CORPORATE AUDIT

What Your Supplier Can Do with the Access You Gave Them

Two of Brazil's largest thefts of 2025 through the Pix ecosystem, the country's instant payment system, did not start by breaking into a bank. In July 2025, police said that an employee of C&M Software, one of the companies approved by the Banco Central do Brasil to connect financial institutions to its systems, had sold his access to criminals. Police said more than 540 million reais had been stolen from at least one institution. Finsiders Brasil, in its review a year later, gives a higher figure of more than 800 million.

The C&M case was reported by The Record on 7 July 2025.
https://therecord.media/brazil-police-arrest-worker-theft

On 29 August 2025 it was the turn of Sinqia, another technology provider in the system. According to the company's own statement, based on preliminary results of its forensic investigation, about 710 million reais in unauthorised transactions went through its Pix environment, made with legitimate credentials belonging to its IT suppliers. Sinqia cut off those credentials. Neither case required guessing a password: the keys existed, and third parties held them.

Sinqia's statement was carried by Convergência Digital on 2 September 2025.
https://convergenciadigital.com.br/mercado/sinquia-ataque-hacker-levou-cerca-de-r-710-milhoes-em-transacoes-b2b-nao-autorizadas/

What the Banco Central Do Brasil Asked for Next

On 5 September 2025, the Banco Central do Brasil capped Pix and TED transfers at 15,000 reais for unauthorised payment institutions and for those connected through a technology provider. The cap could be lifted once they and their provider met the new controls. The same day it published Resolution BCB 498, amended in January 2026 by Resolution 547. These providers' security policy must cover access control, transaction traceability, segregated environments with limited access to production, specific controls on integrations with other parties and monitoring for leaked credentials and keys online. Access control includes regular review of outsourced staff's permissions and multi-factor authentication for access from outside. The rule also requires insurance that covers fraud and cyber security incidents.

The current text of the rule is on the Banco Central do Brasil's page for Resolution BCB 498, with the January 2026 changes.
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=498

According to Finsiders Brasil, of the nine providers of this kind operating in September 2025, only three were still active in July 2026.

The shrinking market was reported by Finsiders Brasil on 22 July 2026.
https://finsidersbrasil.com.br/reportagem-exclusiva-fintechs/mercado-de-provedores-de-tecnologia-encolhe-apos-aperto-nas-regras-do-bc/

Who Holds Keys to Your Business Today

Payments in Venezuela do not work like Pix. The lesson concerns the credentials a third party holds over your money and your systems. Think of the accountant with a login to your online banking, the technician who connects by remote desktop, the developer with access to the server and the payment gateway keys, the point-of-sale integrator, the agency that runs your Instagram and ad account. The question is the same for each: what can they do today with that access, without asking anyone?

- Start a supplier-access register: who, which system, which permission (view, enter or approve), since when, and who in the business authorised it.
- Replace shared logins with accounts in each person’s name, so every action can be traced to someone specific.
- Turn on two-step verification for every third-party account and, in your banking, separate whoever enters a payment from whoever approves it, with limits per transaction.
- Limit each access to the scope of the work and the time it takes: remote support is switched on for the agreed session and off when it ends.
- Confirm that each system keeps logs you can read, and that you know how to cut off any access within minutes without relying on the supplier.
- Review the register every quarter, and put incident notification, a ban on sharing credentials and removal of access at the end of the service into the contract.

How We Review It in Security Audits & Penetration Testing

Within a written, authorised scope, we list every third party that can touch money, payment data or business accounts: business banking users, payment API keys, integrators, remote support for the management system and the social media agency. For each access we record what it can do, whether it requires a second factor, whether it belongs to a named person or is shared, and when it was last used.

Agreed tests check whether a supplier account can step outside its role, for example by creating

users or starting payments when its job is only to view, and whether remote access tools are left running without need. We check whether an out-of-hours transaction would show up in the logs and who would see it. The executive report explains each gap in business terms, and the prioritised plan starts with limits and dual approval on outgoing payments. Once the changes are made, we verify that they work.

> *The review covers the access included in the agreed scope at a particular date. It cannot assess each supplier's internal security or guarantee that a third party will not act in bad faith. Contract clauses are best drafted with a lawyer: this article is not legal advice. Loss figures vary by source and are given with their own.*

A Check You Can Run

Choose the one service that can move money, such as your business online banking, and open its list of users without changing anything. List every user who is not on your staff: accountant, technician, developer or integrator. For each one, note whether the account is named or shared, whether it can only view or can also enter or approve payments, whether it uses two-step verification and, if the service shows it, when it was last used. A shared account, or a supplier who can approve a payment alone, is the first thing to correct.

Supporting guidance: The NCSC's guidance on understanding the access your suppliers have.
https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security/understand-the-risks

Continue with: When Someone Leaves, Which Access Stays?.
https://systems.kavaliero.com/en/blog/when-someone-leaves-which-access-stays

For help with this work, see the scope of Security Audits & Penetration Testing.
https://systems.kavaliero.com/en/services/security-audits