INFORME

El estado de la seguridad de la identidad 2026

Reflexiones de 5000 responsables de TI y ciberseguridad de 17 países

SOPHOS

Introducción

La identidad constituye el perímetro de la ciberseguridad, y dicho perímetro cada vez es más amplio a medida que aumenta el acceso de los sistemas de IA a los datos empresariales a través del correo electrónico, los archivos, las apps SaaS y las identidades tanto humanas como no humanas. El resultado es una mayor exposición, puesto que ahora es más fácil acceder a la información confidencial y transmitirla.

Dado que las organizaciones siguen acelerando la adopción de la nube, el teletrabajo y la proliferación de apps y servicios que dependen de conexiones entre máquinas, el número de identidades digitales (tanto humanas como no humanas) se ha disparado. Cada credencial de usuario, clave de API, cuenta de servicio y token de OAuth representa un posible punto de entrada para los adversarios. Es por ello que la seguridad de la identidad se ha convertido en uno de los aspectos más críticos y complejos de la ciberdefensa en la actualidad.

Los atacantes son conscientes de este cambio. El robo de credenciales, las cuentas de servicio comprometidas y los ataques de ingeniería social dirigidos a los empleados ocupan ahora los primeros puestos entre los vectores de acceso inicial más comunes en las filtraciones de seguridad a nivel mundial. Los adversarios usan la IA y la automatización para actuar con mayor rapidez y extenderse por más sistemas. Las consecuencias van desde el robo de datos y la extorsión hasta incidentes de ransomware a gran escala que pueden paralizar las operaciones de una empresa durante días o semanas.

Para comprender la verdadera magnitud y el impacto de las amenazas relacionadas con la identidad, Sophos encargó una encuesta independiente a 5000 responsables de TI y ciberseguridad de 17 países sobre las experiencias y las repercusiones de este tipo de amenazas en 2025. Este informe presenta los resultados tras examinar la frecuencia de los ataques relacionados con la identidad, la capacidad de las organizaciones para detectarlos y detenerlos, las consecuencias derivadas, las causas raíz de las filtraciones que logran su objetivo, el coste económico y el estado de la higiene de la seguridad de la identidad.

Los resultados dibujan un panorama desolador: las amenazas a la identidad se han generalizado, tienen graves consecuencias y están estrechamente relacionadas con el ransomware. Las organizaciones que no invierten en seguridad de la identidad ponen en riesgo sus operaciones, sus finanzas y su reputación.

5000

responsables de TI y seguridad de 17 países participaron en una encuesta global desvinculada de cualquier proveedor

Conclusiones clave de un vistazo

- **El 71 % de las organizaciones sufrió al menos una filtración relacionada con la seguridad de la identidad** en los últimos 12 meses, y la media de ataques por organización afectada fue de tres.
- **El 14 % de las organizaciones afectadas por una filtración no fue capaz de detectar y detener** el ataque de identidad más grave antes de que se produjeran daños.
- **El coste medio de subsanar una filtración relacionada con la identidad fue de 1,64 millones USD**, mientras que la mediana se situó en 750 000 USD.
- **El robo de datos (49 %) y el ransomware (48 %) fueron las consecuencias más frecuentes** de los ataques de suplantación de identidad perpetrados con éxito.
- **Dos tercios de las víctimas de ransomware (el 67 %) indicaron que el incidente de ransomware fue también el ataque a la identidad más significativo que sufrieron**, lo que pone de manifiesto una clara relación entre los ataques relacionados con la identidad y el ransomware.
- **La gestión deficiente de las identidades no humanas (NHI) se citó en el 41 % de las filtraciones relacionadas con la identidad**, lo que la convierte en la segunda causa individual más frecuente, después del error humano (43 %).
- **Las organizaciones con un sistema deficiente de gestión de NHI tienen un 22 % más de probabilidades de sufrir robos financieros, un 24 % más de probabilidades de ser víctimas de extorsión** y registran unos costes totales de recuperación casi 150 000 USD superiores a la media.
- **Solo una de cada tres organizaciones (34 %) rota o audita periódicamente las cuentas de servicio y las identidades no humanas**, y solo el 11 % lo hace de forma sistemática, lo que genera brechas de seguridad que los atacantes explotan.
- **Solo el 24 % de las organizaciones supervisa de forma continua los intentos de inicio de sesión inusuales**, y más de la mitad lo hace cada tres meses o con menor frecuencia.
- **Los proveedores de energía, petróleo y gas y servicios públicos (80 %) y los gobiernos centrales o federales (78 %) registraron los índices más elevados de filtraciones de seguridad de la identidad**, mientras que los sectores de TI, tecnología y telecomunicaciones (63 %) y el sector sanitario (63 %) registraron los índices más bajos.
- **Las organizaciones pequeñas (entre 100 y 250 empleados) son un 72 % menos propensas a detectar un ataque de suplantación de identidad** en comparación con aquellas que cuentan con entre 1001 y 3000 empleados (el 19 % frente al 11 %).

Resultados detallados

Frecuencia de los ataques relacionados con la identidad

La encuesta revela que las filtraciones relacionadas con la identidad no son casos aislados, sino que constituyen la norma. Más de siete de cada diez organizaciones (70,9 %) han sufrido al menos una filtración relacionada con la identidad en los últimos 12 meses. Solo el 22,6 % afirmó categóricamente que no había sufrido ninguna filtración, mientras que el 6,4 % reconoció que podrían haberse producido filtraciones sin su conocimiento.

