GUIA DE TRANSICIÓN ISO 27001:2022

53,000 CERTIFICATES GLOBALLY

100% TRANSPARENT FEES

1000+ EMPLOYEES WORLDWIDE

AVERAGE CUSTOMER PARTNERSHIP 10 YEARS

OVER 100 OPERATING COUNTRIES

CARBON NEUTRAL

INTRODUCCION

Este documento proporciona una visión general de los cambios clave entre la versión 2013 y 2022 de la norma ISO 27001. Los nuevos requisitos se muestran a continuación. Deberá prepararse para el cambio y adaptar su sistema de gestión de la seguridad de la información para cumplir los nuevos requisitos y los plazos de transición. Este documento debe utilizarse junto con el análisis de deficiencias de NQA.

ESTRUCTURA DE ISO 27001:2022

La ISO 27001:2022 sigue la estructura de alto nivel definida en el Anexo SL:

1. Alcance
2. Refencias normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del rendimiento
10. Mejora

Anexo A

5. Controles organizativos
6. Controles de personas
7. Controles físicos
8. Controles tecnológicos

NUESTROS VALORES

Le ayudaremos a entender los cambios e interpretar los nuevos conceptos y cómo afectan a su SGSI.

Manténgase al día de los cambios en www.nqa.com

Póngase en contacto con nosotros si tiene alguna pregunta.

ANALISIS DE DEFICIENCIAS Y GUIA

Claúsula	Requisito	Deficiencias
4	**Contexto de la organización**	
4.2	Comprender las necesidades y expectativas de las partes interesadas	Este control ahora requiere explícitamente que su organización sea capaz de demostrar cuál de los requisitos relevantes de las partes interesadas será abordado a través del SGSI.
4.4	Sistema de gestión de seguridad de la información (SGSI)	Ahora se centra en sus procesos y en cómo interactúan con el SGSI.
5	**Liderazgo**	
5.3	Funciones, responsabilidades y autoridades de la organización	Esta cláusula contiene ahora un requisito explícito para comunicar las funciones, responsabilidades y autoridades dentro de su organización.
6	**Planificación**	
6.2.d	Objetivos de seguridad de la información y planificación para alcanzarlos	Los objetivos de seguridad de la información deben establecerse en los niveles pertinentes de su organización. La norma ISO 27001:2022 exige que se supervisen los objetivos y el progreso hacia su consecución.
6.3	Planificación de los cambios	Se trata de un nuevo requisito. Esté preparado para demostrar cómo planifica cualquier cambio en el SGSI.
9	**Evaluación del rendimiento**	
9.3.2.c	Entradas de la revisión por la dirección	Durante la revisión por la dirección, ahora se espera que revise cualquier cambio en las necesidades y expectativas de las partes interesadas pertinentes.

ANEXO A

Claúsula	Requisito	Deficiencias
5	**Controles organizativos**	
5.7	Inteligencia sobre amenazas	Un control nuevo que requiere que las organizaciones recopilen información sobre las amenazas a la seguridad de la información y que la analicen para producir inteligencia sobre amenazas. Las organizaciones considerarán de dónde recopilarán la información y cómo determinarán que es relevante para sus necesidades.
5.23	Seguridad de la información para el uso de servicios en la nube	Se trata de un nuevo control que exige que las organizaciones dispongan de procesos para garantizar que han especificado, gestionado y administrado los conceptos de seguridad en relación con los servicios en la nube. También debe tener en cuenta las cuestiones de seguridad a la hora de planificar su salida de los servicios en la nube.
5.30	Preparación de las TIC para la continuidad de la actividad	Este control requiere que identifique los requisitos de continuidad de las TIC en una situación de continuidad empresarial. Se espera que muestre pruebas objetivas de que la preparación de las TIC se ha integrado en su plan de continuidad de la actividad, incluyendo pruebas.
7	**Controles físicos**	
7.4	Vigilancia de la seguridad física	Aunque los controles de seguridad física no son un concepto nuevo, la norma introduce ahora el requisito de vigilar sus instalaciones de forma continua (dentro y fuera del horario laboral) para detectar accesos físicos no autorizados.

ANEXO A

Control	Requisito	Deficiencias
8	**Controles tecnológicos**	
8.9	Gestión de la configuración	La gestión de la configuración de redes y sistemas debe establecerse, aplicarse, supervisarse y revisarse ahora. Esto incluirá la identificación de las amenazas, debilidades y vulnerabilidades de las configuraciones de seguridad.
8.10	Borrado de información	Este control exige que la información que ya no sea necesaria se elimine de forma segura cuando esté obsoleta o ya no sea necesaria.
8.11	Enmascaramiento de datos	Un nuevo requisito que obliga a proteger los datos sensibles mediante técnicas más allá de los controles y protocolos de seguridad habituales de una organización. La información que debe enmascararse puede deberse a un requisito legal, estatutario, contractual o reglamentario.
8.12	Prevención de fugas de datos	Este nuevo control exige que se apliquen medidas de prevención de la fuga de datos para evitar/detectar el acceso, transferencia o extracción no autorizados.
8.16	Actividades de seguimiento	Este control es una ampliación de la "ISO 27001:2013 A.12.4 Registro y supervisión". En esta última edición, se exige a las organizaciones que supervisen las redes y los sistemas en busca de comportamientos anómalos, habiendo comprendido cómo es el comportamiento "normal". También existe el requisito de mostrar cómo se reacciona ante posibles incidentes de seguridad.
8.23	Filtrado web	Se trata de un nuevo control con el que se pretende bloquear el acceso de los usuarios a sitios web externos que puedan contener contenidos maliciosos o que no se ajusten a las políticas de la organización.
8.28	Codificación segura	Se exige a las organizaciones que garanticen que los principios de codificación segura se han diseñado, implantado y se están siguiendo a lo largo de todo el ciclo de vida del desarrollo.

