

L U M B R E



La higiene que cierra el ochenta por ciento del riesgo

Materia: Ciberseguridad esencial para PyME

08/10/2026

Antes de empezar

La mayor parte del riesgo de una PyME no se cierra con herramientas caras sino con pocos hábitos bien puestos. Este módulo es la lista de verificación que se instala en una semana: contraseñas únicas y largas gestionadas con un gestor, doble factor en correo y pagos, permisos por rol que se retiran al terminar una función, equipos que se actualizan solos y se bloquean solos. Nada teórico: cada control con el cómo hacerlo y con el error típico que lo anula.

QUÉ APRENDERÁS

- Instalar los controles prioritarios de higiene digital: contraseñas robustas, doble factor, accesos por rol, equipos actualizados y hábitos de escritorio.

No necesitas diez herramientas: necesitas cinco

hábitos, y hoy



La seguridad de una PyME se parece más a un llavero ordenado que a una bóveda de banco.

Si el módulo uno te dio el mapa del riesgo, este te da la llanería. La evidencia es tozuda: la mayoría de los incidentes que golpean a empresas chicas no usan técnicas sofisticadas; usan **credenciales que se repiten, factores que no están activos y ventanas que nadie cerró**. Y cada una de esas puertas se cierra con un hábito que se instala en días, no en proyectos de seis meses.

Hábito uno: contraseñas únicas y largas, en un gestor. La contraseña repetida es el dominó: cae la del foro de un proveedor y se prueba en el correo, y del correo se entra a la banca. Nadie memoriza cuarenta contraseñas fuertes; por eso existe el

gestor de contraseñas: una sola maestra, fuerte, y el resto largas, únicas y guardadas. Lo que se pierde al no usar gestor no es elegancia: es que el registro se descargó y alguien ya lo está probando en tu correo.

El doble factor: el candado que se pone en cinco minutos

El doble factor (un segundo paso además de la contraseña: aplicación en el teléfono, llave física) convierte una contraseña robada en una llave que no abre. Es **el control con mejor relación costo-beneficio de toda la lista** y debe estar activo, como mínimo, en tres puertas: el **correo corporativo** (la llave maestra de recuperaciones: si toman el correo, toman todo), la **banca en línea y portal del SAT**, y las **plataformas de pagos o de facturación**. El error típico es activarlo solo en el personal y dejar libre el de la empresa, o usar el segundo factor con el mismo número de teléfono que recibe los códigos de recuperación: si secuestran la línea con una SIM clonada, el factor se vuelve de cartón. Para el teléfono, PIN en la línea con la compañía.

Hábito tres: accesos por rol, con baja por defecto. Cada persona tiene acceso a lo que necesita para su función, y nada más. El sueldo de la nómina no le sirve al pasante de redes; la banca en línea no vive en el teléfono del vendedor. Y cuando alguien **sale o cambia de puesto, sus accesos se retiran ese mismo día**: la puerta abierta más común de una PyME es la cuenta del que se fue hace ocho meses y «iba a borrarse después». Se llama revisión de accesos y basta una vez por trimestre: listar quién tiene qué y preguntar qué pasaría si ese nombre desapareciera mañana.

Hábitos cuatro y cinco: equipos que se cuidan solos. Actualización automática del sistema operativo y del navegador (las correcciones de seguridad existen porque alguien las publicó: no posponerlas es gratis), **bloqueo de pantalla automático** (el café y la recepcionista tienen diez segundos con tu sesión abierta), disco cifrado en laptops que salen de la oficina, y nada de cuentas de correo personales para asuntos de la empresa: esa cuenta no la protege la empresa, la proteges tú, y te la llevas cuando te vas.

Nadie recuerda la empresa que invirtió en el muro más alto; todos recuerdan la que cerró la puerta que estaba abierta.

— Lumbre · Empresa

Los cinco hábitos, su costo y su efecto

Hábito	Qué cierra	Tiempo de instalar
Gestor de contraseñas	El efecto dominó de credenciales repetidas	Una tarde
Doble factor en correo, banco y portal fiscal	El secuestro de cuenta con contraseña robada	Cinco minutos por servicio
Accesos por rol y retiro al salir	La puerta que dejó abierta un extrabajador	Una revisión trimestral
Actualizaciones automáticas	Los agujeros ya corregidos y sin parchear	Automático, una vez configurado
Bloqueo de pantalla y disco cifrado	El acceso físico a quien pasa por tu escritorio	Una política de equipo

1. Clasifica cada medida según el hábito al que pertenece:

Elementos:

- Una contraseña larga y distinta para cada servicio, guardada en un gestor
- Confirmar con la aplicación del teléfono además de la contraseña
- Retirar el acceso al banco el día que alguien deja la empresa
- Dar a cada puesto solo los permisos que su función necesita
- Usar un código de un solo uso generado por otra aplicación

Credenciales	. . .
Doble factor	. . .
Control de accesos	. . .

2. La cuenta de correo de la empresa usa el mismo número de celular para el doble factor y para los códigos de recuperación de la contraseña. ¿Cuál es el riesgo real de esa configuración?

- ☐ Ninguno: el doble factor siempre protege
- ☐ Que quien controle ese número (por ejemplo con una SIM clonada) puede recuperar la contraseña y saltarse el segundo paso
- ☐ Que el teléfono se queda sin batería
- ☐ Que el correo llega lento

3. Una contraseña muy larga pero usada en todos los servicios es tan segura como una contraseña distinta por servicio.

- ☐ Verdadero
- ☐ Falso

4. Esta semana, haz el inventario de tus cinco accesos críticos (correo principal, banca en línea, portal del SAT, facturación, red social de la marca). Para cada uno: ¿la contraseña es única?, ¿hay doble factor?, ¿quién más tiene acceso? Instala primero el que esté más expuesto y anota la fecha en que terminaste los cinco.

El orden correcto suele ser: correo primero (porque recupera todo lo demás), después banca y SAT.

Para dominar este tema

Lo esencial que debes saber

- Credenciales únicas y largas en un gestor: corta el efecto dominó de una filtración.
- Doble factor en las tres puertas que más duelen: correo, banca y portal fiscal.
- Que el segundo factor y la recuperación no dependan del mismo número sin protección en la línea.
- Accesos por rol con retiro el día que alguien sale o cambia de puesto.
- Actualizaciones automáticas, bloqueo de pantalla y disco cifrado: el equipo que se cuida solo.

Preguntas clave del tema

1. ¿Por qué la contraseña repetida es un riesgo en cascada?
2. ¿En qué accesos críticos es innegociable el doble factor?
3. ¿Qué falla convierte el doble factor en cartón?
4. ¿Cómo se gobiernan los accesos por rol y las salidas?
5. ¿Qué hábitos de equipo se configuran una vez y trabajan solos?

Lo que debes poder hacer

- Instalar un gestor de contraseñas y renovar los accesos críticos.
- Activar doble factor en correo, banca y portal fiscal con la línea protegida.
- Conducir una revisión trimestral de accesos y el retiro inmediato al salir alguien.

ACTIVIDAD INTERACTIVA DISPONIBLE EN
LUMBRE

5. Chequeo: la llanería en orden



Siguiente: *Respaldo que sí rescata: la prueba que casi nadie hace* — la regla tres dos uno, qué respaldar, dónde guardarlo y por qué un respaldo sin prueba de recuperación es una superstición con disco.

Referencia curricular

Materia:

Ciberseguridad esencial para PyME

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



<https://empresa.lumbre.lat/object/emp-ted-c33-m02-0a01>

Material educativo generado desde Lumbre · lumbre.lat