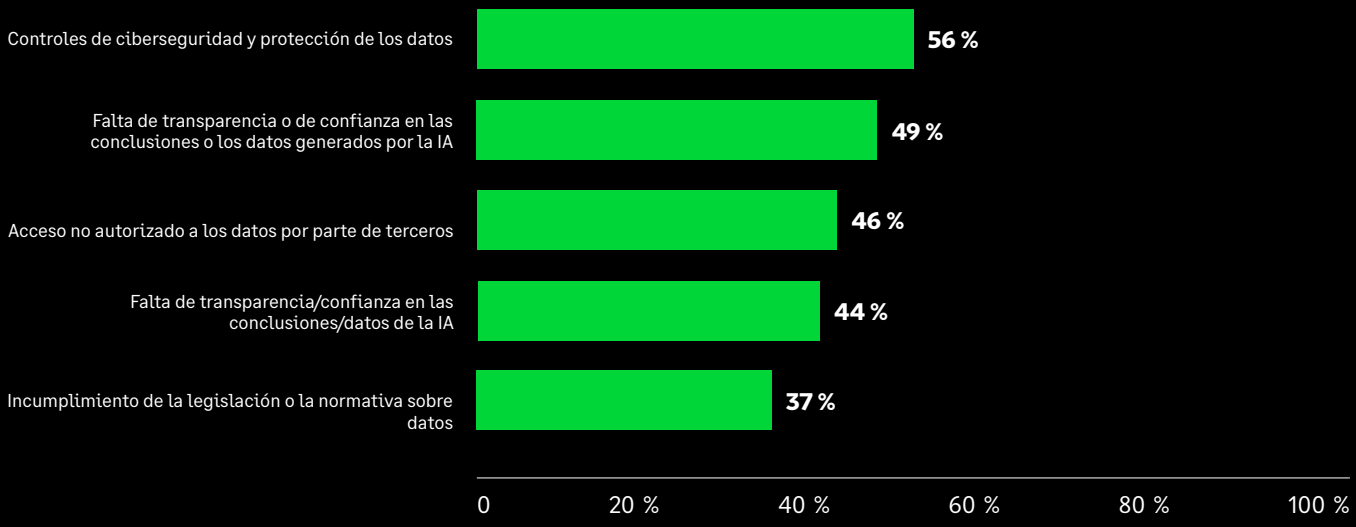
Las microempresas y las pequeñas empresas abordan la IA con mayor cautela. Esto refleja diferencias en la confianza depositada en los controles de seguridad y en la gobernanza, más que en el grado de ambición.

La IA se percibe como una oportunidad de negocio:



Existen preocupaciones en torno a la seguridad de los datos, la gobernanza y la transparencia en la adopción de la IA. Sin una visibilidad clara de cómo se utilizan y protegen los datos, muchas pymes siguen mostrándose cautelosas a la hora de ampliar el uso de la IA.

¿Cuál de las siguientes opciones describe mejor sus principales preocupaciones en relación con la adopción o el uso de la IA en su empresa?



A medida que la IA se integra cada vez más en las operaciones cotidianas, las pymes necesitan una visibilidad clara de dónde y cómo se está utilizando, junto con una gobernanza definida para gestionar los riesgos asociados. Esto incluye identificar las herramientas y sistemas de IA presentes en toda la empresa y establecer la supervisión, las políticas y las responsabilidades adecuadas a nivel directivo. Sin ello, el ritmo de adopción de la IA puede superar la capacidad de una organización para gestionar el riesgo, aumentando la exposición en lugar de generar valor.

Las pymes ya están sentando las bases para el cumplimiento normativo de la IA

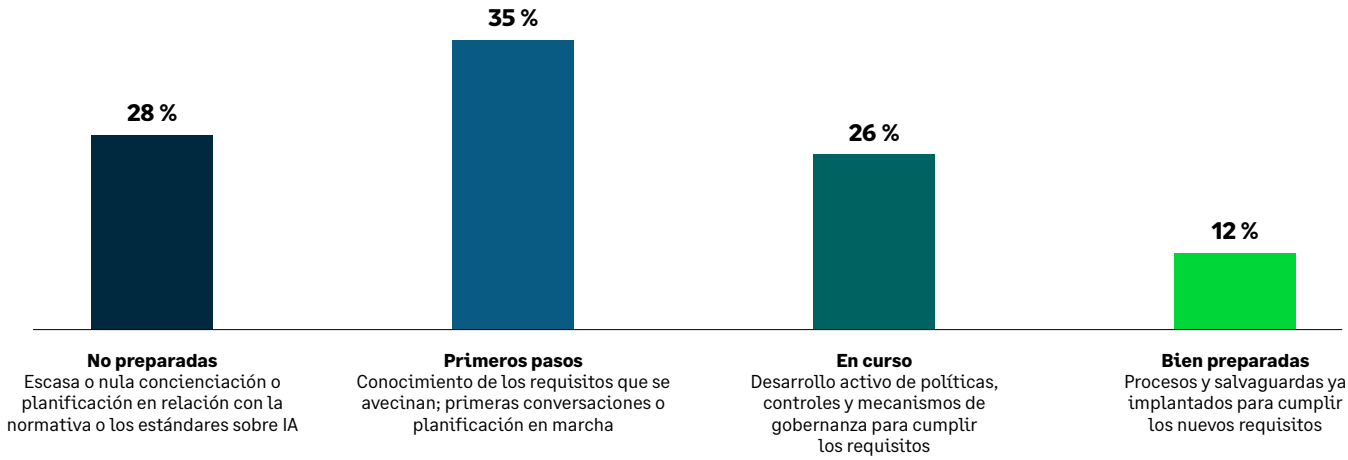
A medida que siguen surgiendo normativas y estándares sobre IA, muchas pymes están empezando a sentar las bases para el cumplimiento normativo.

Marcos como las normativas nacionales sobre IA y los códigos voluntarios de buenas prácticas están concebidos para ayudar a las organizaciones a traducir políticas de alto nivel en medidas prácticas y cotidianas de seguridad y gobernanza. Cada vez más gobiernos reconocen que las prácticas básicas de seguridad del software y de la IA deben adoptarse de forma generalizada en toda la cadena de suministro, y no solo entre las grandes empresas. Países como el Reino Unido están apostando por enfoques prácticos y proporcionados.

Un ejemplo es el Software Security Code of Practice y el correspondiente Software Security Ambassadors Scheme, lanzados como parte del Cyber Action Plan del Gobierno del Reino Unido. El programa reúne a organizaciones de los sectores público y privado, entre ellas Sage, para promover la adopción de principios fundamentales de seguridad del software, compartir experiencias prácticas de implantación y reforzar la resiliencia en el conjunto de la economía.

> “Las pymes son la columna vertebral de la economía británica, pero sabemos que muchas tienen dificultades para invertir en ciberseguridad en un momento en que las amenazas siguen aumentando. Reforzar la ciberresiliencia en todo el Reino Unido es una prioridad para el Gobierno, por eso nuestro National Cyber Security Centre ha desarrollado el Cyber Action Toolkit para ayudar a las pymes a fortalecer sus defensas. Recomendamos a todas las empresas que adopten nuestro eficaz programa Cyber Essentials, que ayuda a protegerse frente a amenazas comunes en línea y reduce la probabilidad de sufrir un ciberataque costoso y disruptivo.»
>
> **The Rt Hon Liz Kendall MP, secretaria de Estado de Ciencia, Innovación y Tecnología del Reino Unido**

Nivel de preparación de las pymes para cumplir la normativa sobre IA y los estándares de aseguramiento



Para las pymes, iniciativas como esta marcan una vía de avance pragmática: alinearse con marcos reconocidos, elegir socios comprometidos con un desarrollo seguro e incorporar desde el principio prácticas básicas de seguridad a medida que se acelera la adopción de la IA.

