

L U M B R E



Respaldo que sí rescata: la prueba que casi nadie hace

Materia: Ciberseguridad esencial para PyME

08/10/2026

Antes de empezar

Nadie presume de no tener respaldo; casi nadie ha recuperado de verdad uno. Este módulo construye el respaldo que sí rescata: qué debe guardarse (no todo, sino lo que no se puede regenerar), la regla tres copias en dos medios con una fuera de casa e inmutable, la diferencia entre respaldar y sincronizar, y la prueba que convierte la superstición en certeza: restaurar un archivo al azar, con reloj en mano, y después restaurar la carpeta completa en un día de simulacro.

QUÉ APRENDERÁS

- Diseñar un esquema de respaldo con la regla tres-dos-uno, definir la retención y ejecutar un ejercicio de recuperación con tiempo medido.

Un respaldo que nadie ha restaurado es una

esperanza con disco duro



El respaldo no se cree porque exista: se cree porque alguien lo restauró una vez con reloj en mano.

Pregunta incómoda: ¿cuándo fue la última vez que restauraste algo de tus respaldos? Si no recuerdas, el problema no es tu memoria: es que **nunca lo probaste**. En una PyME, el respaldo falla de formas muy concretas: la carpeta sincronizada que borra tus versiones cuando alguien borra la original, el disco que estaba desconectado el día del incidente, el respaldo que cifra lo mismo que cifró el ataque, la cinta legible solo por el sistema que ya no existe.

Empecemos por **qué respaldar**. La regla es: se respalda **lo que no se puede regenerar**. Tus facturas electrónicas tienen respaldo en el portal del SAT, pero tu

carpeta de «plantillas y cálculos» no la regenera nadie; los correos críticos de negociación con un cliente no se recuperan de otra parte; la base de datos de clientes, el archivo contable, los diseños, las licencias y contraseñas de los sistemas. Inventario corto, sin nostalgia: una hoja con qué, dónde, cada cuándo y quién.

La regla 3-2-1, y la copia que el ataque no puede tocar

Tres copias de la información (la original cuenta como una), en **dos medios distintos** (por ejemplo, un servidor local y una nube), y **una fuera de casa** (en la nube o en un disco guardado en otro sitio). A esa regla las amenazas modernas le añadieron un requisito: **inmutabilidad o desconexión**. Si el respaldo vive en la misma red que la empresa y el atacante llega con credenciales de administrador, cifra tus archivos y también cifra tus copias: un ataque de cifrado con rescate bien portado se dio el lujo de tumbar respaldos en red. Por eso la copia buena es la que **no se puede borrar durante X días** (retención inmutable en la nube) o la que **está físicamente desconectada** (el disco que se guarda en la cajilla después de su turno).

Segunda confusión cara: **sincronizar no es respaldar**. La carpeta sincronizada de nube es maravillosa para trabajar entre el celular y la laptop, pero replica lo que hagas, incluido el desastre: si alguien borra la carpeta de clientes, se borra «del respaldo» en segundos. La diferencia se llama **versiones y retención**: el respaldo guarda estados anteriores en el tiempo y los conserva aunque el presente se eche a perder. Revisa hoy tu nube: ¿conserva versiones de archivos borrados, cuántos días? Si la respuesta es «no sé», ahí tienes tu primera tarea.

Y ahora la parte que casi nadie hace, la que separa un respaldo real de un ritual: **la prueba de recuperación**. Versión mínima, semanal, dos minutos: elige un archivo al azar, bórralo de un lugar de pruebas y **restáuralo desde el respaldo**. Funcionó: el respaldo existe. Y versión completa, dos veces al año, en un sábado por la mañana: restaura la carpeta crítica entera en un equipo limpio, mide cuánto tardó en bajar todo y anota la fecha. El número que salga es oro puro: es tu **tiempo real de recuperación**, el que después te dirá si aguantas un lunes sin sistemas o si necesitas mejorar el esquema antes del desastre, no durante.

El día del incidente no vas a descubrir si tu respaldo funciona; vas a descubrir si funcionaba el día que lo probaste por última vez.

