

COHESITY

LA CAPA DE IDENTIDAD

ES EL PUNTO CERO DE LOS CIBERATAQUES



*Por qué los responsables de seguridad y TI
deben demostrar que pueden recuperar la
infraestructura de identidad*

INTRODUCCIÓN

Se suponía que la identidad empresarial debía simplificarle la vida. A finales de la década de 1960 y principios de la de 1970, las organizaciones comenzaron a centralizar el acceso digital, lo que les permitió contar con un único lugar desde el cual decidir quién podía acceder y a qué recursos podía hacerlo. Más adelante, el Protocolo ligero de acceso a directorios (Lightweight Directory Access Protocol, LDAP) y plataformas como Active Directory convirtieron esa idea en una única fuente de verdad para toda la red. Funcionó a la perfección.

Ese es justamente el problema.

Esa única fuente de verdad es ahora la vía de acceso más fácil. Los atacantes ya no necesitan irrumpir. Inician sesión con credenciales robadas y acceso legítimo, y van directamente a sus sistemas más críticos. Nada se activa. No suena ninguna alarma. Utilizan la misma puerta que usan sus empleados cada mañana, y eso plantea un problema completamente distinto al que la mayoría de los programas de seguridad fueron diseñados para resolver.

Durante años, construyó sus defensas alrededor de un muro: una barrera destinada a mantener a los intrusos fuera. Ese muro sigue en pie, pero los atacantes han dejado de escalarlo. **Comprometer su infraestructura de identidad es más fácil, más silencioso y más efectivo. Por eso, la identidad ha reemplazado al perímetro de red como el principal campo de batalla.** La mayoría de los entornos de seguridad nunca fueron diseñados para combatir en este terreno.

Las cifras son contundentes. En 2024, el 79 % de los ataques no involucraron malware: no había ningún virus que detectar, sino ingeniería social, credenciales robadas y herramientas de acceso remoto legítimas que lograron eludir los sistemas de detección. En 2025, esa cifra escaló hasta el 82 %, ya que los atacantes recurrieron aún más a credenciales válidas, flujos de identidad de confianza e integraciones de SaaS autorizadas para moverse entre dominios sin ser detectados (*Informe global de amenazas de CrowdStrike*). La tendencia apunta claramente en una sola dirección.

Este es el punto incómodo desde el que cualquier programa de seguridad realmente sólido debe empezar hoy. El sistema que ha creado para controlar el acceso a todo se ha convertido silenciosamente en la forma más fácil de acceder a todo. Esa no es una razón para entrar en pánico. Es una razón para proteger la identidad primero y poder demostrar que puede recuperarla, antes que nada.

Por qué la identidad empresarial está **siendo atacada**

Para un atacante, la identidad es el objetivo más valioso y fácil de comprometer dentro de una empresa, porque una sola credencial comprometida puede abrir la puerta a todo lo que hay detrás. La identidad no es solo otro vector. Es el único vector que un atacante moderno busca activamente.

Pero aquí está el problema: casi nada de lo que tiene implementado en su entorno de seguridad fue diseñado para detener este tipo de ataque. Los EDR, los firewalls y la segmentación de red están diseñados para detectar a alguien que irrumpe en sus sistemas, no para cuestionar a alguien que inició sesión con credenciales válidas. Para sus defensas, el atacante se ve exactamente igual que uno de sus empleados.

Y ese punto ciego se hace cada vez más grande. La mayoría de los entornos de Active Directory tienen décadas de antigüedad. Años de soluciones provisionales, cuentas olvidadas y configuraciones incorrectas que pasaron inadvertidas se han ido acumulando en segundo plano, donde nadie está mirando. Ese cúmulo no es solo deuda técnica. Es una ventana sin cerrar, y es precisamente lo que los atacantes buscan primero.

La identidad híbrida lo hace aún más difícil. La mayoría de las organizaciones ahora operan con una combinación de Active Directory local y proveedores de identidad en la nube como Entra ID y Okta, y cada conexión entre ellos amplía la superficie de ataque. Lo que es aún peor, una vulnerabilidad en Entra ID u Okta a menudo tiene su origen directamente en Active Directory, porque Active Directory suele ser la única fuente de verdad en la que confía todo lo demás. Si se quiebran los cimientos, toda la estructura se tambalea.

ACTIVE DIRECTORY ES EL NÚCLEO DE LA IDENTIDAD EMPRESARIAL

Active Directory ha gestionado la identidad empresarial durante más de 25 años y sigue presente en el 90 % de las organizaciones de todo el mundo. La mayoría de los proveedores de identidad en la nube están federados o sincronizados con él, lo que significa que, incluso a medida que adopta plataformas más nuevas, Active Directory sigue siendo la base que sustenta a todas.