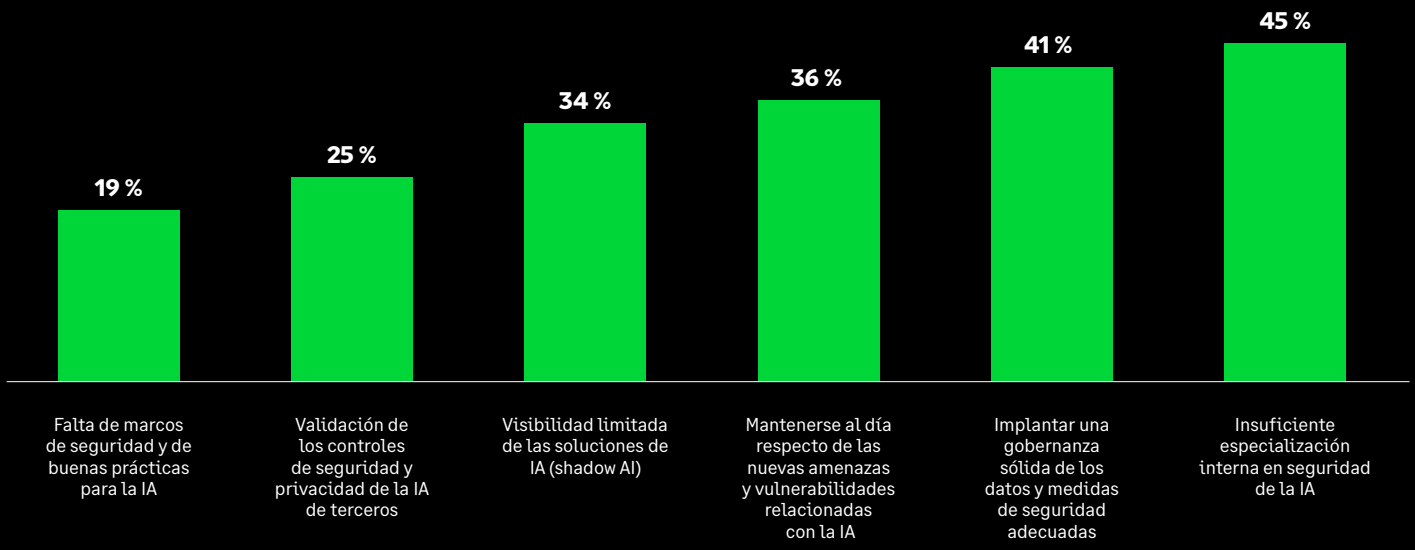
Los retos de seguridad de la IA para las pymes se concentran en la falta de capacidades, la protección de los datos y la rápida evolución de las amenazas

La IA está poniendo de manifiesto una brecha de capacidades en las pymes, no solo una brecha tecnológica. Muchas organizaciones están adoptando la IA más rápido de lo que pueden comprender los riesgos, evaluar su exposición o valorar la seguridad de los proveedores externos.

Esto resulta especialmente difícil para las empresas más pequeñas, donde la responsabilidad suele recaer en un único especialista de TI o en un equipo generalista.

La protección de los datos y la rápida evolución de las amenazas agravan aún más el reto. Dado que las herramientas de IA dependen del acceso a datos empresariales y de clientes, una visibilidad limitada y una supervisión poco rigurosa pueden aumentar rápidamente la exposición. Al mismo tiempo, la IA está haciendo que ataques ya conocidos sean más rápidos, más convincentes y más difíciles de gestionar, lo que deja a muchas pymes con dificultades para seguir el ritmo.

Principales retos para proteger las aplicaciones y la infraestructura de IA y GenAI



Para las pymes con recursos especializados limitados, la prioridad debe ser adoptar un enfoque práctico: limitar el uso de la IA a herramientas aprobadas, establecer reglas sencillas sobre qué datos pueden introducirse y cuáles no, revisar periódicamente el uso de la IA y apoyarse en proveedores de confianza o en socios externos cuando la experiencia interna sea insuficiente. Todo ello contribuirá más a reducir el riesgo que añadir complejidad.

La limitada supervisión de los proveedores SaaS deja expuestas a muchas pymes

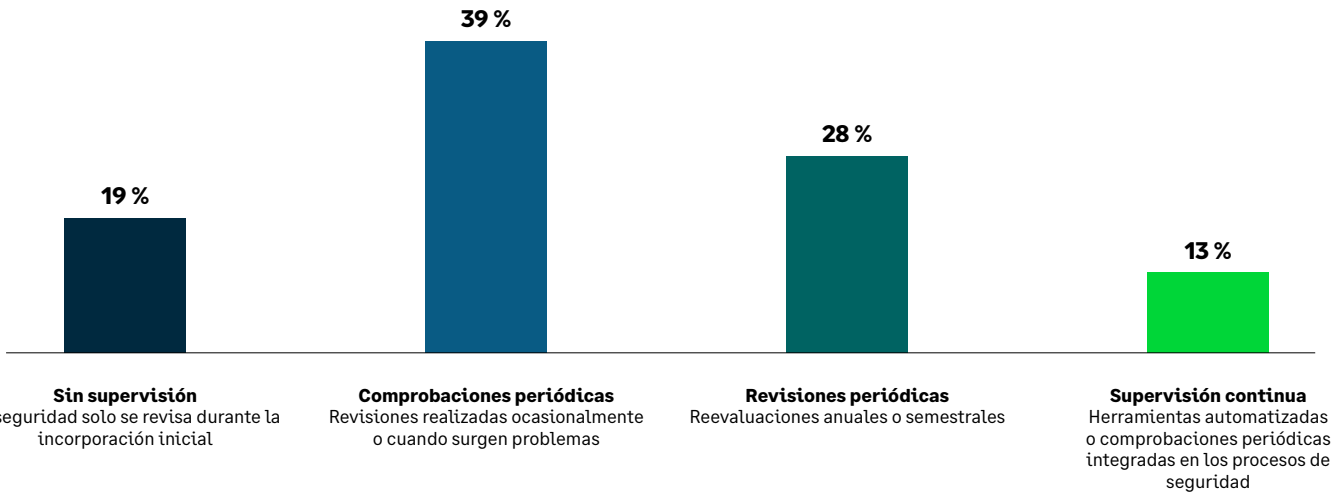
Las aplicaciones SaaS y las plataformas de terceros ocupan ahora un lugar central en muchas operaciones de las pymes, pero la supervisión de la seguridad sigue siendo a menudo intermitente.

En muchas empresas, el riesgo asociado a los proveedores se revisa al inicio de la relación o cuando se renueva el contrato, en lugar de supervisarse de forma continua. Esto genera lagunas de visibilidad, aumenta la exposición y eleva la probabilidad de que los problemas solo se detecten una vez que la disrupción ya se ha producido.

Las microempresas y las pequeñas empresas están especialmente expuestas, y una proporción significativa de ellas afirma realizar poca o ninguna supervisión periódica de los servicios de terceros. Como resultado, los posibles problemas pueden pasar desapercibidos hasta que se produce una interrupción.

Las pymes con mayor grado de madurez adoptan controles de acceso centralizados, una gestión más clara del ciclo de vida de los usuarios y revisiones más frecuentes de los proveedores, lo que mejora su capacidad para identificar anomalías y responder antes. Las conclusiones sugieren que tratar la seguridad de terceros como un proceso continuo, y no como una comprobación puntual, es cada vez más importante a medida que se amplían los ecosistemas SaaS y se introducen herramientas impulsadas por la IA a través de proveedores externos.

¿Con qué frecuencia supervisan las pymes la seguridad de los proveedores externos de software como servicio (SaaS)?



Para las pymes, mejorar la seguridad de los servicios SaaS de terceros empieza por reforzar la disciplina del día a día: saber qué herramientas se están utilizando, controlar quién puede acceder a ellas, eliminar con rapidez las cuentas que ya no se usan y estar atentos a aplicaciones no autorizadas o a actividades inusuales. Especialmente en los equipos más pequeños, un enfoque sencillo y coherente, respaldado por proveedores de confianza o servicios gestionados, será más eficaz que tratar de implantar por sí solos un modelo de supervisión complejo.

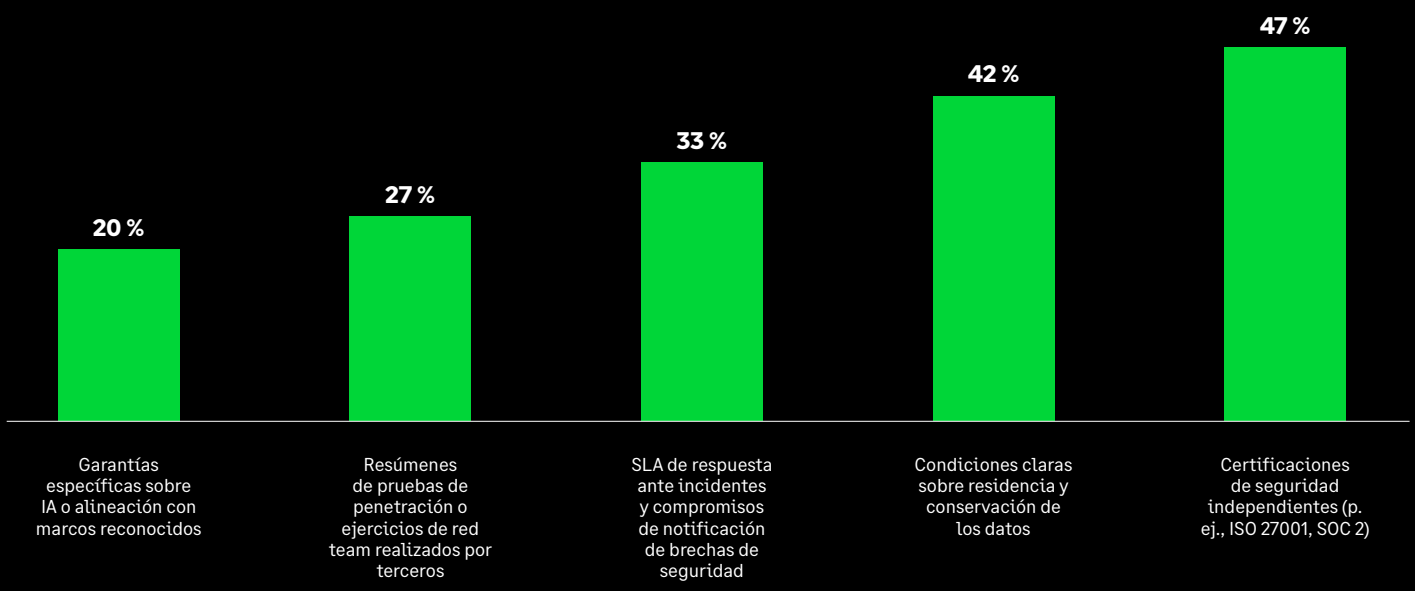
Las pymes confían en pruebas claras y verificables al evaluar a proveedores externos

A medida que los servicios SaaS y los servicios impulsados por la IA se integran cada vez más en las operaciones de las pymes, la confianza en los proveedores depende cada vez más de pruebas claras, comprensibles y fáciles de verificar.

