# De SOC 2 a ISO 27001

Cómo aprovechar su inversión en SOC 2
para obtener la certificación ISO 27001

Cyberneza LLC • cyberneza.com
Ciberseguridad & Consultoría de Cumplimiento
Orlando, Florida

# ¿Por Qué Agregar ISO 27001?

Si ya tiene SOC 2, ha completado una porción significativa del trabajo necesario para ISO 27001. Los dos marcos se superponen sustancialmente en controles técnicos. La diferencia principal está en la estructura: ISO 27001 requiere un sistema de gestión formal que SOC 2 no exige.

Agregar ISO 27001 a su programa de cumplimiento le permite:

- Acceder a mercados internacionales: SOC 2 es principalmente norteamericano, ISO 27001 es global
- Satisfacer clientes europeos y de Asia-Pacífico que requieren específicamente ISO 27001
- Demostrar un compromiso más amplio con la gestión de seguridad
- Aprovechar los controles existentes de SOC 2 en lugar de empezar de cero

# SOC 2 vs. ISO 27001: Diferencias Clave

### SOC 2

- Marco de auditoría del AICPA
- Informe de atestación (no una certificación)
- Predominante en Norteamérica
- Basado en Criterios de Servicio de Confianza (TSC)
- Usted elige qué criterios incluir
- Auditoría realizada por firma CPA

### ISO 27001

- Estándar internacional ISO/IEC
- Certificación formal emitida por organismo acreditado
- Reconocido globalmente
- Basado en cláusulas de gestión + controles del Anexo A
- Requiere un SGSI (Sistema de Gestión de Seguridad de la Información)
- Certificación válida por 3 años con auditorías de vigilancia anuales

## Lo Que Ya Tiene de SOC 2

Su inversión en SOC 2 no se desperdicia. Estos controles y procesos se transfieren directamente a ISO 27001:

- Políticas y procedimientos documentados (seguridad de información, control de acceso, respuesta a incidentes, gestión de cambios)
- Proceso de evaluación de riesgos y registro de riesgos
- Controles de acceso con MFA y principio de mínimo privilegio
- Registro y monitoreo de eventos de seguridad
- Procedimientos de respuesta a incidentes
- Evaluación de seguridad de proveedores
- Capacitación en concientización de seguridad para empleados
- Cifrado en tránsito y en reposo

## Lo Que Necesita Agregar

ISO 27001 requiere elementos específicos del sistema de gestión que SOC 2 no cubre. Estos son los principales añadidos:

1. SGSI formal: Alcance documentado, política y objetivos del sistema de gestión de seguridad de la información
2. Análisis de contexto: Comprensión documentada de factores internos/externos y partes interesadas
3. Declaración de Aplicabilidad (SoA): Mapeo de los 93 controles del Anexo A con justificación de inclusión/exclusión
4. Objetivos de seguridad medibles: Métricas alineadas con los objetivos del negocio
5. Programa de auditoría interna: Auditorías internas periódicas del SGSI (no requerido en SOC 2)
6. Revisión por la dirección: Reuniones formales y documentadas de liderazgo para revisar el desempeño del SGSI
7. Proceso de mejora continua: Acciones correctivas, análisis de tendencias y mejoras del SGSI

# Hoja de Ruta: De SOC 2 a ISO 27001

## Fase 1: Análisis de Brechas (Semanas 1-3)

- Mapear controles SOC 2 existentes a los requisitos de ISO 27001:2022
- Identificar brechas en documentación del sistema de gestión
- Priorizar esfuerzo de remediación por impacto y complejidad

## Fase 2: Construcción del SGSI (Semanas 3-8)

- Definir el alcance del SGSI y los límites
- Documentar contexto organizacional y partes interesadas
- Crear la Declaración de Aplicabilidad
- Desarrollar políticas y procedimientos faltantes
- Establecer objetivos de seguridad y métricas

## Fase 3: Implementación y Auditoría Interna (Semanas 6-14)

- Implementar nuevos controles identificados en el análisis de brechas
- Realizar evaluación formal de riesgos en formato ISO 27001
- Capacitar al personal en los requisitos del SGSI
- Ejecutar auditoría interna
- Realizar revisión por la dirección

## Fase 4: Auditoría de Certificación (Semanas 12-20)

- Auditoría de Etapa 1: Revisión de documentación del SGSI
- Remediar cualquier hallazgo de la Etapa 1
- Auditoría de Etapa 2: Evaluación de implementación y efectividad
- Recibir la certificación ISO 27001

# Errores Comunes a Evitar

- Tratar a ISO 27001 como otra lista de verificación: es un sistema de gestión, no solo controles
- Copiar políticas de SOC 2 textualmente: ISO 27001 requiere formato y estructura específicos
- Omitir la auditoría interna: es un requisito obligatorio, no opcional
- Subestimar los requisitos de la revisión por la dirección: necesita actas formales y documentadas
- Elegir el organismo de certificación equivocado: verificar acreditación, experiencia, costo

# Cómo Cyberneza Facilita la Transición

Cyberneza se especializa en guiar organizaciones que ya tienen SOC 2 a través del camino más eficiente hacia ISO 27001. Maximizamos la reutilización de sus controles e inversión existente.

## Lo que Hacemos

- Análisis de brechas SOC 2 → ISO 27001 con mapeo de controles
- Desarrollo e implementación del SGSI
- Creación de la Declaración de Aplicabilidad y documentación requerida
- Soporte para auditoría interna y revisión por la dirección
- Preparación y acompañamiento en auditoría de certificación
- Soporte continuo post-certificación y auditorías de vigilancia

## ¿Por Qué Cyberneza?

- Experiencia en operaciones de seguridad del Departamento de Defensa (DoD)
- Certificaciones CISSP, CRISC, CCSK v5 y CCZT
- Socio autorizado de Vanta
- Experiencia práctica en ambos marcos (SOC 2 e ISO 27001)
- Enfocados en eficiencia: aprovechar lo que ya tiene, no empezar de cero

## ¿Listo para Expandir su Programa de Cumplimiento?

Agende una evaluación gratuita de brechas SOC 2 → ISO 27001 de 15 minutos.

**calendly.com/larry-cyberneza**