RSA

RSA.com

Informe RSA ID IQ 2026

Estado del mercado de la seguridad de identidades

Tabla de contenido.

Resumen ejecutivo.

El informe RSA ID IQ de 2026 preguntó a más de 2000 expertos globales que detallaran con qué frecuencia les falló la seguridad de la identidad, cuánto perdieron cuando esto ocurrió y las vulnerabilidades que más temen.
Lo que nos informaron fue alarmante: la identidad falló a más organizaciones que el año pasado, lo que causó aún más daños financieros. A menos que los líderes actúen, los riesgos que enfrentan sus organizaciones se agravarán y las consecuencias de esos riesgos les costarán aún más.
Los datos muestran una creciente brecha en la seguridad de la identidad, ya que la mayoría de las organizaciones aún utilizan soluciones obsoletas que no abordan adecuadamente los nuevos desafíos. La mayoría de los usuarios aún dependen de contraseñas para la autenticación; sus organizaciones reportan filtraciones más frecuentes y mayores pérdidas.

Al mismo tiempo, los entornos operativos complejos y los casos de uso desafiantes les impiden avanzar hacia una economía sin contraseñas.
Las organizaciones carecen de las capacidades necesarias para defenderse de la ingeniería social y eludir los ataques a sus servicios de asistencia de TI, incluso cuando esta táctica se convierte en un riesgo cada vez más alarmante. Y si bien las organizaciones monitorean las identidades de personas, máquinas y servicios, la tasa de filtraciones de datos demuestra claramente que no utilizan esa información para reducir los riesgos de forma proactiva o eficaz.
Quizás debido a esos riesgos crecientes, los expertos informan que están totalmente a favor de la IA para la ciberseguridad.

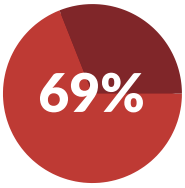
En todos los sectores, cada vez más usuarios creen que la IA contribuirá más a la ciberseguridad que a la ciberdelincuencia, y más organizaciones que nunca informan planes para integrar algún tipo de IA en sus soluciones de ciberseguridad. Las organizaciones también afirman, por un amplio margen, que los agentes IA para la ciberseguridad serán la principal capacidad que priorizarán.
Dejaré que los hallazgos hablen por sí solos. Y si bien esta información en sí misma es útil, es esencial que los líderes actúen en consecuencia priorizando la autenticación sin contraseña, implementando métodos modernos para defenderse de las estafas en el servicio de asistencia, detectando y resolviendo proactivamente los riesgos de identidad antes de que se conviertan en vulneraciones, y utilizando la IA como un factor multiplicador para automatizar una toma de decisiones más rápida.

El primer paso para abordar cualquier problema es reconocer su existencia. El Informe RSA ID IQ de 2026 deja claro que existen importantes preocupaciones con respecto a la seguridad de la identidad en la mayoría de las organizaciones.
La identidad simplemente falla en demasiadas organizaciones con demasiada frecuencia. La probabilidad de una vulneración, y el coste de la inacción, son simplemente demasiado altos para mantener el statu quo.

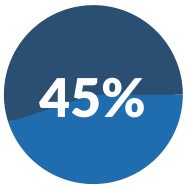
Greg Nelson, CEO de RSA

Hallazgos clave del informe RSA ID IQ de 2026

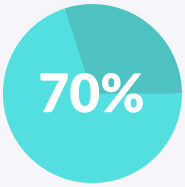
El Informe RSA ID IQ 2026 comparte información de 2120 expertos que trabajan en ciberseguridad, gestión de identidades y accesos (IAM), TI y otros campos. Entre las principales conclusiones se incluyen:



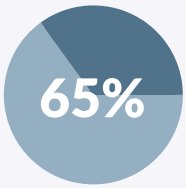
de las organizaciones informaron una violación de identidad en los últimos tres años, un aumento de 27 puntos porcentuales con respecto a 2025



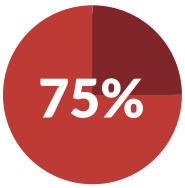
de las organizaciones dijeron que las violaciones de datos relacionadas con la identidad les costaron más que la violación de datos promedio



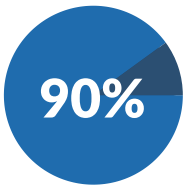
de las organizaciones dijeron que las violaciones de identidad les causaron un daño significativo



de las organizaciones dijeron que estaban seriamente preocupadas de que su Help Desk o servicio de TI no pudiera detener un ataque de ingeniería social.

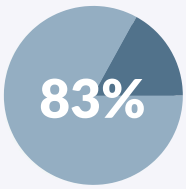


de las organizaciones operan en entornos híbridos, un aumento de 5 puntos porcentuales desde 2025

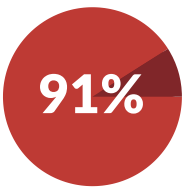


de las organizaciones informaron desafíos para avanzar hacia la autenticación sin contraseña

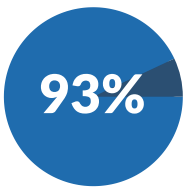
de las organizaciones siguen utilizando contraseñas como su principal método de autenticación



de las organizaciones creen que la IA hará más para ayudar a la ciberseguridad que al ciberdelito, un aumento del 3 por ciento desde 2025



de las organizaciones planean implementar alguna forma de IA en su pila tecnológica durante el próximo año, un aumento de 12 puntos porcentuales desde 2025



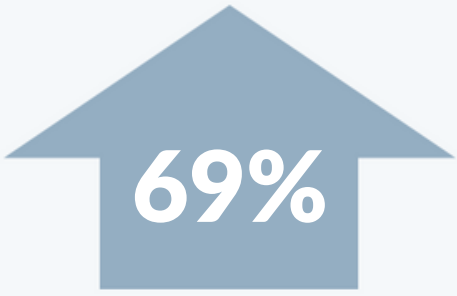
de las organizaciones no han alcanzado la madurez óptima de Confianza Cero o Zero Trust

Más violaciones de identidad causaron aún más daños este año

El análisis de las respuestas de la encuesta encontró que las organizaciones sufrieron más violaciones de seguridad como resultado de fallos de seguridad de identidad este año: el 69 % de las organizaciones informaron una violación en los últimos tres años, un aumento de 27 puntos porcentuales desde el Informe RSA ID IQ de 2025.

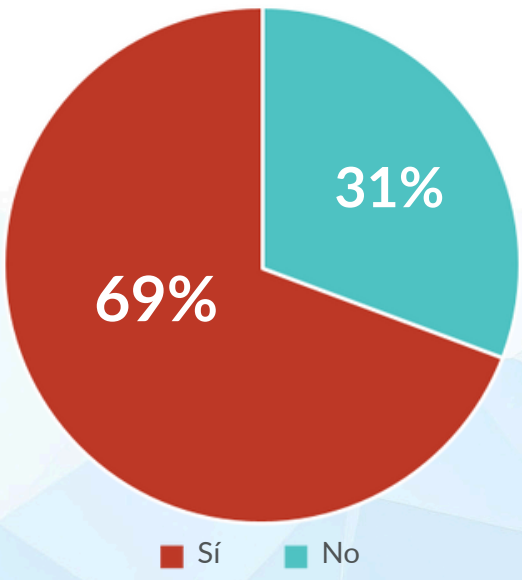
Además de ocurrir con mayor frecuencia, esas infracciones causaron mayores daños y tuvieron mayor impacto. Más de una quinta parte (21%) de los encuestados reportó que una filtración de identidad les costó entre 5 y 10 millones de dólares, mientras que casi una cuarta parte (24%) reportó que el coste de una filtración de identidad superó los 10 millones de dólares. Las filtraciones con costes superiores a 10 millones de dólares aumentaron tres puntos porcentuales en comparación con el informe del año pasado.

Estas cifras son alarmantes desde cualquier punto de vista. Resultan especialmente preocupantes si se comparan con el coste medio global de una filtración de datos resultante de cualquier vector de ataque. Un informe de IBM sobre vulneraciones de datos de 2025 reveló que una vulneración de datos cuesta, en promedio, 4,44 millones de dólares. Cuando falla la identidad, las organizaciones sufren un coste considerable. No es de extrañar que el 70 % de los encuestados calificara la gravedad de una vulneración con un cuatro o un cinco en una escala de cinco.



de las organizaciones informaron haber experimentado una violación relacionada con la identidad en los últimos 3 años, un aumento del **27 puntos porcentuales**

¿Su organización experimentó una violación **de identidad en los últimos 3 años?**

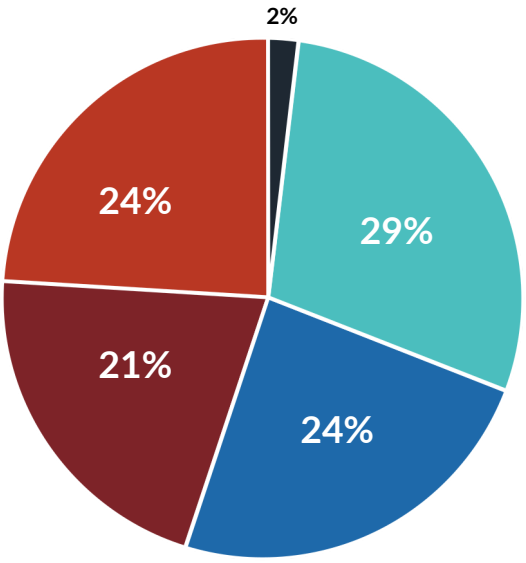


24%

de las organizaciones que experimentaron una violación relacionada con la identidad dijeron que el coste de la violación fue de

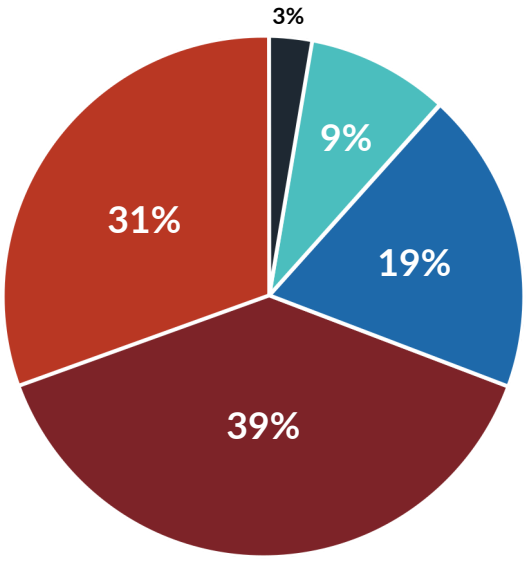
$10 millones o más, un aumento de 3 puntos porcentuales a partir de 2025

¿Cuánto dinero cree que perdió su organización debido a violaciones de datos relacionados con la identidad en los últimos tres años?