Las pymes conceden mayor valor a las certificaciones independientes, a una gestión transparente de los datos y a compromisos claros de respuesta ante incidentes, porque ofrecen una garantía práctica de que existen medidas básicas de seguridad. Las afirmaciones más técnicas y específicas sobre IA pueden parecer avanzadas, pero a las organizaciones más pequeñas les resulta a menudo más difícil evaluarlas con confianza.

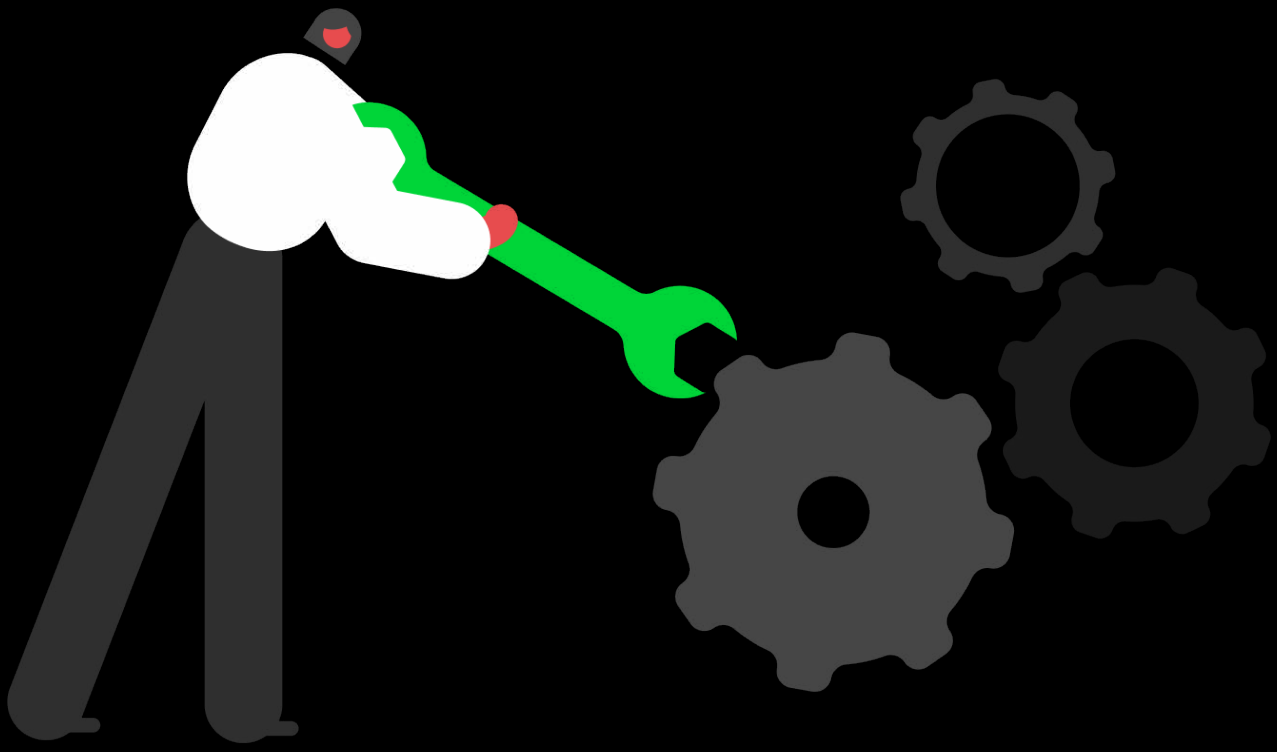
Por eso, la claridad se convierte en una ventaja competitiva. Los proveedores que saben explicar, en términos sencillos, cómo se protegen los datos de los clientes, dónde se almacenan y qué ocurre si algo sale mal están en mejor posición para generar confianza.

Pruebas que generan confianza en la seguridad de la IA y en las prácticas responsables de un proveedor externo



Las pymes deberían priorizar a los proveedores que ofrezcan pruebas claras y auditables de cómo gestionan la seguridad, y revisar esa confianza de forma periódica en lugar de tratarla como una comprobación puntual.

Convertir la información en acción



Sage

Microempresas: reforzar la resiliencia con medidas sencillas y escalables

A medida que se amplía la adopción de la IA, es fundamental reforzar la asignación de responsabilidades, los ciclos de revisión y la gobernanza básica. Las medidas deben seguir siendo de bajo coste y fáciles de implantar, dando prioridad a la sencillez y a una carga de gestión mínima.

Acciones a corto plazo

Postura de ciberseguridad
Asignar responsabilidades claras: Designe a una persona responsable de la seguridad y documente una lista sencilla de comprobación para la respuesta ante incidentes que incluya la escalada, las copias de seguridad y el apoyo externo.

Seguridad de la IA
Asegurar el acceso a sistemas de IA: Restrinja el acceso a los sistemas de IA al personal autorizado, habilite un registro básico de la actividad y exija contraseñas robustas para reducir los riesgos a medida que aumenta el uso de la IA.

Planes a medio plazo

Postura de ciberseguridad
Implantar una disciplina operativa constante: Introduzca revisiones periódicas de seguridad que abarquen los derechos de acceso, las actualizaciones de software, las copias de seguridad y las herramientas de terceros.

Seguridad de la IA
Definir normas y formar al personal: Formalice las normas de tratamiento de los datos y los protocolos de acceso, proporcione formación al personal y siente las bases de una seguridad de la IA escalable.

Consideraciones a largo plazo

Postura de ciberseguridad
Reducir la dependencia del talento interno: Consolide y estandarice los controles, priorizando servicios de bajo coste, integrados o gestionados para reducir la carga operativa y financiera.

Seguridad de la IA
Implantar prácticas de supervisión: Establezca una supervisión continua básica y lleve a cabo comprobaciones básicas de la seguridad de la IA de los proveedores. Seleccione aplicaciones fiables y con un compromiso claro con la seguridad.

Pequeñas empresas: reforzar la seguridad mediante estructura y disciplina

Las pequeñas empresas necesitan estructurar los procesos de seguridad y la gobernanza de la IA. A medida que se amplía la adopción de la IA, formalizar y aplicar de forma coherente las prácticas de seguridad se vuelve esencial para reducir el riesgo no gestionado.

Acciones a corto plazo

Postura de ciberseguridad
Formalizar la visibilidad del riesgo: Haga que los informes de seguridad sean periódicos, confirme quién es responsable de las decisiones clave y garantice que los incidentes y las revisiones de acceso se aborden a nivel directivo.

Seguridad de la IA
Visibilidad de los activos de IA: Mantenga un inventario actualizado de los modelos, agentes, conjuntos de datos y servicios de IA. Supervise el uso no autorizado o encubierto de aplicaciones de IA.

Planes a medio plazo

Postura de ciberseguridad
Profesionalizar las operaciones de seguridad: Aplique las políticas de forma coherente en todos los equipos, introduzca comprobaciones del riesgo de terceros antes de contratar proveedores y racionalice las herramientas existentes para reducir la complejidad.

Seguridad de la IA
Asegurar las interacciones con la IA: Valide las entradas y las salidas para prevenir la inyección de instrucciones, la evasión de restricciones y las fugas de datos.

Consideraciones a largo plazo

Postura de ciberseguridad
Integrar la seguridad en las decisiones empresariales: Incorpore la seguridad a las decisiones de compra, a las iniciativas digitales y a los planes de expansión, de modo que la gestión del riesgo evolucione al mismo ritmo que el crecimiento del negocio.

Seguridad de la IA
Preparación ante incidentes relacionados con la IA: Documente y pruebe un plan de respuesta ante incidentes para fallos o brechas de seguridad relacionados con la IA. Implante una gestión estructurada del riesgo de los proveedores.

Medianas empresas: ampliar la seguridad de forma coherente en toda la empresa

Las medianas empresas cuentan con una seguridad bien estructurada, con funciones específicas, una gestión proactiva y una supervisión formal de terceros. El siguiente paso es garantizar que ese grado de madurez se amplíe de forma coherente a medida que crece la exposición digital y a la IA.

