SOFTWARE A MEDIDA

La Cuenta del Proveedor Es el Dato Más Delicado de Tu Sistema

El 20 de mayo de 2026, la Policía de Singapur advirtió sobre un fraude que se repite. Alguien escribe desde un correo que imita al de un proveedor, o desde el del proveedor ya comprometido, y avisa que sus datos bancarios cambiaron. La empresa paga la siguiente factura a la cuenta nueva. Desde el 1 de enero se habían denunciado al menos 66 casos, con pérdidas de al menos 19 millones de dólares de Singapur.

La advertencia y sus recomendaciones están en el comunicado de la Policía de Singapur del 20 de mayo de 2026.
https://www.police.gov.sg/media-hub/news/2026/05/20260520_police_advisory_on_business_email_compromise_scams_involving_requests_to_update_vendors

En julio, la emisora estadounidense WFAE entrevistó a un periodista de The Wall Street Journal sobre Surfside Beach, un pueblo de Carolina del Sur que envió unos 545.000 dólares a una cuenta en Utah en vez de a su contratista. Según ese relato, alguien que se hacía pasar por el jefe de proyecto del contratista pidió una transferencia electrónica en lugar de un cheque, y el estafador había creado un dominio casi idéntico al del contratista. Ninguna de las dos partes lo notó durante 45 días, y las dos partes discrepan sobre dónde estuvo el fallo.

El caso está contado en la entrevista publicada por WFAE el 27 de julio de 2026.
https://www.wfae.org/business/2026-07-27/sc-beach-town-loses-500-000-in-phishing-scam

En enero, Unit 42, el equipo de investigación de la empresa de seguridad Palo Alto Networks, describió un caso de nómina en una organización que no identifica. Un atacante se hizo pasar por empleados ante varias mesas de ayuda, logró que le restablecieran contraseñas y le registraran de nuevo dispositivos de doble factor, y cambió la cuenta de depósito del salario de varias personas. Se supo cuando los empleados reclamaron que no les había llegado el pago.

Un Cambio de Cuenta Necesita Su Propio Flujo

En muchos sistemas, la cuenta bancaria es un campo más de la ficha. Quien puede corregir una dirección puede cambiar también el destino del dinero, y el siguiente lote de pagos usa el valor nuevo sin preguntar. Es mejor que el cambio abra una solicitud con estados (recibida, confirmada, aprobada, activa) y que, mientras tanto, los pagos sigan a la cuenta anterior o se detengan.

- No aceptes un cambio desde el hilo de correo o chat por el que llegó: confírmalo llamando a un número que ya estaba en la ficha.
- Exige que una segunda persona apruebe el cambio, y que no pueda ser quien lo cargó.
- Retén el primer pago a una cuenta nueva durante un plazo acordado, o limita su monto hasta que el proveedor confirme que lo recibió.
- Avisa del cambio al contacto anterior, por el correo y el teléfono que ya tenías registrados.
- Envía una alerta al dueño por cada cambio aprobado y por cada primer pago a una cuenta nueva.
- Guarda un historial visible de quién pidió, quién confirmó y quién aprobó, con fecha y con los datos enmascarados.

En Venezuela es común pagar a proveedores por transferencia, pago móvil o Zelle. En el pago móvil el destino es un teléfono, una cédula o RIF y un banco; en Zelle, un correo o un teléfono. Esos datos, y la cuenta de nómina de cada empleado, pasan por el mismo flujo. Supón que un proveedor te escribe por WhatsApp desde un número nuevo y pide el próximo pago móvil a otro teléfono. Registras la solicitud, llamas al número que ya tenías y el pago espera la aprobación de otra persona. Si el cambio es real, el proveedor espera un día.

Las Primeras Horas Deciden Cuánto Se Puede Recuperar

Según el informe anual del Internet Crime Complaint Center (IC3) del FBI, publicado en abril de 2026, en 2025 ese centro recibió 24.768 denuncias por compromiso del correo empresarial, con pérdidas declaradas de unos 3.046 millones de dólares, solo detrás del fraude de inversión. Son denuncias presentadas ante un organismo de Estados Unidos y no miden lo que pasa en otros países. Su equipo de recuperación actuó en 3.900 incidentes de varios tipos de fraude, no solo de este, y congeló unos 679 millones de dólares: según el FBI, una tasa de éxito del 58 por ciento. El consejo del informe es contactar de inmediato al banco para pedir que recupere los fondos, y saber de antemano qué ayuda ofrece, porque cada institución tiene sus políticas.

Las cifras y la recomendación están en el informe IC3 2025 del FBI, publicado en abril de 2026.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

- Llama al banco desde el que salió el pago, por su número oficial, con fecha, monto, referencia y cuenta de destino a mano.
- Bloquea en el sistema los pagos a ese beneficiario y revisa qué otros datos bancarios cambiaron en las últimas semanas.

- Avisa al proveedor o al empleado real por el contacto que ya tenías, nunca por el hilo de la solicitud.

- Conserva completos los correos y mensajes, sin borrarlos ni editarlos, y presenta la denuncia ante las autoridades.

Cómo lo Construimos en Software a Medida

Empezamos por el mapa del proceso: quién da de alta proveedores y empleados, por dónde llegan los cambios de cuenta, quién arma el lote de pagos y quién lo aprueba. Luego diseñamos el cambio de datos bancarios como un flujo con roles separados para cargar, confirmar y aprobar, y el servidor comprueba esos permisos aunque la pantalla oculte el botón. El historial registra cada paso con autor y fecha, y ningún rol de la aplicación puede editarlo. Si los pagos se exportan a un archivo del banco, la integración lee solo datos aprobados. Las pruebas automáticas intentan aprobar la propia solicitud, pagar antes de que termine la retención o cambiar una cuenta sin permiso, y comprueban que el sistema lo rechaza. Entregamos documentación, capacitación y una guía escrita de las primeras horas.

> *Estos controles reducen la probabilidad de pagar a una cuenta equivocada y acortan la reacción, pero no eliminan el fraude ni sustituyen la protección de los correos. Funcionan si el equipo los usa, y lo que se pueda recuperar depende del banco y del tipo de pago. Este artículo no es asesoría legal.*

Una Comprobación Concreta

Abre la lista de proveedores y empleados en tu sistema de pagos o en tu hoja de cálculo y busca cada cambio de cuenta bancaria, número de pago móvil o correo de Zelle de los últimos seis meses. Para cada uno, anota quién lo pidió, por qué canal llegó, quién lo cargó y si alguien lo confirmó llamando a un número que ya estaba registrado. Si el sistema no guarda historial, o si una misma persona puede pedir, cargar y pagar, ese es el primer punto que corregir. Revisa después en tu banca en línea qué usuarios pueden registrar beneficiarios nuevos. Solo consulta: no cambies nada durante la revisión.

Documentación de apoyo: Guía del National Business Crime Centre británico sobre el fraude con cambios de datos bancarios.
https://nbcc.police.uk/crime-prevention/cyber-and-fraud/bank-mandate-fraud

Para seguir leyendo: Antes de Dibujar Pantallas, Decide Quién Puede Cambiar Qué.
https://systems.kavaliero.com/blog/el-software-a-medida-empieza-por-los-permisos

Si necesitas ayuda con este trabajo, consulta el alcance de Software a Medida.
https://systems.kavaliero.com/soluciones/software-a-medida