AUDITORÍA CORPORATIVA

Qué Puede Hacer Tu Proveedor con el Acceso que Le Diste

Dos de los mayores robos de 2025 en el ecosistema de Pix, el sistema de pagos instantáneos de Brasil, no empezaron rompiendo la seguridad de un banco. En julio de 2025, la policía informó que un empleado de C&M Software, una de las empresas aprobadas por el Banco Central do Brasil para conectar instituciones financieras con sus sistemas, había vendido su acceso a delincuentes. La policía habló de más de 540 millones de reales robados a al menos una institución. Finsiders Brasil, en su balance de un año después, habla de más de 800 millones.

El caso de C&M lo recogió The Record el 7 de julio de 2025.
https://therecord.media/brazil-police-arrest-worker-theft

El 29 de agosto de 2025 le tocó a Sinqia, otro proveedor de tecnología del sistema. Según un comunicado de la propia empresa, basado en los resultados preliminares de su investigación forense, se procesaron en su entorno Pix unos 710 millones de reales en transacciones no autorizadas, hechas con credenciales legítimas de sus proveedores de tecnología. Sinqia cortó el acceso de esas credenciales. En ninguno de los dos casos hizo falta adivinar una contraseña: las llaves existían y estaban en manos de terceros.

El comunicado de Sinqia lo reprodujo Convergência Digital el 2 de septiembre de 2025.
https://convergenciadigital.com.br/mercado/sinquia-ataque-hacker-levou-cerca-de-r-710-milhoes-em-transacoes-b2b-nao-autorizadas/

Lo que Pidió Después el Banco Central Do Brasil

El 5 de septiembre de 2025, el Banco Central do Brasil limitó a 15.000 reales el valor de los Pix y TED de las instituciones de pago no autorizadas y de las conectadas a través de un proveedor de tecnología. El límite podría retirarse cuando ellas y su proveedor cumplieran los nuevos controles. Ese día publicó también la Resolución BCB 498, modificada en enero de 2026 por la Resolución 547. La política de seguridad de esos proveedores debe incluir control de acceso, trazabilidad de las transacciones, separación de entornos con acceso limitado al de producción, controles específicos para las integraciones con otras partes y vigilancia de credenciales y claves filtradas en internet. El control de acceso incluye revisar con frecuencia los permisos del personal tercerizado y exigir varios factores de autenticación para entrar desde fuera. La norma pide además un seguro que cubra fraude e incidentes de ciberseguridad.

La norma vigente está en la página de la Resolución BCB 498 del Banco Central do Brasil, con los

cambios de enero de 2026.
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=498

Según Finsiders Brasil, de los nueve proveedores de este tipo que operaban en septiembre de 2025, solo tres seguían activos en julio de 2026.

La reducción del mercado la contó Finsiders Brasil el 22 de julio de 2026.
https://finsidersbrasil.com.br/reportagem-exclusiva-fintechs/mercado-de-provedores-de-tecnologia-encolhe-apos-aperto-nas-regras-do-bc/

Quién Tiene Hoy Llaves de Tu Negocio

Los pagos en Venezuela no funcionan como Pix. La lección trata de las credenciales que un tercero tiene sobre tu dinero y tus sistemas. Piensa en el contador con usuario en la banca en línea, el técnico que entra por escritorio remoto, el desarrollador con acceso al servidor y a las claves de la pasarela de pago, el integrador del punto de venta, la agencia que administra Instagram y la cuenta publicitaria. Para cada uno, la pregunta es la misma: qué puede hacer hoy con ese acceso sin pedir permiso a nadie.

- Abre un registro de accesos de proveedores: quién, a qué sistema, con qué permiso (consultar, cargar o aprobar), desde cuándo y quién lo autorizó en la empresa.
- Sustituye los usuarios compartidos por cuentas a nombre de cada persona, para que cada acción quede atribuida a alguien concreto.
- Activa la verificación en dos pasos en todas las cuentas de terceros y, en la banca, separa a quien carga un pago de quien lo aprueba, con límites por operación.
- Limita cada acceso al alcance del trabajo y al tiempo que dura: el soporte remoto se activa para la sesión acordada y se desactiva al terminar.
- Confirma que cada sistema guarda registros que tú puedes leer y que sabes cortar cualquier acceso en minutos sin depender del proveedor.
- Revisa el registro cada trimestre y deja por escrito en el contrato el aviso de incidentes, la prohibición de compartir credenciales y la baja de accesos al terminar el servicio.

Cómo lo Revisamos en Auditoría y Pentesting Corporativo

Con un alcance escrito y autorizado, listamos a cada tercero que puede tocar dinero, datos de pago o cuentas del negocio: usuarios de la banca empresarial, claves de API de pagos, integradores, el soporte remoto del sistema administrativo y la agencia de redes. Para cada acceso registramos qué puede hacer, si exige segundo factor, si está a nombre de una persona o es compartido y cuándo se usó por última vez.

Las pruebas acordadas comprueban si una cuenta de proveedor puede salirse de su papel, por ejemplo crear usuarios o iniciar pagos cuando su función es solo consultar, y si las herramientas de acceso remoto quedan activas sin necesidad. Revisamos si un movimiento fuera de horario quedaría en los registros y quién lo vería. El informe ejecutivo explica cada hallazgo en términos de negocio, y el plan priorizado empieza por límites y doble aprobación en los pagos salientes. Cuando los cambios están hechos, verificamos que funcionan.

> *La revisión cubre los accesos incluidos en el alcance acordado y en una fecha. No puede evaluar la seguridad interna de cada proveedor ni garantizar que un tercero no actúe de mala fe. Las cláusulas de un contrato conviene redactarlas con un abogado: este artículo no es asesoría legal. Las cifras de pérdidas varían según la fuente y se citan con la suya.*

Una Comprobación Concreta

Elige el servicio que puede mover dinero, por ejemplo la banca en línea de la empresa, y abre su lista de usuarios sin cambiar nada. Anota a cada usuario que no sea de tu personal: contador, técnico, desarrollador o integrador. Para cada uno, anota si la cuenta está a nombre de una persona o es compartida, si solo consulta o también carga o aprueba pagos, si usa verificación en dos pasos y, si el servicio lo muestra, cuándo se usó por última vez. Una cuenta compartida, o un proveedor que puede aprobar un pago sin nadie más, es lo primero que conviene corregir.

Documentación de apoyo: Guía del NCSC británico para conocer el acceso que tienen tus proveedores.
https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security/understand-the-risks

Para seguir leyendo: Cuando Alguien Se Va, ¿Qué Accesos Se Quedan?.
https://systems.kavaliero.com/blog/cuando-alguien-se-va-que-accesos-se-quedan

Si necesitas ayuda con este trabajo, consulta el alcance de Auditoría y Pentesting Corporativo.
https://systems.kavaliero.com/soluciones/auditoria-pentesting