QBIT

INGENIERÍA DE RESULTADOS

GUÍA PRÁCTICA PARA GERENTES DE MICRO Y PEQUEÑA EMPRESA

Cómo proteger tu negocio de la ciberdelincuencia (sin ser experto en tecnología)

No necesitas ser una gran empresa para ser un objetivo. Al contrario. Aquí están las puertas por donde entran los delincuentes —y cómo cerrarlas.

> **“Si tú no ganas, nosotros tampoco.”**
> *No es suerte. Es sistema.*

A los delincuentes ya no les interesa solo tu caja. Les interesa tu información.

Existe un mito peligroso en las micro y pequeñas empresas: *“soy muy chico para que me ataquen”*. Es exactamente al revés. Los ciberdelincuentes prefieren a los negocios pequeños precisamente porque manejan dinero e información valiosa, pero casi no invierten en protegerse. Eres el objetivo fácil.

Un ciberataque a una MYPE rara vez es una película de hackers. Es algo mucho más cotidiano: un código que compartes sin darte cuenta, un correo que parece de tu banco, una cuenta bancaria cambiada en una factura. Y el daño no es solo la plata robada: es la paralización, los clientes estafados en tu nombre y la confianza que cuesta años reconstruir.

> **La verdad incómoda**
> La mayoría de los ataques no buscan a las empresas más grandes, sino a las más desprotegidas. No te atacan por importante: te atacan por fácil.

Las 5 puertas abiertas por donde entra la ciberdelincuencia

1. El secuestro de tu WhatsApp

Recibes un mensaje que parece de soporte o de un conocido pidiéndote “un código que te llegó por error”. Lo compartes… y pierdes tu WhatsApp. Con él, los delincuentes escriben a tus clientes y proveedores haciéndose pasar por ti para pedirles dinero o datos.

2. Correos y enlaces falsos (phishing)

Un correo que aparenta ser de tu banco, de SUNAT o de un proveedor te pide “verificar tus datos” o “pagar una factura”. Un solo clic en el enlace equivocado puede entregarles tus contraseñas o instalar algo dañino en tu equipo.

3. Estafas de transferencia y facturas alteradas

Te llega la factura de siempre, pero con el número de cuenta cambiado. O un “proveedor” te apura para que pagues a una cuenta nueva. Pagas de buena fe… al delincuente. Es una de las estafas que más dinero mueve y casi nadie la ve venir.

4. Contraseñas débiles y accesos compartidos

La misma clave para el correo, la banca y las redes; sin verificación en dos pasos; y varias personas usando los mismos accesos. Cuando un empleado se va —o una clave se filtra— tienes todas las puertas abiertas a la vez.

5. Sin respaldos ni control de tu información

Un equipo que se malogra, un archivo que alguien borra, un programa que “secuestra” tu información y pide rescate. Si no tienes copias de seguridad, un solo incidente puede borrar años de trabajo en minutos.

Cómo cerrar cada puerta

La buena noticia: la mayoría de ataques a una MYPE se previenen con medidas simples y disciplina, no con tecnología cara.

Puerta abierta	Cómo cerrarla
Secuestro de WhatsApp	Activa la verificación en dos pasos y nunca compartas códigos que te lleguen.
Correos y enlaces falsos	Desconfía de las urgencias; verifica por otro canal antes de hacer clic.
Facturas y cuentas alteradas	Confirma por teléfono todo cambio de cuenta bancaria de un proveedor.
Contraseñas y accesos	Claves distintas y fuertes, doble factor y un acceso por persona.
Pérdida de información	Copias de seguridad automáticas y periódicas, guardadas en otro lugar.

El costo real de un ciberataque

El daño casi nunca es solo el dinero que se llevan. Es todo lo que se detiene y lo que se rompe alrededor.

> **EJEMPLO CON NÚMEROS**
> Secuestran el WhatsApp de tu negocio un viernes.
> 2 días sin poder atender ni vender por tu canal principal.
> Varios clientes “compran” a un estafador que se hace pasar por ti → pérdidas y reclamos.
> Semanas recuperando la cuenta y la confianza. El robo directo fue lo más barato de todo.

Autodiagnóstico: ¿qué tan expuesto está tu negocio?

Cada afirmación verdadera hoy es una puerta abierta esperando a que alguien entre.

1	Uso la misma contraseña para varias cuentas del negocio.
2	No tengo activada la verificación en dos pasos en WhatsApp, correo y banca.
3	Varias personas comparten los mismos usuarios y claves.
4	No hago copias de seguridad periódicas de mi información.
5	No estoy seguro de saber reconocer un correo o enlace falso.

> **Cómo leerlo**
> 0–1: tienes una base sana; mantén la disciplina.
> 2–3: hay puertas abiertas; un incidente es cuestión de tiempo.
> 4–5: tu negocio está muy expuesto. La prioridad es blindarlo antes de que pase algo.

La seguridad no es un producto. Es un sistema.

Aquí está la clave: la ciberseguridad **no es un programa que instalas una vez y te olvidas**. Los delincuentes cambian de táctica todo el tiempo; la protección tiene que ser continua. Por eso funciona como un sistema, no como una compra puntual:

- Diagnóstico de riesgos: saber por dónde te pueden entrar antes de que lo intenten.
- Capacitación de tu equipo: la mayoría de ataques entra por una persona, no por una máquina.

- Blindaje de accesos: contraseñas, doble factor y permisos ordenados.
- Monitoreo y acompañamiento continuo: alguien atento y un plan para reaccionar si algo pasa.

Da el siguiente paso con QBIT

En QBIT la ciberseguridad no es un software que te vendemos: es un sistema de prevención integral que te acompaña —diagnóstico, capacitación, blindaje de accesos y monitoreo continuo— para que un ciberataque no paralice ni ponga en riesgo tu negocio.

Agenda tu diagnóstico sin costo

En 45 minutos identificamos las tres mayores oportunidades de crecimiento en tu negocio —con números concretos, no con promesas.

WhatsApp: +51 947 466 827
Email: info@qbit.com.pe · **Web:** qbit.com.pe

No es suerte. Es sistema.