

POR QUÉ RAZÓN

**LA PROTECCIÓN,
LA SEGURIDAD
Y LA IA**

**DEBEN
CONVERGER**

COHESITY

POR QUÉ RAZÓN LA PROTECCIÓN, LA SEGURIDAD Y LA IA DEBEN CONVERGER

Durante años, las organizaciones han tratado la protección de datos, la seguridad de datos y las iniciativas de IA como prioridades separadas. Los equipos de respaldo se centraron en la recuperación. Los equipos de seguridad se centraron en la prevención de amenazas. Los equipos de IA se centraron en el análisis, la automatización y la innovación. Cada equipo operaba con sus propias herramientas, objetivos y arquitecturas.

Es hora de reimaginar este modelo fragmentado.

Las razones son prácticas. Los ciberataques son cada vez más específicos y los datos ahora residen en todas partes: en las instalaciones, en la nube y en SaaS. Al mismo tiempo, las empresas están luchando por acceder a los datos para mejorar sus resultados de IA. Esos datos a menudo se dividen en sistemas dispares, lo que aumenta tanto la complejidad como los puntos ciegos.

Agregar más herramientas no soluciona eso. Lo empeora.

Las organizaciones que están tomando la delantera no están añadiendo más capas.

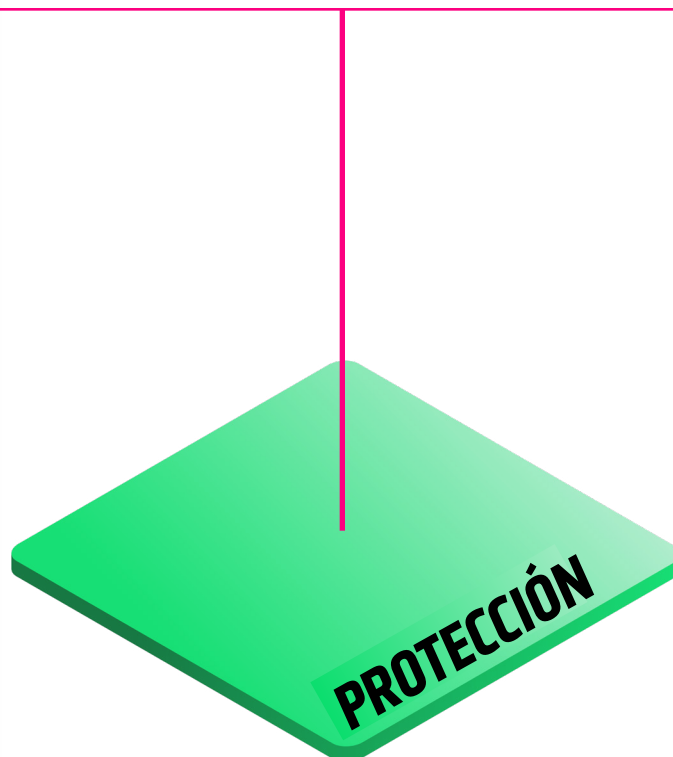
Están reconsiderando la base.

LA PROTECCIÓN es la base

La protección es el primer paso hacia la resiliencia cibernética. Comienza con una cobertura integral en todo el conjunto de datos, que abarca máquinas virtuales, bases de datos, sistemas de archivos y cargas de trabajo no estructuradas.

La protección debe cubrir todos estos datos, de manera consistente y sin brechas. La recuperación depende de ello. Cuando la protección está incompleta, fragmentada o inconsistente, no se puede contar con una recuperación rápida y limpia. Cuando la protección es integral y consistente, usted puede hacerlo, sin corrupción, pérdida ni riesgo residual.

La resiliencia cibernética comienza con este nivel fundamental de protección.



LA SEGURIDAD

debe integrarse en la capa de datos

Una vez establecida la protección, el siguiente desafío queda claro.

Si los sistemas de copia de seguridad pueden verse comprometidos, cifrados o ser objeto de un acceso indebido, los datos de recuperación en sí se convierten en otra superficie de ataque. La seguridad no puede seguir siendo una superposición externa. Debe funcionar directamente en la capa de datos.

