

COMPARACIÓN · SEGURIDAD DE LA INFORMACIÓN

¿SOC 2 o ISO/IEC 27001?

Los proveedores de software y servicios cloud de Sudamérica suelen atender clientes en EE. UU. y en Europa. Unos piden SOC 2 y otros ISO/IEC 27001. Aquí explicamos en qué se diferencian y cuál cuenta para la UE.

SOC 2 informe de auditoría según norma AICPA (EE. UU.)	ISO/IEC 27001 certificado según norma internacional	PARA CLIENTES DE LA UE en general ISO/IEC 27001	PARA CLIENTES DE EE. UU. en general SOC 2
---	---	--	--

En pocas palabras

SOC 2 es un informe de auditoría. Un contador público certificado de EE. UU. (CPA) examina los controles de un proveedor de servicios según las normas de la asociación profesional estadounidense AICPA y los evalúa frente a los Trust Services Criteria. Los criterios abarcan cinco áreas: seguridad, disponibilidad, integridad del procesamiento, confidencialidad y privacidad. La seguridad siempre está incluida; las demás las elige la empresa según lo que necesite. Un informe de tipo 1 describe si los controles están bien diseñados a una fecha determinada. Un informe de tipo 2 verifica además si efectivamente funcionaron a lo largo de un período. Por lo general, el informe se comparte con clientes solo bajo confidencialidad.

[ISO/IEC 27001](#) es una norma internacional para un sistema de gestión de seguridad de la información. Un organismo certificador acreditado verifica si su SGSI cumple los requisitos y emite un certificado. Tiene una vigencia de tres años, con auditorías de seguimiento anuales, y se puede mostrar públicamente.

	SOC 2	ISO/IEC 27001
Tipo de prueba	informe de auditoría (tipo 1 o tipo 2)	certificado
Base	AICPA Trust Services Criteria	ISO/IEC 27001:2022 con Anexo A
Quién audita	contador público de EE. UU. (CPA)	organismo certificador acreditado
Difusión	confidencial, a clientes	se puede mostrar públicamente
Enfoque	controles individuales y su eficacia	sistema de gestión, riesgos, mejora
Muy extendido en	EE. UU., mercado SaaS estadounidense	UE, América Latina, Asia, licitaciones públicas

Por qué los clientes de la UE prefieren ISO/IEC 27001

Los compradores de la UE suelen aceptar un informe SOC 2 si lo tiene. Pero lo primero que piden es ISO/IEC 27001. Hay razones concretas para eso:

- La norma es internacional e igual en todos los países. Un comprador en Fráncfort no necesita conocer las normas de auditoría de EE. UU. para entender el certificado.
- La certificación pasa por organismos acreditados con reconocimiento mutuo. Se pueden verificar la autenticidad y el alcance.
- Los cuestionarios de proveedores y las licitaciones en Europa suelen mencionar ISO/IEC 27001 de forma expresa o piden una prueba equivalente.
- Un informe SOC 2 es largo y hay que leerlo. Evaluar las excepciones de los informes de tipo 2 le cuesta tiempo al cliente.

Detrás de ambas pruebas están las mismas obligaciones de su cliente. [NIS2](#) exige a las entidades importantes y esenciales gestionar la seguridad de su cadena de suministro. [DORA](#) exige a las entidades financieras evaluar a los proveedores de servicios TIC antes de firmar. El [RGPD \(Reglamento General de Protección de Datos\)](#) exige a los encargados del tratamiento garantías suficientes sobre las medidas técnicas y organizativas. Ninguna de estas normas impone un certificado en particular, pero ISO/IEC 27001 es la prueba que mejor conocen los auditores de sus clientes. Si presta servicios cloud a clientes alemanes, le van a preguntar además por el catálogo de criterios C5 de la BSI, la autoridad federal alemana de seguridad informática.

Quién necesita qué en Sudamérica

- Proveedores SaaS que vendieron primero en EE. UU. y ahora van a Europa: mantener SOC 2 y sumar ISO/IEC 27001.
- Empresas de software y proveedores de nearshoring con clientes mayormente europeos, por ejemplo en Montevideo o Medellín: primero ISO/IEC 27001.
- Fintechs y proveedores de TI para bancos de la UE: ISO/IEC 27001, porque lo esperan el supervisor y la auditoría interna del banco. SOC 2 solo si lo exigen clientes de EE. UU.
- BPO y contact centers: casi siempre ISO/IEC 27001, y con datos personales a menudo complementada con ISO/IEC 27701.

Si solo puede financiar uno y quiere ganar clientes en la UE, elija ISO/IEC 27001.

Un ejemplo: un proveedor SaaS de Florianópolis con clientes en Miami y Lisboa tiene un informe SOC 2 tipo 2. Aun así, el banco portugués le envía su propio cuestionario de más de cien preguntas y le

pide el certificado ISO. Con ISO/IEC 27001 además, el proveedor remite al certificado y a la Declaración de Aplicabilidad y solo responde las preguntas adicionales que exige DORA.

Proceso: combinar ambos de forma eficiente

1. Armar un conjunto común de controles que cubra el Anexo A de ISO/IEC 27001 y los Trust Services Criteria. La superposición es grande.
2. Implementar el SGSI según ISO/IEC 27001: alcance, análisis de riesgos, Declaración de Aplicabilidad, políticas, auditoría interna.
3. Certificación ISO/IEC 27001 en etapa 1 y etapa 2.
4. Para SOC 2, encargar como punto de partida un informe de tipo 1 y luego iniciar el período de observación para el tipo 2.
5. Reunir las evidencias una sola vez y usarlas para ambas auditorías; coordinar las fechas de auditoría.