No sé | Menos de un millón de dólares | Entre 1 y 5 millones de dólares | Entre 5 y 10 millones de dólares | Más de 10 millones de dólares

Si sufrió una violación de identidad en los últimos tres años, evalúe la gravedad de su efecto en su organización del 1 al 5.



1 | 2 | 3 | 4 | 5

$4.44 Millón

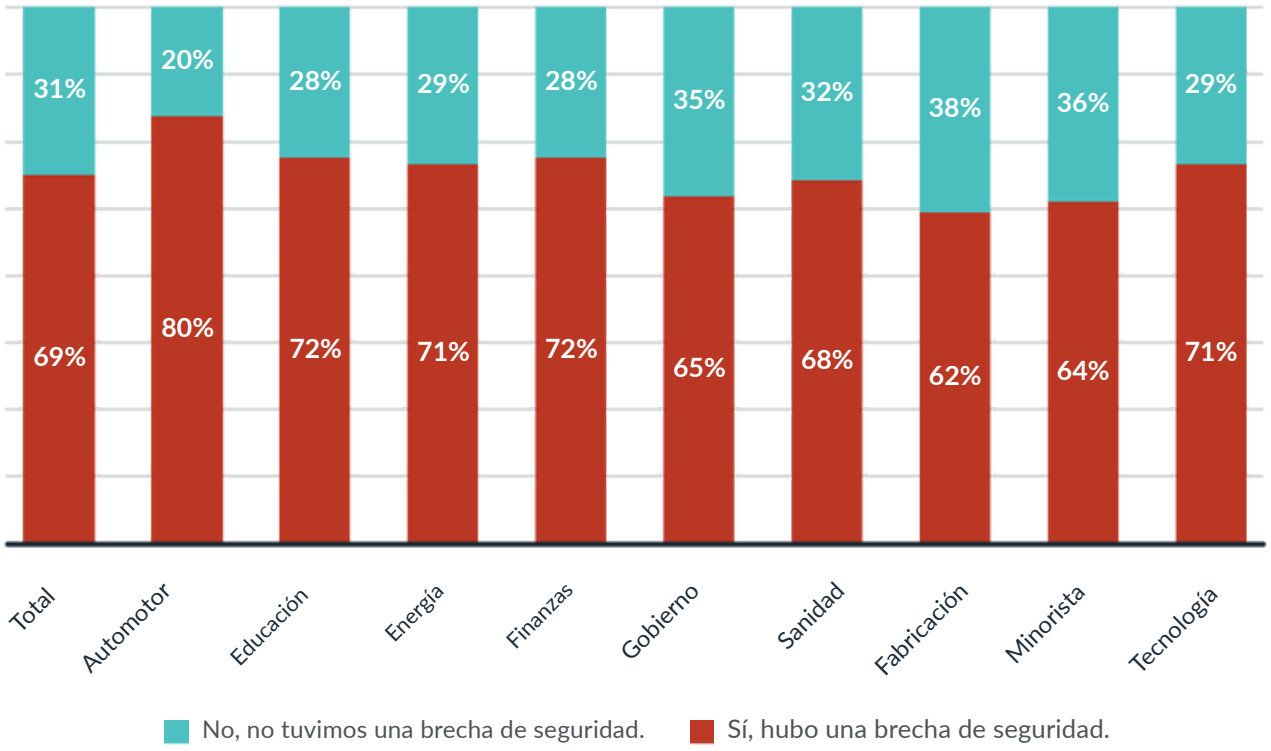
Promedio mundial del coste de todas las violaciones de datos, según el Informe de coste de una violación de datos de **IBM 2025**

Brechas de seguridad por sector

Al examinar las tasas de vulneraciones de datos por sector, la industria automotriz (80%), las finanzas (72%), la energía y los servicios públicos (71%) y la tecnología (71%) registraron la mayor frecuencia de vulneraciones de datos. El comercio minorista (64%) y la manufactura (62%) representan los sectores menos atacados por industria.

Por sector: ¿Su organización experimentó un problema relacionado con la identidad?

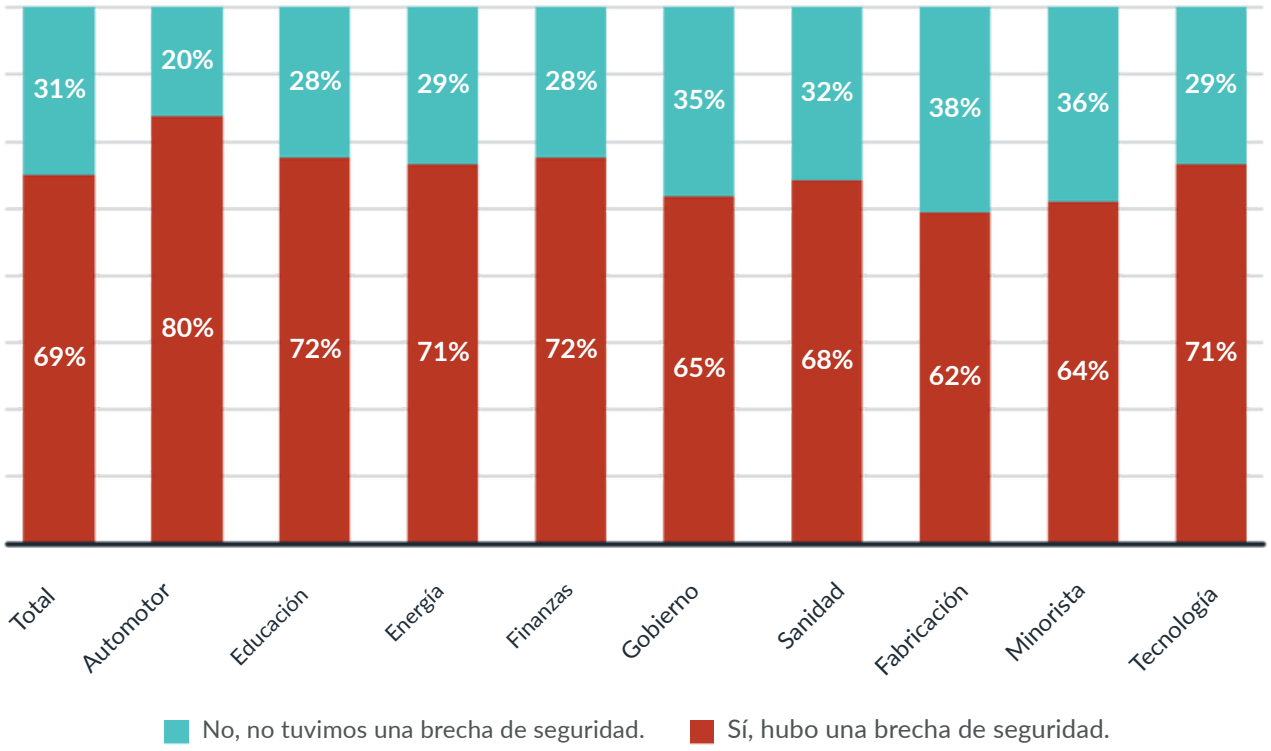
¿Se ha producido una infracción en los últimos tres años?



Brechas de seguridad por sector

Al examinar las tasas de vulneraciones de datos por sector, la industria automotriz (80%), las finanzas (72%), la energía y los servicios públicos (71%) y la tecnología (71%) registraron la mayor frecuencia de vulneraciones de datos. El comercio minorista (64%) y la manufactura (62%) representan los sectores menos atacados por industria.

