AKBAL

GUÍA PARA PYMES

5 errores de ciberseguridad que cuestan dinero

Una guía práctica, sin tecnicismos, para dueños y gerentes que necesitan proteger su negocio sin convertirse en expertos en seguridad.

5	Acciones	Akbal
errores frecuentes	concretas por error	Cybersecurity

I INTRODUCCIÓN

La seguridad no es un lujo de las grandes empresas

Las pequeñas y medianas empresas suelen pensar que no son un objetivo interesante para un atacante. En la práctica ocurre lo contrario: los atacantes automatizan sus ataques y prueban miles de negocios buscando la puerta más fácil de abrir, no la más valiosa.

La mayoría de los incidentes que vemos en PYMEs no son ataques sofisticados de un grupo experto. Son consecuencia de errores comunes, conocidos y evitables: una contraseña reutilizada, un sistema sin actualizar, un respaldo que nunca se probó, un empleado que no sabía identificar un correo falso.

Esta guía describe los cinco errores que más veces encontramos al evaluar la seguridad de negocios de este tamaño, el impacto real que tienen en la operación y el dinero del negocio, y qué hacer en su lugar — con acciones que puedes empezar a implementar esta misma semana, sin presupuesto de empresa grande.

> *"El objetivo de esta guía no es asustarte. Es darte el mismo criterio con el que nosotros evaluamos un negocio, para que puedas priorizar con claridad."*

01 ERROR FRECUENTE

Contraseñas débiles y sin doble factor

Reutilizar la misma contraseña en el correo, el banco y los sistemas del negocio, y no activar la verificación en dos pasos donde está disponible.

POR QUÉ CUESTA DINERO

Cuando una contraseña se filtra en cualquier otro servicio (algo fuera de tu control), un atacante la prueba automáticamente contra el correo y los sistemas del negocio. Si funciona, puede desviar pagos, leer contratos confidenciales o bloquear el acceso a tus propias cuentas hasta que pagues un rescate.

✓ QUÉ HACER EN SU LUGAR

- Activa la verificación en dos pasos (MFA) en correo, banca y cualquier sistema que la ofrezca — es gratis y toma minutos.
- Usa un gestor de contraseñas para el equipo, para que nadie reutilice ni anote contraseñas en post-its o en el chat.
- Exige contraseñas únicas y largas para cuentas administrativas (correo, dominio, hosting, banca empresarial).
- Revisa y elimina accesos de exempleados el mismo día que dejan la empresa.

02 ERROR FRECUENTE

Sistemas y software sin actualizar

Posponer las actualizaciones de Windows, del sitio web, del router o de las aplicaciones del negocio "porque interrumpen el trabajo".

POR QUÉ CUESTA DINERO

Cada actualización de seguridad corrige fallas ya conocidas públicamente. Un sistema sin actualizar es una puerta con la cerradura rota y el aviso pegado en la puerta: los ataques automatizados escanean internet buscando exactamente esas versiones vulnerables, sin necesidad de un atacante humano dedicado a tu negocio.

✓ QUÉ HACER EN SU LUGAR

- Activa actualizaciones automáticas en equipos, sitio web (CMS y plugins) y dispositivos de red.
- Define una ventana fija al mes para revisar y aplicar actualizaciones que no se instalan solas.
- Da de baja software y plugins que ya no uses — cada uno es una puerta adicional que hay que vigilar.
- Prioriza actualizar lo expuesto a internet (sitio web, VPN, correo) antes que lo que solo usa la red interna.

03 ERROR FRECUENTE

Respaldos que nunca se prueban

Tener un respaldo automático configurado, pero nunca haber intentado restaurarlo para confirmar que realmente funciona.

POR QUÉ CUESTA DINERO

El momento en que más se necesita un respaldo — después de un ransomware, un error humano o una falla de hardware — es el peor momento para descubrir que el respaldo lleva meses fallando en silencio, que no incluye lo que realmente importa, o que también fue cifrado por estar conectado a la misma red.

✓ QUÉ HACER EN SU LUGAR

- Mantén al menos una copia de respaldo desconectada de la red o en un proveedor separado (offline u offsite).
- Programa una restauración de prueba real cada trimestre, no solo la revisión del log de "respaldo exitoso".
- Define por escrito qué información es crítica y cada cuánto se respalda — no todo necesita la misma frecuencia.
- Calcula cuánto tiempo tardarías en operar de nuevo con ese respaldo; si no lo sabes, aún no está listo.

04 ERROR FRECUENTE

Equipo sin capacitación básica

Asumir que la seguridad es "cosa de sistemas" y que el resto del equipo no necesita saber reconocer un intento de fraude.

POR QUÉ CUESTA DINERO

La mayoría de los incidentes que terminan en pérdida de dinero no entran por una falla técnica, sino por una persona: un correo que parece del director pidiendo una transferencia urgente, una llamada que suplanta a soporte técnico, un enlace que parece de un proveedor conocido. Ninguna herramienta reemplaza a un equipo que sabe reconocer la señal de alerta.

✓ QUÉ HACER EN SU LUGAR

- Establece un segundo canal de verificación obligatorio para cualquier cambio de datos bancarios o transferencia inusual (una llamada, no solo un correo).
- Capacita al equipo al menos una vez al año con ejemplos reales de phishing y vishing dirigidos a su industria.
- Define a quién reportar un correo o llamada sospechosa, y celebra que lo reporten aunque sea falsa alarma.
- Haz simulacros controlados de phishing para medir el riesgo real, no el que se supone que hay.

05 ERROR FRECUENTE

No tener un plan cuando algo sí pasa

No haber definido, antes de que ocurra un incidente, quién decide qué, a quién se llama primero y qué se apaga o desconecta.

POR QUÉ CUESTA DINERO

En un incidente real, las primeras horas son las que determinan si el daño se contiene o se extiende. Sin un plan, ese tiempo se pierde decidiendo a quién llamar, quién autoriza qué, y si conviene pagar un rescate — decisiones que deberían tomarse con calma, no bajo presión y con el reloj corriendo.

✓ QUÉ HACER EN SU LUGAR

- Escribe un plan corto (una página basta) con contactos clave: quién decide, a quién se llama (interno y externo), y los primeros 3 pasos.
- Ten a la mano el contacto de un proveedor de respuesta a incidentes antes de necesitarlo, no durante la crisis.
- Define criterios simples para saber cuándo desconectar un equipo de la red en lugar de "esperar a ver si se resuelve solo".
- Revisa el plan una vez al año o después de cualquier cambio importante en tus sistemas.

✓ RESUMEN

Tu checklist de los 5 errores

Imprime esta página o compártela con tu equipo. Marcar "sí" en las cinco no te hace inmune, pero elimina la mayoría de los incidentes que vemos en negocios de tu tamaño.

1

MFA activo

Correo, banca y sistemas clave con doble factor.

2

Todo actualizado

Equipos, sitio web y red sin versiones vencidas.

3

Respaldo probado

Restauración verificada este trimestre.

4

Equipo capacitado

Saben reconocer y reportar un fraude.

5

Plan por escrito

Contactos y primeros pasos ante un incidente.

¿Cuántas de las cinco tienes cubiertas?

Un diagnóstico gratuito de 30 minutos te dice exactamente dónde estás y qué priorizar primero.

Solicitar diagnóstico

akbalcybersecurity.com · contacto@akbalcybersecurity.com · 55 4165 8022