De hecho:

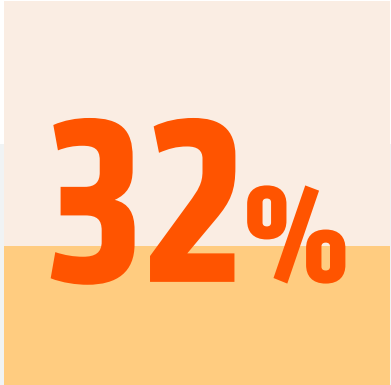
- Los atacantes logran vulnerar un controlador de dominio en más del 78 % de las intrusiones operadas por personas.
- En el 35 % de esos casos, el controlador de dominio se convierte en el punto desde el que el ransomware se propaga por todo el entorno.

Cuando llega un ataque, Active Directory suele ser lo único que se interpone entre su organización y la recuperación. Piense en lo que significa: si no puede iniciar sesión en su propia solución de copia de seguridad, no puede empezar a recuperar nada. Los atacantes lo entienden perfectamente, por lo que cada vez más atacan sus sistemas de copia de seguridad y su Active Directory al mismo tiempo. Si ambos quedan fuera de servicio ya no solo tendrá un mal día. Tendrá una situación de rehenes.

Y el reloj no da tregua. Una recuperación completa de un bosque de Active Directory puede tardar días o incluso semanas, y cada hora de inactividad puede costar a las organizaciones hasta 730 000 USD por hora ([*Forrester, The Total Economic Impact™ of Quest Recovery Manager for Active Directory Disaster Recovery Edition*](#)).

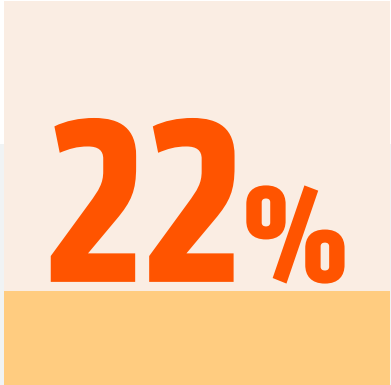
Las herramientas de copia de seguridad tradicionales no lo salvarán en este caso. Pueden copiar controladores de dominio individuales y archivos, pero no pueden orquestar los pasos precisos y ordenados necesarios para reconstruir todo un bosque de Active Directory. Hacer copias de seguridad de las piezas no es lo mismo que poder volver a ensamblarlas.

SUPPORTING DATA

A vertical bar chart with a light orange top half and a darker orange bottom half. The number '32%' is displayed in large orange font, with the percentage sign slightly smaller and to the right of the '2'.

Aumento del 32 % en los ataques basados en identidad durante el primer semestre de 2025. El 97 % fueron ataques de password spraying o fuerza bruta

(Microsoft Digital Defense Report 2025)

A vertical bar chart with a light orange top half and a darker orange bottom half. The number '22%' is displayed in large orange font, with the percentage sign slightly smaller and to the right of the '2'.

El 22 % de las brechas implicó el robo de credenciales en general; el 88 % de los ataques a aplicaciones web básicas implicó específicamente el robo de credenciales

(Verizon 2025 Data Breach Investigations Report)

A vertical bar chart with a light orange top half and a darker orange bottom half. The number '35%' is displayed in large orange font, with the percentage sign slightly smaller and to the right of the '5'.

El 35 % de los incidentes en la nube estuvieron relacionados con el uso indebido de cuentas válidas

(CrowdStrike 2025 Global Threat Report)

La identidad es la base de MVC y la confianza, hoy y en el futuro

Una Empresa mínimamente viable (Minimum Viable Company, MVC) es la versión más pequeña y austera de una organización que necesita existir para sobrevivir y mantener sus operaciones esenciales. Cuando las organizaciones sufren un incidente de ciberseguridad, no dejan de recuperarse porque sus copias de seguridad fallen. A menudo fracasan porque intentan recuperar todo a la vez o en el orden incorrecto.

La capa que la mayoría de las organizaciones pasan por alto se centra en la confianza y el control, y la identidad se encuentra en la intersección de ambos. Es la llave maestra de la empresa. Si no puede establecer una identidad de confianza, no puede restaurar nada más de forma segura.

La gestión de identidad y acceso (Identity and access management, IAM) es responsable de tres funciones principales:

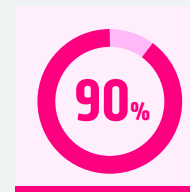
- **Gestión del ciclo de vida de la identidad:** Automatiza la incorporación de usuarios, la actualización de roles y la baja de accesos para que los permisos se mantengan actualizados a medida que las personas se incorporan, cambian de función o dejan la organización.
- **Autenticación:** Verifica que una persona sea quien dice ser, normalmente mediante autenticación multifactor (multifactor authentication, MFA) e inicio de sesión única (single sign-on, SSO).
- **Autorización:** Otorga a cada usuario autenticado el acceso específico que necesita para hacer su trabajo, al tiempo que restringe todo lo demás.