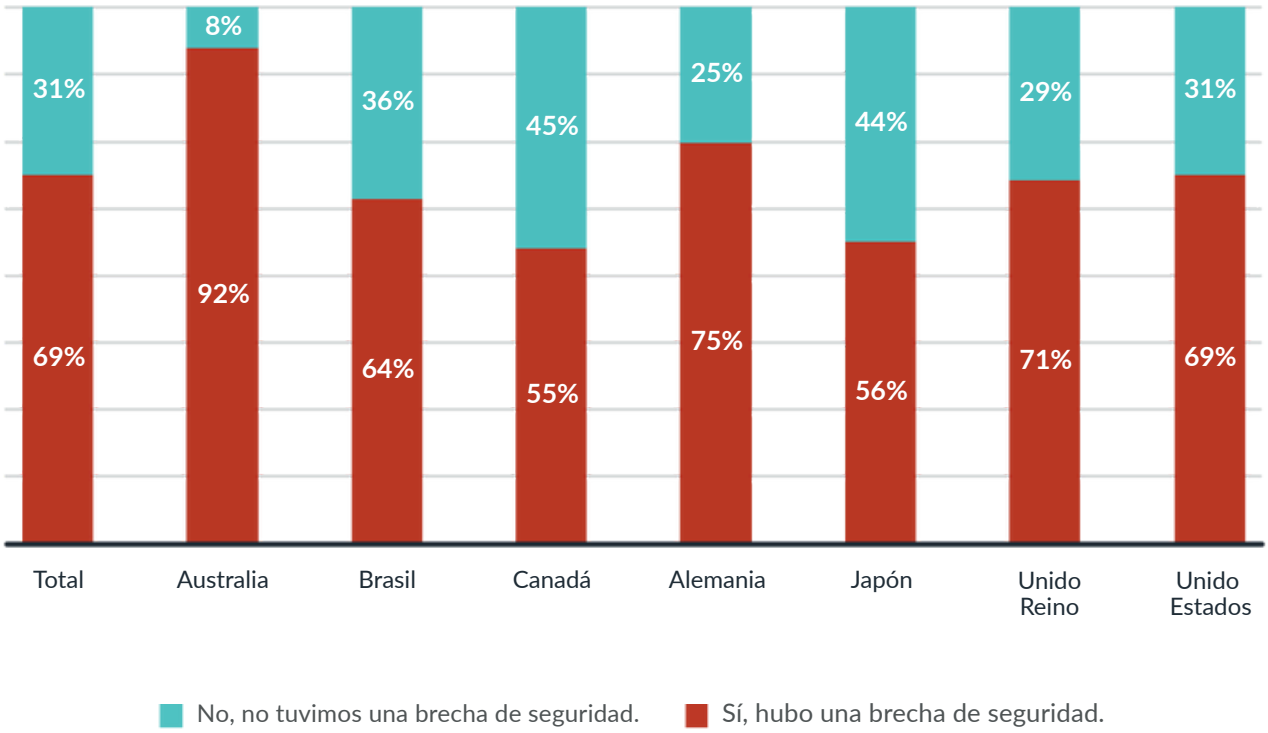
Por sector: ¿Su organización sufrió una violación de identidad en los últimos tres años?



Violaciones de seguridad por país

Por país, Australia (92%), Alemania (75%), Reino Unido (71%) y Estados Unidos (69%) reportaron las vulneraciones de identidad más frecuentes en los últimos tres años, mientras que Japón (56%) y Canadá (55%) reportaron el menor número de casos. Más adelante en el informe, explicamos cómo ciertas prácticas se correlacionan con la frecuencia y el impacto de estas vulneraciones.

Por país: ¿Su organización sufrió una violación de identidad en los últimos tres años?



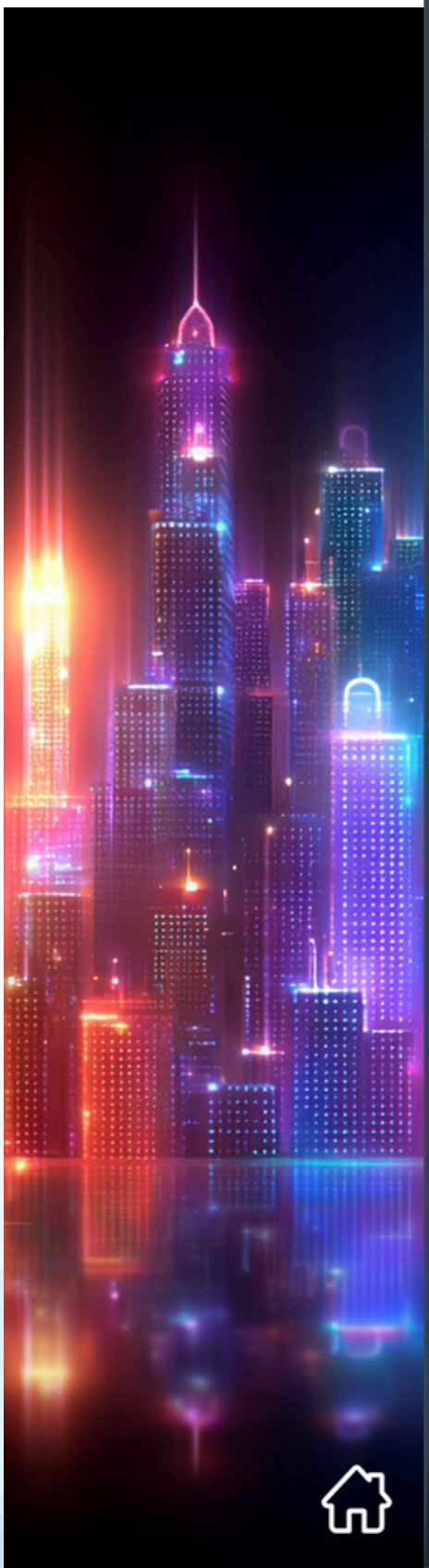
El “progreso” de la Confianza Cero o Zero Trust

Si bien solo el 7 % de las organizaciones informan que han alcanzado la madurez óptima de Confianza Cero para la identidad según lo define CISA, la mayoría (el 57 %) cree que ha alcanzado la etapa de Confianza Cero "Avanzada", que incluye:

- MFA resistente a la suplantación de identidad (phishing)
- Consolidación e integración segura de almacenes de identidad
- Evaluaciones automatizadas de riesgos de identidad
- Acceso basado en necesidad/sesión

Esa confianza se contradice con el hecho de que el **69% de las organizaciones fueron atacadas** y el **70% informó de que esos ataques fueron graves.**

Esto no pretende disuadir a las organizaciones de intentar consolidar su postura de Confianza Cero; todo lo contrario. La diferencia entre el punto en el que las organizaciones creen estar en su camino hacia la Confianza Cero y la frecuencia con la que sufren vulneraciones debería servir de advertencia a los responsables de seguridad para que se esfuercen más por protegerse.



Los riesgos de ciberseguridad que quitan el sueño a los expertos

Los encuestados seleccionaron el phishing como el vector de amenaza que representa el mayor riesgo de ciberseguridad para su organización. Y hay buenas razones para priorizarlo: año tras año, el phishing (que conlleva el robo de credenciales) y el uso de credenciales robadas se mantienen entre los ataques más frecuentes y de mayor impacto. Una de las mejores maneras de evitar el phishing es eliminar las credenciales que los estafadores intentan robar: en lugar de usar secretos compartidos, las organizaciones deberían esforzarse por implementar una autenticación sin contraseña y resistente al phishing.

192 días

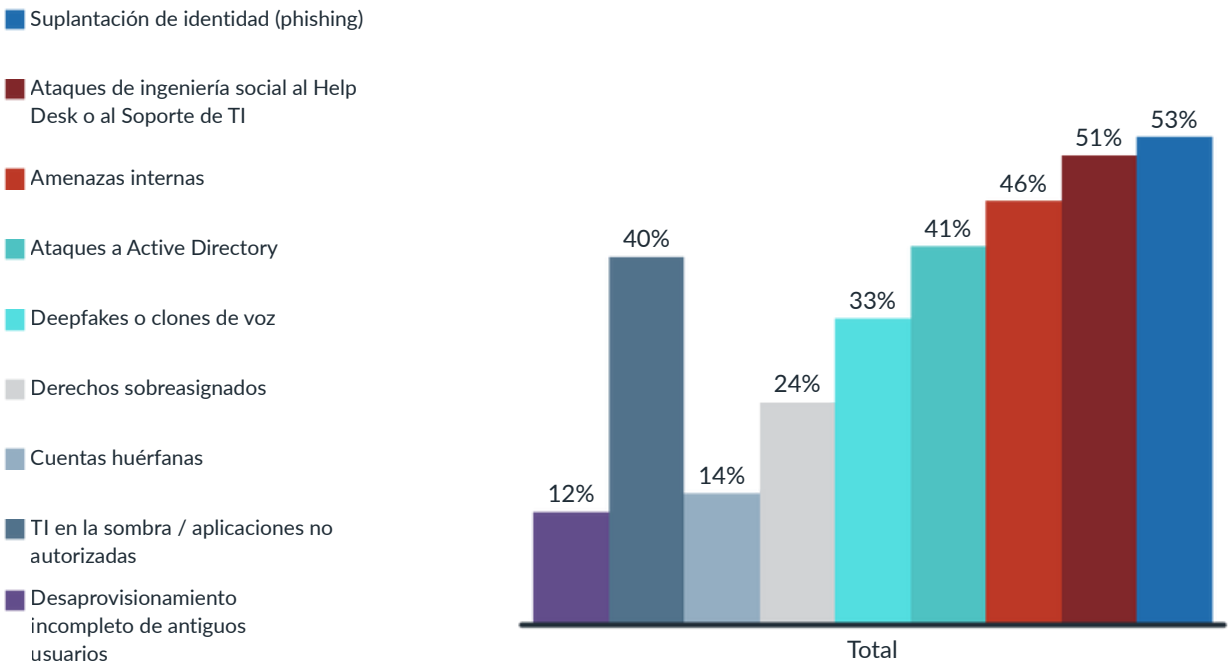
Tiempo promedio que tardan las organizaciones para identificar y contener un ataque originado por phishing

$4.8 Millón

Coste promedio de las violaciones de datos originados por phishing

Informe de IBM sobre el coste de una filtración de datos (2025)

Si bien el phishing es un riesgo cibernético perenne, los riesgos cibernéticos emergentes están ganando terreno rápidamente como riesgos importantes. El 51% de los encuestados dijo que los ataques de ingeniería social al Help Desk o al soporte de TI eran el riesgo más significativo para su organización.