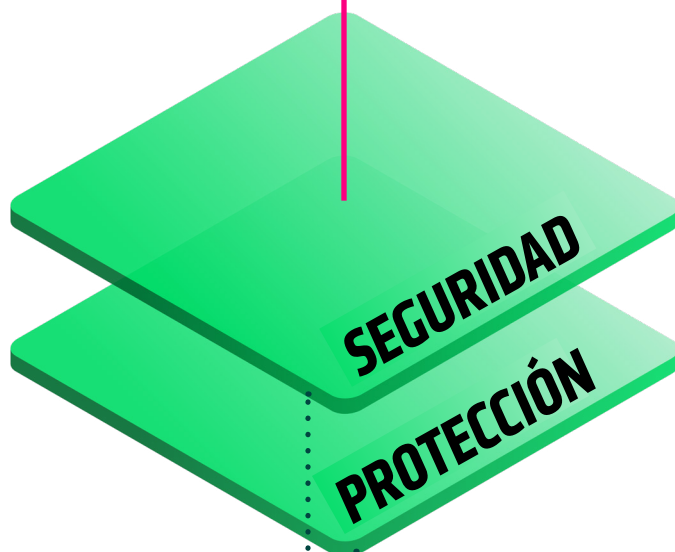
Eso significa:

- Detectar actividad anómala dentro de entornos de respaldo
- Hacer cumplir los controles de identidad y acceso en el origen
- Aplicar la gobernanza de manera consistente en todo el conjunto de datos

Cuando la protección y la seguridad operan en sistemas separados, los equipos se ven obligados a conciliar señales y políticas entre herramientas, a menudo durante situaciones de alta presión. Las brechas no aparecen porque las capacidades no existen, sino porque estas capacidades no están unificadas.

Incorporar la seguridad en la capa de protección de datos cierra esas brechas, lo que permite que la seguridad y la recuperación se refuercen entre sí. La detección de amenazas favorece una recuperación limpia, y la gobernanza se aplica una vez y se hace cumplir en todas partes.

Juntos, crean una base de datos confiable.



La protección
establece la resiliencia.

La seguridad
la fortalece.

CÓMO HACER QUE LA IA SEA práctica a escala empresarial

Solo después de que los datos estén protegidos y asegurados de manera confiable surge plenamente una nueva oportunidad.

Para que la IA tenga impacto, las organizaciones deben:

- Reunir datos no estructurados en todos los entornos
- Capturar cambios históricos
- Mantener una gobernanza consistente, acceso basado en roles y auditabilidad
- Reducir el riesgo de duplicación y exposición no deseada

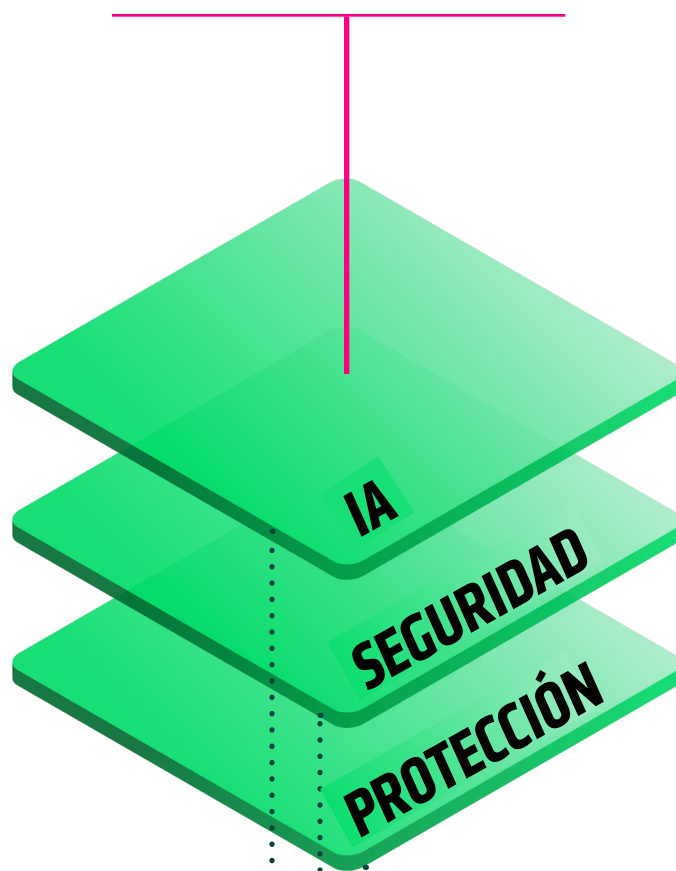
Muchos equipos intentan resolver esto copiando datos en plataformas de análisis o IA separadas. El resultado es un costo más alto, una mayor complejidad y una superficie de ataque ampliada.

Una base unificada cambia la ecuación. Permite a las organizaciones acceder a datos listos para IA y usarlos de manera segura, precisa y completa.

Cuando la protección y la seguridad ya están integradas, el mismo conjunto de datos confiable puede ser detectable y utilizable, sin romper los modelos de gobernanza ni duplicar los datos y la infraestructura. Los datos que protegen la continuidad se convierten en datos listos para la IA que alimentan la información.