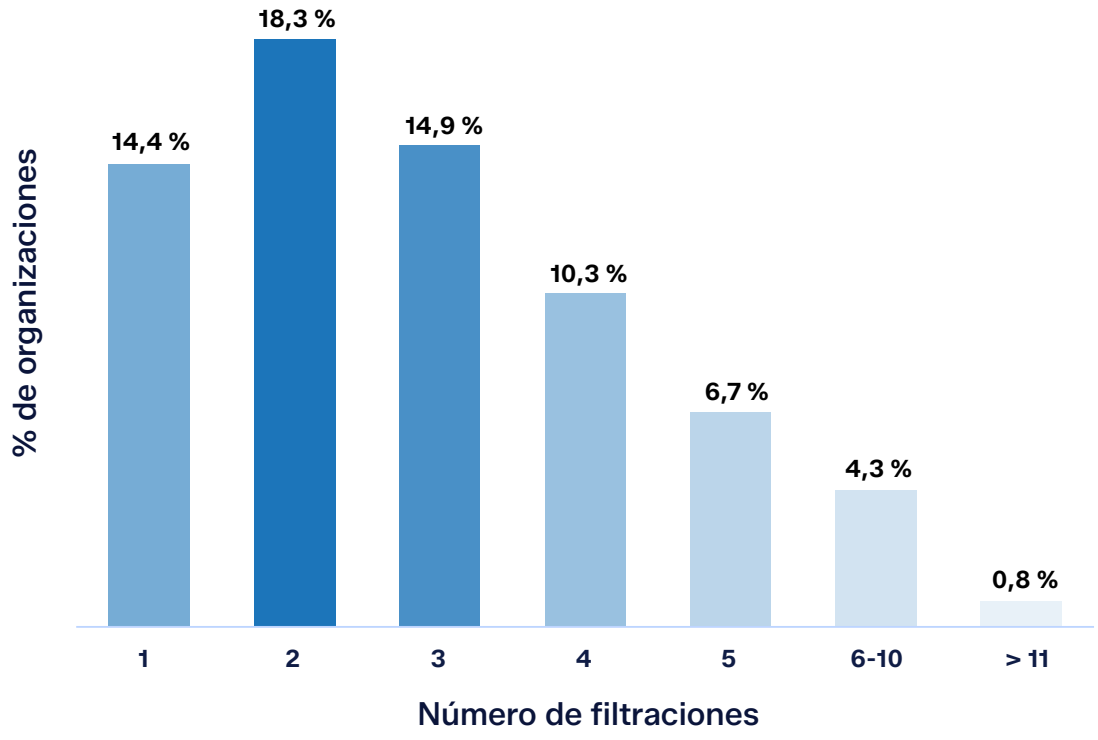
Entre las empresas afectadas, el número medio de incidentes fue de 3,1, lo que indica que los ataques de suplantación de identidad rara vez son casos aislados. El 5 % de los encuestados declaró haber sufrido seis o más filtraciones en el último año.

67 %

Porcentaje de todos los incidentes investigados por el equipo de Sophos de respuesta a incidentes y Sophos MDR en 2025 que se debieron a ataques relacionados con la identidad.

Datos de Sophos X-Ops

Distribución de la frecuencia de las filtraciones



¿Ha sufrido su organización alguna filtración relacionada con la seguridad de la identidad en los últimos 12 meses? En caso afirmativo, ¿cuántas? n = 5000.

Datos por países

Existen grandes diferencias geográficas en los índices de filtraciones. Suiza (88,7 %) registró el índice más alto, 18 puntos porcentuales por encima de la media mundial, seguida de México (83,3 %) e Italia (80,0 %). Alemania (62,6 %), Colombia (62,7 %) y Japón (64,7 %) fueron los países menos afectados, aunque incluso los índices más bajos superan el 60 %.

País	Índice de filtraciones	vs. índice global (70,9 %)
Suiza	88,7 %	+17,8 pp
México	83,3 %	+12,4 pp
Italia	80,0 %	+9,1 pp
Australia	79,7 %	+8,8 pp
India	76,8 %	+5,9 pp
Sudáfrica	75,0 %	+4,1 pp
Brasil	74,0 %	+3,1 pp
EAU	73,3 %	+2,4 pp
Singapur	72,0 %	+1,1 pp
España	70,0 %	-0,9 pp
Chile	66,7 %	-4,2 pp
EE. UU.	66,1 %	-4,8 pp
Francia	66,0 %	-4,9 pp
Reino Unido	65,3 %	-5,6 pp
Japón	64,7 %	-6,2 pp
Colombia	62,7 %	-8,2 pp
Alemania	62,6 %	-8,3 pp

¿Ha sufrido su organización alguna filtración relacionada con la seguridad de la identidad en los últimos 12 meses? En caso afirmativo, ¿cuántas? n = 5000.

Datos por sectores

Si se analizan los datos desde una perspectiva sectorial, los sectores de la energía, el petróleo y el gas, y los servicios públicos (80,3 %), así como los gobiernos centrales y federales (78,4 %), registraron los índices de filtración más elevados. Los sectores de TI, tecnología y telecomunicaciones (63,1 %) y el sector sanitario (63,4 %) fueron los menos afectados, lo que tal vez refleje una mayor madurez en la inversión en seguridad en dichos sectores.

Sector	Índice de filtraciones
Energía, petróleo/gas y servicios públicos	**80,3 %**
Gobierno central/federal	78,4 %
Construcción y propiedad	76,1 %
Fabricación y producción	73,6 %
Comercio minorista	72,0 %
Educación primaria y secundaria	71,1 %
Servicios financieros	71,0 %
Medios de comunicación, ocio y entretenimiento	70,9 %
Gobierno local/estatal	69,6 %
Distribución y transporte	67,6 %
Educación superior	65,9 %
Servicios empresariales y profesionales	64,5 %
Sanidad	63,4 %
TI, tecnología y telecomunicaciones	63,1 %

¿Ha sufrido su organización alguna filtración relacionada con la seguridad de la identidad en los últimos 12 meses? En caso afirmativo, ¿cuántas? n = 5000.

El cumplimiento normativo como indicador

Las organizaciones que creían que cumplir con los requisitos normativos era «muy difícil» presentaron un índice de filtraciones del 82,4 %, lo que supone 14 puntos porcentuales más que aquellas que consideraban que el cumplimiento era «bastante difícil» o «nada difícil» (68,3 %). Esto sugiere que las dificultades en materia de cumplimiento normativo son un indicador claro de deficiencias de seguridad más generales.