Su Help Desk necesita ayuda

Dados los ataques a centros de soporte que han acaparado titulares en MGM Resorts, Ceasars Entertainment Group, Marks & Spencer, Co-op y House of Dior, existen buenas razones para priorizar este riesgo. Como han demostrado Scattered Spider y otros grupos cibercriminales, existe un riesgo significativo cuando los cibercriminales intentan eludir la autenticación multifactor (MFA) llamando a un centro de asistencia o servicio de TI haciéndose pasar por un usuario legítimo y solicitando que creen nuevas cuentas, suspendan la MFA o registren nuevos usuarios o dispositivos. De hecho, expertos en ciberseguridad clasificaron específicamente los ataques de ingeniería social a centros de asistencia de TI como el principal riesgo al que se enfrenta su organización.

Este riesgo se agrava por el hecho de que las organizaciones simplemente no están utilizando métodos más nuevos y resistentes al phishing para proteger las identidades de los usuarios.
La mayoría de las organizaciones utilizan métodos más antiguos para autenticar a los usuarios: el 58 % utiliza contraseñas, el 50 % utiliza contraseñas de un solo uso (OTP) y el 46 % utiliza secretos compartidos. En comparación, solo el 36 % indicó utilizar autenticación bidireccional, que permite que ambas partes se verifiquen mutuamente, y solo una cuarta parte (25 %) indicó utilizar soluciones basadas en riesgos para priorizar usuarios y casos de uso.

Métodos más antiguos para asegurar la identidad de los usuarios

58%
de las organizaciones usan contraseñas

50%
usa OTP

Métodos más nuevos para asegurar la identidad de los usuarios

36%
utiliza la garantía de identidad bidireccional

25%
utiliza soluciones basadas en riesgos

¿Quién llama?

Desde 2023, BlackCat, ALPHV, Scattered Spider y otros grupos cibercriminales han utilizado ingeniería social para manipular al personal de soporte técnico de TI de las organizaciones para lanzar ataques de bypass de MFA, lo que ha provocado daños y pérdidas importantes:

MGM Resorts:

145 millones de dólares

Caesars Entertainment:

15 millones de dólares

Marks & Spencer:

300 millones de libras

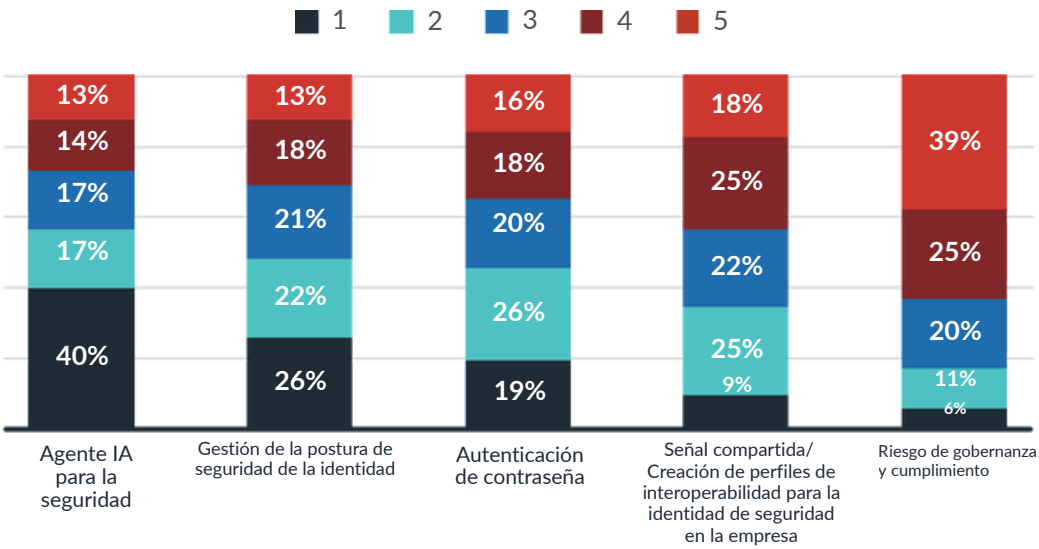
Un tercio (33%) de los usuarios afirmó que las nuevas técnicas, como los deepfakes o los clones de voz, representaban el mayor riesgo para su organización. Estas tácticas podrían resultar más eficaces sin métodos modernos para prevenir los ataques de omisión de MFA.

Algunos de los otros riesgos que los expertos más temen se agrupan en torno a las etapas del ciclo de vida de la identidad y la expansión de los derechos. Las amenazas internas (46%), las TI en la sombra y las aplicaciones no provisionadas (40%), y el exceso de derechos (24%) se destacan como riesgos prioritarios para los usuarios. Estos problemas pueden verse agravados por la visibilidad insuficiente del riesgo de identidad, los procesos manuales del ciclo de vida de la identidad y la mitigación retroactiva de riesgos.

Las capacidades de ciberseguridad que los usuarios priorizan

Los agentes IA para seguridad fue la opción preferida por los usuarios con un amplio margen, con un 40% de los encuestados considerándola su prioridad número uno. La gestión de la postura de seguridad de la identidad (ISPM), un nuevo marco de ciberseguridad que permite a las organizaciones gestionar riesgos, aplicar políticas y fortalecer el cumplimiento normativo en entornos cada vez más complejos, se posicionó como la segunda capacidad más crítica, siendo la preferida por el 26% de los encuestados.

Clasifique las siguientes capacidades de ciberseguridad del 1 al 5.



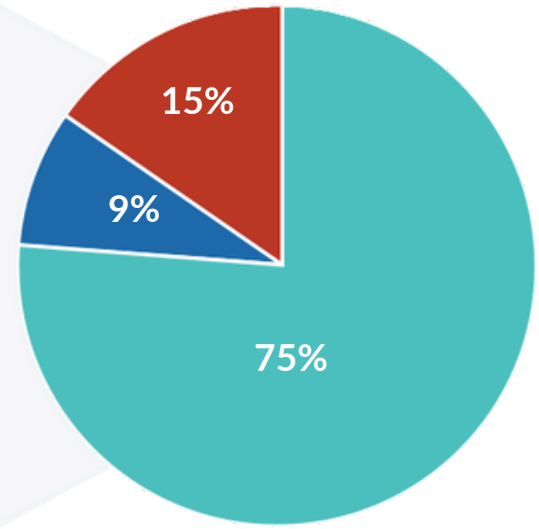
Entornos operativos

La mayoría de las organizaciones operan en entornos híbridos, utilizando una combinación de recursos en la nube y locales. Las empresas deben garantizar que todos los usuarios, dispositivos, permisos y entornos estén adecuadamente protegidos.

¿En cuál de los siguientes entornos brinda soporte a aplicaciones y usuarios?

75%

de las organizaciones operan de forma híbrida con un aumento de **5 puntos porcentuales**



Híbrido (nube y local) Solo en la nube Solo en las instalaciones

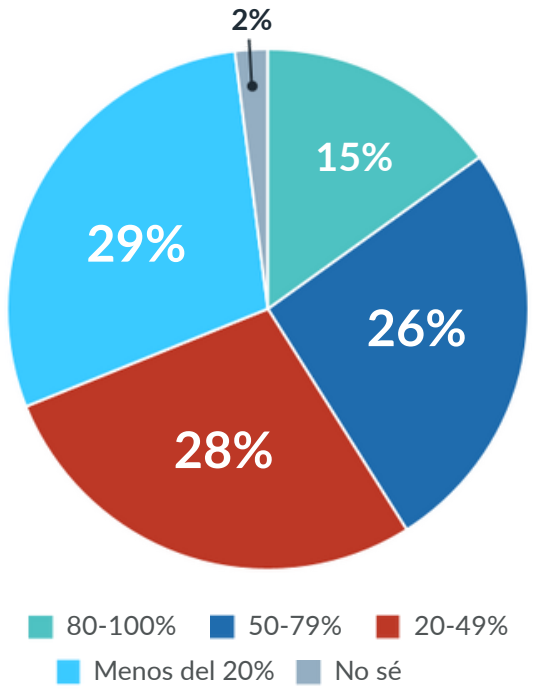
Las contraseñas y los riesgos de las contraseñas persisten

La mayoría de las organizaciones no utilizan la autenticación sin contraseña como método principal. Esto es una gran noticia para los ciberdelincuentes: año tras año, el uso de credenciales robadas es la principal causa de filtraciones de datos.

Los entornos complejos y los casos de uso mixto y los grupos de usuarios hacen que sea un desafío para las organizaciones implementar una seguridad integral sin contraseñas.

La persistencia de la autenticación basada en contraseñas se correlaciona con filtraciones de datos más frecuentes y costosas. Las organizaciones australianas informaron una de las tasas más bajas de adopción de sistemas sin contraseña por país, con un 50 % aún en la etapa inicial de adopción. Las organizaciones australianas también sufren la tasa más alta de filtraciones de datos relacionadas con la identidad por país (el 92 % de las organizaciones informaron de una brecha en los últimos tres años), las más graves consecuencias (el 47% dijo que la brecha causó daños importantes) y la mayor cantidad de pérdidas financieras (el 44% informó que una brecha les costó más de 10 millones de dólares).

¿Qué porcentaje de sus usuarios utiliza principalmente factores de forma sin contraseña para completar la autenticación?



Comparen estos resultados con los de Japón, donde se reportó el mayor número de casos de uso de la autenticación sin contraseña como método principal (el 37 % de las organizaciones afirmó usarla al menos el 80 % del tiempo). Japón también reporta una de las tasas más bajas de vulneraciones de datos relacionadas con la identidad (el 56 % de las organizaciones) y resultados menos graves.

