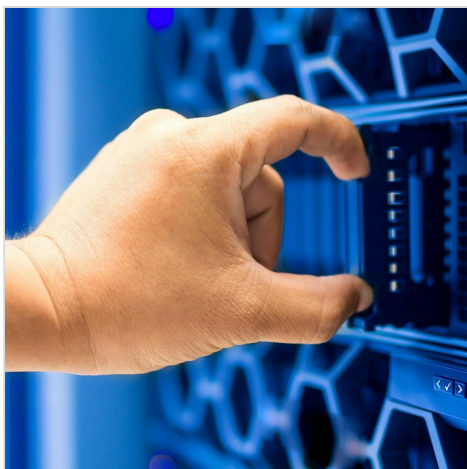


L U M B R E



Protocolo de incidente: las primeras cuatro horas

Materia: Ciberseguridad esencial para PyME

08/10/2026

Antes de empezar

El curso cierra con el plan para cuando todo lo demás falló. En las primeras cuatro horas se define el tamaño real del incidente: quién decide, qué equipo se aísla y cuál no, qué evidencia se conserva antes de reiniciar, a quién se avisa (banco, clientes, autoridad) y cuándo. El proyecto integra todo el curso en un protocolo de dos páginas y una agenda anual de higiene. Producto final: tu protocolo escrito, con nombres y teléfonos.

QUÉ APRENDERÁS

- Integrar el protocolo de reacción ante un incidente: roles, aislamiento, evidencia, recuperación y obligaciones de aviso, con la agenda anual de higiene.

El incidente no espera a que decidas bien: decide

tú por adelantado



En la hora cero nadie inventa el plan: se ejecuta el que se escribió en un día tranquilo.

Un viernes a las cuatro empieza a correr una hora que define semanas: el servidor se comporta raro, la carpeta compartida amanece cifrada, la clienta de siempre llama «extrañamente» pidiendo un cambio de cuenta, el cobro de la banca en línea aparece sin que nadie lo haya hecho. La tentación natural es **reiniciar, borrar, llamar al técnico de confianza y poner la operación primero**. Y cada una de esas reacciones, sin protocolo, destruye algo: la evidencia, la trazabilidad, o la obligación legal de aviso a tiempo.

Un protocolo de incidente para una PyME cabe en dos páginas y tiene cuatro columnas: **quién decide, qué se aísla, qué se conserva, a quién se avisa**. Escríbelo hoy, con nombres y teléfonos reales, porque en la hora cero nadie piensa bien: la gente ejecuta lo que ya estaba dicho. Y el primer renglón es tan simple como decisivo: **«el que descubre la anomalía avisa de inmediato a [nombre], y no apaga ni reinicia nada sin su visto bueno»**.

Las cuatro horas, en orden de prioridad

Primera hora — contención sin destrucción: desconecta de la red el equipo afectado (el cable se puede quitar; apagar el equipo pierde evidencia en memoria), pausa las cuentas comprometidas en correo y banca y cambia esas credenciales. **Segunda hora — dimensión y evidencia:** ¿qué más está tocado? Anota todo en una hoja con hora: qué se vio, cuándo, qué se hizo. Una bitácora de papel bien llevada vale un peritaje. **Tercera hora — avisos que no se pueden posponer:** la banca (para congelar el fraude: cada minuto cuenta), el proveedor «suplantado» (para que advierta a otros), y si hay datos personales de por medio, preparar el aviso a afectados: la ley mexicana de protección de datos exige avisar **sin demora** cuando la seguridad de los titulares está afectada. **Cuarta hora — recuperación con criterio:** decidir desde qué respaldo y con qué pruebas se levanta, sabiendo que restaurar sin saber qué pasó reabre la misma puerta al día siguiente.

Dos decisiones difíciles que el protocolo debe responder **por adelantado**, porque en caliente no se piensa: **el rescate y el comunicado**. Sobre pagar o no pagar un rescate: la postura práctica es que **no es decisión de quien está en la oficina ese día**; es del dueño, con su asesor, con su respaldo funcional en la mano y sabiendo que pagar no garantiza recuperar nada y financia la siguiente extorsión. Sobre el comunicado: la presión de «no hagamos olas» es natural y casi siempre mala consejera; si hubo datos de clientes, el aviso oportuno es ley y es reputación; el daño de descubrirlo por terceros siempre es mayor que el de contarla uno mismo, con el plan de reparación en la mano.