Declaración de aplicabilidad

Su Declaración de Aplicabilidad (SOA) debe contener los controles necesarios y la justificación de su inclusión, si los controles necesarios están implantados o no y la justificación de cualquier control excluido.

Las organizaciones deben haber mapeado su SOA anterior a los requisitos de la norma ISO 27001:2022. El uso de atributos, que no es obligatorio, puede introducirse para comprender mejor los controles y cómo abordan las áreas de riesgo identificadas por su organización.

Evaluaciones de riesgos/registro

El auditor querrá ver pruebas de que las evaluaciones/registros de riesgos se han actualizado para tener en cuenta los nuevos controles que ha introducido la norma ISO 27001:2022.

PRÓXIMOS PASOS

Preparación de su transición a la norma ISO 27001

- Debe realizar la transición de su sistema de gestión de acuerdo con los requisitos de la norma ISO 27001:2022 antes de que se lleve a cabo la auditoría de transición. Debe incluir cambios en la documentación, junto con pruebas de cualquier requisito de proceso nuevo.
- Las organizaciones deben realizar una auditoría interna y una revisión por la dirección de los nuevos requisitos antes de que se lleve a cabo la transición.
- Puede realizar un análisis de deficiencias con NQA antes de su auditoría oficial de transición. Esto podría llevarse a cabo junto con una auditoría de mantenimiento, o en cualquier otro momento independiente antes de su auditoría de transición.

Auditoría de transición ISO 27001

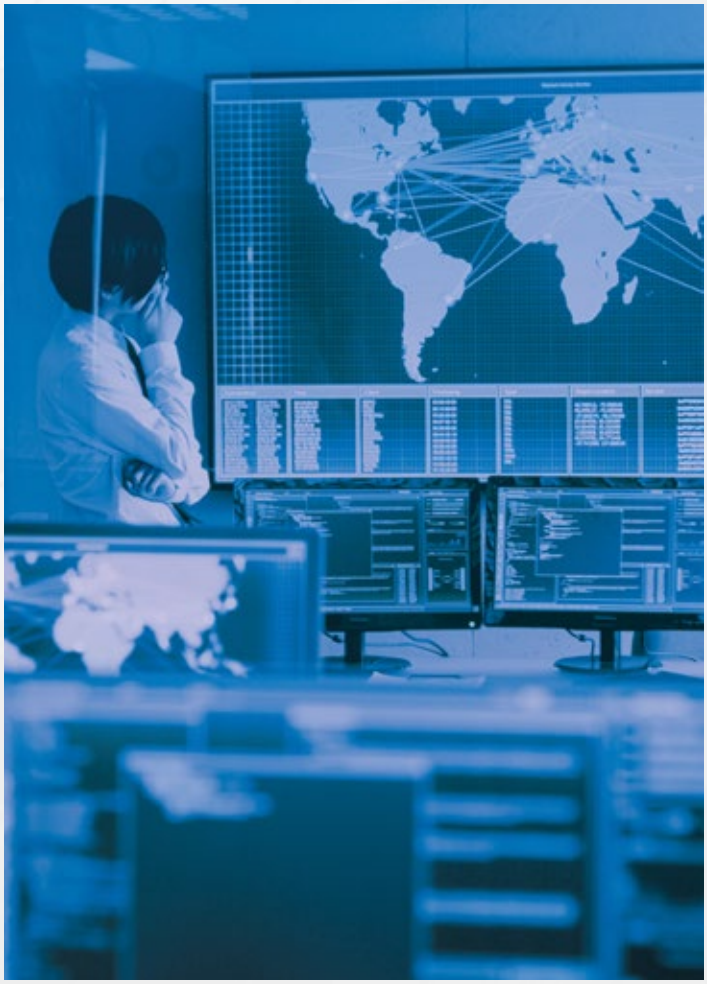
- Todas las organizaciones deben someterse a una auditoría de transición para confirmar la aplicación de la nueva norma. Puede realizarse junto con una auditoría ya existente o puede ser una auditoría independiente.
- Si la auditoría de transición se realiza junto con a una auditoría de mantenimiento o recertificación, se añadirá tiempo adicional a la duración de la auditoría para cubrir los nuevos requisitos introducidos por la norma ISO 27001:2022.
- Si se realiza una auditoría independiente para la auditoría de transición, la duración se calculará en función de cada organización.

Nota: *La duración específica de la auditoría de transición dependerá del tamaño de su organización y de la complejidad del SGSI. NQA le informará de la duración específica de su auditoría de transición.*

Certificados ISO 27001:2022 revisados

Como en cualquier auditoría, las no conformidades identificadas durante una auditoría de transición requerirán la presentación y aprobación de un plan de acciones correctivas. Se emitirá una certificación ISO 27001:2022 actualizada tras la aprobación de la acción correctiva. **La emisión y validez actualizadas del certificado ISO 27001:2022 será:**

- **Transición en mantenimiento:** Se mantendrá la actual "fecha de validez" de la organización.
- **Transición en recertificación:** Se emitirá una nueva "fecha de validez" para el periodo renovado de tres años.
- **Transición autónoma:** Se mantendrá la actual "Fecha de validez" de la organización.



nqa.

www.nqa.com