[Muestra · paretoseries]

Ciberseguridad para tu negocio

El 20% que te protege de las estafas y el desastre

Muestra — Introducción y las estafas reales

NODEVELOP · MMXXVI · MUESTRA

PRINCIPIO PARETO · GUÍA PRÁCTICA

El mejor momento

Durante décadas, la tecnología fue territorio de especialistas. Automatizar era caro, tener presencia en internet tomaba meses, y la inteligencia artificial era ciencia ficción. Eso terminó. Hoy las mismas herramientas que usan las grandes empresas están al alcance de cualquier persona con un negocio y ganas de hacerlo crecer.

No necesitas permiso ni un título. Necesitas decidirte a probar. Los negocios que crecen no son los que más saben de tecnología: son los que se atreven a usarla antes que el resto. Cada tarea que automatizas, cada proceso que digitalizas, cada hora que recuperas, se acumula a tu favor.

Esta guía existe para eso: para que empieces hoy, con lo que ya tienes, y veas el resultado el mismo día. Y el primer paso es dejar tu negocio protegido, esta misma semana.

Introducción

A una PYME no la atacan como en las películas. No hay un hacker encapuchado tecleando a oscuras para entrar a tu sistema. Lo que de verdad pasa es mucho más simple y mucho más común: te llega un correo que parece de tu banco, un WhatsApp que parece de un proveedor con "los datos nuevos para el pago", una factura falsa, un link que no deberías haber abierto. Y alguien, sin saberlo, hace clic o transfiere.

Eso es lo que le pasa a los negocios reales. No es ciencia ficción: es una estafa bien hecha. Y la buena noticia es que **protegerte de lo que de verdad te va a pasar no requiere ser experto ni gastar una fortuna.** Requiere unos pocos hábitos y configuraciones que puedes dejar listas esta semana.

Esta guía no es para asustarte

El marketing de seguridad vive del miedo: amenazas terribles, todo es urgente, compra esto ya. Aquí no. Vamos a lo práctico: cuáles son los riesgos *reales* de un negocio pequeño y qué haces, paso a paso, para cubrirlos. Sin alarmismo y sin tecnicismos.

Para quién es

Para dueños de negocio y emprendedores **que usan correo, banco en línea y WhatsApp para su negocio**. Ya tienes lo que hace falta: esta guía es para ti.

Qué vas a poder hacer

- Reconocer las estafas que más le llegan a una PYME, antes de caer.

- Proteger tus cuentas clave (correo, banco, redes) para que no te las roben.
- Tener respaldos que te salven si pierdes un equipo o te llega un virus.
- Manejar los datos de tus clientes con responsabilidad.
- Saber qué hacer, con calma, si algo pasa.
- Dejar tu negocio cubierto con una **checklist** que marcas en una tarde.

Qué NO es

Te deja cubierto frente a los riesgos reales de un negocio pequeño —el **20% que previene el 80% de los problemas**— sin montajes de empresa grande (servidores, equipos de seguridad, normas técnicas). Para eso, cuando crezcas, habrá especialistas.

El piso mínimo (honesto)

Necesitas tus cuentas (correo, banco, redes), un teléfono, un computador y un par de tardes para dejar todo configurado. Algunas herramientas que recomendamos son gratis; otras cuestan poco. Nada caro.

Cómo leerlo

Lee la Sección 1 sí o sí: las estafas son el riesgo número uno y lo más urgente. Después sigue en orden; cada sección deja una parte de tu negocio protegida. La Sección 7 es la checklist para que no se te escape nada.

✕ LO QUE NO HACER

Pensar “a mí no me va a pasar, soy un negocio chico”. Justamente los negocios chicos son el blanco favorito: tienen menos defensas y el estafador lo sabe. No te atacan por grande ni por importante; te atacan porque es fácil. La buena noticia es que dejar de ser fácil toma poco.

Sección 1 — Las estafas que de verdad te van a llegar

Si solo lees una sección, que sea esta. La gran mayoría de los problemas de una PYME no entran por un fallo técnico: entran por un mensaje que engaña a una persona. Conocer las estafas comunes y una sola regla de verificación te cubre de casi todas.

Las que más le llegan a un negocio

El correo o SMS que imita a tu banco o a una plataforma. "Detectamos un movimiento sospechoso, verifica tu cuenta aquí." El link lleva a una página idéntica a la real, pero falsa. Escribes tu clave y se la entregas al estafador. *Tu banco nunca te pide la clave por correo, SMS ni WhatsApp.*

El cambio de datos bancarios de un proveedor. Te llega un correo (a veces desde una cuenta muy parecida a la real) diciendo "cambiamos de banco, paga a esta cuenta nueva". Pagas… al estafador. Es de las estafas que más dinero le cuesta a las PYMES.

La suplantación del jefe o del dueño. "Hola, estoy en una reunión, necesito que transfieras [monto] urgente a este proveedor, después te explico." Viene con urgencia y autoridad para que no preguntes.

