ISO 27001:2022 · SOC 2 TIPO 2 · LATAM

Los 10 controles que un regulador revisa primero en tu fintech o microfinanciera

Checklist de autodiagnóstico rápido — basado en criterios de ISO 27001:2022, SOC 2 Tipo 2 y experiencia real auditando plataformas financieras en LATAM.

En nuestra experiencia auditando fintechs y microfinancieras en LATAM, los hallazgos críticos casi siempre se concentran en los mismos diez controles. **Antes de revisar cualquier otra cosa**, un regulador, un banco corresponsal o un inversionista empieza por aquí.

QUÉ VAS A ENCONTRAR

- 10 preguntas de autodiagnóstico, una por control clave
- Un «tip del auditor» por cada control
- Una guía para leer tu resultado y priorizar

PARA QUIÉN ES

- Fundadores y equipos de riesgo/TI de fintechs
- Microfinancieras en proceso de licenciamiento
- Equipos que preparan ISO 27001, SOC 2 o due diligence

CÓMO USAR ESTE CHECKLIST

1. Marca Sí, No o Parcial en cada uno de los 10 controles (páginas 2 a 5).
2. Suma tus Sí en la casilla de resultado, al final de la página 5.
3. Lee qué significa tu puntaje y cuál sería tu siguiente paso.

Elaborado por **Rogelio Barajas González** — Auditor Líder ISO 27001:2022 · ISO 9001 · ISO 27017 · ISO 27018 · SOC 1 Tipo 2 y SOC 2 Tipo 2 · MBA · Ingeniería en Sistemas Computacionales.

Controles 01 — 03

Marca Sí / No / Parcial en cada uno. Al final sumamos tu resultado.

01 Gobierno y roles de seguridad

¿Existe un responsable formal de seguridad de la información (CISO o rol equivalente) con autoridad real, no solo en el papel?

Tip del auditor: un organigrama no basta — el auditor pide evidencia de decisiones tomadas por ese rol (actas, aprobaciones, presupuesto asignado).

☐ **Sí** ☐ **No** ☐ **Parcial**

02 Gestión de riesgos documentada

¿Hay una matriz de riesgos vigente, revisada al menos una vez al año, con dueños y planes de tratamiento?

Tip del auditor: una matriz sin dueño asignado por cada riesgo suele ser la primera observación que levanta un auditor.

☐ **Sí** ☐ **No** ☐ **Parcial**

03 Control de accesos

¿Los accesos a sistemas críticos se otorgan bajo mínimo privilegio y se revisan periódicamente (altas, bajas y cambios)?

Tip del auditor: pide evidencia de la última revisión de accesos; si no puedes mostrarla con fecha, para el auditor no existe.

☐ **Sí** ☐ **No** ☐ **Parcial**

Controles 04 — 06

Sigue marcando tu autodiagnóstico control por control.

04 Gestión de proveedores críticos

¿Existen cláusulas de seguridad y continuidad en los contratos con proveedores cloud y de procesamiento de datos?

Tip del auditor: un proveedor sin SLA de seguridad firmado es un riesgo que hereda tu organización, no el proveedor.

☐ **Sí** ☐ **No** ☐ **Parcial**

05 Cifrado de datos sensibles

¿Los datos de clientes (financieros, biométricos, PII) están cifrados en tránsito y en reposo, con gestión formal de llaves?

Tip del auditor: cifrar no basta si nadie documenta quién administra las llaves y cada cuánto rotan.

☐ **Sí** ☐ **No** ☐ **Parcial**

06 Gestión de incidentes

¿Hay un procedimiento documentado y probado para detectar, escalar y notificar incidentes de seguridad?

Tip del auditor: un procedimiento que nunca se ha simulado es, en la práctica, un documento sin probar.

☐ **Sí** ☐ **No** ☐ **Parcial**

Controles 07 — 09

Ya casi terminas — falta el control que más certificaciones detiene.

07 Continuidad del negocio y recuperación

¿Existe un plan de continuidad (BCP/DRP) con RTO/RPO definidos y al menos una prueba de recuperación reciente?

Tip del auditor: definir RTO/RPO en un documento no cuenta si nunca se ha ejecutado un ejercicio de recuperación real.

☐ **Sí** ☐ **No** ☐ **Parcial**

08 Registro y monitoreo (logging)

¿Los sistemas críticos generan bitácoras centralizadas, protegidas contra alteración, con retención suficiente para una auditoría?

Tip del auditor: sin una retención mínima (típicamente 12 meses) no hay forma de reconstruir un incidente pasado.

☐ **Sí** ☐ **No** ☐ **Parcial**

09 Gestión de cambios

¿Los cambios a sistemas en producción siguen un flujo de aprobación, prueba y rollback documentado?

Tip del auditor: un cambio en producción sin aprobación registrada es, para efectos de auditoría, un cambio no controlado.

☐ **Sí** ☐ **No** ☐ **Parcial**

Control 10

El que decide si tus otros nueve controles realmente sirven en una auditoría.

10 Evidencia de cumplimiento continuo

¿Se conservan evidencias (capturas, bitácoras, actas) que demuestren que los controles operan en el tiempo, no solo el día de la auditoría?

Tip del auditor: este es el control que más certificaciones detiene: tener el control no basta, hay que poder probarlo con fecha y responsable.

☐ **Sí** ☐ **No** ☐ **Parcial**

Total de controles en Sí _____ **/ 10**

Cómo leer tu resultado

7 o más ✓

Tu organización probablemente ya está lista para una certificación formal. El siguiente paso es una revisión de brecha final antes de agendar la auditoría.

Entre 4 y 6

Hay una brecha manejable pero real. Priorizar los controles faltantes ahora evita sorpresas costosas en 3–6 meses.

3 o menos

Un cliente, banco o inversionista que pida ISO 27001 o SOC 2 hoy encontraría huecos críticos. Vale la pena mapear la brecha completa antes de comprometerte con una fecha de auditoría.

¿Y ahora qué? Sea cual sea tu puntaje, en la página siguiente te explicamos cómo obtener un mapa completo de tu brecha, con hallazgos priorizados y cuantificados.

¿Quieres saber exactamente dónde está tu brecha, con números y prioridades?

Un **Diagnóstico Combinado** entrega, en 2–3 semanas, un reporte único con hallazgos de compliance (ISO 27001 / SOC 2) y costos cloud, priorizados y cuantificados. Sin compromiso de largo plazo.

barajas-advisory.com · Agenda tu diagnóstico sin costo en el sitio

Agenda tu Diagnóstico Combinado gratuito →

Tus datos de registro se usan únicamente para preparar y darle seguimiento a tu diagnóstico — no se comparten con terceros ni se usan para otros fines. *(Confirma que este texto sea consistente con tu aviso de privacidad real antes de publicar.)*

¿Tiene costo el diagnóstico inicial?
No. Es una revisión sin costo y sin compromiso de largo plazo.

¿Cuánto tarda?
Entre 2 y 3 semanas, dependiendo del alcance de tu plataforma.

¿Qué recibo al final?
Un reporte único con hallazgos de compliance y costos cloud, priorizados y cuantificados.

Rogelio Barajas González · Auditor Líder ISO 27001:2022 · ISO 9001 · SOC 1 Tipo 2 y SOC 2 Tipo 2 · MBA · Ingeniería en Sistemas Computacionales

ISO 27001:2022 | ISO 9001:2015 | SOC 2 TIPO 2 | ISO 27017 | ISO 27018

LinkedIn: **linkedin.com/in/rogelio-barajas-gonzalez**