10 reglas de oro para blindar tu tesorería corporativa ante fraudes

Recopilado por el Staff de El Inversionista

La digitalización ha hecho que la gestión de tesorería sea más rápida y eficiente, pero también exige que los protocolos de seguridad de tu empresa evolucionen. Cuando tu equipo financiero ejecuta la compra y venta de divisas para empresas o autoriza pagos de alto valor, un simple error humano puede comprometer la liquidez del negocio.

La Asociación de Bancos de México (ABM) ha emitido directrices fundamentales para la prevención de fraudes. En Banco BASE, con el respaldo de 40 años de experiencia protegiendo los recursos de empresas importadoras y exportadoras, han adaptado estas reglas al entorno corporativo para que operes tu Banca Digital con total certidumbre.

Control estricto de credenciales y accesos

El eslabón más vulnerable en cualquier estrategia de ciberseguridad suele ser
1. Intransferibilidad absoluta: El NIP, token y contraseñas de tus cuentas digitales son personales e intransferibles. Nunca deben compartirse entre miembros del equipo, ni siquiera por urgencia operativa.
2. No compartas datos sensibles por teléfono: Ningún ejecutivo llamará para pedirte claves, números de token o contraseñas para "desbloquear" tu banca en línea. Si recibes una llamada de este tipo, corta la comunicación y contacta a tu asesor de inmediato.
3. Renovación estratégica de contraseñas: Implementa políticas internas para que los usuarios autorizados cambien sus claves de acceso regularmente. Una contraseña de alta seguridad caduca, no debe repetirse y jamás debe ser predecible.

El entorno seguro para tus Operaciones Internacionales

Saber cómo hacer transferencias internacionales de forma eficiente sólo sirve si el canal por el que se ejecutan está protegido.
4. Cuidado con el Wi-Fi público: Evita acceder a tu banca digital desde redes públicas en aeropuertos, hoteles o cafés, ya que los atacantes pueden interceptar los datos. Utiliza siempre redes privadas, VPNs o datos móviles.
5. Verificación de dominios (El candado de seguridad): Las páginas clonadas son la principal herramienta para robar credenciales corporativas. Al entrar a tu portal de banca digital siempre escribe la URL oficial directamente en el navegador (debe comenzar con https://).
6. Cero clics a enlaces no solicitados: Un correo que exige "acción inmediata" sobre un supuesto bloqueo de cuenta y contiene un enlace directo, es una señal de alerta. Estos links pueden instalar software malicioso en los equipos de tu tesorería.
7. Apps estrictamente oficiales: Asegúrate de que tú y tu equipo descarguen nuestra aplicación únicamente desde las tiendas oficiales (App Store o Play Store).

Protocolos de validación y respuesta

Al evaluar cuáles son los mejores bancos para pagos internacionales, la capacidad tecnológica para monitorear y reaccionar es clave. Sin embargo, la última línea de defensa está en tu operación interna.
8. Activa las alertas en tiempo real: Configura las notificaciones por SMS o correo electrónico para cada movimiento de tu cuenta digital. La visibilidad inmediata permite una reacción oportuna ante cualquier anomalía.
9. Duda de la urgencia inusual: En el ámbito B2B, los fraudes no llegan como "premios", sino como correos de proveedores (suplantados) exigiendo pagos urgentes a cuentas nuevas. Si un escenario rompe tus procesos habituales o parece demasiado fácil, detén la operación y verifica por otro medio.
10. El filtro de la doble validación: Antes de ejecutar cualquier movimiento, aplica una validación interna cruzada: ¿Es realmente el proveedor quien solicita el cambio de cuenta? ¿Estoy en el sitio oficial? ¿Este pago fue autorizado en el comité?