El "ejecutivo del banco" por teléfono o WhatsApp. Te llama alguien muy amable que "detectó un problema" y necesita que le confirmes un código que te acaba de llegar, o que apruebes algo en la app. Ese código es justo lo que le falta para entrar a tu cuenta.

El premio, la oferta o el archivo inesperado. Ganaste algo que no jugaste, una oferta irresistible, una factura o foto adjunta que no esperabas. El link o el archivo trae el problema.

Las señales de alarma

Casi todas las estafas tienen una o más de estas marcas:

- **Urgencia.** “Paga ahora”, “tu cuenta se cierra hoy”, “es urgente”. El apuro es para que no pienses.
- **Te piden una clave, un código o una transferencia.** Nadie legítimo te pide tu contraseña.
- **El remitente no calza.** Un correo de “tu banco” que viene de una dirección rara, o un número desconocido.
- **El link no corresponde.** El texto dice una cosa, pero la dirección real es otra.
- **Demasiado bueno (o demasiado malo) para ser verdad.**
- **Algo se siente raro.** Hazle caso a esa sensación.

Cómo se ven en la práctica

No hay nada como ver una de cerca. Estos son tres mensajes-estafa típicos. Léelos buscando las señales de alarma.

1. El “banco” por correo:

```
De: Seguridad BancoChile <alertas@bancochile-
seguridad.net>
Asunto: ⚠️ Tu cuenta será bloqueada en 24
horas

Estimado cliente, detectamos un acceso no
autorizado. Para
evitar el bloqueo de tu cuenta, verifica tu
identidad ahora:

   >> Verificar mi cuenta <<
```

```
Si no validas en 24 horas, tu cuenta será
suspendida.
```

Lo que delata: el remitente no es el dominio real del banco (`bancochile-seguridad.net`, no `bancochile.cl`), la urgencia ("24 horas"), y que te manda a "verificar" por un link. Tu banco no opera así.

2. El proveedor que "cambió de cuenta":

```
De: Juan Pérez <juan.perez@proveedor-
insumos.com>
Asunto: Cambio de datos para el pago de la
factura

Hola, te cuento que cambiamos de banco. Para
la factura
pendiente, por favor transfiere a nuestra
cuenta nueva:

   Banco: ...
   Cuenta: ...
   Titular: Comercial Insumos SpA

Gracias, quedo atento.
```

Lo que delata: un cambio de datos bancarios *siempre* hay que confirmarlo por teléfono al número de siempre del proveedor. Aunque el correo parezca real, la cuenta puede ser del estafador (a veces incluso entran al correo del proveedor de verdad).

3. El "jefe" por WhatsApp:

```
Hola, ¿estás? Estoy en una reunión y no puedo
llamar.
Necesito que hagas una transferencia urgente a
un
proveedor, es para cerrar un trato hoy.
¿Puedes? Te paso
los datos. No alcanzo a explicarte ahora,
después te cuento.
```

Lo que delata: número desconocido (o un perfil nuevo con la foto del jefe), urgencia, autoridad y la excusa de "no puedo hablar ahora" para que no verifiques. Llámalo tú, por donde siempre le hablas.

La regla de oro: verifica por otro canal

Antes de hacer clic en un link, abrir un adjunto inesperado o transferir dinero por un mensaje, **confirma por un canal distinto al del mensaje.**

- ¿Un proveedor "cambió de cuenta"? Llámalo a su número de siempre (no al que viene en el correo) y confírmalo.
- ¿Tu "jefe" pide una transferencia urgente? Escríbele o llámalo tú, por donde siempre le hablas.
- ¿Tu "banco" detectó algo? Entra a la app o llama al número del reverso de tu tarjeta, nunca por el link del mensaje.

Treinta segundos de verificación evitan la pérdida. El estafador apuesta a que el apuro te gane; la regla de oro le quita esa ventaja.

Y siempre

- **Nunca entregues claves ni códigos** a nadie, por ningún canal. Son tuyas.

- **No hagas clic por curiosidad.** Si dudas, no abras.
- **Mira la dirección real del link** antes de entrar (en el computador, deja el cursor encima sin hacer clic; verás la dirección verdadera).

✕ LO QUE NO HACER

Actuar apurado porque el mensaje dice que es urgente. La urgencia es la herramienta principal del estafador: te empuja a hacer clic o pagar antes de pensar. Ninguna operación legítima se cae por esperar cinco minutos a que verifiques. Ante la urgencia, frena: es justo la señal de que algo huele mal.

Esto es una muestra

Acabas de leer la introducción y la sección más importante —las estafas que de verdad le llegan a una PYME—. La guía completa continúa con:

- **Tus llaves: contraseñas y doble factor.**
- **Respaldos: tu seguro contra el desastre.**
- **Protege tus cuentas y dispositivos.**
- **Los datos de tus clientes** (y la Ley 19.628).
- **Si te pasa algo: qué hacer**, con calma.
- **La checklist de seguridad de tu negocio** — todo en una lista para marcar.

Consíguelo en paretoseries.com