Marcos y certificaciones en ciberseguridad

Comisión de Ciberseguridad - CUF
Diciembre 2025

CÁMARA URUGUAY FINTECH

Introducción

En el ecosistema fintech, donde la confianza digital es tan importante como la propuesta de valor del negocio, comprender los distintos marcos y esquemas de aseguramiento en ciberseguridad se vuelve clave para tomar decisiones estratégicas. SOC 1, SOC 2, ISO 27001 y NIST suelen mencionarse juntos, pero responden a objetivos distintos: algunos buscan dar garantías a terceros, otros ordenar la gestión interna, y otros servir como guía para madurar capacidades de seguridad. Tener claridad sobre sus diferencias evita inversiones incorrectas, expectativas desalineadas con clientes y sobrecarga innecesaria de cumplimiento.

Para las empresas fintech, entender qué exige el mercado —bancos, inversores, partners tecnológicos y reguladores— es tan relevante como la implementación técnica en sí misma. Definir correctamente qué marco aplicar según la etapa de crecimiento y el tipo de servicio permite acelerar negocios, reducir fricciones comerciales y construir confianza sostenible. Este comparativo busca aportar una visión clara y práctica que facilite esa toma de decisiones dentro de la industria.

Comparativo:
SOC 1, SOC 2, ISO 27001 y NIST

Marco / Informe	¿Para qué sirve?	¿Qué evalúa?	¿Quién lo pide?	¿Certificación o informe?	Tipo 1 vs Tipo 2
SOC 1	Dar confianza sobre procesos que impactan en información financiera	Controles que afectan reportes financieros	Bancos, auditores, clientes corporativos	Informe de auditor externo	Tipo 1 = diseño del control Tipo 2 = diseño + funcionamiento en el tiempo
SOC 2	Dar confianza sobre seguridad y gestión de datos	Seguridad, disponibilidad, confidencialidad, integridad, privacidad	Clientes, partners, fintechs, big tech	Informe de auditor externo	Tipo 1 = foto del momento Tipo 2 = prueba real en el tiempo
ISO 27001	Gestionar la seguridad de la información como sistema	Riesgos, políticas, procesos, controles de seguridad	Reguladores, clientes, mercado	Certificación	No tiene tipo 1 / tipo 2
NIST CSF	Marco de referencia para organizar la ciberseguridad	Identificar, proteger, detectar, responder, recuperar	Uso interno, reguladores, sectores críticos	Marco (no certificable)	No aplica

Diferencias clave
(en palabras simples)

Tema	SOC	ISO 27001	NIST
Enfoque	Evidencia para terceros	Gestión interna estructurada	Guía técnica/estratégica
Resultado	Informe para clientes	Certificado público	Diagnóstico interno
Periodicidad	Anual	3 años con auditorías anuales	Cuando la empresa quiera
Valor comercial	Alto en clientes internacionales	Alto en licitaciones y confianza	Bajo comercialmente
Nivel de formalidad	Medio	Alto	Bajo–medio

SOC Tipo 1 vs Tipo 2
(claro para no técnicos)

Tipo	Qué demuestra	Cuándo sirve
Tipo 1	Que los controles existen y están bien diseñados	Startups, primeras ventas, pilotos
Tipo 2	Que los controles funcionan en el tiempo (3–12 meses)	Escalar, vender a bancos, grandes clientes

¿Cuál conviene a una fintech?

Situación de la fintech	Recomendado
Etapa inicial	ISO 27001 o SOC 2 Tipo 1
Venta a bancos / EE.UU.	SOC 2 Tipo 2
Procesa info financiera de terceros	SOC 1
Ordenarse internamente	NIST + ISO 27001
Internacionalizar	ISO 27001 + SOC 2

Resumen en una frase

- SOC 1 → confianza financiera
- SOC 2 → confianza en seguridad
- Tipo 1 → diseño
- Tipo 2 → funcionamiento real
- ISO 27001 → gestión formal de seguridad
- NIST → guía de buenas prácticas