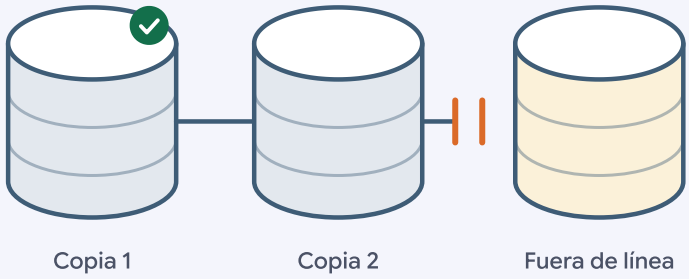
ENTIENDE. COMPRUEBA. MEJORA.

¿Cómo saber si tus copias de seguridad funcionan?

Solo lo sabrás restaurándolas. Haz pruebas de restauración con regularidad, mantén al menos una copia fuera de línea y cifra los datos críticos. La regla 3-2-1 es un buen punto de partida: tres copias, en dos soportes distintos, y una en una ubicación separada y fuera de línea.



Una guía para pasar a la acción

Explicaciones claras, un ejemplo ficticio y una hoja para organizar tus próximas tres acciones.

Consulta la versión web y sus actualizaciones ↗

¿Cómo saber si tus copias de seguridad funcionan?

01 / COMPRENDER

Por qué una copia puede fallar cuando la necesitas

Según CISA, muchas variantes de ransomware buscan las copias accesibles para borrarlas o cifrarlas, y por eso importa que haya una fuera de línea. Además, una copia puede llevar tiempo fallando sin que nadie lo sepa, o no incluir lo que creías.

3	2	1
copias de los datos	soportes distintos	copia fuera de la ubicación principal

02 / COMPRENDER

Cómo hacer una prueba de restauración

- Elige algo concreto: una carpeta, una base de datos o un equipo.
- Restáuralo en un lugar aparte, sin sobrescribir lo que está en uso.
- Comprueba que los archivos se abren y están completos.
- Anota cuánto ha tardado y qué fecha tenía la copia.
- Repítelo con regularidad, y siempre que cambien tus sistemas.

¿Cómo saber si tus copias de seguridad funcionan?

03 / COMPRENDER

Los servicios en la nube también cuentan

Que tus datos estén en la nube no significa que tengas una copia. Comprueba qué cubre tu proveedor, durante cuánto tiempo y cómo se recupera la información.

04 / COMPRENDER

Qué conviene documentar

- Qué se copia, con qué frecuencia y dónde se guarda.
- Quién es responsable de las copias.
- Cuándo fue la última prueba de restauración y qué resultado dio.

DEL CONOCIMIENTO A LA PRÁCTICA

Llévalo a tu empresa

EJEMPLO FICTICIO

El mensaje «copia completada» no es la prueba final

En este ejercicio ficticio, la copia nocturna termina sin errores. Al recuperar un documento en una carpeta de prueba, el archivo abre, pero faltan datos del último día. Ahora la empresa sabe qué información podría perder con esa frecuencia de copia.

La prueba debe comprobar que la información recuperada es útil y cuánto se tarda en volver a trabajar. Hazla en un entorno separado para no sobrescribir datos reales.

01

Antes de la prueba

Elige algo importante

Selecciona un documento, una aplicación o una base de datos relevante. Define cuántos datos sería aceptable perder y cuánto tiempo puede estar parado el trabajo.

02

Durante la prueba

Restaura y comprueba

Recupera la información en un destino de prueba autorizado. Abre los archivos o valida la aplicación, revisa permisos y comprueba fechas e integridad con su responsable.

03

Al terminar

Registra y corrige

Anota los tiempos, los errores y lo que faltó. Si la prueba no cumple lo acordado, asigna una mejora y repítela después de corregir el problema.

Qué conviene conservar

Fecha, copia utilizada, destino de prueba, tiempo de recuperación, validación del responsable y acciones pendientes. Guarda los resultados sin exponer el contenido recuperado.

TU HOJA DE TRABAJO

Tres acciones. Un siguiente paso.

Completa esta hoja con tu equipo. Define cómo comprobaréis cada mejora. No anotes contraseñas, claves ni información confidencial.

01 / Acción

Responsable: _____ Fecha: _____

Cómo comprobarla: _____

02 / Acción

Responsable: _____ Fecha: _____

Cómo comprobarla: _____

03 / Acción

Responsable: _____ Fecha: _____

Cómo comprobarla: _____

Preguntas frecuentes

¿Cada cuánto hay que probar las copias?

No hay una cifra universal: CISA e INCIBE piden hacerlo con regularidad. Decídelo según lo que te costaría perder esos datos, y repítelo cuando cambien tus sistemas.

¿Una copia en la nube cuenta como copia fuera de línea?

No necesariamente. Si se puede alcanzar desde un equipo comprometido con las mismas credenciales, un atacante también podría llegar a ella. Comprueba que esté aislada.

Fuentes y siguiente paso

- CISA: #StopRansomware Guide ↗
- INCIBE: Los hábitos de la pyme ciberresiliente ↗
- INCIBE: Copias de seguridad, una guía de aproximación para el empresario ↗

Las copias de seguridad son una de las áreas del análisis gratuito. Mira cómo están las tuyas. Hacer el análisis gratuito ↗

Información general. No es una auditoría, una certificación ni una garantía de seguridad. Ejemplos ficticios. Edición: 5 de noviembre de 2026.