En este modelo, la IA cumple dos funciones. Mejora la plataforma subyacente a través de la automatización y una detección más inteligente. Y potencia las aplicaciones posteriores, desde asistentes de productividad hasta agentes especializados, utilizando datos empresariales gobernados como fuente.

Cada capa se basa en la anterior.



La protección hace que los datos sean recuperables.

La seguridad la hace confiable.

La IA la hace valiosa.

LA CONVERGENCIA tiene sentido

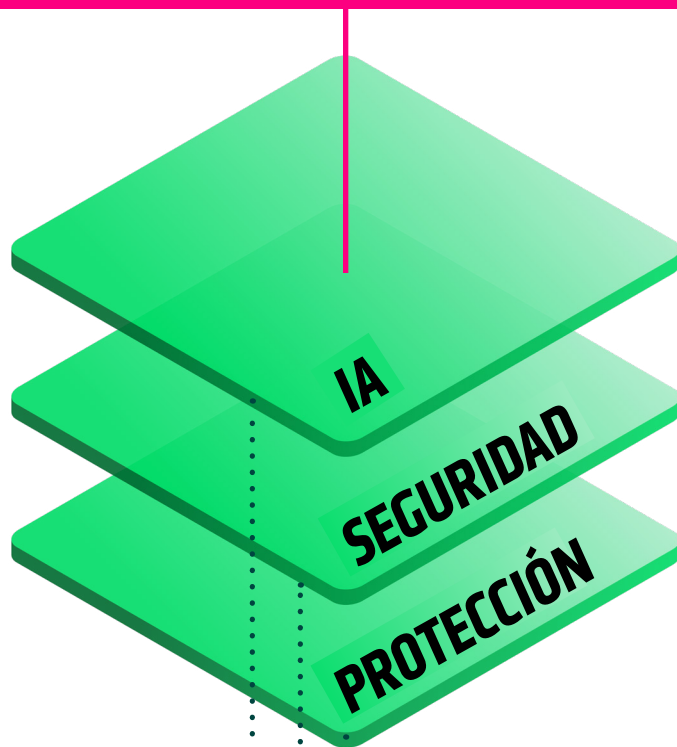
Cuando la protección, la seguridad y la preparación para la IA convergen en una sola base, sus datos:

- Son gobernados una vez y usados muchas veces
- Están protegidos dondequiera que residan
- Están asegurados en el origen
- Están listos para IA sin duplicación

De repente, la copia más segura de sus datos se ha convertido en la copia más inteligente de sus datos.

En un mundo definido por el riesgo cibernético y la aceleración de la adopción de la IA, la elección arquitectónica es clara: un conjunto de datos, administrado como un sistema único y escalable, construido para soportar interrupciones y generar información al mismo tiempo.

ESO ES COHESITY DATA CLOUD.



La **protección** garantiza la recuperabilidad.

La **seguridad** reduce la exposición.

La **IA** extrae valor.

PROBADO A ESCALA EMPRESARIAL

Cohesity Data Cloud es la única plataforma unificada construida para fortalecer la resiliencia cibernética y extraer más valor de sus datos.

Protege a más de **1000** cargas de trabajo en las instalaciones, la nube y SaaS,

ofreciendo copias de seguridad hasta **18 veces** más rápidas,

restauraciones un **97 %** más rápidas y tiempo de obtención de valor de IA instantáneo,

con un **50 %** menos almacenamiento y

hasta un **40 %** de ahorro en costos generales.

Obtenga más información en cohesity.com/DataCloud

© 2026 Cohesity, Inc. Todos los derechos reservados.

Cohesity, el logotipo de Cohesity, SnapTree, SpanFS, DataPlatform, DataProtect, Helios y otras marcas de Cohesity son marcas comerciales o marcas comerciales registradas de Cohesity, Inc. en los EE. UU. o a nivel internacional. Otros nombres de empresas y productos pueden ser marcas comerciales de las respectivas empresas con las que están asociados. Este material (a) tiene como objetivo proporcionarle información sobre Cohesity y nuestros negocios y productos; (b) se consideró verdadero y preciso en el momento en que se escribió, pero está sujeto a cambios sin previo aviso; y (c) se proporciona "TAL CUAL". Cohesity renuncia a todas las condiciones, las declaraciones y las garantías expresas o implícitas de cualquier tipo.

COHESITY

cohesity.com

1-855-926-4374

2625 Augustine Drive, Santa Clara, CA 95054

6300010-001-ES 03-2026