Al reunir esas tres funciones, Active Directory, Entra ID y Okta dejan de ser una simple infraestructura técnica y se convierten en la columna vertebral operativa de su empresa. Autentican a cada empleado, cada aplicación y cada transacción. Esto conduce a una verdad simple e incómoda: si la infraestructura de identidad deja de funcionar, la empresa también se detiene.

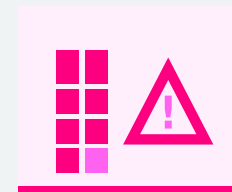
Y esta columna vertebral operativa está a punto de quedar mucho más expuesta. A medida que las organizaciones se apresuran a adoptar la IA y flujos de trabajo agénticos, esos agentes dependen de la infraestructura de identidad para operar de forma segura. Este cambio ya se refleja en los datos: el 93 % de las organizaciones ya utilizan o planifican utilizar agentes de IA para tareas de seguridad sensibles, como restablecer contraseñas y gestionar el acceso a VPN (Semperis, mayo de 2026).

Y aquí está lo que debería llamar su atención: estos agentes suelen utilizar la identidad de los empleados que les dan instrucciones para ejecutar tareas y acceder a datos sensibles. Cada uno de ellos representa un nuevo conjunto de llaves de acceso. Nunca había sido tan importante proteger, asegurar y poder recuperar la identidad.

SUPPORTING DATA



Active Directory y Entra ID son utilizados por más del **90 % de las empresas** de todo el mundo (Semperis).



Active Directory está involucrado en **9 de cada 10 ciberataques**, no porque esté mal diseñado, sino porque está presente en todas partes. ([Cohesity CERT](#)).

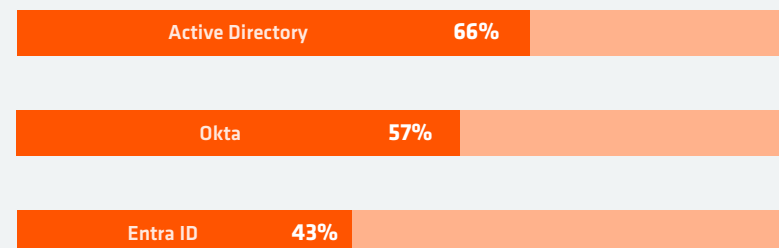
La intersección entre identidad, continuidad del negocio y resiliencia cibernética

La planificación tradicional de la continuidad del negocio trata la identidad como la electricidad: una infraestructura que asume que estará disponible cuando encienda el interruptor. Esa suposición es precisamente lo que puede dejar a una organización fuera de juego. La identidad ya no puede ser una suposición. Necesita su propio plan de recuperación.

La resiliencia cibernética da vuelta por completo a esa suposición. Considera la identidad como el primer objetivo que será atacado y como el primer elemento que usted debe poder recuperar (de forma independiente, probada, aislada y confiable) incluso cuando todo lo que la rodea haya sido comprometido. La brecha entre “asumimos que funcionará” y “hemos demostrado que funcionará” es exactamente donde las organizaciones pierden días o semanas después de un ataque. Pueden restaurar sus archivos perfectamente. Lo que no pueden hacer es iniciar sesión ni siquiera para una sola persona que pueda utilizarlos.

Para los líderes ejecutivos, de seguridad y de TI, la conclusión es clara: la continuidad del negocio y la resiliencia cibernética solo tienen éxito cuando la seguridad y la recuperación proactivas de la identidad se planifican, se prueban y cuentan con los recursos necesarios como disciplinas independientes. Nunca asuma que sucederán automáticamente mientras restaura todo lo demás. La esperanza no es un plan de recuperación.

DATOS DE RESPALDO



Los planes de recuperación ante desastres incluyen Active Directory en solo el 66 % de las organizaciones, Entra ID en el 43 % y Okta en el 57 %, lo que deja a una gran parte de los planes de continuidad con un punto ciego precisamente en la capa de identidad (*Semperis, Nov 2025*).



El 90 % de las organizaciones analiza las vulnerabilidades de identidad, pero solo el 51 % cuenta con procedimientos de remediación y apenas el 57 % automatiza la recuperación de la identidad (*Semperis, Nov 2025*).

El costo de la inacción

Hablemos del precio de esperar, porque esperar también es una decisión, y es la más cara de todas. No solo financieramente, sino también en términos operativos y reputacionales.