Conceptos básicos sobre la seguridad de la identidad

Cuatro tipos de identidades que las organizaciones deben gestionar

Todas las organizaciones conceden acceso a diferentes tipos de identidades. Cada una de ellas conlleva sus propios riesgos.

Categoría 1 – Identidades de la plantilla

Las personas dentro de la organización que necesitan acceder a los sistemas y a los datos para desempeñar su trabajo.

- Empleados
- Contratistas
- Administradores de TI y de seguridad de la información (personas cuyo puesto requiere un acceso con privilegios al sistema)
- Directivos (personas cuyo puesto las convierte en un objetivo especialmente valioso para un adversario)

Categoría 2 – Identidades externas

Las personas ajenas a la organización a las que se concede acceso, ya sea de forma temporal o permanente, para desempeñar una función o interacción específica y definida.

- Partners
- Proveedores
- Clientes

Categoría 3 – Identidades no humanas (NHI)

Software, sistemas y procesos automatizados a los que se concede acceso para realizar tareas sin la intervención de una persona.

- Cuentas de servicio (p. ej., copias de seguridad programadas)
- Claves de API (p. ej., integraciones de apps)
- Agentes de IA (p. ej., tareas autónomas)
- Dispositivos IoT (p. ej., sensores, cámaras)

Categoría 4 – Identidades con privilegios (riesgo máximo)

Cualquier identidad, humana o no, con permisos elevados que otorguen un acceso completo a sistemas y datos confidenciales.

- Superadministradores (es decir, personas con control total del sistema)
- Cuentas root (p. ej., acceso de administrador en la nube)
- Cuentas compartidas (p. ej., inicios de sesión de equipo)
- Acceso de emergencia (p. ej., cuentas de emergencia)

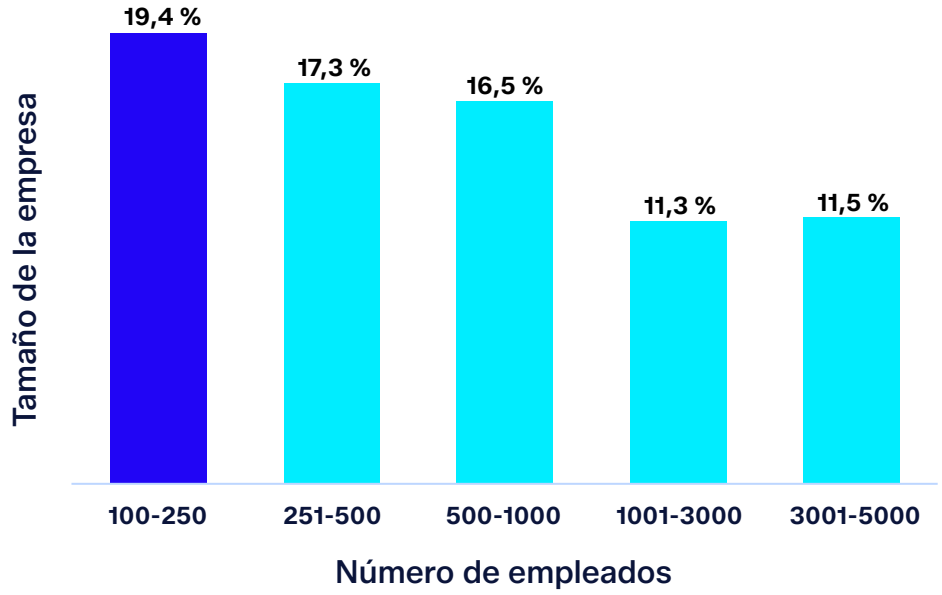
Cada identidad constituye un posible punto de acceso. Gestionar quién y qué tiene acceso a sus sistemas, y garantizar que dicho acceso sea adecuado y esté supervisado, es una de las medidas más importantes que una organización puede adoptar para garantizar su seguridad.

Capacidad para detectar y detener los ataques relacionados con la identidad

De los 3545 encuestados que sufrieron una filtración relacionada con la identidad en 2025, el 85,4 % fue capaz de detectar y detener su ataque más grave antes de que se produjeran daños. Si bien esto demuestra que la mayoría cuenta con cierta capacidad de detección, el 14,4 % que no pudo detener el ataque representa un riesgo extremo considerable y, tal y como revelan los resultados posteriores, las consecuencias para esas organizaciones son graves.

Índice de ataques no detectados por tamaño de la organización

Las organizaciones pequeñas tienen significativamente menos probabilidades de detectar los ataques. Entre las empresas más pequeñas encuestadas (100-250 empleados), el 19,4 % no pudo detener el ataque, lo que supone casi el doble del índice registrado en las organizaciones con 1001-3000 empleados (11,3 %). Esta diferencia pone de relieve los retos en materia de recursos y capacidades a los que se enfrentan las empresas más pequeñas.



Piense en el ataque relacionado con la identidad más grave que ha sufrido su organización en los últimos 12 meses: ¿logró detectarlo y detenerlo antes de que se produjeran daños? Base: la organización ha sufrido una filtración relacionada con la identidad. n = 3545.

Índice de ataques no detectados por país

Brasil (21,6 %) y Suiza (21,1 %) registraron los índices más elevados de fallos en la detección, mientras que el Reino Unido (7,1 %) y México (9,6 %) obtuvieron los mejores resultados. Cabe destacar que el elevado índice de filtraciones de Suiza, sumado al alto índice de fallos en la detección, lo convierte en un mercado especialmente vulnerable.