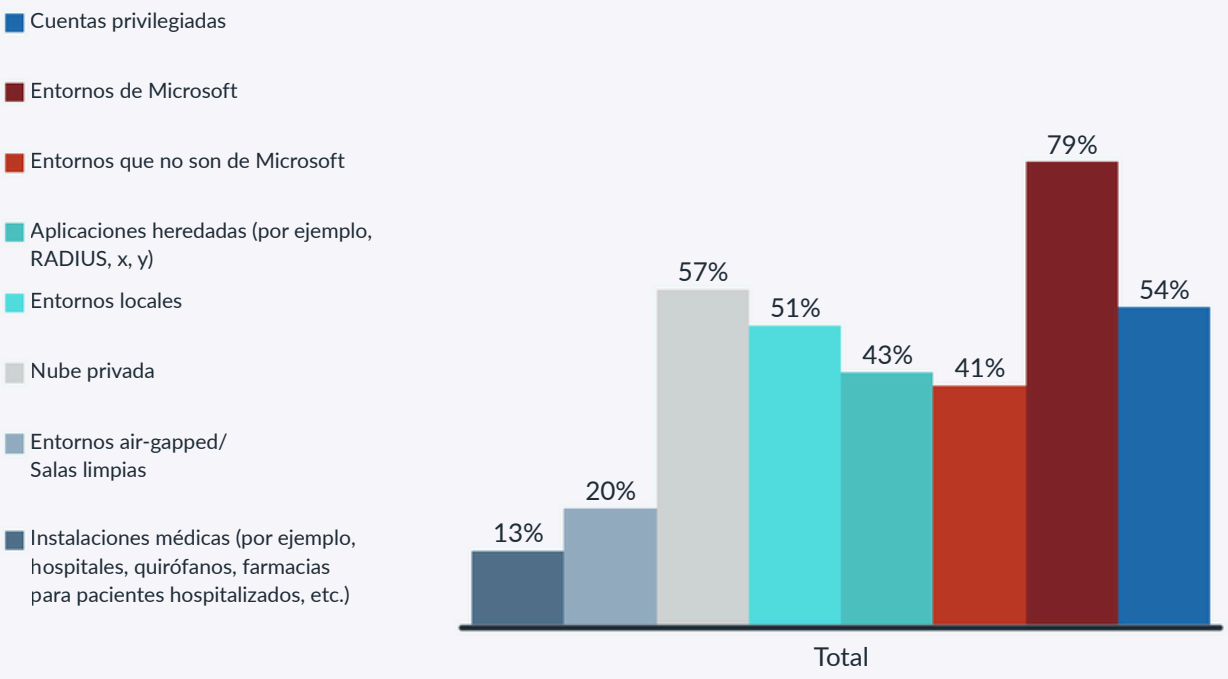
	Organizaciones australianas	Organizaciones japonesas
Clasificación en el uso general de sistemas sin contraseña, por país	#5	#1
Porcentaje de usuarios que utilizan sistemas sin contraseña como su principal forma de autenticación	10%	37%
Informaron de una infracción	92%	56%
Porcentaje de quienes informaron que la infracción causó un daño importante (5 de 5)	47%	44%
Porcentaje de infracciones que costaron más de $10 millones	24%	28%

> “Los entornos complejos, los casos de uso mixto y los grupos de usuarios hacen que sea un desafío para las organizaciones implementar una seguridad integral sin contraseñas”.

¿Qué está ralentizando el uso de la tecnología sin contraseñas?

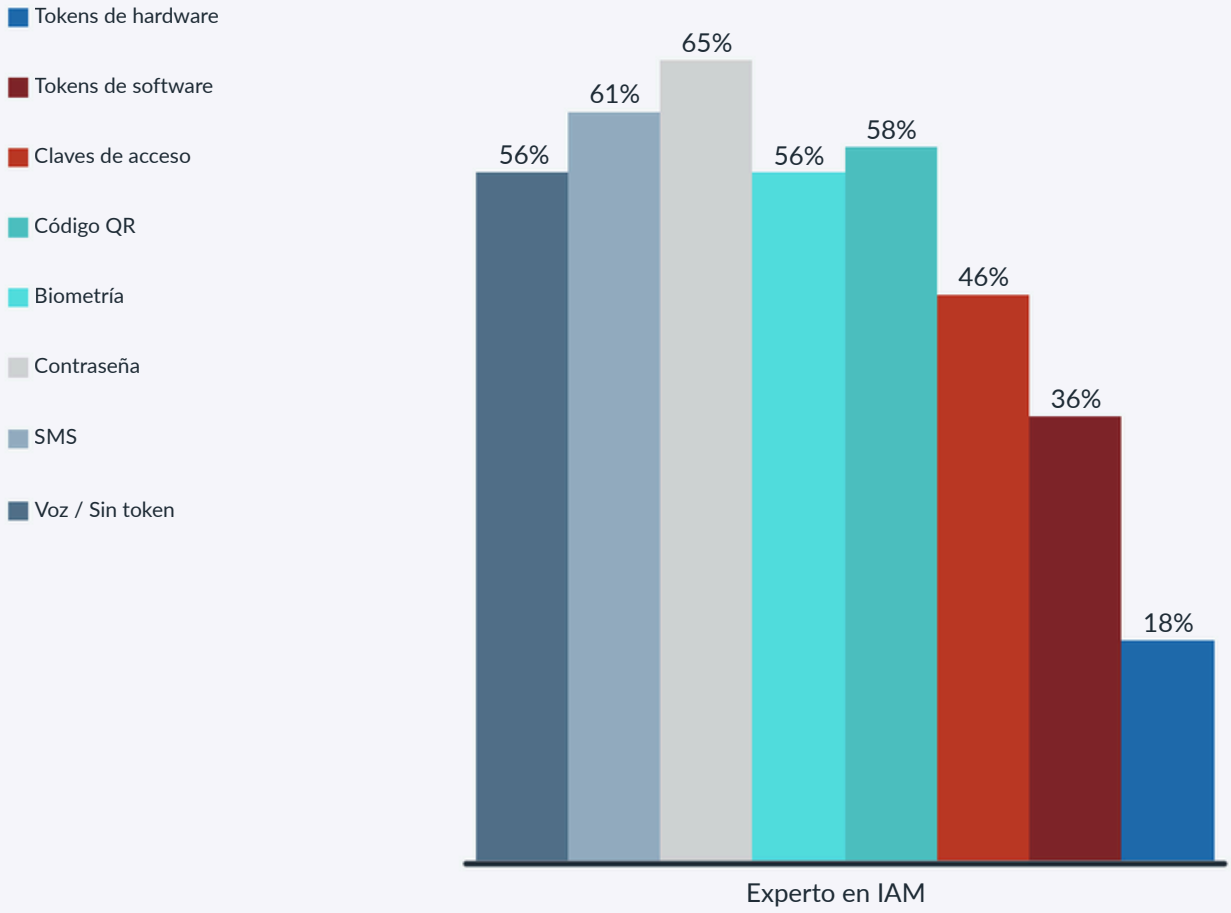
Al implementar la seguridad sin contraseña, la mayoría de las organizaciones deben considerar una amplia gama de usuarios y casos de uso. Creemos que esto representa un desafío importante para las organizaciones, ya que la seguridad sin contraseña aún está rezagada.

¿Cuáles de los siguientes entornos, grupos de usuarios o casos de uso admite su organización?



Debido a que la mayoría de las organizaciones operan en entornos híbridos y deben brindar soporte a diversos usuarios y casos de uso, los especialistas en identidad se están preparando para utilizar una amplia gama de factores de forma para brindar a cada usuario una autenticación sin contraseña.

¿Cuál de los siguientes factores de forma pretende utilizar para implementar soluciones sin contraseña?