Acciones a corto plazo

Postura de ciberseguridad

Reforzar los controles existentes: Identifique los activos críticos y los proveedores clave, revise los derechos de acceso en todos los equipos e identifique las herramientas de seguridad solapadas o infrautilizadas.

Seguridad de la IA

Gestión del riesgo de la IA: Formalice un marco de seguridad para la IA que incorpore visibilidad sobre la IA y los datos, supervisión continua de anomalías del sistema y una gestión estructurada del riesgo de los proveedores.

Planes a medio plazo

Postura de ciberseguridad

Estandarizar las prácticas de seguridad: Aplique los mismos controles y normas en todos los departamentos, introduzca revisiones estructuradas de los proveedores e informe periódicamente a la dirección sobre los indicadores clave de riesgo.

Seguridad de la IA

Alineación normativa: Garantice que el uso de la IA cumpla la normativa en materia de privacidad y de IA. Integre las consideraciones relativas a la IA en los marcos existentes de aseguramiento de la seguridad.

Consideraciones a largo plazo

Postura de ciberseguridad

Integrar la seguridad en la gobernanza corporativa: Integre la ciberseguridad en las compras, la continuidad de negocio y la planificación estratégica para que la protección evolucione en línea con el crecimiento de la organización.

Seguridad de la IA

Pruebas adversariales: Ponga a prueba la resiliencia de los sistemas de IA frente a ataques adversariales o ejercicios de intrusión controlada.

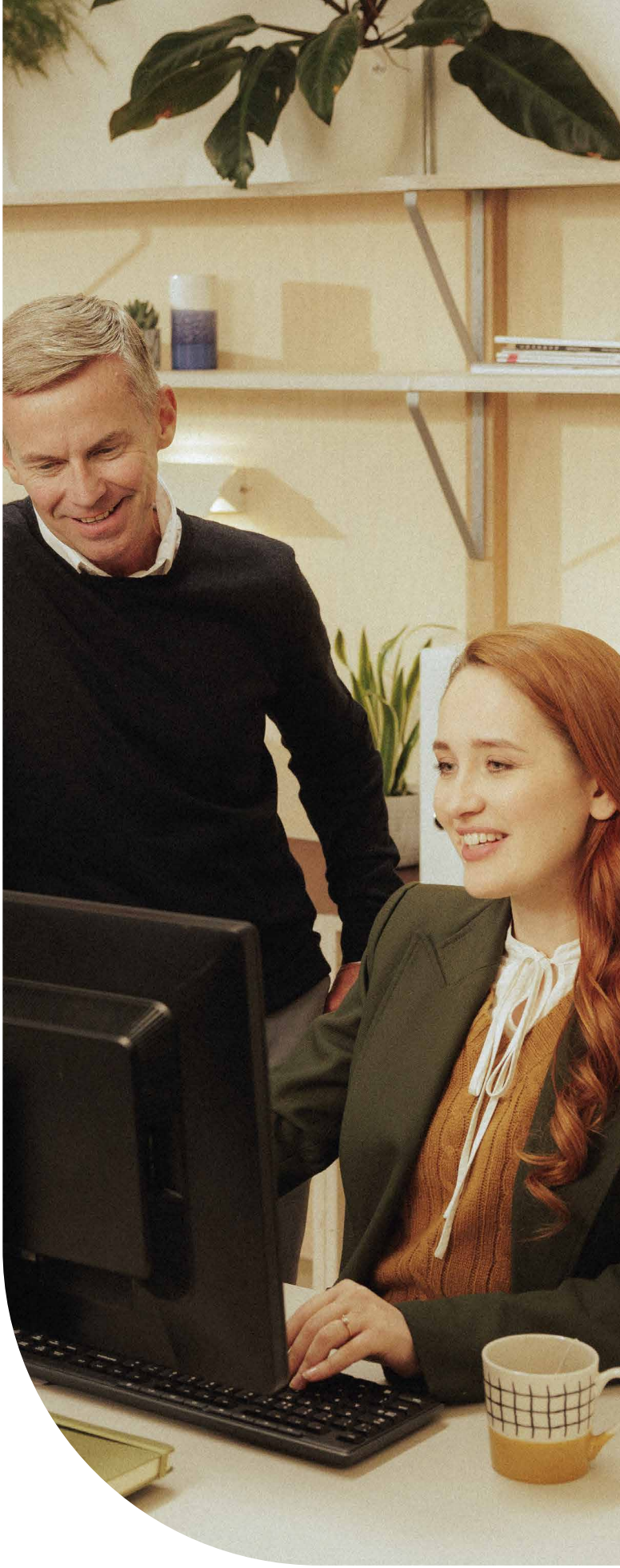
Mensaje de Sage

Sage lleva mucho tiempo apoyando a las pequeñas y medianas empresas y comprende las oportunidades y las presiones a las que se enfrentan. Este informe muestra que la ciberseguridad es ya una prioridad empresarial clave para las pymes. Se sitúa justo por detrás del crecimiento en la agenda empresarial, lo que refleja hasta qué punto la ciberresiliencia está hoy estrechamente vinculada a la confianza, la continuidad y el éxito a largo plazo.

Muchas pymes están afrontando un ciber riesgo creciente con tiempo, personal y presupuesto limitados, al tiempo que la IA y la tecnología de terceros se integran cada vez más en la actividad diaria. No deberían tener que gestionar esto solas.

En Sage, nos centramos en ayudar a las pymes a aplicar buenas prácticas de seguridad mediante orientaciones claras, principios de seguridad desde el diseño y transparencia sobre cómo se protegen los datos y cómo se utiliza la IA. El objetivo es permitir que las pymes mitiguen los riesgos mientras utilizan la tecnología para impulsar su crecimiento.

Los gobiernos, los organismos sectoriales, los proveedores de software y los distintos suministradores deberían colaborar estrechamente para ofrecer a las pymes orientaciones más claras, salvaguardas más sencillas y apoyo práctico ajustado a la realidad a la que se enfrentan cada día.



Anexo: Conclusiones por país

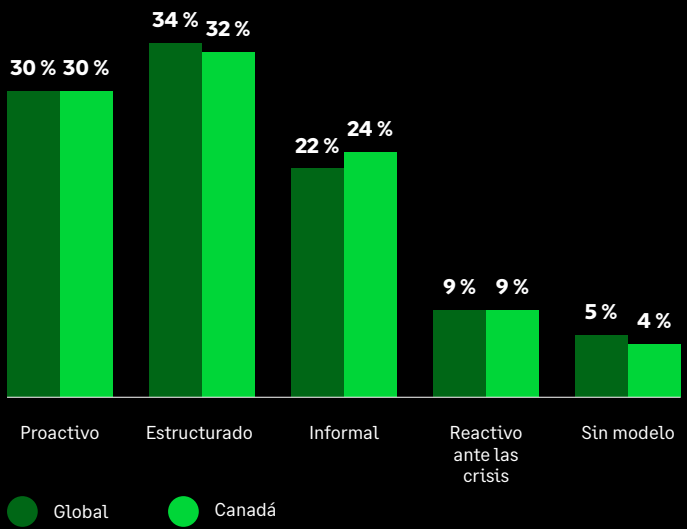
Sage

Canadá

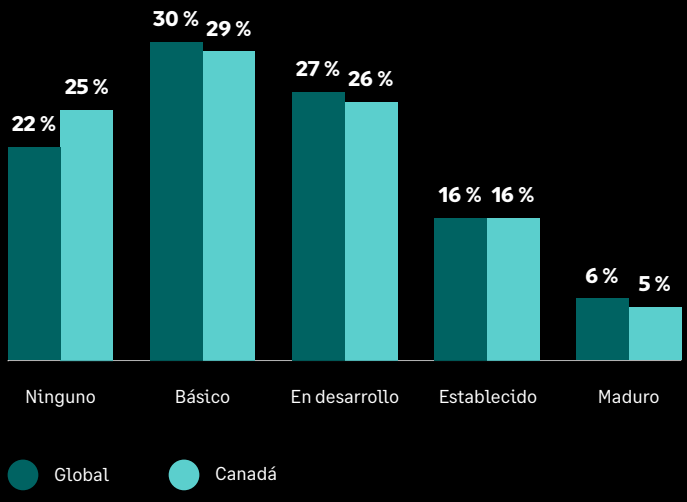
Canadá se sitúa por encima de la media mundial en medidas básicas de seguridad, lo que le proporciona una base sólida para la protección diaria y contribuye a mantener los niveles de incidentes cerca de la media global.

La brecha aparece en la preparación para la IA. Canadá parece menos preparado para convertir esa base sólida en una seguridad eficaz de la IA, con una adopción más limitada de salvaguardas prácticas, un menor grado de preparación para el cumplimiento normativo y la mayor escasez declarada de especialización en seguridad de la IA. Ahora el foco debe pasar de mantener lo básico a desarrollar las capacidades, la supervisión y las barreras prácticas necesarias para gestionar con mayor eficacia el riesgo relacionado con la IA.