País	% de ataques no detectados
Brasil	**21,6 %**
Suiza	21,1 %
Japón	19,6 %
España	18,1 %
Chile	18,0 %
Singapur	17,6 %
Alemania	17,4 %
Francia	14,6 %
Italia	14,6 %
Australia	13,8 %
Colombia	13,8 %
EE. UU.	12,8 %
EAU	11,8 %
India	11,2 %
Sudáfrica	10,7 %
México	9,8 %
Reino Unido	7,1 %

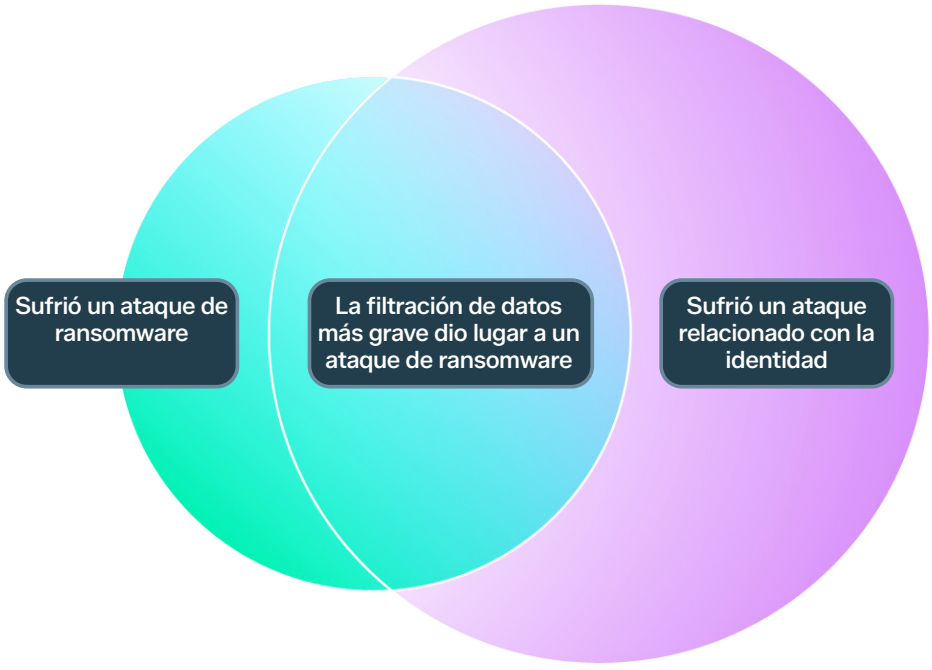
Piense en el ataque relacionado con la identidad más grave que ha sufrido su organización en los últimos 12 meses: ¿logró detectarlo y detenerlo antes de que se produjeran daños? Base: la organización ha sufrido una filtración relacionada con la identidad. n = 3545.

Índice de ataques no detectados por sector

El sector de los medios de comunicación, el ocio y el entretenimiento (22,4 %) registró el índice más alto de fallos en la detección, seguido del sector de la fabricación (18,4 %) y el de los servicios financieros (17,9 %). El sector sanitario (8,1 %) fue el que mejor detectó las amenazas, lo que posiblemente refleje la presión normativa para invertir en la supervisión de las amenazas.

La relación entre los ataques a la identidad y el ransomware

Una de las conclusiones más llamativas de este estudio es la relación directa que existe entre los ataques dirigidos a la identidad y el ransomware. Entre las organizaciones que sufrieron un ataque de ransomware en 2025, dos tercios (66,5 %) confirmaron que dicho incidente coincidió con su ataque más significativo a la identidad. Aunque no todos los ataques dieron lugar al cifrado de datos, esto confirma que el robo de identidad es uno de los principales mecanismos de distribución del ransomware.



En el último año, ¿se ha visto afectada su organización por el ransomware? (n=5000). ¿Ha sufrido su organización alguna filtración relacionada con la seguridad de la identidad en los últimos 12 meses? En caso afirmativo, ¿cuántas? (n = 5000) [Si la respuesta es afirmativa a ambas preguntas] ¿Fue ese incidente de ransomware el mismo que su ataque más grave relacionado con la identidad?

Relación entre el ransomware y los ataques a la identidad por tamaño de la organización

La relación entre los ataques relacionados con la identidad y el ransomware es más marcada en las organizaciones con entre 1001 y 3000 empleados (71,6 %) y menos marcada en aquellas con entre 100 y 250 empleados (62,4 %). Esta variación puede deberse a las diferencias en la complejidad de la infraestructura organizativa, los niveles de visibilidad o la capacidad para establecer una relación entre el vector de ataque y el resultado del ataque en los distintos segmentos.

Tamaño de la organización	Ransomware = Ataque relacionado con la identidad
100-250 empleados	62,4 %
251-500 empleados	68,2 %
501-1000 empleados	62,5 %
1001-3000 empleados	**71,6 %**
3001-5000 empleados	64,6 %

En el último año, ¿se ha visto afectada su organización por el ransomware? (n=5000). ¿Ha sufrido su organización alguna filtración relacionada con la seguridad de la identidad en los últimos 12 meses? En caso afirmativo, ¿cuántas? (n = 5000) [Si la respuesta es afirmativa a ambas preguntas] ¿Fue ese incidente de ransomware el mismo que su ataque más grave relacionado con la identidad?

Datos por sectores

La educación superior (76,8 %) y la distribución y el transporte (75,0 %) registraron la relación más estrecha entre el ransomware y los ataques relacionados con la identidad, mientras que los servicios financieros (57,6 %) y el sector de las tecnologías de la información, la tecnología y las telecomunicaciones (61,1 %) se situaron en niveles más bajos (aunque aún muy por encima del umbral de la mayoría).

Consecuencias de las filtraciones relacionadas con la identidad no detectadas

En el caso de las 510 organizaciones que no lograron detener su ataque más significativo relacionado con la identidad, las repercusiones fueron graves y se manifestaron de múltiples formas. De media, las víctimas señalaron dos consecuencias a raíz del incidente.

Consecuencia	% de organizaciones afectadas
Robo de datos: los atacantes sustrajeron datos confidenciales	**48,8 %**
Ransomware: se usaron credenciales robadas para ejecutar el ataque de ransomware	48,4 %
Extorsión: los atacantes exigieron dinero mediante amenazas	43,9 %
Sabotaje: los atacantes utilizaron credenciales para causar daños a la organización	30,0 %
Robo financiero: desviación de pagos	28,0 %
Robo financiero: sustracción de dinero de cuentas	25,5 %
Resumen: robo financiero (en cualquiera de sus formas)	**46,7 %**

¿Qué consecuencias tuvo para su organización esta filtración relacionada con la identidad? Base: la organización no pudo detener la filtración. n=510.