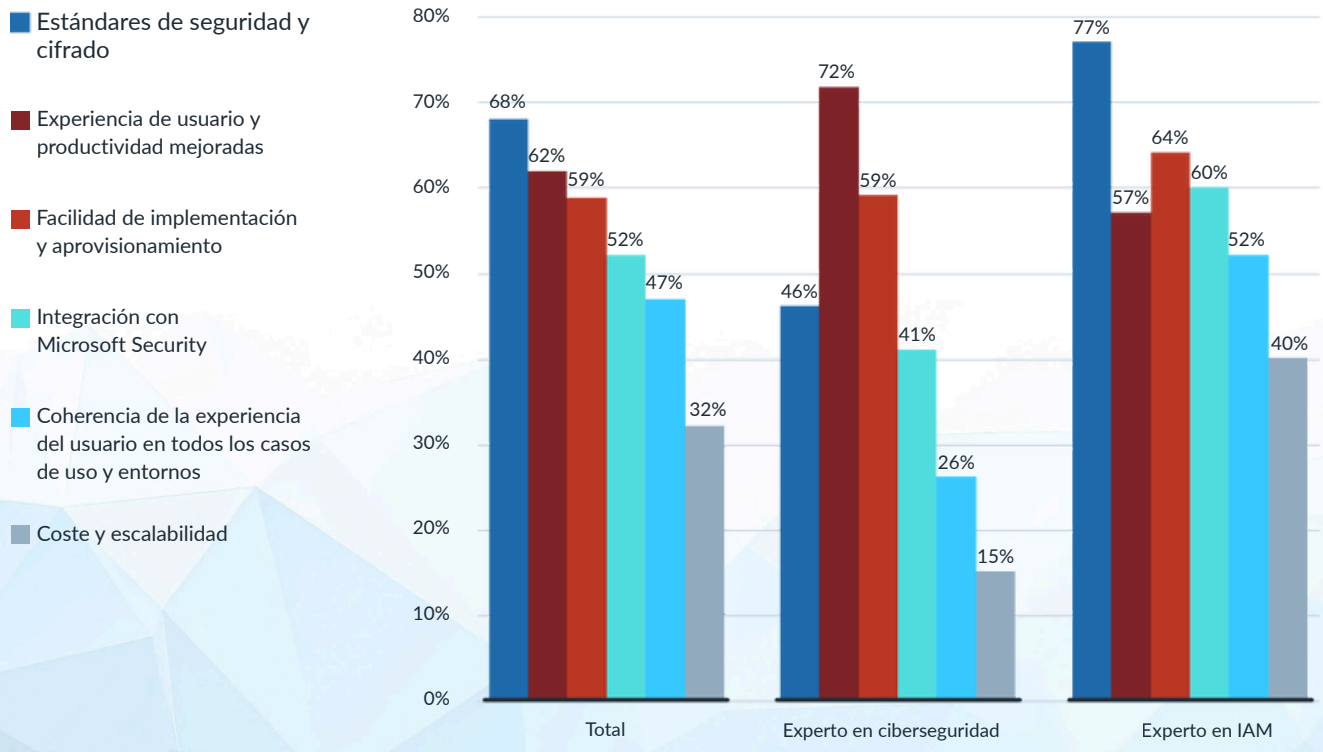
Experto en IAM

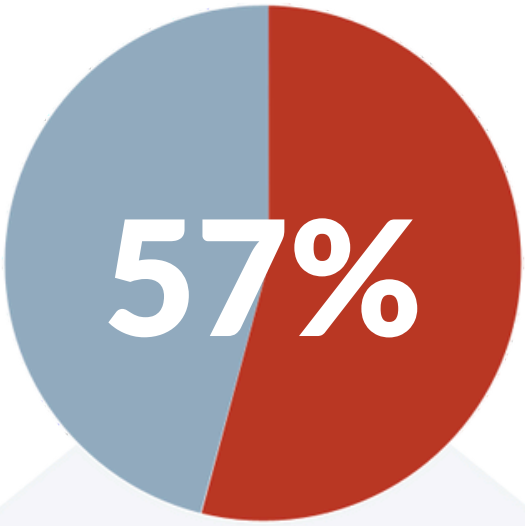
La lucha por la seguridad sin contraseñas

Casi todos los encuestados (el 90 %) afirmaron que algún desafío les impedía implementar soluciones sin contraseña. Sin embargo, estos usuarios no tienen un desafío específico que abordar. En cambio, hay tres: el 57 % afirmó que las preocupaciones de seguridad estaban ralentizando la implementación sin contraseña, el 56 % mencionó inquietudes sobre la experiencia del usuario y el 52 % indicó que la falta de compatibilidad completa con la plataforma (incluyendo aplicaciones antiguas y sistemas de terceros) era el principal desafío que les impedía implementar la implementación sin contraseña.

Todas estas son preocupaciones vitales que las organizaciones deben superar para implementar la seguridad sin contraseñas de forma eficaz. Curiosamente, las limitaciones prácticas son mucho menos problemáticas: solo el 47 % de los usuarios afirmó no tener el presupuesto para implementar la seguridad sin contraseñas.
No existe un único desafío claro que las organizaciones deban abordar. Para abordar las diferentes prioridades de los expertos en materia de seguridad sin contraseñas (y superar los desafíos que les impiden implementar este tipo de sistemas), las empresas deben encontrar un equilibrio entre los estándares de seguridad y cifrado, una mejor experiencia de usuario (UX) y la facilidad de uso.

¿Qué factores son los más importantes para usted a la hora de seleccionar una solución sin contraseña?





De las organizaciones no utilizan la opción sin contraseña como su medio principal de autenticación

Año nuevo, mismo problema

Año tras año, las contraseñas son una de las principales causas de violaciones de datos:

Informe de investigaciones sobre violaciones de datos de Verizon de 2025: el abuso de credenciales "sigue siendo el problema" "vector más común".

Informe de investigaciones sobre violaciones de datos de Verizon de 2024: "En los últimos 10 años, las credenciales robadas han aparecido en casi un tercio (31 %) de las violaciones".

Informe de investigaciones sobre filtraciones de datos de Verizon de 2023: «Las credenciales han ganado terreno en los últimos cinco años, ya que el uso de credenciales robadas se convirtió en el punto de entrada más popular para las filtraciones».

El Informe de investigaciones de violaciones de datos de Verizon de 2022 señaló que las malas prácticas de uso de contraseñas fueron "una de las principales causas de violaciones de datos" cada año durante los últimos quince años.

Monitoreo y gestión de riesgos de identidad

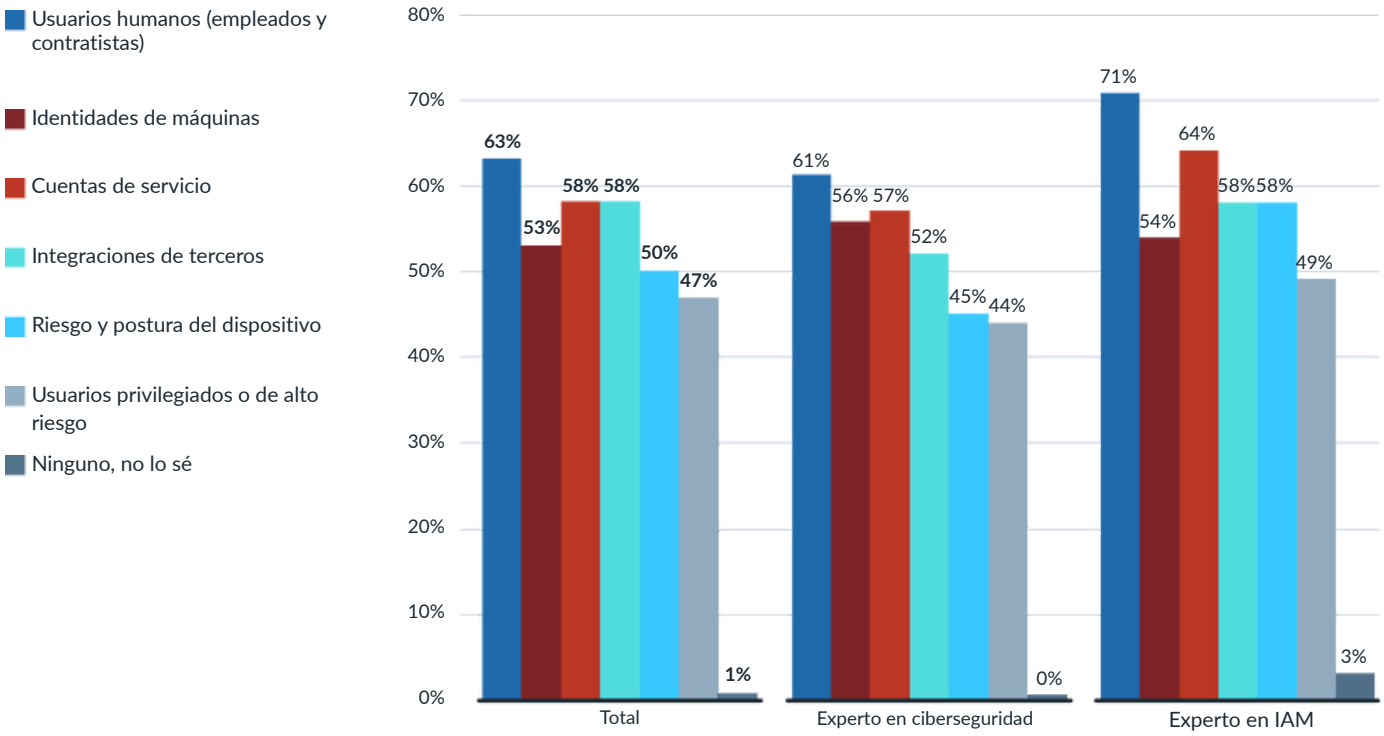
Las organizaciones muestran una alta tasa de monitoreo del riesgo de identidad en todos los usuarios y tipos. La mayoría de los encuestados afirma monitorear usuarios humanos, cuentas de máquinas, cuentas de servicio e integraciones de terceros, y la mitad afirma que también monitorea el riesgo y la postura de los dispositivos. Los expertos en IAM son más propensos a monitorear estas cuentas para detectar riesgos de identidad que sus colegas en ciberseguridad.

Es alentador que las organizaciones estén abordando la amplitud de su superficie de ataque de identidad.
Pero integrar toda esa información y usarla eficazmente será un desafío. Con miles de derechos por cuenta, existe una cantidad considerable de ruido que los equipos de seguridad deberán analizar para identificar riesgos y priorizar acciones.

Ese enorme conjunto de datos podría estar impulsando las prioridades de inversión en ciberseguridad de los encuestados: más de una cuarta parte (26 %) de los encuestados afirmó que la ISPM era su principal prioridad. La ISPM puede ayudar.
Las organizaciones evalúan su exposición al acceso y priorizan acciones para limitar los riesgos.

Un ejemplo de por qué las organizaciones necesitan ISPM para identificar la señal en el ruido y reducir el riesgo son las identidades de las máquinas. Las organizaciones que monitorean las identidades de las máquinas reportaron las vulneraciones más frecuentes, con el mayor impacto y las mayores pérdidas. Casi tres cuartas partes (72%) de las organizaciones que monitorean las identidades de las máquinas reportaron una vulneración relacionada con la identidad en el último año. Estas organizaciones también reportaron el mayor daño causado por estas vulneraciones, con un 34% que indicó que causaron daños significativos, y las pérdidas más catastróficas, con un 27% que reportó pérdidas de más de $10 millones.

