



ISO 27001:2022 SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD — SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN — REQUISITOS

PLAN DE TRANSICIÓN DE STAREGISTER

1.0 Introducción

ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Los requisitos se publican el 25 de octubre de 2022.

Documento relevante; ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad: los controles de seguridad de la información se publicaron el 15 de febrero de 2022.

2.0 Cambios clave

ISO/IEC 27001:2022 no es una edición completamente revisada. Sus principales cambios incluyen:

- El Anexo A hace referencia a los controles en ISO/IEC 27002:2022, que incluye la información del título del control y el control;
- Las notas de la Cláusula 6.1.3 c) se revisan editorialmente, incluyendo la eliminación de los objetivos de control y el uso de "control de seguridad de la información" para reemplazar "control";
- La redacción de la Cláusula 6.1.3 d) se reorganiza para eliminar la posible ambigüedad.

3.0 Transición

La certificación inicial del CAB según ISO/IEC 27001: 2022 comenzará a más tardar 12 meses después del último día del mes de publicación de ISO/IEC 27001:2022 (24 de octubre de 2023)

Transiciones STAREGISTER de clientes certificados completadas en 36 meses a partir del último día del mes de publicación de ISO/IEC 27001:2022 (24 de octubre de 2025)

Plan 4.0 STAREGISTER

- a. Los cambios en ISO/IEC 27001 y el análisis de brechas;
- b. La necesidad de modificar los procesos de certificación relacionados, los documentos y, en su caso, los sistemas informáticos para gestionar las actividades de certificación;
- c. el personal relevante es competente para ISO/IEC 27001:2022 y el proceso de transición;
- d. El equipo de auditoría, en su conjunto, debe tener conocimiento de todos los controles contenidos en ISO/IEC 27002:2022 y su implementación (ver ISO/IEC 27006:2015, 7.1.2.1.3 b)); El programa de auditoría de transición;



ISO 27001:2022 SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD — SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN — REQUISITOS

PLAN DE TRANSICIÓN DE STAREGISTER

- e. existe una comunicación oportuna a los clientes sobre el programa de transición, como el cronograma, el enfoque de la auditoría de transición y las consecuencias si el cliente no realiza la transición antes del final del período de transición.
- f. actualizar los documentos de certificación para el cliente certificado si su SGSI cumple con los requisitos de ISO/IEC 27001:2022;
- g. Todas las certificaciones basadas en ISO/IEC 27001:2013 vencerán o se retirarán al final del período de transición;
- h. la competencia del personal relacionado se demuestra antes de que participen en las actividades de certificación ISO/IEC 27001:2022;

5.0 Auditoría de transición

STAREGISTER puede realizar la auditoría de transición junto con la auditoría de seguimiento, la auditoría de recertificación o a través de una auditoría separada. La auditoría de transición no se basará únicamente en la revisión de documentos, especialmente para la revisión de los controles tecnológicos.

La auditoría de transición incluirá, entre otros, lo siguiente:

- a. el análisis de brechas de ISO/IEC 27001:2022, así como la necesidad de cambios en el SGSI del cliente;
- b. la actualización de la declaración de aplicabilidad (DdA);
- c. en su caso, la actualización del plan de tratamiento de riesgos;
- d. la implementación y efectividad de los controles nuevos o modificados elegidos por los clientes.
- e. El CAB puede realizar la auditoría de transición de forma remota si se asegura de que se cumplan los objetivos de la auditoría de transición.
- f. Como mínimo, la auditoría deberá incluir 0,5 días adicionales de auditor para confirmar la transición de los clientes certificados cuando la transición se realice durante una auditoría de vigilancia o como una auditoría separada.

6.0 Los clientes de STAREGISTER a certificar ISO 27001:2022 deberán

- a. el análisis de brechas de ISO/IEC 27001:2022
- b. en su caso, la actualización del plan de tratamiento de riesgos;
- c. la implementación y efectividad de los controles nuevos o modificados
- d. la competencia del personal relacionado se demuestra antes de que participaran en las actividades de certificación ISO/IEC 27001:2022;

7.0 Documento de referencia

IAF MD:26:2022 Requisitos de transición para ISO/IEC 27001:2022