Casi la mitad de las organizaciones afectadas sufrieron el robo de datos (48,8 %) y una proporción casi idéntica fue víctima de ransomware (48,4 %). Casi la mitad (46,7 %) sufrió algún tipo de robo financiero directo (desvío de pagos, sustracción de fondos o ambos). Si a esto le sumamos la extorsión (43,9 %), estos resultados ponen de manifiesto que los ataques relacionados con la identidad que pasan desapercibidos casi siempre tienen consecuencias de gran repercusión.

Por qué las organizaciones sufren ataques

Comprender por qué prosperan los ataques es fundamental para prevenirlos. La encuesta ha revelado una combinación de fallos humanos, de procesos y técnicos que provoca que las organizaciones sufran ataques relacionados con la identidad. Asimismo, pone de manifiesto que rara vez existe una única causa raíz, ya que los encuestados señalaron, de media, dos factores causantes del incidente.

Causa raíz	% de organizaciones afectadas
Error humano: se engaña a un empleado para que dé sus credenciales	**42,7 %**
Gestión deficiente de las identidades no humanas (p. ej., claves de API almacenadas en el código, credenciales estáticas, cuentas de servicio huérfanas que anteriormente conectaban apps con los sistemas, etc.)	40,6 %
Gestión deficiente de las identidades humanas de los empleados	38,6 %
Falta de visibilidad sobre los accesos y permisos concedidos a aplicaciones externas	35,7 %
Gestión deficiente de las identidades humanas de los proveedores y contratistas	31,4 %
Falta de control sobre el acceso y los permisos concedidos a aplicaciones externas	30,8 %
Usuario interno malintencionado: un empleado propició intencionadamente el ataque	26,7 %
Resumen: gestión deficiente de las identidades humanas (en cualquiera de sus formas)	**60,2 %**
Resumen: problemas con el acceso y los permisos concedidos a apps externas (en cualquiera de sus formas)	**56,1 %**

¿Por qué sufrió su organización un ataque relacionado con la identidad? Seleccione todas las opciones aplicables. Base: la organización no pudo detener la filtración. n=510.

Según el 42,7 % de las víctimas, el error humano fue la principal causa individual de las filtraciones relacionadas con la identidad. En segundo lugar se sitúa la gestión deficiente de identidades no humanas (40,6 %), lo cual resulta especialmente preocupante, ya que abarca claves de API almacenadas en el código, credenciales estáticas y cuentas de servicio huérfanas, que son más difíciles de auditar y supervisar.

En más de una cuarta parte (26,7 %) de los ataques se detectó actividad maliciosa dentro de la propia organización, es decir, empleados que propiciaron deliberadamente el ataque, lo que pone de relieve la importancia de mantener controles internos rigurosos y una vigilancia constante.

En conjunto, la gestión deficiente de las identidades humanas (60,2 %) es la causa más frecuente por la que las organizaciones se ven afectadas por ataques relacionados con la identidad, mientras que los problemas relacionados con el acceso y los permisos concedidos a apps externas fueron un factor determinante en el 56,1 % de los incidentes.

59,5 %

En el 59,5 % de los casos de MDR analizados para el informe de Sophos sobre adversarios activos de 2025, la MFA, una tecnología que lleva décadas en uso, no estaba disponible en el sistema afectado.

Datos de Sophos X-Ops

Datos por tamaño de la organización

Las organizaciones grandes tienen más dificultades que las pequeñas en varios aspectos relacionados con la exposición de identidades, lo que probablemente se deba al mayor tamaño y complejidad de los entornos que deben supervisar y proteger.

Más de la mitad (55,6 %) de las empresas con entre 1001 y 3000 empleados señalaron el error humano como causa raíz, en comparación con solo el 29,0 % de las que cuentan con entre 251 y 500 empleados. Del mismo modo, el 68,6 % de las organizaciones con entre 3001 y 5000 empleados afirmaron que una gestión deficiente de las identidades humanas contribuyó a que sufrieran un ataque, en comparación con el 58,5 % de aquellas con entre 100 y 250 empleados.

Claves para entender las identidades no humanas

Una identidad no humana (NHI) es una credencial digital que se asigna a un programa informático, un sistema o un proceso automatizado para que pueda acceder a recursos sin intervenir un ser humano. En lugar de contraseñas, las NHI utilizan credenciales no humanas para demostrar su identidad, entre las que se incluyen:

- Claves de API que conectan apps
- Cuentas de servicio que ejecutan copias de seguridad
- Tokens de OAuth para integraciones SaaS
- Agentes de IA que acceden a bases de datos

Las credenciales de las NHI pueden ser robadas y utilizadas indebidamente de forma muy similar a los datos de inicio de sesión de las personas. Esto se vuelve aún más preocupante cuando las organizaciones no auditan periódicamente los permisos de las NHI, que con frecuencia son amplios y significativos.

Las NHI superan con creces el número de personas, y en algunas organizaciones esta proporción supera el 100:1. La IA agente es uno de los principales factores que han impulsado este aumento de la proporción en los últimos años.