Modelo de gestión de la ciberseguridad



Nivel actual de seguridad de las aplicaciones impulsadas por la IA



Incidentes de ciberseguridad o brechas de seguridad en el último año

Canadá	55 % Sin incidentes	33 % Incidentes menores, resueltos con rapidez	10 % Incidentes que causaron una disrupción significativa
Global	54 % Sin incidentes	34 % Incidentes menores, resueltos con rapidez	11 % Incidentes que causaron una disrupción significativa

Principales medidas de seguridad implantadas

Canadá	86 % Protección del correo electrónico	82 % Mantenimiento (actualización, aplicación de parches y copias de seguridad)	77 % MFA/SSO
Global	79 % Protección del correo electrónico	71 % Mantenimiento (actualización, aplicación de parches y copias de seguridad)	67 % Protección de terminales

Principales retos para proteger las aplicaciones de IA

Canadá	48 % Especialización insuficiente en seguridad de la IA	38 % Implantar una sólida seguridad de los datos	41 % Mantener el ritmo frente a las amenazas emergentes de la IA
Global	45 % Especialización insuficiente en seguridad de la IA	41 % Implantar una sólida seguridad de los datos	36 % Mantener el ritmo frente a las amenazas emergentes de la IA

Principales salvaguardas frente a los riesgos y amenazas de la IA

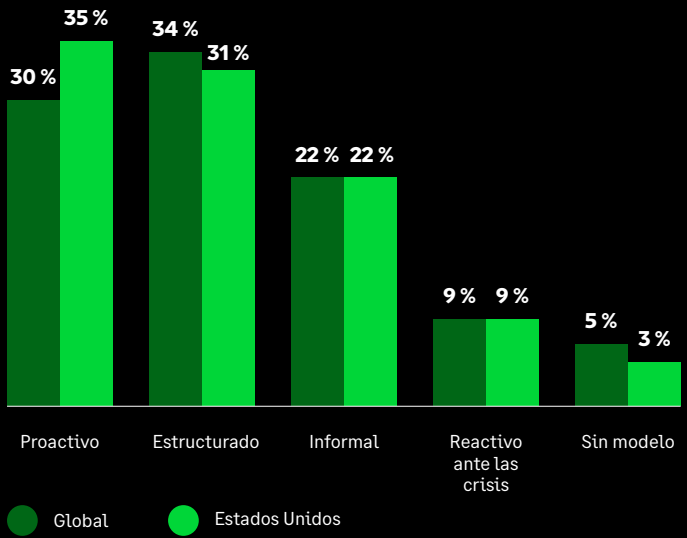
Canadá	35 % Política clara de uso de la IA	34 % Herramientas de IA aprobadas con controles de administración	32 % Pruebas de las herramientas de IA antes de su despliegue
Global	41 % Política clara de uso de la IA	38 % Herramientas de IA aprobadas con controles de administración	33 % Pruebas de las herramientas de IA antes de su despliegue

Estados Unidos

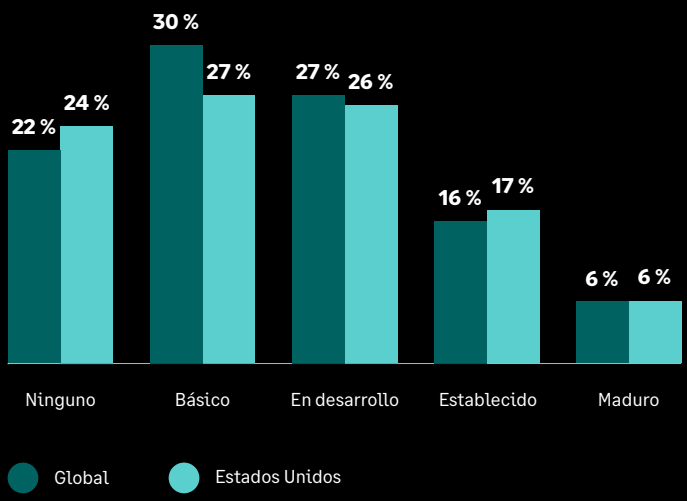
Estados Unidos se sitúa por encima de la media global en la transición desde la concienciación en materia de ciberseguridad hacia una práctica diaria más estructurada. Esto le proporciona un punto de partida más sólido que el de muchos mercados a medida que la IA se integra cada vez más en las operaciones empresariales.

La mayor proporción de incidentes más graves sugiere que ahora el foco debe pasar de construir los fundamentos a mejorar la resiliencia en la práctica, especialmente en lo relativo a la seguridad de los datos, la supervisión y la capacidad de respuesta a medida que las amenazas evolucionan con mayor rapidez.

Modelo de gestión de la ciberseguridad



Nivel actual de seguridad de las aplicaciones impulsadas por la IA



Incidentes de ciberseguridad o brechas de seguridad en el último año

Estados Unidos	55 % Sin incidentes	32 % Incidentes menores, resueltos con rapidez	13 % Incidentes que causaron una disrupción significativa
Global	54 % Sin incidentes	34 % Incidentes menores, resueltos con rapidez	11 % Incidentes que causaron una disrupción significativa

Principales medidas de seguridad implantadas

Estados Unidos	85 % Protección del correo electrónico	71 % Mantenimiento (actualización, aplicación de parches y copias de seguridad)	69 % Protección de terminales
Global	79 % Protección del correo electrónico	71 % Mantenimiento (actualización, aplicación de parches y copias de seguridad)	67 % Protección de terminales

Principales retos para proteger las aplicaciones de IA

Estados Unidos	43 % Especialización insuficiente en seguridad de la IA	38 % Implantar una sólida seguridad de los datos	38 % Mantener el ritmo frente a las amenazas emergentes de la IA
Global	45 % Especialización insuficiente en seguridad de la IA	41 % Implantar una sólida seguridad de los datos	36 % Mantener el ritmo frente a las amenazas emergentes de la IA

Principales salvaguardas frente a los riesgos y amenazas de la IA

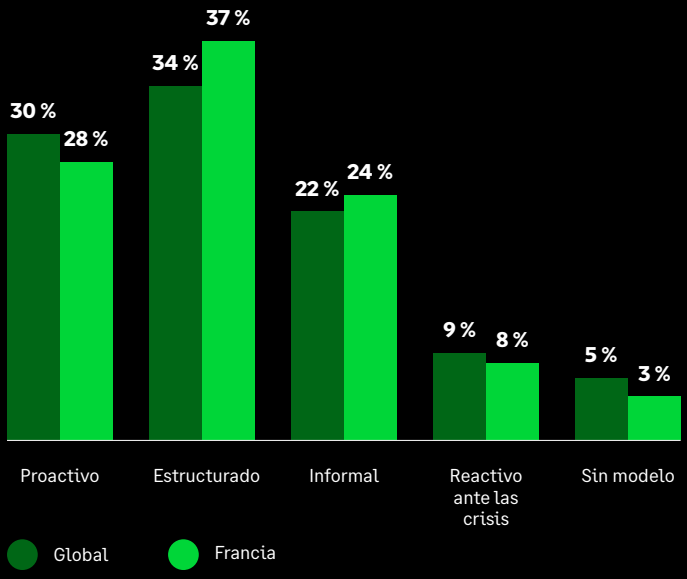
Estados Unidos	40 % Política clara de uso de la IA	39 % Herramientas de IA aprobadas con controles de administración	34 % Pruebas de las herramientas de IA antes de su despliegue
Global	41 % Política clara de uso de la IA	38 % Herramientas de IA aprobadas con controles de administración	33 % Pruebas de las herramientas de IA antes de su despliegue

Francia

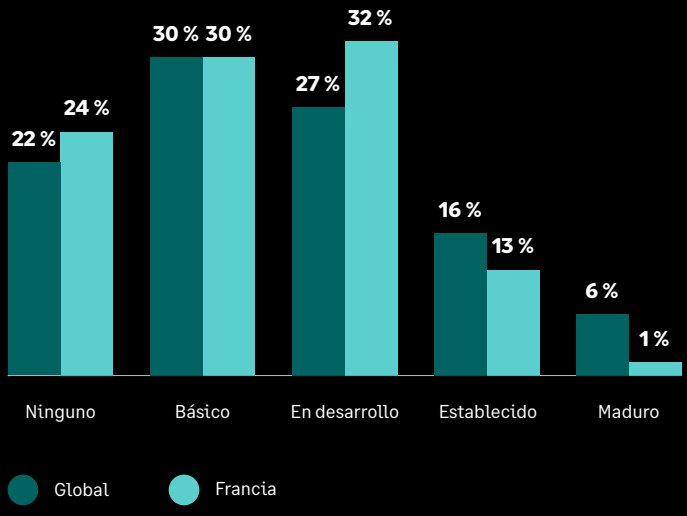
Francia afronta un nivel de presión en materia de ciberseguridad superior a la media global. Las medidas básicas de seguridad están menos implantadas, la proporción de organizaciones que declaran haber sufrido disrupciones significativas es mayor y la madurez de la seguridad de la IA sigue siendo más baja, con menos organizaciones situadas en los niveles más avanzados. Esto apunta a un mercado en el que los fundamentos de la seguridad son menos consistentes y en el que el impacto empresarial del ciber riesgo es más acusado.

