CHECKLIST TÉCNICO / CBR CONSULTORIA

Checklist de Cumplimiento para Fintechs

Una guía rápida de autoevaluación: los controles que reguladores y auditores verifican primero en instituciones financieras.

BACEN 4.893 | LGPD / ANPD | ISO/IEC 27001 | PCI DSS

CBR.Consultoria

Tecnología y Seguridad de la Información
Edición 2026

Cómo usar este checklist

Autoevaluación rápida, sin rodeos

Marque lo que su empresa ya tiene implementado **y documentado** — no cuenta lo que "existe en la cabeza de alguien". Al final, sume los ítems marcados para obtener una lectura honesta de su etapa.

Gobernanza | Acceso | Datos | Continuidad | Terceros

1 Gobernanza y política

- [ ] Política de seguridad de la información formalizada y aprobada por la dirección.
- [ ] Estructura de responsabilidades definida — quién responde por la seguridad, quién aprueba excepciones.
- [ ] Revisión periódica de la política (mínimo anual) con registro de fecha y responsable.
- [ ] Capacitación de concientización aplicada a todos los colaboradores, con evidencia de participación.

2 Gestión de identidad y acceso

- [ ] Autenticación multifactor obligatoria para sistemas críticos y acceso remoto.
- [ ] Revisión periódica de permisos (quién tiene acceso a qué, y por qué).
- [ ] Proceso formal de baja que revoca el acceso el mismo día.
- [ ] Principio de mínimo privilegio aplicado — acceso mínimo necesario por función.

3 Datos personales y LGPD

- [ ] Inventario de datos personales actualizado — dónde están, quién accede, para qué se usan.
- [ ] Base legal documentada para cada tipo de tratamiento de datos.
- [ ] Proceso de respuesta a incidentes capaz de notificar a la ANPD dentro del plazo exigido.
- [ ] Los contratos con proveedores incluyen cláusulas de protección de datos.

4 Continuidad de negocio

- [ ] Plan de continuidad de negocio (PCN) formal, que cubre los sistemas críticos.
- [ ] Prueba del PCN ejecutada en los últimos 12 meses, con informe de resultado.
- [ ] Backup probado — no basta con que exista, hay que comprobar que restaura correctamente.
- [ ] RTO y RPO definidos para cada sistema crítico (tiempo y punto de recuperación aceptables).

5 Respuesta a incidentes

- [ ] Plan de respuesta a incidentes documentado, con roles y flujo de escalamiento claros.
- [ ] Simulación de incidente (tabletop o real) realizada en el último año.
- [ ] Canal de notificación definido para reguladores, clientes y socios afectados.
- [ ] Registro histórico de incidentes, incluso los de bajo impacto, con lección aprendida.

6 Terceros y cadena de proveedores

- [ ] Evaluación de riesgo aplicada antes de contratar proveedores con acceso a datos o sistemas críticos.
- [ ] Cláusulas contractuales de seguridad exigidas a proveedores críticos, con derecho de auditoría.
- [ ] Inventario de terceros críticos mantenido actualizado, con plan de contingencia si alguno falla.

Lectura rápida del resultado

18 ítems en total

Hasta 8 marcados: etapa inicial, priorice gobernanza e inventario de datos. De 9 a 14: base sólida, enfóquese en probar lo que ya está en el papel. 15 o más: madurez avanzada, el próximo paso es formalizar evidencia para la auditoría externa.