96 %

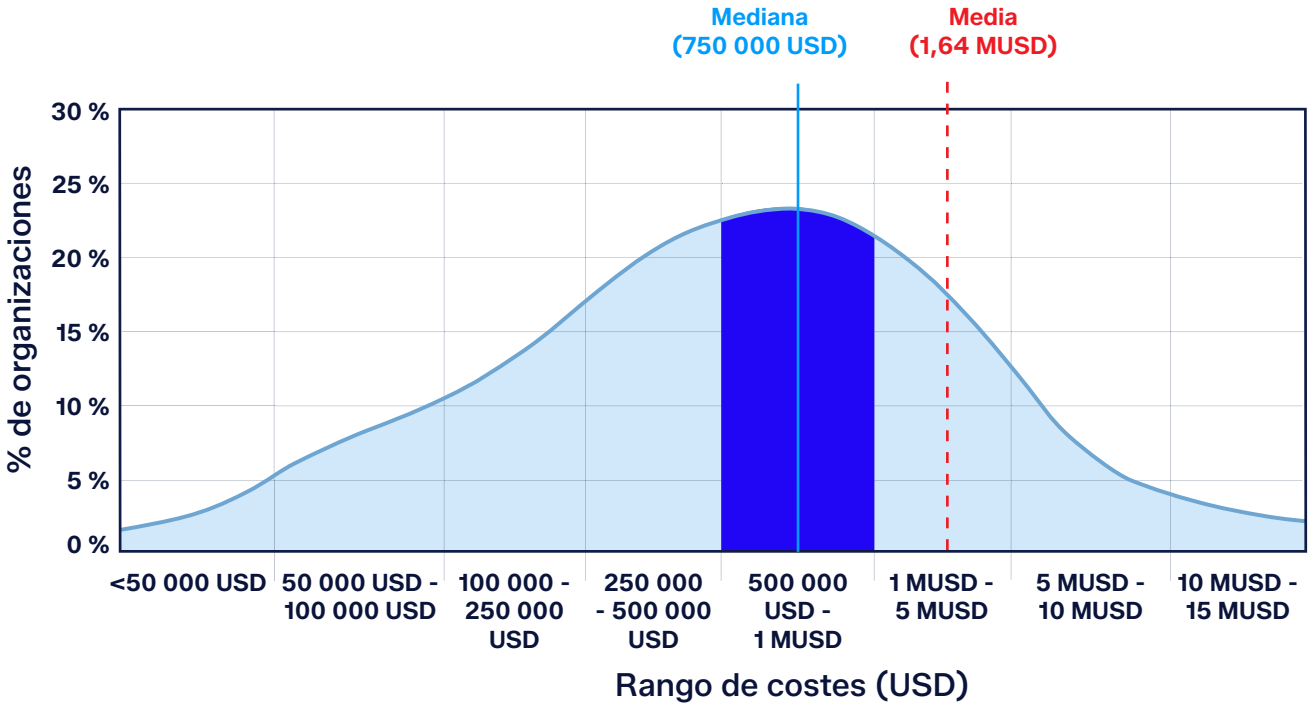
Porcentaje de entornos de clientes de Sophos ITDR que cuentan con apps de varios inquilinos. Auditar, o incluso simplemente enumerar, las NHI implicadas en esas relaciones puede resultar complicado.

Datos de Sophos X-Ops

El coste económico de las filtraciones relacionadas con la identidad

Las organizaciones que sufrieron una filtración relacionada con la identidad incurrieron en importantes costes de remediación. El coste medio global de la recuperación ascendió a 1 637 363 USD y, la mediana, a 750 000 USD. El 73 % de las organizaciones afectadas estimó unos costes de 250 000 USD o más, y casi una cuarta parte (23,7 %) registró costes comprendidos entre 500 000 y 1 millón USD.

Distribución de costes



¿Cuál cree que será el coste total que supondrá para su organización la subsanación de la filtración relacionada con la identidad? Base: la organización no pudo detener la filtración. n=510.

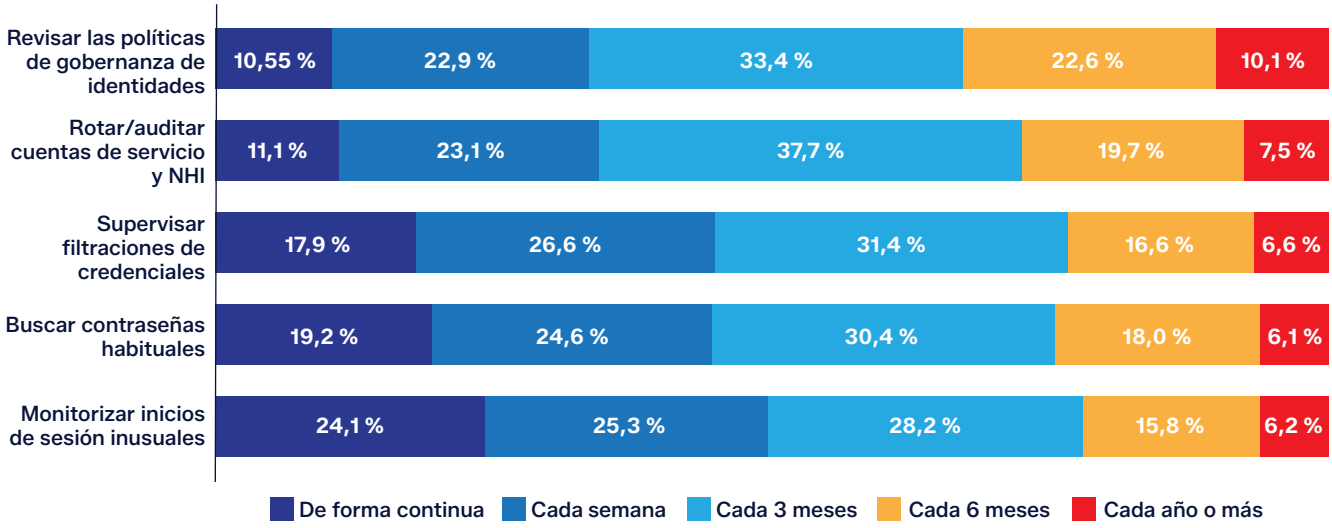
Coste según el tamaño de la organización

Tamaño de la organización	Coste (media)	Coste (mediana)
100-250 empleados	1 125 562 MUSD	375 000 USD
251-500 empleados	1 978 043 MUSD	750 000 USD
501-1000 empleados	1 009 205 MUSD	375 000 USD
1001-3000 empleados	1 907 594 MUSD	750 000 USD
3001-5000 empleados	2 452 929 MUSD	750 000 USD

¿Cuál cree que será el coste total que supondrá para su organización la subsanación de la filtración relacionada con la identidad? Base: la organización no pudo detener la filtración. n=510.

Higiene de la seguridad de la identidad

La encuesta analizó cinco actividades básicas en materia de gestión de identidades y la frecuencia con la que las organizaciones las llevan a cabo. Los resultados revelan importantes discrepancias entre las prácticas recomendadas y la realidad, discrepancias que aumentan la vulnerabilidad ante los ataques a la identidad.