El siguiente paso es reforzar tanto los aspectos básicos como la capacidad de gestionar en la práctica el riesgo relacionado con la IA. Una mayor visibilidad, una protección de los datos más sólida y una preparación más estructurada para la respuesta serán fundamentales, especialmente en un mercado donde la confianza parece depender en gran medida de la capacidad de las organizaciones para reaccionar cuando algo sale mal.

Modelo de gestión de la ciberseguridad



Nivel actual de seguridad de las aplicaciones impulsadas por la IA



Incidentes de ciberseguridad o brechas de seguridad en el último año

Francia	51 % Sin incidentes	33 % Incidentes menores, resueltos con rapidez	15 % Incidentes que causaron una disrupción significativa
Global	54 % Sin incidentes	34 % Incidentes menores, resueltos con rapidez	11 % Incidentes que causaron una disrupción significativa

Principales medidas de seguridad implantadas

Francia	77 % Protección del correo electrónico	El 60 % Mantenimiento (actualización, aplicación de parches y copias de seguridad)	69 % Protección de terminales
Global	79 % Protección del correo electrónico	71 % Mantenimiento (actualización, aplicación de parches y copias de seguridad)	67 % Protección de terminales

Principales retos para proteger las aplicaciones de IA

Francia	48 % Especialización insuficiente en seguridad de la IA	43 % Implantar una sólida seguridad de los datos	35 % Visibilidad limitada de las herramientas de IA en uso
Global	45 % Especialización insuficiente en seguridad de la IA	41 % Implantar una sólida seguridad de los datos	36 % Mantener el ritmo frente a las amenazas emergentes de la IA

Principales salvaguardas frente a los riesgos y amenazas de la IA

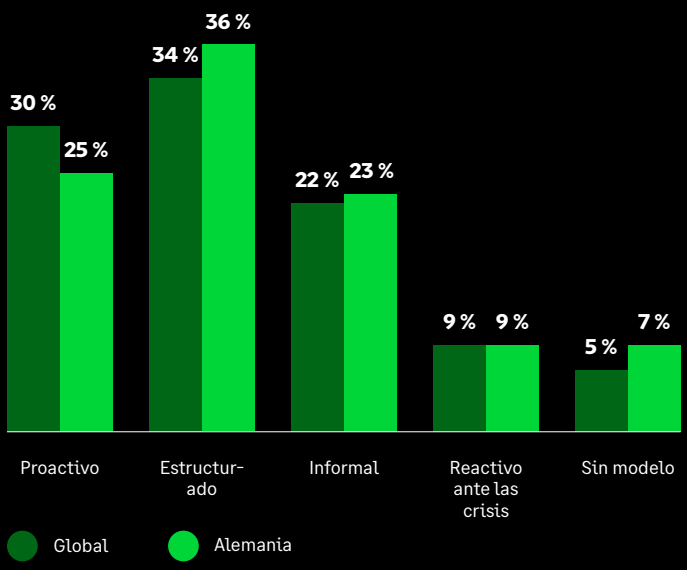
Francia	42 % Política clara de uso de la IA	38 % Herramientas de IA aprobadas con controles de administración	34 % Pruebas de las herramientas de IA antes de su despliegue
Global	41 % Política clara de uso de la IA	38 % Herramientas de IA aprobadas con controles de administración	33 % Pruebas de las herramientas de IA antes de su despliegue

Alemania

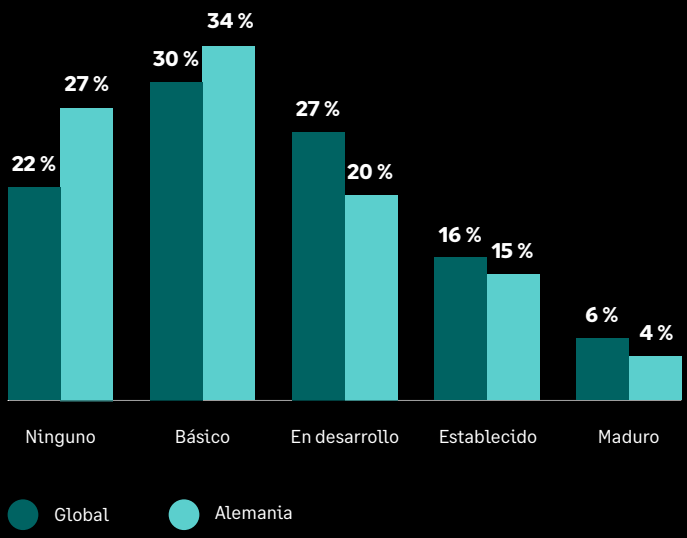
Alemania muestra un perfil más cauteloso y más orientado al cumplimiento normativo que la media global. Las medidas básicas están menos implantadas, la gestión proactiva es menor y la madurez de la seguridad de la IA sigue siendo más baja, con más organizaciones aún en fases iniciales. Los niveles de incidentes se mantienen cerca de los valores globales, por lo que la presión hoy es menos visible, pero los fundamentos para gestionar el riesgo relacionado con la IA siguen estando poco desarrollados.

La prioridad de Alemania es pasar de la cautela a una preparación práctica. La fuerte preocupación por el uso de los datos y la visibilidad limitada sobre las herramientas de IA ponen de manifiesto un mercado centrado en el control y el cumplimiento. El siguiente paso es reforzar las salvaguardas prácticas, mejorar la visibilidad sobre el uso de la IA y asegurarse de que la cautela se traduzca en una mayor resiliencia a medida que crece la adopción de la IA.

Modelo de gestión de la ciberseguridad



Nivel actual de seguridad de las aplicaciones impulsadas por la IA



Incidentes de ciberseguridad o brechas de seguridad en el último año

Alemania	**54 %** Sin incidentes	**36 %** Incidentes menores, resueltos con rapidez	**10 %** Incidentes que causaron una disrupción significativa
Global	**54 %** Sin incidentes	**34 %** Incidentes menores, resueltos con rapidez	**11 %** Incidentes que causaron una disrupción significativa

Principales medidas de seguridad implantadas

Alemania	**77 %** Protección del correo electrónico	**68 %** Mantenimiento (actualización, aplicación de parches y copias de seguridad)	**El 61 %** MFA/SSO
Global	**79 %** Protección del correo electrónico	**71 %** Mantenimiento (actualización, aplicación de parches y copias de seguridad)	**67 %** Protección de terminales

Principales retos para proteger las aplicaciones de IA

Alemania	**43 %** Especialización insuficiente en seguridad de la IA	**39 %** Implantar una sólida seguridad de los datos	**37 %** Visibilidad limitada de las herramientas de IA en uso
Global	**45 %** Especialización insuficiente en seguridad de la IA	**41 %** Implantar una sólida seguridad de los datos	**36 %** Mantener el ritmo frente a las amenazas emer-gentes de la IA

Principales salvaguardas frente a los riesgos y amenazas de la IA

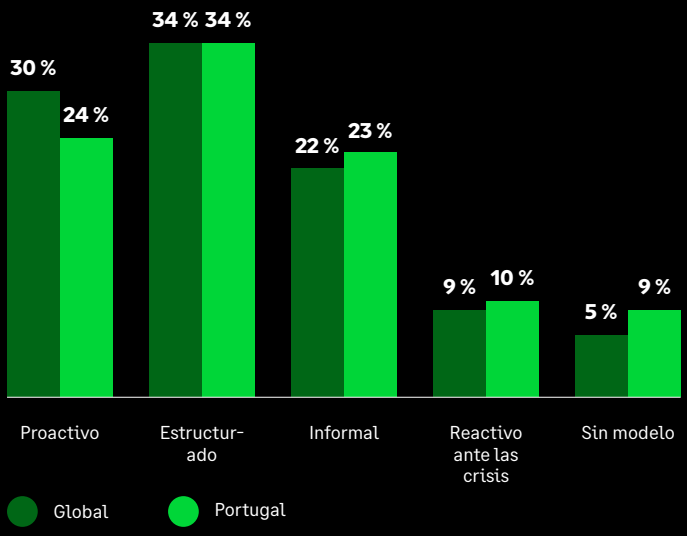
Alemania	**42 %** Política clara de uso de la IA	**32 %** Herramientas de IA aprobadas con controles de administración	**26 %** Controles de protección de datos sensibles
Global	**41 %** Política clara de uso de la IA	**38 %** Herramientas de IA aprobadas con controles de administración	**33 %** Pruebas de las herra-mientas de IA antes de su despliegue

Portugal

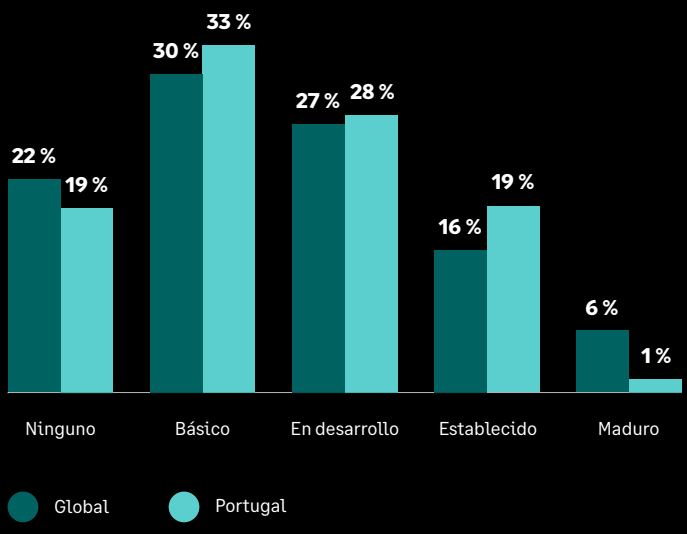
Portugal muestra un perfil de seguridad menos maduro que la media global. Las medidas básicas de seguridad están menos implantadas, los niveles de incidentes son más altos y las disrupciones significativas son más frecuentes. La madurez de la seguridad de la IA también sigue siendo desigual, con más organizaciones concentradas en la fase básica y muy pocas alcanzando un nivel maduro de adopción.