— Lumbre · Empresa

Qué es cada mecanismo y para qué sirve de verdad

Mecanismo	Qué hace	Cuándo sirve
Sincronización de nube	Replica el estado actual en todos tus dispositivos	Trabajar en varios equipos; NO es respaldo
Respaldo con versiones	Conserva estados anteriores y los retiene	Borrado accidental, ediciones desastrosas
Copia inmutable o desconectada	No se puede borrar ni cifrar desde la red	El cifrado con rescate ataca también las copias
Imagen del equipo completo	Copia el sistema tal como está, no solo archivos	El equipo muere y hay que levantar otro
Exporte periódico a otro formato	Saca los datos del sistema que los guarda	El proveedor del sistema desaparece o te bloquea los datos

1. Clasifica cada situación según el componente del esquema que debe cubrirla:

Elementos:

- Alguien sobrescribió la plantilla de cotización y nadie recuerda cómo estaba
- Un ataque cifró la red entera, incluidos los respaldos en línea
- El disco de respaldo lleva tres meses sin actualizarse y nadie lo notó
- Hay que saber cuánto tardaría recuperar la carpeta contable completa
- La carpeta sincronizada «respetó» el borrado: desapareció de todos lados

Versiones y retención	. . .
Copia inmutable o desconectada	. . .
Prueba de recuperación	. . .

2. Una PyME tiene su carpeta de trabajo sincronizada con la nube y considera que «ya tiene respaldo». Un viernes alguien mueve mal una selección y borra tres años de expedientes. ¿Qué van a encontrar el lunes en la nube?

- ☐ Los expedientes intactos, porque la nube siempre conserva todo
- ☐ Los expedientes borrados también en la nube, porque la sincronización replicó el borrado; salvo que exista retención de versiones vigente
- ☐ Solo los expedientes del último día
- ☐ Un aviso pidiendo el rescate antes de restaurar

3. Un simulacro de recuperación que toma medio día y termina con la carpeta crítica restaurada en un equipo limpio es parte de un buen esquema de respaldo, no una pérdida de tiempo.

☐ Verdadero

☐ Falso

4. Escribe tu hoja de respaldo: cinco cosas que tu empresa no puede regenerar, dónde están, cuál es su copia fuera de casa y con qué frecuencia se respaldan. Agenda hoy la prueba semanal de dos minutos y la fecha del próximo simulacro completo.

Si algo importante vive en un solo lugar —en la computadora de una sola persona—, hoy no tiene respaldo: tiene suerte.

Para dominar este tema

Lo esencial que debes saber

- Se respalda lo que no se puede regenerar; el inventario cabe en una hoja.
- La regla 3-2-1: tres copias, dos medios, una fuera de casa.
- Una copia debe ser inmutable o estar desconectada: si no, el ataque también la cifra.
- Sincronizar es un espejo; respaldar es una máquina del tiempo con retención de versiones.
- La prueba semanal y el simulacro semestral convierten el respaldo en certeza y miden tu tiempo de recuperación.

Preguntas clave del tema

1. ¿Qué información de tu empresa es irrecuperable si se pierde?
2. ¿Qué exige la regla 3-2-1 y por qué se le añadió la inmutabilidad?
3. ¿En qué se distingue sincronizar de respaldar?
4. ¿Cómo se prueba un respaldo sin esperar al desastre?
5. ¿Qué número produce un simulacro y para qué sirve?

Lo que debes poder hacer

- Inventariar la información crítica y su esquema de copias 3-2-1.

- Asegurar una copia inmutable o desconectada y verificar la retención de versiones de tu nube.
- Ejecutar la prueba semanal y un simulacro de restauración con tiempo medido.

ACTIVIDAD INTERACTIVA DISPONIBLE
EN LUMBRE

5. Chequeo: el respaldo que sí rescata



Siguiente: *El correo del proveedor que ya no es tu proveedor* — ingeniería social, suplantación y el protocolo de verificación que se aplica antes de pagar o de entregar datos.

Referencia curricular

Materia:	Ciberseguridad esencial para PyME
-----------------	-----------------------------------

Versión interactiva completa (con actividades, videos y autoevaluación):



<https://empresa.lumbre.lat/object/emp-ted-c33-m03-0a01>

Material educativo generado desde Lumbre · lumbre.lat