¿Con qué frecuencia lleva a cabo su organización las siguientes actividades de gestión de identidades? n=5000

La supervisión de intentos de inicio de sesión inusuales es la actividad que se lleva a cabo con mayor frecuencia en tiempo real (24,1 % de forma continua); sin embargo, incluso en este caso, más de la mitad de las organizaciones (50,6 %) no lo comprueban más de una vez cada tres meses. En cuanto a la rotación o auditoría de identidades no humanas (una actividad fundamental, dado que se trata de la segunda causa raíz de las filtraciones), solo el 34,3 % lo hace semanalmente o con mayor frecuencia.

La revisión de las políticas de gobernanza de identidades es la actividad que se lleva a cabo con menor frecuencia de forma continua (10,5 %); un tercio de las organizaciones (33,3 %) revisa las políticas no más de una vez al trimestre y el 22,6 % lo hace solo cada seis meses. Dado que las amenazas relacionadas con la identidad evolucionan rápidamente, las revisiones anuales, semestrales o incluso trimestrales dejan lagunas peligrosas.

La IA agente agrava el problema de las NHI

La IA agente ha complicado exponencialmente el reto que supone la gestión de las NHI: más identidades, creadas más rápidamente, con un acceso más amplio y una supervisión humana mucho menor. Entre los principales retos que plantean las NHI se encuentran:

- **Los agentes de IA multiplican automáticamente las NHI**
  Cada agente de IA necesita su propia identidad y credenciales. Cada agente de IA necesita su propia identidad y credenciales. Y lo que es crucial: los agentes pueden crear de forma autónoma nuevos agentes para completar subtareas, y cada uno de ellos genera más credenciales sin intervención ni supervisión humana.
- **Los agentes de IA requieren un acceso amplio y permanente**
  Para realizar su trabajo, los agentes de IA necesitan acceder a numerosos sistemas: calendarios, bases de datos, sistemas de gestión de relaciones con los clientes (CRM), almacenes de archivos y API. A diferencia de las cuentas humanas, estos derechos de acceso rara vez caducan y rara vez se someten a auditoría.
- **Los agentes de IA son más difíciles de supervisar que las NHI tradicionales**
  Una cuenta de servicio de copia de seguridad ejecuta la misma tarea a la misma hora todas las noches, lo cual es fácil de supervisar. Los agentes de IA, por el contrario, toman decisiones autónomas, actúan de forma impredecible y funcionan 24/7, lo que hace muy difícil detectar cuándo se ha producido un problema.
- **Los agentes de IA de terceros conllevan riesgos desconocidos**
  Hay estudios que indican que, cuando las organizaciones utilizan las capacidades de agentes de IA de terceros, estas heredan todas las credenciales y permisos de acceso de dichos agentes, aunque con una visibilidad limitada sobre el nivel de seguridad con el que se han desarrollado o sobre a qué pueden acceder.
- **Las reglas de seguridad no se diseñaron pensando en los agentes de IA**
  La mayoría de los marcos de seguridad de la identidad se crearon para usuarios humanos y cuentas de máquina sencillas. No tienen en cuenta a los agentes que pueden crear, delegar y retirar sus propias credenciales de forma autónoma en mitad del flujo de trabajo, lo que deja importantes lagunas en materia de gobernanza.

La IA agente es una de las razones principales por las que la seguridad de las NHI ha pasado a formar parte de las prioridades de los CISO.

Consecuencias de una gestión deficiente de las identidades no humanas

Como ya se ha señalado, la gestión deficiente de las identidades no humanas (NHI) fue la causa raíz del 40,6 % de los ataques fructíferos. Al analizar los datos con mayor detalle, se observa que las NHI vulneradas aumentan drásticamente las consecuencias económicas de la filtración.

En particular, las organizaciones con una gestión deficiente de las NHI son considerablemente más propensas al robo financiero (en el que los atacantes desvían pagos de las cuentas), con un 27,9 % por encima de la media, y a la extorsión (en la que los atacantes exigen dinero mediante amenazas), con un 24,4 % por encima de la media. Las únicas categorías en que las organizaciones con una gestión deficiente de las NHI obtuvieron resultados ligeramente mejores que la media fueron el robo de datos y el ransomware, aunque esas diferencias son mínimas.

Consecuencia	% del total de organizaciones afectadas por una filtración	% de organizaciones afectadas por una filtración con una gestión deficiente de las NHI	Variación porcentual en el caso de una gestión deficiente de las NHI
Robo de datos: los atacantes sustrajeron datos confidenciales	48,8 %	47,8 %	-2,1 %
Ransomware: se usaron credenciales robadas para ejecutar el ataque de ransomware	48,4 %	46,4 %	-4,1 %
Extorsión: los atacantes exigieron dinero mediante amenazas	43,9 %	**54,6 %**	**+24,4 %**
Sabotaje: los atacantes utilizaron credenciales para causar daños a la organización	30,0 %	33,8 %	+12,7 %
Robo financiero: desviación de pagos	28,0 %	**35,8 %**	**+27,9 %**
Robo financiero: sustracción de dinero de cuentas	25,5 %	29,9 %	+15,7 %
Resumen: robo financiero (en cualquiera de sus formas)	**46,7 %**	**57,0 %**	**+22 %**

¿Qué consecuencias tuvo para su organización esta filtración relacionada con la identidad? Base: la organización no pudo detener la filtración. n = 510 (todas las filtraciones), n = 207 (filtraciones que tenían que ver con NHI)

Dado el creciente impacto financiero que tienen las NHI poco seguras, no es de extrañar que las organizaciones con una gestión deficiente de las NHI registren unos costes totales de recuperación notablemente más elevados tras las filtraciones relacionadas con la identidad, con una factura media que supera en casi 150 000 USD la media.