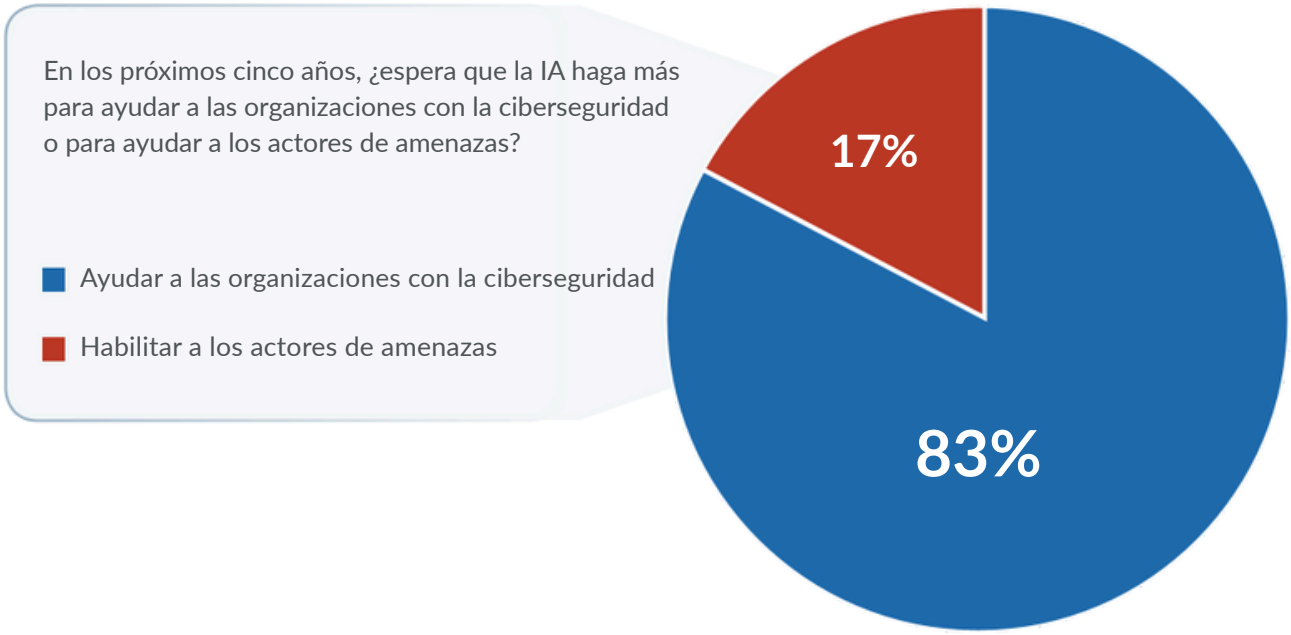
¿Qué áreas está monitoreando o calificando activamente en cuanto a riesgo de identidad?

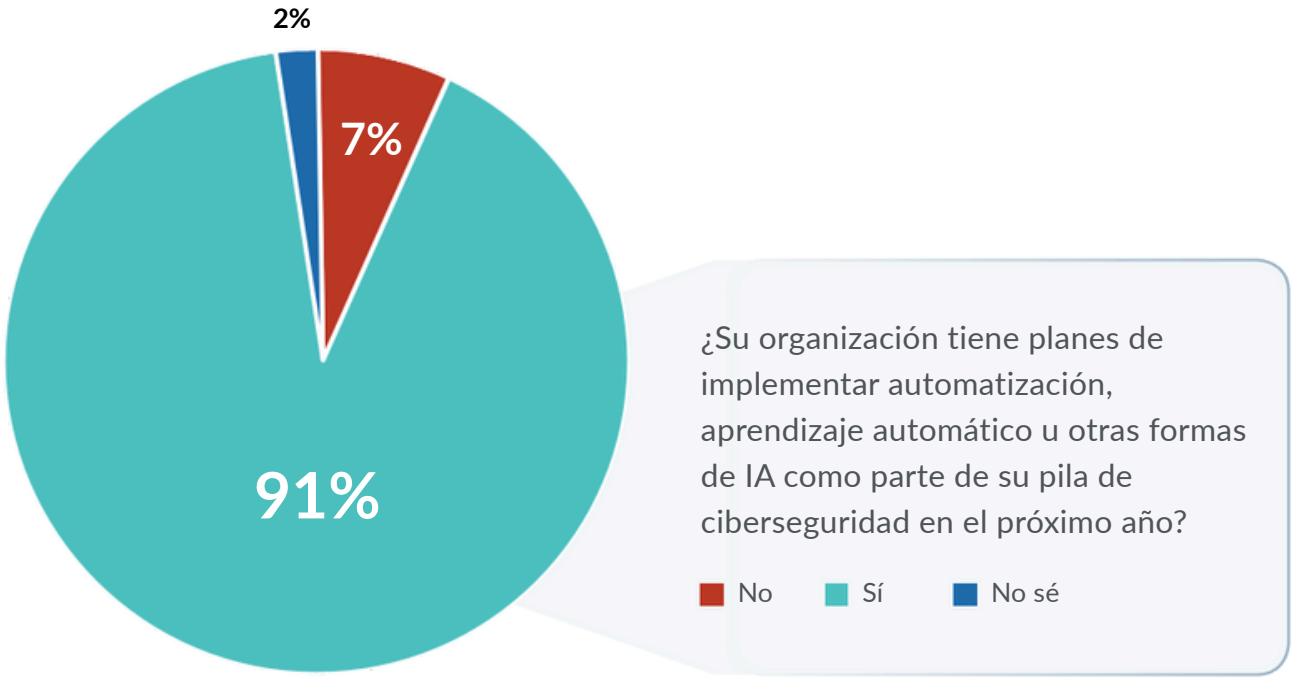


IA para la ciberseguridad

Existe una creciente aceptación de que la IA contribuirá más a la seguridad que a la ciberdelincuencia. El 83% de los usuarios afirma que la tecnología representa un activo más valioso para la defensa de las organizaciones que para los adversarios. Asimismo, el 91% de los encuestados afirmó que planea implementar la IA en su conjunto de tecnologías durante el próximo año, un aumento de 12 puntos porcentuales con respecto a la encuesta del año pasado.

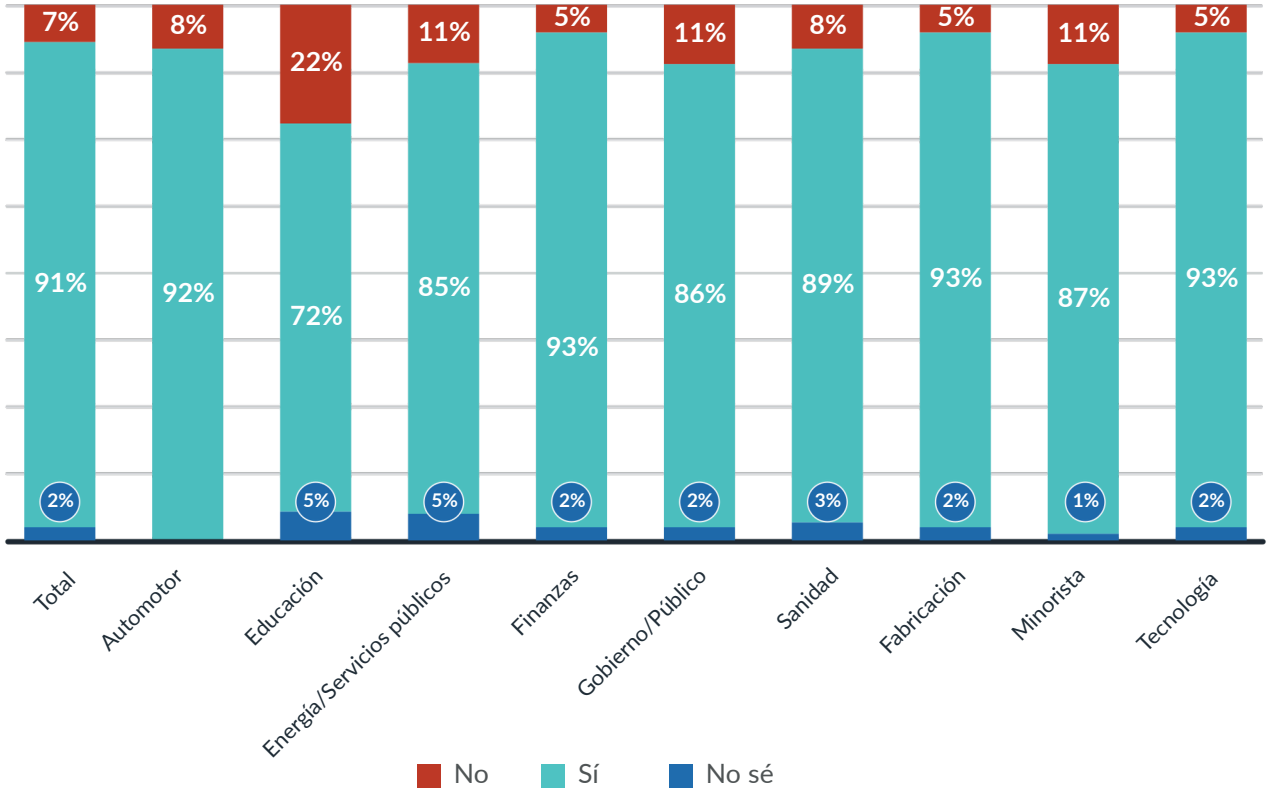
Estas respuestas se alinean con lo que los usuarios dijeron que sería su prioridad entre las capacidades de ciberseguridad: el 40% de los encuestados coloca los agentes IA para seguridad como su principal opción, la mayor de todas las características.





Por sector, casi todas las industrias reportan una alta probabilidad de implementar algún tipo de IA en su conjunto de tecnologías durante el próximo año. Finanzas (93%), manufactura (93%), tecnología (93%) y la industria automotriz (92%) reportaron altos niveles de integración de IA en su conjunto de tecnologías. Educación (72%) reporta los niveles más bajos de implementación de IA.

Por sector: ¿Su organización tiene planes para implementar automatización, aprendizaje automático u otras formas de IA como parte de su pila de ciberseguridad en el próximo año?