Y cuando el incendio se apaga, el protocolo se sienta una última vez: la **revisión posterior** de media hora con tres preguntas —qué pasó, por qué funcionó o no lo que teníamos, qué dos cosas cambiaremos ya— que se convierte en tareas con nombre y fecha. Porque el incidente deja de ser tragedia solo si se paga la lección: la mayoría de las empresas invadidas dos veces no tuvieron un segundo ataque más astuto: tuvieron la misma puerta sin cerrar.

Un protocolo de incidente no se escribe para el día que todo salga bien: se escribe para el día que alguien no piense con claridad, y ese alguien puedes ser tú.

— Lumbre · Empresa

Las primeras cuatro horas, renglón por renglón

Hora	Qué se hace	Qué se protege
Primera	Desconectar de red, pausar cuentas, cambiar credenciales	La extensión del daño
Segunda	Medir alcance y abrir bitácora con horas	La evidencia y el peritaje futuro
Tercera	Avisar a banca, proveedor suplantado y preparar aviso a titulares	El dinero y la obligación legal
Cuarta	Decidir desde qué respaldo se levanta y con qué verificación	La recuperación sin repetir el ataque
Día siguiente	Revisión posterior con dos cambios concretos	Que el incidente haya servido de algo

1. Clasifica cada reacción del incidente en la hora del protocolo en que debe ocurrir:

Elementos:

- Desconectar de la red la laptop desde donde se notó el cifrado
- Llamar a la banca para congelar la transferencia no autorizada
- Preparar el aviso a los clientes cuyos datos quedaron expuestos
- Cambiar las contraseñas de los correos comprometidos
- Reunión de revisión con los dos cambios que se implementan ya

Primera hora	. . .
Tercera hora	. . .
Después del incidente	. . .

2. A las cuatro de la tarde del viernes la contadora descubre que la carpeta compartida está cifrada con un aviso de rescate. ¿Cuál es la reacción correcta según el protocolo?

- ☐ Reiniciar el servidor para ver si el problema desaparece y seguir operando
- ☐ Avisar al dueño de inmediato, desconectar el equipo afectado de la red sin apagarlo y abrir la bitácora con hora de cada paso
- ☐ Buscar en internet el nombre del ransomware y pagar rápido mientras el bitcoin está bajo
- ☐ Borrar los archivos cifrados para detener el contagio

3. Cuando un incidente expone datos personales de clientes, avisarles sin demora es opcional: basta con resolver el problema técnico internamente.

- ☐ Verdadero
- ☐ Falso

4. Escribe hoy tu protocolo de dos páginas, con nombres y teléfonos: quién es el que decide a la hora cero, quién desconecta, quién habla con el banco, quién redacta el aviso. Léelo con tu equipo de pagos en diez minutos y agenda el simulacro de una hora este trimestre. ¿Qué teléfono faltó?

El simulacro no busca asustar: busca encontrar los huecos mientras el incidente todavía es de mentira.

Para dominar este tema

Lo esencial que debes saber

- El protocolo cabe en dos páginas con roles, acciones y teléfonos: se escribe en día tranquilo.
- Primera hora: aislar sin destruir evidencia (desconectar, no apagar) y escalar a quien decide.
- La bitácora con horas es la evidencia barata que hace posible el peritaje y el aviso puntual.
- Los avisos imposibles de posponer: banca, proveedor suplantado y titulares de datos sin demora.
- La revisión posterior con dos cambios cerrados es lo que separa el incidente único del recurrente.

Preguntas clave del tema

1. ¿Quién decide en la hora cero y con qué datos?
2. ¿Qué se aísla primero y qué evidencia se conserva?
3. ¿A quién se avisa y en qué ventana de tiempo?
4. ¿Cómo se decide la recuperación sin reabrir la puerta?
5. ¿Qué convierte la revisión posterior en tareas con fecha?

Lo que debes poder hacer

- Escribir el protocolo de incidente con roles, teléfonos y orden de acciones.
- Conducir la primera hora: contención, evidencia y avisos sin destruir nada.
- Cerrar el ciclo con la revisión posterior y la agenda anual de higiene.

ACTIVIDAD INTERACTIVA
DISPONIBLE EN LUMBRE

5. Chequeo final: tu protocolo de las primeras cuatro horas



Con este protocolo cierras **Ciberseguridad esencial para PyME**: del mapa de riesgos a la agenda anual de higiene, con respaldos probados y una política de pagos que frena el fraude. Llévalo a la práctica esta semana: el mejor protocolo es el que ya estaba escrito. **Fin del curso.**

Referencia curricular

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

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



<https://empresa.lumbre.lat/object/emp-ted-c33-m05-0a01>

Material educativo generado desde Lumbre · lumbre.lat