Coste medio para recuperarse de las filtraciones relacionadas con la identidad

Existe una clara correlación entre una mala gestión de las NHI y la probabilidad de sufrir una filtración relacionada con las NHI. Si bien un tercio (34 %) de todas las organizaciones cambia o audita las cuentas de servicio y las NHI de forma continua o semanal, este porcentaje se reduce a una cuarta parte (24 %) entre aquellas cuya filtración se debió a la vulneración de las NHI.

Conclusión

Los resultados de esta encuesta no dejan lugar a la complacencia. En el último año, las filtraciones relacionadas con la identidad afectaron a más de siete de cada diez organizaciones, con una media de más de tres incidentes por empresa afectada. No estamos ante un riesgo puramente teórico ni un problema limitado a sectores o zonas geográficas concretos. Se trata de una amenaza universal y generalizada que afecta a organizaciones de cualquier tamaño, sector y región. Los datos muestran que los ataques relacionados con la identidad son la puerta de entrada por la que el ransomware, el robo de datos y la extorsión se cuelan en una organización: el 67 % de las víctimas de ransomware atribuyeron el incidente directamente a una vulneración de la identidad.

Cuando los ataques basados en la identidad logran su objetivo, el impacto es grave y abarca múltiples vertientes. Casi la mitad de las organizaciones afectadas sufrieron robos de datos o ataques de ransomware, y el coste medio de la remediación, que asciende a 1,64 millones USD, convierte cada incidente en un acontecimiento financiero muy significativo.

Las causas raíz apuntan a deficiencias sistémicas: el error humano (42,7 %), la gestión deficiente de las identidades no humanas (40,6 %) y la visibilidad insuficiente de los permisos de las aplicaciones de terceros (35,7 %) son problemas que pueden resolverse, pero solo con una inversión y una atención constantes. El hecho de que las organizaciones pequeñas tengan casi el doble de probabilidades de no detectar los ataques que las grandes pone de manifiesto una brecha en materia de ciberseguridad que exige la atención de la comunidad de seguridad.

Quizás lo más preocupante sea el estado de la higiene de la seguridad de la identidad. Solo alrededor de una cuarta parte de las organizaciones supervisa de forma continua la actividad inusual en los inicios de sesión, y menos de una de cada tres renueva periódicamente las credenciales de los sistemas automatizados, precisamente las vulnerabilidades que explotan los atacantes.

Las organizaciones deben reconocer que la seguridad de la identidad no es un proyecto puntual, sino una disciplina operativa continua. Aquellas que la traten como tal estarán en una posición mucho más favorable para defenderse de las amenazas que caracterizaron el año 2025 y que seguirán intensificándose en 2026 y en los años venideros.

Recomendaciones

Como ha puesto de manifiesto la encuesta, una sólida seguridad de la identidad es un elemento esencial de una estrategia eficaz de mitigación de ciberriesgos. Para reducir la exposición a los ataques relacionados con la identidad, las organizaciones deben procurar implantar una defensa multicapa tanto para las identidades humanas como para las no humanas. Comience por los pasos básicos y siga con los pasos recomendados como parte de un programa de mejora continua.

Pasos básicos

Identidades humanas

- Aplique la autenticación multifactor (MFA) a todas las cuentas de usuario.
- Utilice credenciales distintas para las operaciones con privilegios y sin privilegios.
- Implemente el bloqueo de cuentas y la protección contra ataques por fuerza bruta.
- Centralice la gestión de identidades mediante el inicio de sesión único (SSO).
- Compruebe que la formación en concienciación de los usuarios refleje las últimas técnicas de phishing y robo de credenciales.

Identidades no humanas

- Realice periódicamente un inventario y clasifique todas las identidades no humanas.
- Utilice credenciales de corta duración en lugar de claves de larga duración.

Identidades humanas y no humanas

- Establezca un acceso basado en el principio del mínimo privilegio.
- Proteja y gestione las credenciales de forma adecuada.
- Desactive o elimine sin demora las identidades inactivas.
- Aplique un proceso formal de baja para auditar y eliminar el acceso de los empleados a los recursos.
- Registre y supervise toda la actividad de autenticación, y conserve los registros durante al menos 30 días.

Pasos recomendados

Identidades humanas

- Aplique políticas de acceso condicional y basadas en el riesgo.
- Utilice claves de acceso (ya sean de hardware o de software) como método principal de autenticación.
- Federe las identidades utilizando protocolos de identidad ampliamente aceptados, como Security Assertion Markup Language (SAML) o el más reciente OpenID Connect (OIDC).

Identidades no humanas

- Utilice la federación de identidades de cargas de trabajo en lugar de secretos estáticos.
- Adopte una plataforma de gestión de secretos para NHI a escala.
- Habilite el análisis de secretos en las plataformas compatibles (GitHub, GitLab).

Identidades humanas y no humanas

- Implemente una solución de gestión de acceso con privilegios (PAM).
- Adopte un modelo de seguridad Zero Trust.
- Lleve a cabo revisiones periódicas de los accesos y la recertificación de permisos.
- Implemente capacidades de detección y respuesta a amenazas relacionadas con la identidad (ITDR).
- Segmente el acceso a la red en función de la identidad y del rol.
- Defina y pruebe uno o varios manuales de estrategias de respuesta a incidentes que aborden filtraciones relacionadas con la identidad, como las descritos en este informe.

Saber más

Lea nuestra Guía de prácticas recomendadas en materia de seguridad de la identidad.

Metodología

Esta encuesta fue realizada por Vanson Bourne por encargo de Sophos durante el primer trimestre de 2026. Se entrevistó a 5000 responsables de la toma de decisiones en materia de TI y ciberseguridad en 17 países: Estados Unidos, Brasil, Chile, Colombia, México, Reino Unido, Francia, Alemania, Italia, España, Suiza, Australia, India, Japón, Singapur, Sudáfrica y los Emiratos Árabes Unidos. Los encuestados procedían de organizaciones con entre 100 y 5000 empleados, repartidas por 15 sectores.

SOPHOS

Para analizar sus necesidades en materia de seguridad de la identidad y cómo Sophos puede ayudarle, visite nuestro sitio web o hable con un asesor.

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

2026-05-08 ES (TA) CRE-5312