Metodología y muestra

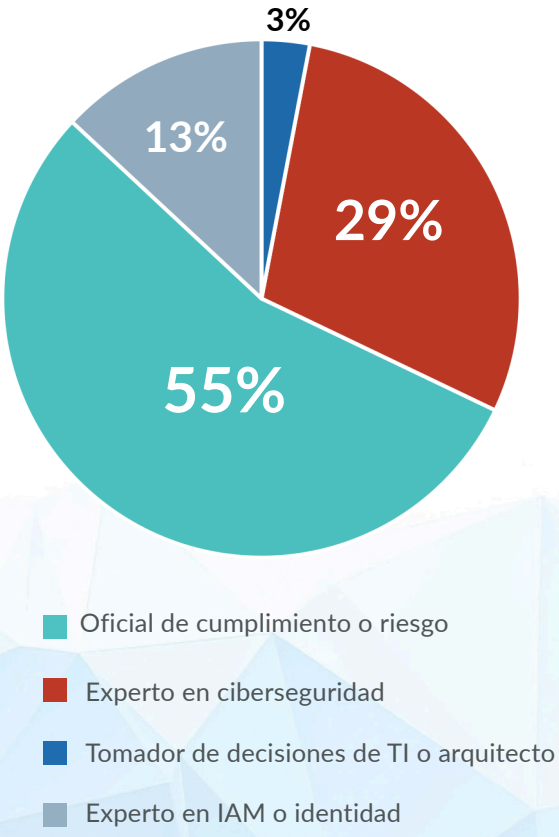
RSA compartió la encuesta RSA ID IQ 2026 del 20 de julio al 15 de agosto de 2025. En ella, se pidió a los usuarios que respondieran a 26 preguntas sobre sus prioridades de ciberseguridad, los riesgos que enfrentan sus organizaciones, la frecuencia y el impacto de las filtraciones de datos de identidad, y otros factores relacionados con el sector. Durante ese periodo, recibimos 2120 respuestas de Australia, Brasil, Canadá, Alemania, Japón, Reino Unido y Estados Unidos.

Se pidió a los encuestados que identificaran su función en su organización, el sector en el que trabajan. trabajaron y el tamaño de su organización.

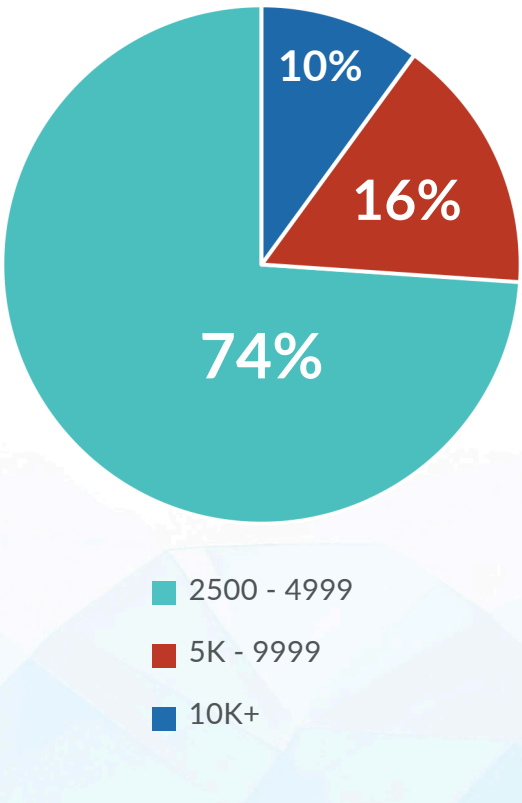
RSA revisó todas las respuestas, correlacionando algunas respuestas con otras para ver si había alguna relación entre ellas.

Datos demográficos de RSA ID IQ 2026

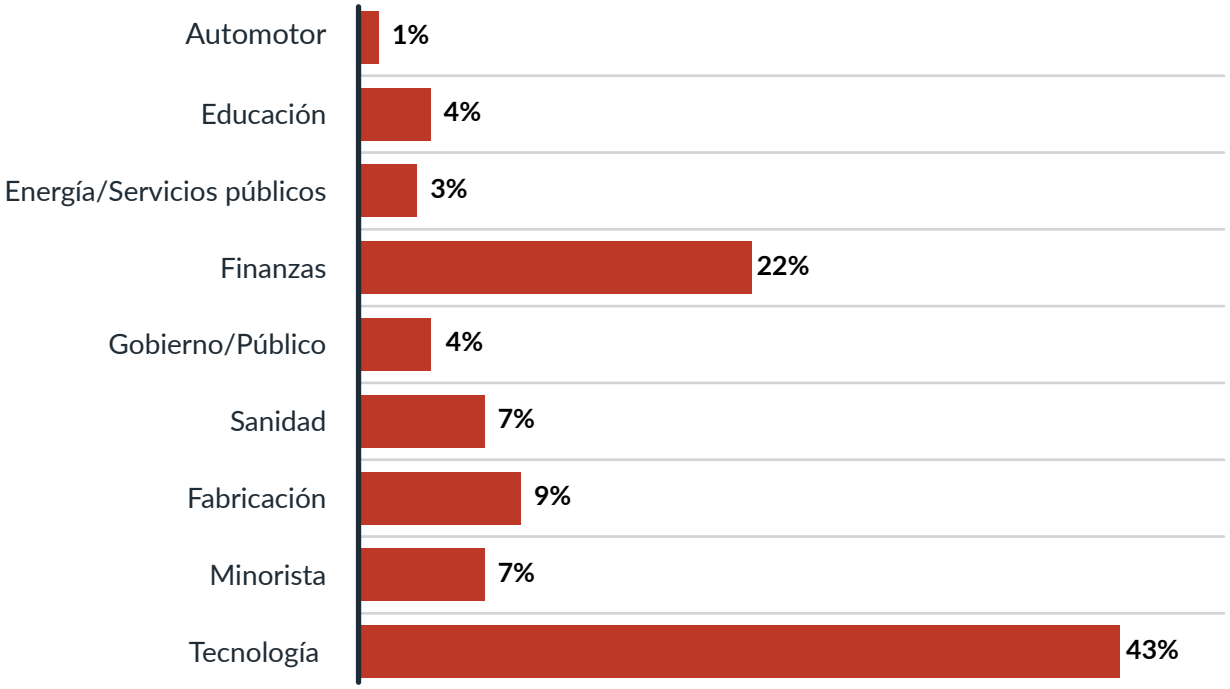
Rol en la organización



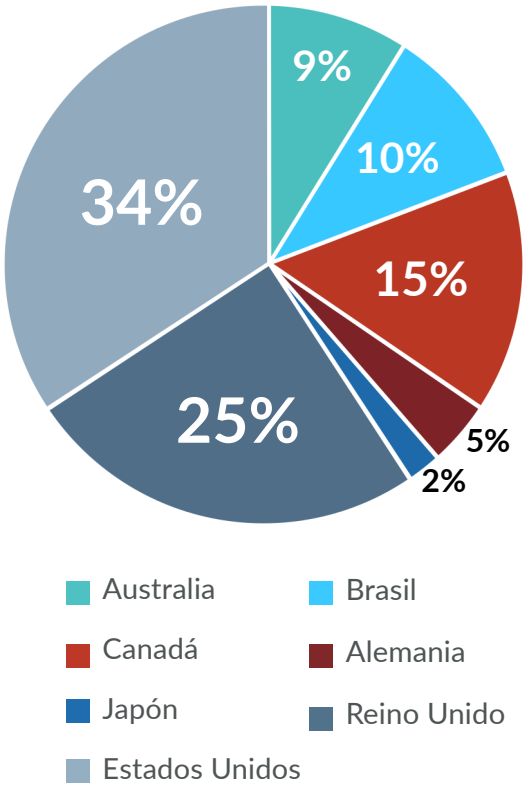
Tamaño de la organización



Sector


Automotor
1%
Educación
4%
Energía/Servicios públicos
3%
Finanzas
22%
Gobierno/Público
4%
Sanidad
7%
Fabricación
9%
Minorista
7%
Tecnología
43%

País


9%
10%
15%
5%
2%
25%
34%
Australia
Brasil
Canadá
Alemania
Japón
Reino Unido
Estados Unidos

De la información a la acción

El primer paso para solucionar cualquier problema es reconocerlo. El Informe RSA ID IQ de 2026 demuestra que la identidad es un problema importante para muchas organizaciones, lo que provoca filtraciones de datos de alto impacto y alto coste.

Las organizaciones deben priorizar las capacidades que pueden mantenerlas seguras, incluyendo:

- Autenticación sin contraseña que funciona para todos los usuarios, en todos los entornos y en todo momento
- ISPM para detectar riesgos y recomendar acciones
- Soporte entre entornos capaz de proteger a los usuarios en la nube, híbridos y locales
- Verificación de identidad bidireccional para defender el Help Desk de TI y a los usuarios de ataques de bypass de MFA e ingeniería social
- Inteligencia de identidad automatizada para evaluar dinámicamente el riesgo y automatizar las respuestas

Contacte con RSA para obtener una demostración de estas funciones. O descubra por qué las organizaciones más seguras del mundo están protegidas por RSA: **comience ahora su prueba gratuita de 45 días de RSA ID Plus.**

Acerca de RSA

RSA ofrece soluciones de ciberseguridad esenciales que protegen a las organizaciones más vulnerables del mundo. La Plataforma de Identidad Unificada de RSA proporciona una auténtica seguridad de identidad sin contraseñas, acceso basado en riesgos, inteligencia de identidad automatizada y una gobernanza integral de identidades en entornos de nube, híbridos y locales. Más de 9000 organizaciones de alta seguridad confían en RSA para gestionar más de 60 millones de identidades, detectar amenazas, proteger el acceso y garantizar el cumplimiento normativo.

Para obtener información adicional, visite nuestro sitio web para **comunicarse con el departamento de ventas**, **encontrar un socio** o **conocer más** sobre RSA.