

L U M B R E



Qué le duele a una PyME: amenazas reales, no de película

Materia: Ciberseguridad esencial para PyME

08/10/2026

Antes de empezar

A una PyME no la tumba un ataque de película: le basta un correo abierto con prisa un viernes. Este módulo baja la ciberseguridad del mito al terreno: qué buscan quienes atacan, por dónde entran a una empresa sin área de sistemas, y cuánto cuesta cada golpe en días de operación, dinero y confianza. Saldrás con un mapa sobrio de riesgos —cifrado de archivos con rescate, fraude del proveedor falso, robo de datos y secuestro de correo— y la calma para priorizar sin comprar miedo.

QUÉ APRENDERÁS

- Reconocer las amenazas cibernéticas que realmente golpean a una empresa pequeña y estimar su costo en operación, dinero y reputación.

El riesgo no es que te hackeen como en la tele: es

que pase algo común y caro



La ciberseguridad de una PyME se mide en días sin facturar, no en títulos de noticiero.

Cuando se habla de ciberseguridad, la imagen que llega es la del genio solitario vulnerando un gran banco. La realidad de una empresa chica es más terrenal y, por eso, más manejable: **no te atacan por ser interesante, te atacan por ser fácil**. Los que buscan blancos barren redes y correos buscando lo barato: una contraseña repetida, un equipo sin actualizar, un pago que alguien hace sin verificar. Y cuando entran, no roban secretos: **paran tu operación o desvían un pago**.

El primer paso no es comprar software: es **entender qué te puede pasar y cuánto cuesta**. Un riesgo se piensa en tres preguntas: ¿qué tan probable es?, ¿a qué le pone

precio? (días sin vender, un pago perdido, datos de clientes al aire) y ¿cuánto tardas en recuperarte? Con eso en la mesa, la prioridad deja de ser «lo que suena urgente» y pasa a ser «lo que más duele y es barato de cerrar».

Las cinco amenazas que de verdad golpean a una PyME

1. Fraude del proveedor falso o del cambio de cuenta: un correo que parece de un proveedor habitual pide «actualizar la cuenta para el depósito de hoy». Es el que más dinero mueve, porque no rompe nada técnico: engaña a quien paga. **2. Cifrado con rescate:** un programa cifra tus archivos y pide rescate; suele entrar por una contraseña débil o un adjunto. Duele en días sin operar. **3. Robo o filtración de datos personales:** se cae una base con clientes o empleados; activa obligaciones legales de aviso. **4. Secuestro de cuenta de correo:** toman el correo de un humano para pedir pagos o espiar; la llave suele ser una contraseña reutilizada. **5. Error humano sin intención:** borrar una carpeta, configurar mal algo, perder un equipo. No es un ataque: es el costo de no tener respaldo.

¿Por dónde entran casi siempre? No por muros de fuego sofisticados sino por **la puerta que dejaste abierta sin saberlo**: accesos con permisos de más que nadie revisa, credenciales que sirven para todo, equipos viejos que ya no reciben actualizaciones, y copias de seguridad que nadie ha probado. Cada una es una decisión de administración, no de tecnología, y cada una se puede cerrar con hábitos baratos.

Y una verdad incómoda sobre el costo: el daño casi nunca es solo el pago perdido. Es **la semana que no facturas** mientras recuperas sistemas, **el cliente que se fue** porque sus datos quedaron expuestos, y **el seguro o el préstamo** que ahora necesitas para pasar el bache. Una PyME que pierde su operación cinco días pierde algo que no está en ninguna factura: la confianza de que «con esta empresa sí se puede contar». Poner ese número en la mesa es lo que convierte la higiene digital de «molestia» a «responsabilidad del dueño».

El ataque que sí le llega a una PyME no usa película ni matriz verde: usa un remite que conoces y una prisa que entiendes.

— Lumbre · Empresa

Amenaza, cómo entra y qué te cuesta

Amenaza	Cómo suele entrar	Lo que duele más
Fraude del proveedor falso	Correo suplantado + prisa	Un pago que se va y no vuelve

Amenaza	Cómo suele entrar	Lo que duele más
Cifrado con rescate	Contraseña débil o adjunto	Días sin operar ni facturar
Filtración de datos	Acceso con permisos de más	Obligación de avisar y reputación
Secuestro de correo	Contraseña reutilizada	Estafas desde tu propia identidad
Error o equipo perdido	Sin respaldo probado	Información que ya no está

1. Clasifica cada incidente según la amenaza que mejor lo explica:

Elementos:

- Llegó un pago a una cuenta que «el proveedor» cambió por correo
- Amaneció toda la carpeta compartida cifrada con un aviso de rescate
- Alguien borró la carpeta de clientes y la copia tampoco estaba
- El contador recibió instrucciones de pago desde el correo de siempre
- Se perdió el equipo con la única copia del expediente

Fraude de proveedor	. . .
Cifrado con rescate	. . .
Error sin respaldo	. . .

2. Una PyME sin área de sistemas tiene presupuesto para atender UNA sola cosa este trimestre. Según impacto y facilidad de cierre, ¿cuál debería atacar primero?

- ☐ Comprar el antivirus más caro del mercado
- ☐ Poner doble factor y contraseñas únicas a los correos y accesos de pago
- ☐ Contratar un consultor que audite todo
- ☐ Cambiar todas las computadoras

3. Una empresa pequeña está relativamente a salvo porque a los criminales solo les interesan los bancos y las grandes corporaciones.

- ☐ Verdadero
- ☐ Falso

4. Enumera tres golpes que le dolerían a tu empresa esta semana: un pago desviado, la carpeta compartida cifrada, un correo de un socio tomado. Para cada uno, anota cuánto te costaría en días y en dinero, y qué tan fácil sería hoy que ocurriera. ¿Cuál te preocupa más?

Si un mismo correo sirve para entrar a la banca en línea, ahí no tienes un riesgo de sistemas: tienes un riesgo de tesorería.

Para dominar este tema

Lo esencial que debes saber

- A la PyME la atacan por fácil, no por famosa: se busca volumen de blancos alcanzables.
- Cinco amenazas concentran el daño: fraude de proveedor, ransomware, filtración, secuestro de correo y error sin respaldo.
- La puerta casi siempre es una credencial débil, un acceso de más o un equipo sin actualizar.
- El costo real incluye días sin operar y la confianza perdida, no solo el dinero.
- Priorizar = cerrar primero lo que más duele con lo más barato y rápido.

Preguntas clave del tema

1. ¿Por qué una PyME es un objetivo atractivo para el atacante?
2. ¿Cuáles son las amenazas que más la golpean?
3. ¿Por dónde entran, en la práctica?
4. ¿Qué costo real tiene un incidente, además del pago?
5. ¿Cómo se prioriza sin comprar miedo?

Lo que debes poder hacer

- Listar las amenazas reales de tu empresa y cómo entrarían.
- Estimar el impacto de cada una en días, dinero y reputación.
- Elegir qué riesgo cerrar primero por relación daño-costos.

ACTIVIDAD INTERACTIVA DISPONIBLE EN
LUMBRE

5. Chequeo: riesgo sin dramatismo



Siguiente: *La higiene que cierra el ochenta por ciento del riesgo* — contraseñas, doble factor, accesos por rol y equipos: la lista de controles que se instala en una semana.

Referencia curricular

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

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



<https://empresa.lumbre.lat/object/emp-ted-c33-m01-0a01>

Material educativo generado desde Lumbre · lumbre.lat