GESTIONE SU TRANSICIÓN

ANÁLISIS DE DEFICIENCIAS ISO 9001 A ISO 27001

TRUSTED GLOBALLY 30 YEARS SINCE 1988

nqa.

43,000 CERTIFICATES GLOBALLY

100% ALL INCLUSIVE FEES

1000+ EMPLOYEES WORLDWIDE

AVERAGE CUSTOMER PARTNERSHIP 10 YEARS

OPERATING COUNTRIES OVER 90

La ISO 27001: 2013 es la norma de gestión de seguridad de la información y cuenta con un rápido crecimiento en este momento, en parte debido al panorama digital en constante evolución y a la reciente introducción del nuevo Reglamento General de Protección de Datos.

De manera similar a la ISO 27001, la ISO 9001: 2015 es la norma internacional para la gestión de la calidad. Es la norma para SGC más utilizado en el mundo, con más de 1,1 millones de certificados emitidos en 178 países.

¿Qué tienen estas normas en común? Y si tiene un sistema de gestión, ¿puede tener el otro?

La mejor manera de implementar otro sistema de gestión, si ya tiene uno, es implementar un Sistema de Gestión Integrado (SGI). De esta manera, ambos sistemas cumplen con los requisitos del estándar y no duplicará trabajo.

¿Cómo empezar? En primer lugar, observe las partes fáciles: lo común. Si ya está cumpliendo con un requisito de una norma, es probable que no esté lejos de lograr el mismo requisito en otra norma.

En este resumen verá que hemos trazado las distintas cláusulas dentro de ISO 9001:2015 e ISO 27001:2013 para ayudarlo a comprender cómo implementar otro estándar con los procesos y procedimientos existentes.

A continuación se muestra una descripción de las cláusulas principales y las similitudes.

- **Contexto de la organización**
  Ambas normas requieren que la organización identifique los problemas internos y externos relevantes, aunque desde un punto de vista diferente. La ISO 9001 se centra en la calidad y la ISO 27001 se centra en la seguridad de la información
- **Partes interesadas**
  La organización debe determinar las partes interesadas y sus necesidades y expectativas relacionadas con la calidad o seguridad de la información. Esto se puede lograr en el mismo proceso con una lista combinada.
- **Responsabilidad y autoridad**
  Ambas normas requieren que se definan los roles y responsabilidades del SGC y del SGSI. Aunque estos roles pueden ser diferentes, el proceso para la identificación y definición de estos roles puede ser el mismo.
- **Competencia, conciencia, comunicación e información documentada**
  Estos requisitos son similares para muchas normas y no solo para ISO 9001 e ISO 27001. Se pueden abordar de la misma manera y en muchos casos al mismo tiempo.
- **Auditorías internas y revisión por la dirección**
  Aunque los criterios de auditoría y la entrada de revisión de la dirección y los resultados serán diferentes, el proceso es exactamente el mismo y, según el tamaño o la complejidad de la organización, se pueden realizar juntos o por separado
- **No conformidad y acción correctiva**
  Ambos sistemas requieren un proceso para manejar no conformidades y acciones correctivas. Esto puede ser lo mismo sin razón para mantenerlos separados.

LA DIFERENCIA

ISO 27001: 2013 difiere de ISO 9001: 2015 en que agrega la Evaluación de riesgos de seguridad de la información y el tratamiento de riesgos en el SGSI. Para dicha evaluación de riesgos, la organización debe desarrollar una metodología para la identificación de riesgos de seguridad de la información. Este es un proceso diferente al de abordar los riesgos y las oportunidades en ISO 9001.

El proceso de tratamiento de riesgos de seguridad de la información requiere que una organización aplique uno o varios de los controles de seguridad de la información enumerados en el Anexo A en un intento por mitigar el riesgo.

ESQUEMATIZACIÓN

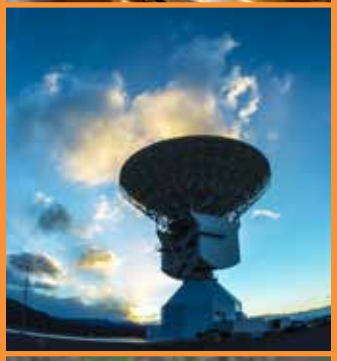
La siguiente tabla muestra las cláusulas de las normas y sus similitudes:

