

Guía de ciberseguridad para tu operación

QUÉ TE ATAQA Y CON QUÉ SE ATAQA · SEIS MEDIDAS PARA PALOMEAR · LO QUE NUNCA HAY QUE HACER

Un ransomware no te roba dinero: te roba diez años de pruebas.

No es un tema de tecnología: es un tema de prueba. El **art. 95 Bis LGOAAC** te obliga a conservar la información **al menos diez años**; el **art. 49 del Código de Comercio**, a conservarla **íntegra e inalterada**. El día del ataque pierdes la operación y la defensa: la obligación sigue siendo tuya aunque el ataque sea de otro.

8 ciberataques al sistema financiero a mayo de 2026
El doble que en todo 2025.
BANXICO

Qué te ataca y con qué se ataja

AMENAZA → CONTROL

LA AMENAZA	QUÉ TE HACE A TI	EL CONTROL QUE LA ATAQA
01 · BEC El correo del falso jefe business email compromise	Un correo que parece del dueño, del corresponsal o del proveedor pide una transferencia urgente o el cambio de una cuenta. El dinero sale con una orden que parecía legítima y en tu bitácora queda como operación autorizada.	→ MFA y contraseñas administradas. Con doble factor, una clave robada no basta para entrar al correo. Y ninguna instrucción de pago o cambio de cuenta se ejecuta sin confirmarla con la persona por otra vía — al número que ya tenías, no al del correo —, dejando constancia.
02 · RANSOMWARE El secuestro de tus datos cifrado y extorsión	Cifra tus expedientes, tus bitácoras y tus acuses, y te pide rescate. No te quita el dinero del día: te quita los diez años de pruebas que estás obligado a conservar.	→ Respaldo cifrado fuera de sitio y WORM con hash. La copia vive en otra bodega, cifrada, donde el ataque no la alcanza: con ella restauras . Y como el WORM se escribe una vez y no se altera y el hash delata cualquier cambio, además demuestras que lo restaurado es lo mismo.
03 · DEEPFAKE El rostro que no existe identidad generada	Un rostro o una voz generados pasan por un cliente real en una identificación a distancia, o por tu jefe en una videollamada. Tu expediente queda con los datos de alguien que nunca estuvo ahí, y lo firmaste tú.	→ Equipo de captura blindado y prueba de vida. La captura se hace en la máquina crítica, aislada y actualizada, con validación de prueba de vida —que verifica que hay una persona viva frente a la cámara—: la regulación bancaria ya la exige. Toda autorización sensible se confirma con la persona.

Seis medidas alcanzables. Ninguna requiere consultor.

PALÓMEALAS

☐ MFA (doble factor) Segunda contraseña temporal en cada acceso: aunque roben la clave, no entran.	☐ Contraseñas administradas Nada de claves compartidas ni en un post-it; un gestor por persona.
☐ Respaldo cifrado fuera de sitio Copia de todo en otra bodega, cifrada, que un ataque no pueda tocar.	☐ Equipo de captura blindado La máquina crítica, aislada y actualizada, solo para lo esencial.
☐ Almacenamiento WORM + hash Se escribe una vez y no se altera; el hash delata cualquier cambio.	☐ Plan de incidentes (1 pág.) Qué hacer el día malo, escrito antes de que pase.

EL VACÍO JUEGA A TU FAVOR Para CC/TD aún no hay un régimen de ciber como el de bancos: **adoptarlo es señal de diligencia y ventaja.**

Nunca hagas esto

LOS TRES NUNCA

- 01** **Compartir claves.** Una contraseña que usan tres personas no identifica a nadie. El día que pregunten quién capturó, quién cerró esa alerta o quién autorizó ese pago, tu bitácora no tiene respuesta: **sin usuario propio no hay autor, y sin autor no hay prueba.**
- 02** **El respaldo en la misma máquina.** Si la copia vive en el mismo equipo, en la misma red o en la carpeta que todos ven, **el ataque que se lleva la operación se lleva también el respaldo:** es el mismo archivo dos veces.
- 03** **Pagar el rescate sin asesoría.** Pagar no garantiza que recuperes tus archivos ni que el atacante no conserve copia de los datos de tus clientes, y puede abrirte **responsabilidades adicionales por el destino de ese dinero.** Se decide con asesoría legal, no en caliente.

FUNDAMENTO

Conservación: art. 95 Bis LGOAAC, al menos diez años; art. 49 del Código de Comercio, diez años íntegros e inalterados — un ataque que cifra o altera tus registros golpea exactamente esa obligación. · **NOM-151-SCFI-2016:** no es obligación directa del 95 Bis; se adopta por conveniencia probatoria — el prestador de servicios de certificación sella la huella y la fecha, la autoría sigue siendo tuya. · **Acuerdo 115/2026** (DOF 7-ago-2026): rige Actividades Vulnerables por la vía SAT/UIF, **no aplica** a centros cambiarios ni a transmisores de dinero. · **Dato:** Banxico, ocho incidentes cibernéticos a mayo de 2026, el doble que en todo 2025.

I5 · v1.0 · agosto de 2026