Ese costo no se reduce a una sola factura. Son tres, y se acumulan:

- **La factura de la brecha:** respuesta a incidentes, multas reglamentarias y exposición legal
- **La factura del tiempo de inactividad:** pérdida de productividad, ingresos bloqueados y ataques repetidos mientras la capa de identidad permanece expuesta
- **La factura de la confianza:** aumento de las primas del seguro cibernético, responsabilidad de los directivos y riesgo para los acuerdos

Y esperar no detiene el contador. La identidad es una de las principales superficies de ataque en las empresas y una frente a la que las defensas tradicionales no pueden avanzar al mismo ritmo. Por eso, el costo de no actuar no permanece estático: aumenta con el tiempo. Aumenta con cada trimestre que pasa sin resolverlo. Retrasarlo no es actuar con cautela. Es el interés compuesto de una deuda que usted nunca eligió asumir.

DATOS DE RESPALDO



A lo largo de tres años, las organizaciones pueden enfrentarse a un ataque de identidad exitoso con un costo de 1.2 millones de dólares, la supervisión manual de la identidad híbrida con un costo de 109 000 dólares, y las pérdidas de productividad y los tiempos de inactividad debido a la recuperación manual de Active Directory con un costo de 3.9 millones de dólares. (Forrester Total Economic Impact study).



El costo promedio global de una filtración de datos es de 4.44 millones de dólares, pero las filtraciones basadas en credenciales cuestan aproximadamente 4.67 millones de dólares y tardan unos 292 días en identificarse y contenerse, el período más largo de todos los vectores de ataque (IBM Cost of a Data Breach 2025).



La economía del ransomware está cambiando, pero no sin consecuencias: el pago medio del rescate cayó a 115 000 USD, y el 64 % de las víctimas se negaron a pagar, lo que significa que más organizaciones están absorbiendo el costo operativo de la recuperación en lugar de pagar el rescate, lo que aumenta la presión para acelerar la recuperación de la identidad (Verizon DBIR 2025).



Ocho de las ocho principales aseguradoras cibernéticas ya solicitan y validan medidas específicas de seguridad y resiliencia de la identidad al evaluar las pólizas cibernéticas. Demostrar un sólido nivel de protección de la identidad se relaciona directamente con primas más bajas y una mayor cobertura (Cohesity, “*Identity resilience is critical for cyber insurance*”).

Estos datos no son hechos aislados. Son las facturas desglosadas de una brecha de seguridad y del tiempo de inactividad, a las que se suma rápidamente el costo de la pérdida de confianza, a medida que las aseguradoras vinculan cada vez más las primas con el nivel de seguridad de tu infraestructura de identidad. Cada una de ellas se vuelve más cara cuanto más tiempo permanezca sin abordar la identidad. Esta factura la pagará de todos modos. La única pregunta es si paga un poco ahora, en sus propios términos, o si termina pagando todo después, bajo las condiciones del atacante.

CONCLUSIÓN

El compromiso basado en la identidad ahora está presente en prácticamente todas las brechas importantes, y el patrón nunca cambia. Los atacantes no necesitan irrumpir. Inician sesión con credenciales válidas y flujos de identidad de confianza y se mueven sin ser detectados por entornos que nunca se diseñaron para detectarlos. Luego, roban sus datos, se apoderan de sus sistemas e implementan su ransomware.

Nada de esto es inevitable.

Lo que separa a las organizaciones que se recuperan en horas de las que pasan semanas reconstruyendo la confianza en sus servicios de identidad no tiene nada que ver con la suerte ni con cuánto gastan. Todo se reduce a una sola decisión: si construyeron la resiliencia de la identidad como una disciplina propia, a lo largo de todo el ciclo de vida del ataque, antes de necesitarla.

Por eso, trate la resiliencia de identidad como lo que se ha convertido: no en algo opcional, sino en un requisito fundamental de la seguridad empresarial. La identidad es, al mismo tiempo, la puerta de entrada, los cimientos y el principal cuello de botella para la recuperación. Un conjunto fragmentado de herramientas independientes siempre se quedará corto. Lo mismo ocurrirá con cualquier plan de continuidad que simplemente dé por hecho que la identidad estará disponible cuando llegue el momento. La única estrategia que sobrevive al contacto con un ataque real es aquella que ha probado y validado antes de necesitarla.

La buena noticia es que puede adelantarse a este escenario. Puede acelerar la resiliencia cibernética para sus sistemas de identidad más críticos.

Y podemos ayudar.

Más información sobre cómo Cohesity puede ayudar a construir y fortalecer la resiliencia de la identidad

Obtenga una evaluación gratuita de seguridad de la identidad para identificar vulnerabilidades y brechas en Active Directory, Entra ID y OktaDirectory, Entra ID, and Okta





© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.