



PLANTILLAS

Backups 3-2-1 y prueba de restauración

Copias de seguridad es el dominio más flojo en casi todos los diagnósticos. La regla 3-2-1 explicada para una empresa real, con el registro de prueba de restauración que convierte un backup en una garantía.

Cómo usar esta plantilla: los campos [ENTRE CORCHETES] de las secciones 4 y 6 se completan con la realidad de tu empresa.

Versión 1.0 · Agosto 2026

Casi todas las empresas que atienden un ransomware descubren dos cosas el mismo día. La primera es que sí tenían backup. La segunda es que el backup estaba conectado al mismo servidor que se cifró, o que nunca nadie había probado restaurarlo.

Tener copias no es lo que te salva. Lo que te salva es tener una copia que el atacante no pudo tocar y haber comprobado, antes del incidente, que de esa copia se puede volver.

1. Qué es 3-2-1 y cuál de los tres números importa

- 3 copias de la información: la que usás todos los días más dos respaldos.
- 2 medios distintos: por ejemplo el servidor y un disco externo, o el servidor y la nube. Si los dos respaldos viven en el mismo lugar, un incendio, un robo o un cifrado se los lleva juntos.
- 1 copia fuera del alcance: en otra ubicación física, y sobre todo desconectada o inmutable.

Ese último "1" es el único que te salva de un ransomware, y es el que casi nadie tiene. Un disco externo permanentemente enchufado al servidor no es una copia fuera de alcance: es un archivo más que se va a cifrar. Una carpeta sincronizada tampoco, porque sincroniza el archivo cifrado sobre el sano.

Alcanza con desenchufar el disco cuando termina la copia, o con contratar un almacenamiento con retención inmutable. Lo primero es gratis y funciona.

2. Qué hay que respaldar de verdad

El error habitual es respaldar el servidor y olvidarse de la mitad de la empresa. Completá esta lista antes de diseñar nada.

Qué	Dónde vive hoy	¿Respaldado?
Sistema de gestión o facturación	[COMPLETAR]	[SÍ / NO]
Base de datos de clientes	[COMPLETAR]	[SÍ / NO]
Documentos contables e impositivos	[COMPLETAR]	[SÍ / NO]
Correo electrónico	[COMPLETAR]	[SÍ / NO]
Archivos en las computadoras de cada persona	[COMPLETAR]	[SÍ / NO]
Fotos, diseños, material de marketing	[COMPLETAR]	[SÍ / NO]
Configuraciones y licencias de los sistemas	[COMPLETAR]	[SÍ / NO]

Dos advertencias sobre esta tabla. El correo en la nube no está respaldado por defecto: el proveedor te garantiza que el servicio funciona, no que puedas recuperar lo que alguien borró hace seis meses. Y las computadoras personales son donde vive el trabajo real de la mayoría de la gente, y casi nunca entran en el esquema.

3. Las dos preguntas que definen todo

Antes de elegir herramienta, respondé esto con el dueño, no con el técnico.

- ¿Cuánta información podés permitirte perder? ¿Un día de facturación? ¿Una hora? Eso define cada cuánto se hace la copia.
- ¿Cuánto tiempo podés estar parado? ¿Dos horas? ¿Dos días? Eso define cuánto vas a tener que invertir para poder volver rápido.

Las respuestas no son técnicas, son de negocio. Y son las que justifican el gasto ante quien firma.

4. Tu esquema, escrito

- Copia diaria de [QUÉ] hacia [DÓNDE], automática, a las [HORA].
- Copia semanal hacia [MEDIO DESCONECTADO O INMUTABLE], a cargo de [RESPONSABLE].
- Retención: se conservan [N] copias diarias, [N] semanales y [N] mensuales.
- Las copias están cifradas y la clave de recuperación se guarda en [DÓNDE], fuera del sistema que se respalda.
- Responsable de revisar que las copias corrieron: [NOMBRE], con frecuencia [DIARIA / SEMANAL].

Si nadie mira los avisos de error, el backup falla en silencio durante meses. Es el modo de falla más común de todos.

5. Un backup que nunca restauraste no es un backup

Es una suposición. La prueba de restauración es lo que la convierte en un hecho, y lo que separa a una empresa que se recupera en horas de una que descubre el problema el peor día posible.

1. Elegí un archivo o una base representativa, no la más chica.
2. Restauralo en un lugar separado, nunca encima del original.
3. Abrilo y verificá que sirve: que la base abra, que el documento no está corrupto, que los datos lleguen hasta la fecha esperada.
4. Cronometrá cuánto tardó todo el procedimiento. Ese número es tu tiempo real de recuperación, y suele ser bastante peor que el estimado.
5. Anotalo en el registro de la sección 6.

Frecuencia sugerida: trimestral para lo crítico, y siempre después de cualquier cambio en los sistemas o en el esquema de copias.

6. Registro de prueba de restauración

Fecha	Quién	Qué se restauró	Tiempo	¿Funcionó?
[FECHA]	[NOMBRE]	[ARCHIVO / BASE]	[HH:MM]	[SÍ / NO]

Este registro es también evidencia: sirve ante un cliente que te audita, ante un seguro y ante cualquier reclamo por pérdida de información.

7. Errores caros

- El disco de backup siempre enchufado. El ransomware lo cifra junto con todo lo demás. Es el error más frecuente y el más caro.
- Confundir sincronización con copia de seguridad. Una carpeta sincronizada replica el borrado y el cifrado. Sirve para trabajar, no para recuperarse.
- Suponer que el correo en la nube ya está respaldado. No lo está.
- No cifrar las copias. Un disco de backup robado es la base de clientes completa en manos de cualquiera, y con Ley 25.326 encima.
- Guardar la única clave de cifrado adentro del sistema que se respalda. Si se pierde el sistema, se pierde la clave, y el backup queda inservible.
- No mirar los avisos de error. Falla en silencio; se descubre el día que hace falta.

8. Una sola cosa para hacer hoy

No hace falta rehacer el esquema ni comprar nada para empezar. Elegí un archivo importante, restauralo en una carpeta aparte, abrilo y anotá cuánto tardaste. Si funciona, ya tenés la primera línea del registro. Si no funciona, acabás de enterarte hoy y no el día del incidente, que es exactamente para lo que sirve esta prueba.



Esto no termina acá

Si querés enterarte de las estafas que están circulando de verdad, qué revisar y los documentos nuevos, sumate al correo de CiberConscientes. Sin vueltas y con baja en un clic. www.ciberconscientes.io

Material orientativo elaborado por CiberConscientes con fines educativos. No reemplaza el asesoramiento profesional para tu caso particular. Los procedimientos y las pantallas de las aplicaciones pueden cambiar: verificá las fuentes oficiales vigentes.

Versión 1.0 · Agosto 2026 · Próxima revisión: Agosto 2027 · www.ciberconscientes.io