DOCUMENTO TÉCNICO / CBR CONSULTORIA

Madurez de Seguridad para Fintechs en 2026

Una radiografía práctica de los requisitos que reguladores y auditores más exigen hoy — y cómo priorizar la inversión en seguridad sin frenar la operación.

CBR.Consultoria

Tecnología y Seguridad de la Información
Edición 2026

01 — Contexto

Por qué la madurez de seguridad se volvió tema de directorio

El sector financiero regulado opera hoy bajo un volumen de exigencias que crece más rápido de lo que la mayoría de las estructuras internas puede seguir. Esta guía organiza, de forma práctica, dónde concentrar el esfuerzo primero.

Fintechs, instituciones de pago y plataformas de crédito digital comparten un mismo desafío: crecer rápido sin dejar brechas que un auditor, un regulador o un atacante puedan explotar. La presión viene de varias direcciones a la vez — exigencias del Banco Central, adecuación a la LGPD, expectativas de socios e inversionistas, y una superficie de ataque que crece con cada nuevo producto lanzado.

El error más común no es la ausencia de controles, sino la falta de priorización: las empresas invierten esfuerzo disperso en varios puntos y dejan brechas justo donde las auditorías e incidentes más exigen — gobernanza documentada, gestión de accesos y respuesta a incidentes.

3
frentes regulatorios que más generan observaciones en fintechs

3 días hábiles
plazo regulatorio para la comunicación de incidentes sujetos a notificación a la ANPD, salvo legislación específica

01
una política documentada es el ítem más exigido en la auditoría inicial

> Este documento no sustituye el asesoramiento legal ni una auditoría formal. Su objetivo es ofrecer un punto de partida estructurado para priorizar la inversión en seguridad y gobernanza.

02 — Panorama regulatorio

Qué exige realmente cada frente

Tres frentes concentran la mayor parte de la exigencia regulatoria sobre tecnología y seguridad en instituciones financieras.

A pesar de usar lenguajes distintos, las tres exigen esencialmente lo mismo: documentación viva (que refleje el proceso real, no una plantilla genérica), trazabilidad (saber quién accedió a qué, y cuándo) y capacidad de respuesta comprobada (no basta tener un plan, hay que demostrar que ya fue probado).

FRENTE	QUÉ EXIGE EN LA PRÁCTICA	DÓNDE MÁS FALLAN LAS FINTECHS
Banco Central (Res. 4.893)	Política de ciberseguridad formal, plan de continuidad de negocio, gestión de incidentes relevantes y contratos de tercerización auditables.	La política existe en el papel pero no refleja el proceso real; el PCN nunca fue probado.
LGPD / ANPD	Base legal para cada tratamiento de datos, mapeo del flujo de datos personales, y notificación de incidentes dentro del plazo definido.	Ausencia de un inventario de datos actualizado; nadie sabe exactamente por dónde circula el dato personal.
ISO 27001 / PCI DSS	Sistema de gestión de seguridad de la información con alcance definido, controles mapeados por riesgo y evidencia de operación continua.	Controles implementados de forma aislada, sin proceso de revisión periódica ni responsable formal.

El patrón común entre las tres frentes

Política de seguridad · Gestión de accesos · Continuidad de negocio · Respuesta a incidentes · Gestión de terceros

03 — Modelo de madurez

Cuatro etapas de madurez en seguridad

Use este modelo para identificar en qué etapa está su operación hoy y qué cambia en el siguiente nivel.

Etapa 1 — Reactiva

Seguridad tratada caso por caso, sin política formal. Las decisiones dependen de una o dos personas. No hay registro sistemático de incidentes.

Etapa 2 — Documentada

Existen políticas y procesos escritos, pero la adherencia real varía. La auditoría encuentra brechas entre lo que está en el papel y lo que ocurre en la operación.

Etapa 3 — Gestionada

Los procesos se siguen de forma consistente, con indicadores y responsables definidos. La empresa logra demostrar evidencia de control a un auditor externo.

Etapa 4 — Optimizada

La seguridad forma parte del ciclo de desarrollo y de las decisiones de negocio. Las métricas de riesgo alimentan las decisiones del directorio. La respuesta a incidentes se prueba periódicamente.

> La mayoría de las fintechs en crecimiento acelerado está entre las etapas 1 y 2 — suficiente para operar, pero insuficiente para resistir una auditoría profunda o un incidente real sin daño reputacional.

04 — Priorización

Por dónde empezar cuando el presupuesto es limitado

No toda fintech tiene presupuesto para atacar todo al mismo tiempo. Este es el orden que suele generar mayor reducción de riesgo por cada real invertido.

- [ ] **Inventario de datos y accesos.** Sin saber dónde están los datos personales y financieros y quién accede a ellos, ningún control posterior es confiable.
- [ ] **Política de seguridad documentada y aprobada por la dirección.** Es el primer ítem que pide cualquier auditor, y la base para todo lo demás.
- [ ] **Gestión de identidad y acceso (IAM).** Autenticación fuerte, revisión periódica de permisos y baja ágil de accesos.
- [ ] **Plan de respuesta a incidentes probado.** Tener el documento no basta — hay que simular un incidente y medir el tiempo de respuesta real.
- [ ] **Gestión de proveedores y terceros críticos.** Buena parte de los incidentes en fintechs entra por la cadena de proveedores, no por el perímetro propio.
- [ ] **Continuidad de negocio.** Plan formal, con pruebas periódicas, para los sistemas que no pueden detenerse.

Señales de que es hora de actuar

Una auditoría o socio pidió evidencia que la empresa no tenía lista; el crecimiento del equipo hizo insostenible el control de acceso informal; un incidente pequeño reveló la ausencia de un proceso de respuesta.

Qué no hacer

Comprar una herramienta antes de mapear el proceso; copiar la política de otra empresa sin adaptarla a la realidad operativa; tratar la seguridad como un proyecto de TI aislado del negocio.

05 — Sobre este material

Quién preparó este documento

CBR Consultoria estructura, opera y protege entornos de tecnología para fintechs y negocios de alta regulación — con gestión de proyectos, asignación de especialistas y respuesta a incidentes, en Brasil y en el exterior.

CA

Claudio Araujo

Director Ejecutivo de CBR Consultoria. Más de 31 años de carrera en Tecnología y Seguridad de la Información, con actuación en gobernanza, gestión de riesgos y cumplimiento regulatorio para el sector financiero.

¿Quiere aplicar este modelo en su operación?

Agende un diagnóstico gratuito y sin compromiso con uno de nuestros especialistas.