

COMPARAÇÃO · SEGURANÇA DA INFORMAÇÃO

SOC 2 ou ISO/IEC 27001?

Fornecedores de software e nuvem da América do Sul costumam atender clientes nos EUA e na Europa. Uns pedem SOC 2, outros ISO/IEC 27001. Aqui você vê em que os dois se diferenciam e qual deles conta para a UE.

SOC 2	ISO/IEC 27001	PARA CLIENTES DA UE	PARA CLIENTES DOS EUA
relatório de auditoria conforme padrão do AICPA (EUA)	certificado conforme norma internacional	em geral ISO/IEC 27001	em geral SOC 2

Em resumo

O SOC 2 é um relatório de auditoria. Um auditor independente certificado nos EUA (CPA) examina os controles de um prestador de serviços segundo os padrões da associação profissional norte-americana AICPA e os avalia com base nos Trust Services Criteria. Os critérios cobrem cinco áreas: segurança, disponibilidade, integridade do processamento, confidencialidade e privacidade.

Segurança está sempre incluída; as demais a empresa escolhe conforme a necessidade. Um relatório do Tipo 1 descreve se os controles estão bem desenhados em uma data de referência. Um relatório do Tipo 2 verifica, além disso, se eles de fato funcionaram ao longo de um período. Em geral, você só repassa o relatório a clientes mediante confidencialidade.

A [ISO/IEC 27001](#) é uma norma internacional para um sistema de gestão da segurança da informação. Um organismo certificador acreditado verifica se o seu SGSI atende aos requisitos e emite um certificado. Ele vale por três anos, com auditorias de manutenção anuais, e pode ser apresentado publicamente.

	SOC 2	ISO/IEC 27001
Tipo de comprovação	relatório de auditoria (Tipo 1 ou Tipo 2)	certificado
Base	AICPA Trust Services Criteria	ISO/IEC 27001:2022 com Anexo A
Quem audita	auditor certificado nos EUA (CPA)	organismo certificador acreditado
Divulgação	confidencial, para clientes	pode ser apresentado publicamente
Foco	controles individuais e sua eficácia	sistema de gestão, riscos, melhoria
Muito difundido em	EUA, mercado de SaaS norte-americano	UE, América Latina, Ásia, licitações públicas

Por que clientes da UE preferem a ISO/IEC 27001

Compradores da UE muitas vezes aceitam um relatório SOC 2 quando ele existe. Mas a primeira pergunta é pela ISO/IEC 27001. Há motivos concretos para isso:

- A norma é internacional e igual em todos os países. Um comprador em Frankfurt não precisa conhecer as regras de auditoria dos EUA para entender o certificado.
- A certificação passa por organismos acreditados com reconhecimento mútuo. Autenticidade e escopo podem ser verificados.
- Questionários de fornecedores e licitações na Europa citam com frequência a ISO/IEC 27001 de forma expressa ou pedem uma comprovação equivalente.
- Um relatório SOC 2 é longo e precisa ser lido. Avaliar as exceções em relatórios do Tipo 2 custa tempo ao cliente.

Por trás das duas comprovações estão as mesmas obrigações do seu cliente. A [NIS2](#) exige que entidades importantes e essenciais gerenciem a segurança da sua cadeia de fornecimento. O [DORA](#) exige que entidades financeiras avaliem os prestadores de serviços de TIC antes de fechar contrato. O [RGPD \(Regulamento Geral sobre a Proteção de Dados\)](#) exige que operadores ofereçam garantias suficientes de medidas técnicas e organizacionais. Nenhuma dessas regras prescreve uma certificação específica, mas a ISO/IEC 27001 é a comprovação que os auditores dos seus clientes conhecem melhor. Quem fornece serviços de nuvem a clientes alemães também ouvirá perguntas sobre o catálogo de critérios C5 do BSI.

Quem precisa de quê na América do Sul

- Fornecedores de SaaS que venderam primeiro nos EUA e agora estão indo para a Europa: manter o SOC 2 e acrescentar a ISO/IEC 27001.
- Software houses e prestadores de nearshoring com clientes majoritariamente europeus, por exemplo em Montevideu ou Medellín: primeiro a ISO/IEC 27001.
- Fintechs e prestadores de TI para bancos da UE: ISO/IEC 27001, porque a supervisão e a auditoria interna do banco esperam por ela. SOC 2 só se clientes dos EUA exigirem.
- BPO e contact centers: quase sempre ISO/IEC 27001, muitas vezes complementada pela ISO/IEC 27701 quando há dados pessoais.

Quem só pode financiar uma das duas e quer conquistar clientes na UE deve optar pela ISO/IEC 27001.

Um exemplo: um fornecedor de SaaS de Florianópolis com clientes em Miami e Lisboa tem um relatório SOC 2 Tipo 2. Mesmo assim, o banco português envia seu próprio questionário com mais de cem perguntas e pede o certificado ISO. Tendo também a ISO/IEC 27001, o fornecedor remete ao certificado e à declaração de aplicabilidade e só responde às perguntas que o DORA exige além disso.