El reto de Portugal es la ejecución. La prioridad ahora es reforzar los fundamentos, reducir la incertidumbre en torno al tratamiento de los datos relacionados con la IA y consolidar unas prácticas de seguridad diarias más coherentes para que el riesgo se gestione con menos disrupciones. La mayor dependencia de certificaciones independientes también revela un mercado que busca pruebas externas claras de confianza a medida que crece la adopción de la IA.

Modelo de gestión de la ciberseguridad



Nivel actual de seguridad de las aplicaciones impulsadas por la IA



Incidentes de ciberseguridad o brechas de seguridad en el último año

Portugal	43 % Sin incidentes	39 % Incidentes menores, resueltos con rapidez	16 % Incidentes que causaron una disrupción significativa
Global	54 % Sin incidentes	34 % Incidentes menores, resueltos con rapidez	11 % Incidentes que causaron una disrupción significativa

Principales medidas de seguridad implantadas

Portugal	65 % Protección del correo electrónico	65 % Mantenimiento (actualización, aplicación de parches y copias de seguridad)	El 61 % Protección de terminales
Global	79 % Protección del correo electrónico	71 % Mantenimiento (actualización, aplicación de parches y copias de seguridad)	67 % Protección de terminales

Principales retos para proteger las aplicaciones de IA

Portugal	44 % Especialización insuficiente en seguridad de la IA	40 % Implantar una sólida seguridad de los datos	34 % Visibilidad limitada de las herramientas de IA en uso
Global	45 % Especialización insuficiente en seguridad de la IA	41 % Implantar una sólida seguridad de los datos	36 % Mantener el ritmo frente a las amenazas emergentes de la IA

Principales salvaguardas frente a los riesgos y amenazas de la IA

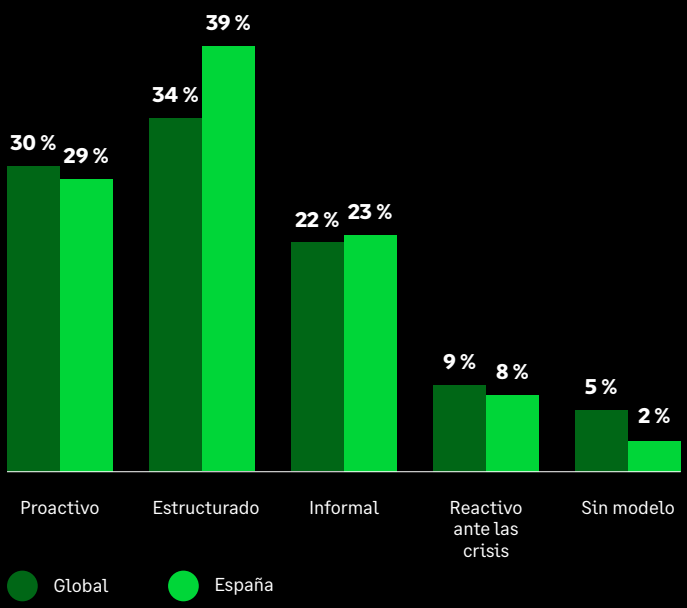
Portugal	43 % Política clara de uso de la IA	34 % Herramientas de IA aprobadas con controles de administración	33 % Pruebas de las herramientas de IA antes de su despliegue
Global	41 % Política clara de uso de la IA	38 % Herramientas de IA aprobadas con controles de administración	33 % Pruebas de las herramientas de IA antes de su despliegue

España

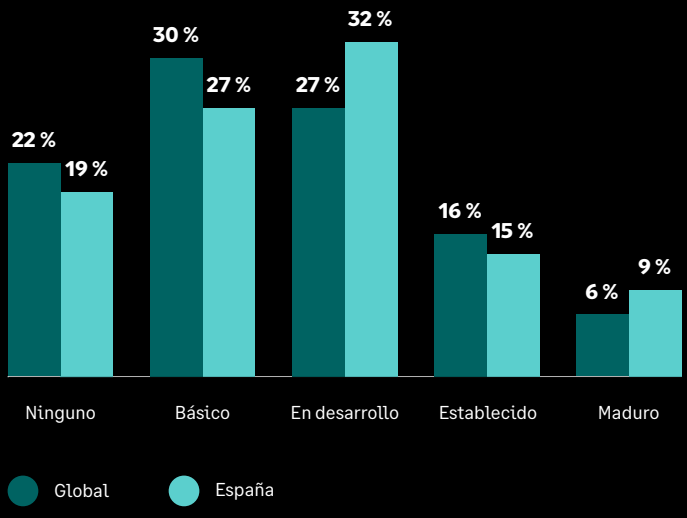
España muestra un perfil de seguridad más maduro que la media global. Los niveles de incidentes son más bajos, la gestión estructurada de la seguridad está más extendida y la madurez de la seguridad de la IA es mayor, con más organizaciones que superan las fases iniciales y alcanzan un nivel maduro de adopción.

El reto de España es mantener esa posición a medida que aumenta la adopción de la IA. La prioridad ahora es reforzar la protección frente a los riesgos relacionados con el factor humano, mejorar la visibilidad sobre el uso de la IA y cerrar las lagunas en la supervisión continua de terceros para evitar que un punto de partida más sólido se vea debilitado por puntos ciegos a medida que evolucionan las amenazas.

Modelo de gestión de la ciberseguridad



Nivel actual de seguridad de las aplicaciones impulsadas por la IA



Incidentes de ciberseguridad o brechas de seguridad en el último año

España	El 60 % Sin incidentes	29 % Incidentes menores, resueltos con rapidez	10 % Incidentes que causaron una disrupción significativa
Global	54 % Sin incidentes	34 % Incidentes menores, resueltos con rapidez	11 % Incidentes que causaron una disrupción significativa

Principales medidas de seguridad implantadas

España	75 % Protección del correo electrónico	72 % Mantenimiento (actualización, aplicación de parches y copias de seguridad)	62 % Protección de terminales
Global	79 % Protección del correo electrónico	71 % Mantenimiento (actualización, aplicación de parches y copias de seguridad)	67 % Protección de terminales

Principales retos para proteger las aplicaciones de IA

España	42 % Especialización insuficiente en seguridad de la IA	36 % Implantar una sólida seguridad de los datos	34 % Visibilidad limitada de las herramientas de IA en uso
Global	45 % Especialización insuficiente en seguridad de la IA	41 % Implantar una sólida seguridad de los datos	36 % Mantener el ritmo frente a las amenazas emergentes de la IA

Principales salvaguardas frente a los riesgos y amenazas de la IA

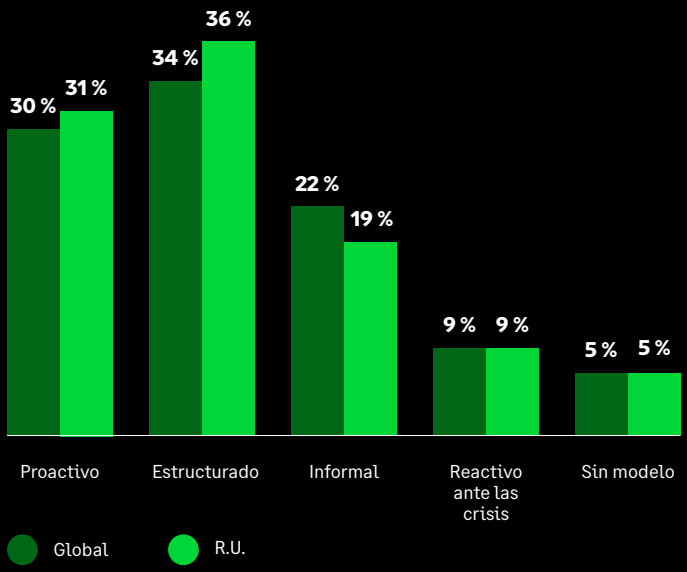
España	43 % Política clara de uso de la IA	38 % Herramientas de IA aprobadas con controles de administración	32 % Pruebas de las herramientas de IA antes de su despliegue
Global	41 % Política clara de uso de la IA	38 % Herramientas de IA aprobadas con controles de administración	33 % Pruebas de las herramientas de IA antes de su despliegue