ISO/IEC 27001 lleva normalmente entre 6 y 12 meses hasta la certificación. Un informe SOC 2 tipo 2 requiere un período de observación de varios meses; los clientes suelen esperar períodos más bien largos. Por eso, quien arma ambos en paralelo normalmente necesita más de un año hasta tener el primer paquete completo. Los costos dependen mucho del tamaño, el alcance y el auditor; en SOC 2 se suman los honorarios de los contadores públicos, que pueden variar bastante.

Acreditación y habilitación del auditor

En SOC 2 no hay acreditación en el sentido ISO. El informe lo emite un contador público habilitado en EE. UU. (CPA), que responde por él según las normas profesionales. Si trabaja con auditores de la región, pregunte si el informe lo firma una firma de CPA.

En ISO/IEC 27001 cuenta la acreditación del organismo certificador por un organismo firmante del acuerdo internacional de reconocimiento: hasta fines de 2025 el IAF MLA, desde el 1 de enero de 2026 el MRA de la Global Accreditation Cooperation Incorporated (Global ACI). En los nueve países existe un organismo así: Cgcre del INMETRO en [Brasil](#), OAA en [Argentina](#), INN en [Chile](#), ONAC en [Colombia](#), INACAL en [Perú](#), SAE en [Ecuador](#), OUA en [Uruguay](#), ONA en [Paraguay](#) y DTA-IBMETRO en [Bolivia](#). Si la acreditación incluye seguridad de la información figura en el certificado de acreditación de cada organismo certificador.

Errores frecuentes

- Se presenta a clientes de la UE un informe SOC 2 como «certificado». Da una imagen poco profesional y genera preguntas.
- El informe SOC 2 cubre un solo producto, pero el cliente de la UE usa otro.
- Dos proyectos separados para SOC 2 e ISO/IEC 27001, con políticas duplicadas, evidencias duplicadas y dos equipos.
- ISO/IEC 27001 se hace con un organismo no acreditado porque es más barato. Entonces el cliente de la UE no reconoce el certificado.
- Se vende un informe de tipo 1 como suficiente. Para demostrar eficacia hace falta el tipo 2.

Cómo ayuda Sightadel

[Sightadel](#) gestiona un conjunto común de controles para ISO/IEC 27001 y SOC 2, de modo que usted registra las evidencias una vez y las usa en ambas auditorías. Con un [paquete de consultoría](#), consultores con experiencia lo acompañan hasta la certificación y durante la auditoría SOC 2.

FAQ

¿Los clientes de la UE aceptan SOC 2?

A menudo sí, sobre todo si hay un informe de tipo 2. Pero lo primero que piden es ISO/IEC 27001, y algunas licitaciones la exigen de forma expresa.

¿Cuál es la diferencia entre SOC 2 tipo 1 y tipo 2?

El tipo 1 evalúa el diseño de los controles a una fecha determinada. El tipo 2 verifica además si fueron eficaces a lo largo de un período.

Solo tenemos presupuesto para uno. ¿Cuál elegimos?

Para clientes de la UE, ISO/IEC 27001. Para un mercado formado casi solo por clientes de EE. UU., SOC 2.

¿Se pueden combinar ambas pruebas?

Sí. Los controles se superponen mucho. Con un conjunto común de controles y una sola colección de evidencias se ahorra mucho trabajo duplicado.

¿Qué herramienta ayuda a llevar SOC 2 e ISO/IEC 27001 juntos?

[Sightadel](#) trae SOC 2 e ISO/IEC 27001 como marcos, y las evidencias que registra una vez sirven para ambas auditorías. La plataforma se aloja en Alemania. El informe SOC 2 lo emite un CPA y el certificado ISO, un organismo acreditado.

Fuentes · Actualizado: 11 de octubre de 2026

AICPA: 2017 Trust Services Criteria (Points of Focus 2022): <https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022>

AICPA: SOC 2 Guide: <https://www.aicpa-cima.com/cpe-learning/publication/soc-2-reporting-on-an-examination-of-controls-at-a-service-organization-relevant-to-security-availability-processing-integrity-confidentiality-or-privacy>

ISO: ISO/IEC 27001:2022: <https://www.iso.org/standard/27001>

Directiva (UE) 2022/2555 (NIS2): <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

Reglamento (UE) 2022/2554 (DORA): <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>

Global ACI: organismos de acreditación reconocidos: <https://global-aci.org/en/recognised-abs/>

Información general, no constituye asesoramiento legal. Prevalecen los textos oficiales.

PÓNGALO EN PRÁCTICA CON HERRAMIENTAS HECHAS EN ALEMANIA



Sightadel guía a su equipo por SOC 2: plantillas, tareas, evidencias y preparación de auditorías en un solo lugar. Desarrollado y alojado en Alemania, con paquete de consultoría opcional.

[Ver Sightadel →](#)



veyrisk muestra lo que un atacante ve de su empresa desde fuera: servicios abiertos, certificados, vulnerabilidades conocidas. Puede presentar el informe a clientes europeos y auditores.

[Ver veyrisk →](#)

Sightadel, veyrisk y Valar son productos de neonotu GmbH, empresa que opera MercoEU.

¿Qué parte de esto aplica a su empresa?

El diagnóstico UE gratuito se lo muestra en 10 minutos, según su sector y su país.

<https://www.mercoeu.com/es/diagnostico-ue>