Etapas: como combinar os dois com eficiência

1. Montar um conjunto comum de controles que cubra o Anexo A da ISO/IEC 27001 e os Trust Services Criteria. A sobreposição é grande.
2. Implantar o SGSI conforme a ISO/IEC 27001: escopo, análise de riscos, declaração de aplicabilidade, políticas, auditoria interna.
3. Certificação ISO/IEC 27001 em estágio 1 e estágio 2.
4. Para o SOC 2, encomendar um relatório do Tipo 1 como ponto de partida e depois iniciar o período de auditoria do Tipo 2.
5. Coletar as evidências uma única vez e usá-las nas duas auditorias; alinhar as datas das auditorias.

A ISO/IEC 27001 costuma levar de 6 a 12 meses até o certificado. Um relatório SOC 2 Tipo 2 pressupõe um período de observação de vários meses; os clientes muitas vezes esperam períodos mais longos. Quem monta os dois em paralelo, por isso, costuma precisar de mais de um ano até ter o primeiro pacote completo. Os custos dependem muito do porte, do escopo e do auditor; no SOC 2 somam-se os honorários dos auditores, que podem variar bastante.

Acreditação e habilitação dos auditores

No SOC 2 não existe acreditação no sentido ISO. O relatório pode ser emitido por um auditor habilitado nos EUA (CPA), que responde profissionalmente por ele. Ao falar com auditores da região, pergunte se o relatório será assinado por uma firma de CPA.

Na ISO/IEC 27001, o que conta é a acreditação do organismo certificador por um organismo signatário do acordo internacional de reconhecimento: até o fim de 2025, o IAF MLA; desde 01/01/2026, o MRA da Global Accreditation Cooperation Incorporated (Global ACI). Nos nove países existe um organismo assim: a Cgcre do INMETRO no [Brasil](#), o OAA na [Argentina](#), o INN no [Chile](#), o ONAC na [Colômbia](#), o INACAL no [Peru](#), o SAE no [Equador](#), o OUA no [Uruguai](#), o ONA no [Paraguai](#) e o DTA-IBMETRO na [Bolívia](#). Se a acreditação abrange segurança da informação, isso consta no certificado de acreditação de cada organismo certificador.

Erros comuns

- Um relatório SOC 2 é apresentado a clientes da UE como “certificado”. Isso passa uma imagem pouco profissional e gera perguntas.
- O relatório SOC 2 cobre apenas um produto, mas o cliente da UE usa outro.
- Dois projetos separados para SOC 2 e ISO/IEC 27001, com políticas duplicadas, evidências duplicadas e duas equipes.
- A ISO/IEC 27001 é feita com um organismo não acreditado porque sai mais barato. O cliente da UE, então, não reconhece o certificado.
- Um relatório do Tipo 1 é apresentado como suficiente. Quem quer comprovar eficácia precisa do Tipo 2.

Como o Sightadel ajuda

O [Sightadel](#) gerencia um conjunto comum de controles para a ISO/IEC 27001 e o SOC 2, de modo que você registra as evidências uma vez e as usa nas duas auditorias. Com um pacote de consultoria, consultores experientes acompanham você até a certificação e durante a auditoria SOC 2.

Para controles sobre gestão de vulnerabilidades, o [veyrisk](#) verifica de fora sua superfície de ataque e gera um relatório que você pode usar como evidência nas duas auditorias.

FAQ

Clientes da UE aceitam SOC 2?

Muitas vezes, sim, principalmente quando há um relatório do Tipo 2. Mas a primeira pergunta é pela ISO/IEC 27001, e algumas licitações a exigem expressamente.

Qual é a diferença entre SOC 2 Tipo 1 e Tipo 2?

O Tipo 1 avalia o desenho dos controles em uma data de referência. O Tipo 2 verifica, além disso, se eles foram eficazes ao longo de um período.

Só temos orçamento para um. Qual escolher?

Para clientes da UE, a ISO/IEC 27001. Para um mercado formado quase só por clientes dos EUA, o SOC 2.

É possível combinar as duas comprovações?

Sim. Os controles se sobrepõem bastante. Com um conjunto comum de controles e um único repositório de evidências, você evita muito retrabalho.

Qual ferramenta ajuda a gerenciar SOC 2 e ISO/IEC 27001 juntos?

O **Sightadel** suporta os dois frameworks e reaproveita o que você elaborou para um no outro. Ele é desenvolvido e hospedado na Alemanha. O certificado ISO e o relatório SOC 2 continuam sendo emitidos pelo organismo certificador acreditado ou pelo auditor CPA.

Fontes · Atualizado em: 11 de outubro 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>

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

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

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

Informações gerais, sem caráter de consultoria jurídica. Valem os textos oficiais.

COLOQUE EM PRÁTICA COM FERRAMENTAS FEITAS NA ALEMANHA



Sightadel

O Sightadel conduz sua equipe por o SOC 2: modelos, tarefas, evidências e preparação para auditoria em um só lugar. Desenvolvido e hospedado na Alemanha, com pacote de consultoria opcional.

[Conhecer o Sightadel →](#)



O veyrisk mostra o que um atacante enxerga da sua empresa por fora: serviços abertos, certificados, vulnerabilidades conhecidas. Você pode apresentar o relatório a clientes europeus e auditores.

[Conhecer o veyrisk →](#)

Sightadel, veyrisk e Valar são produtos da neonotu GmbH, empresa que opera o MercoEU.

O que disso se aplica à sua empresa?

O Diagnóstico UE gratuito mostra isso por setor e país em 10 minutos.

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