Reino Unido

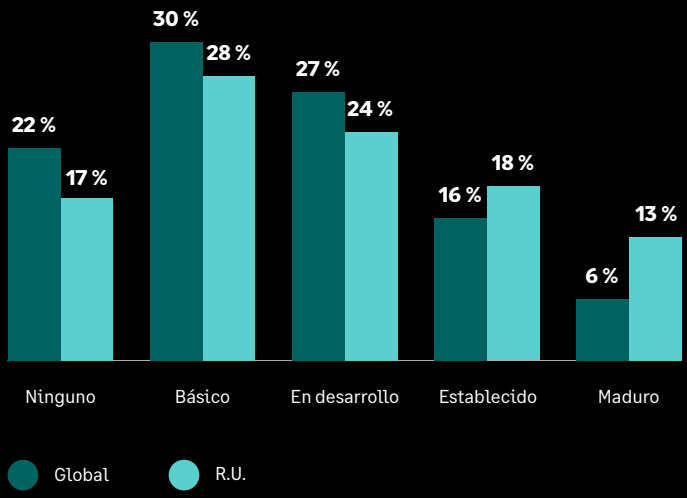
El Reino Unido destaca por avanzar más y con mayor rapidez en materia de seguridad de la IA que la media global. Las organizaciones presentan un mayor grado de madurez en la implantación de salvaguardas prácticas, es más probable que utilicen herramientas aprobadas y políticas formales, y están más avanzadas en la consolidación de una postura madura de seguridad de la IA. Esto apunta a un mercado que no espera a reaccionar, sino que está adoptando un enfoque más deliberado para prepararse frente al riesgo asociado a la IA a medida que aumenta su adopción.

La prioridad ahora es reforzar el control a medida que se amplía el uso de la IA, especialmente en lo relativo a la protección de los datos, la rápida evolución de las amenazas y la capacidad de convertir una postura más sólida en materia de IA en resiliencia efectiva en la práctica. El nivel ligeramente superior de disrupciones significativas también muestra que los avances en preparación todavía deben ir acompañados de una ejecución coherente cuando se producen incidentes.

Modelo de gestión de la ciberseguridad



Nivel actual de seguridad de las aplicaciones impulsadas por la IA



Incidentes de ciberseguridad o brechas de seguridad en el último año

R.U.	55 % Sin incidentes	32 % Incidentes menores, resueltos con rapidez	13 % Incidentes que causaron una disrupción significativa
Global	54 % Sin incidentes	34 % Incidentes menores, resueltos con rapidez	11 % Incidentes que causaron una disrupción significativa

Principales medidas de seguridad implantadas

R.U.	75 % Protección del correo electrónico	79 % Mantenimiento (actualización, aplicación de parches y copias de seguridad)	67 % Protección de terminales
Global	79 % Protección del correo electrónico	71 % Mantenimiento (actualización, aplicación de parches y copias de seguridad)	67 % Protección de terminales

Principales retos para proteger las aplicaciones de IA

R.U.	44 % Especialización insuficiente en seguridad de la IA	46 % Implantar una sólida seguridad de los datos	37 % Mantener el ritmo frente a las amenazas emergentes de la IA
Global	45 % Especialización insuficiente en seguridad de la IA	41 % Implantar una sólida seguridad de los datos	36 % Mantener el ritmo frente a las amenazas emergentes de la IA

Principales salvaguardas frente a los riesgos y amenazas de la IA

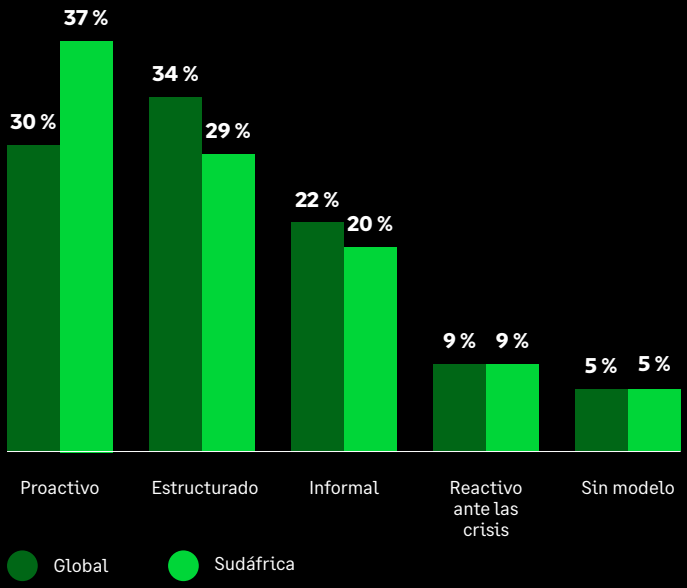
R.U.	43 % Política clara de uso de la IA	45 % Herramientas de IA aprobadas con controles de administración	38 % Pruebas de las herramientas de IA antes de su despliegue
Global	41 % Política clara de uso de la IA	38 % Herramientas de IA aprobadas con controles de administración	33 % Pruebas de las herramientas de IA antes de su despliegue

Sudáfrica

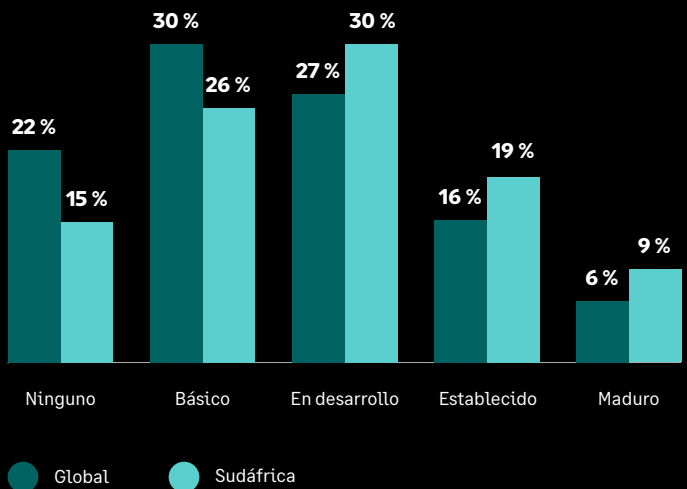
Sudáfrica se sitúa por encima de la media global en madurez de la seguridad de la IA. Las organizaciones muestran una mayor probabilidad de haber revisado a fondo su enfoque en respuesta a la IA, presentan un mayor grado de madurez en su postura de seguridad para las aplicaciones impulsadas por la IA y ofrecen un mejor desempeño en la supervisión continua de terceros. Esto apunta a un mercado que se toma en serio el riesgo asociado a la IA y que está implantando más salvaguardas prácticas a medida que crece la adopción.

El reto es convertir ese avance en una mayor consistencia. Las medidas básicas de seguridad siguen siendo desiguales y la preocupación por la protección de los datos y por la rápida evolución de las amenazas continúa siendo elevada. La prioridad ahora es cerrar esas brechas para que una postura más sólida en materia de IA vaya acompañada de unas prácticas diarias de seguridad más resilientes.

Modelo de gestión de la ciberseguridad



Nivel actual de seguridad de las aplicaciones impulsadas por la IA



Incidentes de ciberseguridad o brechas de seguridad en el último año

Sudáfrica	55 % Sin incidentes	35 % Incidentes menores, resueltos con rapidez	9 % Incidentes que causaron una disrupción significativa
Global	54 % Sin incidentes	34 % Incidentes menores, resueltos con rapidez	11 % Incidentes que causaron una disrupción significativa

Principales medidas de seguridad implantadas

Sudáfrica	75 % Protección del correo electrónico	74 % Mantenimiento (actualización, aplicación de parches y copias de seguridad)	70 % Protección de terminales
Global	79 % Protección del correo electrónico	71 % Mantenimiento (actualización, aplicación de parches y copias de seguridad)	67 % Protección de terminales

Principales retos para proteger las aplicaciones de IA

Sudáfrica	45 % Especialización insuficiente en seguridad de la IA	44 % Implantar una sólida seguridad de los datos	37 % Mantener el ritmo frente a las amenazas emergentes de la IA
Global	45 % Especialización insuficiente en seguridad de la IA	41 % Implantar una sólida seguridad de los datos	36 % Mantener el ritmo frente a las amenazas emergentes de la IA

Principales salvaguardas frente a los riesgos y amenazas de la IA

Sudáfrica	45 % Política clara de uso de la IA	39 % Herramientas de IA aprobadas con controles de administración	36 % Controles de protección de datos sensibles
Global	41 % Política clara de uso de la IA	38 % Herramientas de IA aprobadas con controles de administración	33 % Pruebas de las herramientas de IA antes de su despliegue

sage.com