

GUÍA DE SEGURIDAD

Protegé el WhatsApp de tu empresa

Cómo evitar el robo de cuentas, cómo trabajar con aplicaciones de terceros sin riesgo y qué hacer si ya pasó.



En Paraguay se repiten los robos de cuentas de WhatsApp. **Casi nunca se “hackea” la aplicación:** se engaña a una persona para que entregue su acceso. Para una empresa, perder el número es perder la atención al cliente y la confianza de quienes escriben.



Regla de oro: nadie de WhatsApp, de la operadora ni de la empresa te pide el código de 6 dígitos. Si alguien lo pide —por llamada, mensaje o “por error”— es un intento de robo.

1 CÓMO TE ROBAN LA CUENTA

Código de verificación

Piden el código de 6 dígitos haciéndose pasar por soporte, la operadora o un contacto.

Dispositivo vinculado

Te hacen escanear un QR o ingresar un código y quedan dentro, como WhatsApp Web.

Línea o buzón de voz

Cambio de SIM, o una llamada de verificación que cae en un buzón sin PIN.

Herramienta de terceros

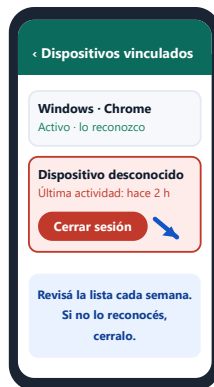
Paneles y extensiones por QR: quien entra a ellos, o los infecta, tiene la cuenta.

2 QUÉ HACER EN CADA NÚMERO



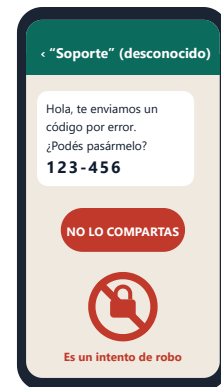
Activá el PIN

Ajustes > Cuenta > Verificación en dos pasos
Cargá también un correo de recuperación con su propio 2FA.



Revisá cada semana

Ajustes > Dispositivos vinculados
Cerrará sesión en todo lo que no reconozcas. Nunca escanees un QR que te envíe otra persona.



No compartas códigos

Ejemplo de mensaje falso
Nadie legítimo te lo pide, ni siquiera “por error”.

✓ **Buzón de voz:** ponele PIN a la línea.

✓ **Operadora:** pedí bloqueo de cambio de SIM y de portabilidad.

✓ **Personal:** todos deben conocer la regla de oro.

3 CUENTAS CORPORATIVAS Y APLICACIONES DE TERCEROS

Número propio de la empresa

Línea a nombre de la empresa, no del celular de un empleado, y con **dos responsables** que conozcan la recuperación.

API oficial de WhatsApp Business

Preferila a las herramientas con QR o no oficiales: no hay sesión que robar y se evita el riesgo de que Meta bloquee el número.

Exigí al proveedor

2FA, **usuarios nominales por agente**, registro de quién hizo qué y baja inmediata cuando alguien se va.

Protegé el acceso central

Meta Business Manager con 2FA y pocos administradores. Tokens en un gestor de secretos, no en chats ni planillas.

SI YA TE ROBARON LA CUENTA

1. **Volvé a registrar** tu número con el código por SMS: eso desconecta al atacante.
2. Si puso su propio PIN, esperá hasta **7 días** y escribí a soporte desde la app.
3. **Avisá a clientes y contactos** para que no paguen ni den datos por esa cuenta.
4. Cambiá la clave del correo vinculado, revisá dispositivos y **denunciá al CERT-PY** (Mitic) y a la policía.