ISO 9001:2015	ISO 27001:2013	ORIENTACIÓN
4 Contexto de la organización	**4 Contexto de la organización**	
4.1. Comprensión de la organización y de su contexto	**4.1. Comprensión de la organización y de su contexto**	Ambas normas requieren que las organizaciones determinen cuestiones internas y externas relacionadas con la idoneidad del sistema de gestión para lograr el resultado previsto.
4.2. Comprensión de las necesidades y expectativas de las partes interesadas	**4.2. Comprensión de las necesidades y expectativas de las partes interesadas**	Ambas normas requieren que las organizaciones identifiquen las partes interesadas relevantes, así como sus necesidades y expectativas.
4.3 Determinación del alcance del sistema de gestión de la calidad	**4.3 Determinación del alcance del sistema de gestión de seguridad de la información**	El alcance del sistema de gestión debe definirse para ambas normas. La diferencia es que la ISO 9001 requiere que se consideren productos y servicios, y la ISO 27001 requiere que se consideren las interfaces y dependencias entre los procesos al definir el alcance.
4.4. Sistema de gestión de la calidad y sus procesos	**4.4. Sistema de gestión de seguridad de la información**	Los requisitos son exactamente los mismos, cada sistema debe establecerse, implementarse, documentarse y mejorarse continuamente.
5 Liderazgo	**5 Liderazgo**	
5.1 Liderazgo y compromiso	**5.1 Liderazgo y compromiso**	Ambas normas requieren que la gerencia implemente políticas, haga provisiones para recursos, mejora de forma continua asignando roles y responsabilidades, etc.
5.1.1 Generalidades		No hay cláusula similar en ISO 27001.
5.1.2 Enfoque al cliente		No hay cláusula similar en ISO 27001.
5.2 Política	**5.2 Política**	Los requisitos son muy similares y podrían cumplirse en un solo documento. Algunas políticas están redactadas como documentos separados, en etse caso deben ser compatibles entre sí.
5.2.1 Establecimiento de la política de la calidad		No hay cláusula similar en ISO 27001.
5.2.2 Comunicación de la política de la calidad		No hay cláusula similar en ISO 27001.
5.3 Roles, responsabilidades y autoridades en la organización	**5.3 Roles, responsabilidades y autoridades en la organización**	Los requisitos de la norma son los mismos: los roles, las responsabilidades y las autoridades pueden comunicarse de la misma manera. Esto significa, por ejemplo, que el Gerente de Calidad también puede ser el Gerente de Seguridad de la Información y, en función de su competencia, podría realizar las auditorías internas en ambos sistemas.

ISO 9001.2015	ISO 27001:2013	ORIENTACIÓN
6 Planificación	**6 Planificación**	
6.1 Acciones para abordar riesgos y oportunidades	**6.1 Acciones para abordar riesgos y oportunidades**	Ambas normas requieren la identificación de riesgos y oportunidades que surgen del contexto de la organización en términos de calidad y seguridad de la información. La única diferencia con ISO 27001 es que la norma proporciona una lista de medidas de control que se pueden utilizar para mitigar estos riesgos en el Anexo A.
6.2 Objetivos de la calidad y planificación para lograrlos	**6.2 Objetivos de seguridad y planificación para lograrlos**	Ambas normas estipulan la necesidad de establecer objetivos y planes para su realización. Estos pueden reflejarse en documentos separados o integrados.
6.3 Planificación de los cambios		No hay cláusula similar en ISO 27001.
7 Apoyo	**7 Apoyo**	
7.1 Recursos	**Recursos**	Las normas requieren que la organización determine y proporcione los recursos necesarios para la ejecución del proceso. Esto significa que se pueden utilizar los mismos procesos.
7.1.1 Generalidades		No hay cláusula similar en ISO 27001.
7.1.2 Personas		No hay cláusula similar en ISO 27001.
7.1.3 Infraestructura		No hay cláusula similar en ISO 27001.
7.1.4 Ambiente para la operación de los procesos		No hay cláusula similar en ISO 27001.
7.1.5 Recursos de seguimiento y medición		No hay cláusula similar en ISO 27001.
7.1.5.2 Trazabilidad de las mediciones		No hay cláusula similar en ISO 27001.
7.1.6 Conocimientos de la organización		No hay cláusula similar en ISO 27001.
7.2 Competencia	**7.2 Competencia**	Ambas normas requieren que la organización identifique y proporcione capacitación para las competencias necesarias de los empleados y también mantenga registros sobre esas competencias.
7.3 Toma de conciencia	**7.3 Toma de conciencia**	Un requisito de ambas normas es que los empleados conozcan las políticas y procedimientos relevantes. Esto también incluye la conciencia del papel que juegan dentro del sistema de gestión y cómo impacta el desempeño en la calidad y seguridad de la información.
7.4 Comunicación	**7.4 Comunicación**	Ambas normas requieren lo mismo y pueden cumplirse mediante los mismos métodos o procesos.
7.5 Información documentada	**7.5 Información documentada**	El requisito es el mismo y se pueden aplicar los mismos procesos/procedimientos.

ISO 9001.2015	ISO 27001:2013	ORIENTACIÓN
8 Operación	**8 Operación**	
8.1 Planificación y control operacional	8.1 Planificación y control operacional	Aunque los nombres de las cláusulas son los mismos, tienen diferentes alcances entre normas. La ISO 9001: se centra en definir y controlar el proceso, y la ISO 27001 se enfoca en establecer controles de seguridad de la información.
8.2 Requisitos para los productos y servicios		No hay cláusula similar en ISO 27001
8.3 Diseño y desarrollo de los productos y servicios	A.6.1.5 Seguridad de la información en la gestión de proyectos	A.6.1.5 es una medida de control de ISO 27001 Anexo A y puede ser parte del procedimiento de diseño y desarrollo.
8.4 Control de los procesos, productos y servicios suministrados externamente	A.15 Realciones con proveedores	Aún con nº de cláusula diferente, los requisitos son muy similares. Los contratos celebrados con proveedores deben incluir una consideración de las cláusulas de seguridad de la información. Esta puede utilizarse como criterio para la evaluación de proveedores.
8.5 Producción y provisión del servicio	A.12 Seguridad en las operaciones	Cualquier proceso de TI que respalde la producción y la prestación de servicios debe tener en cuenta los requisitos de seguridad de la información.
8.6 Liberación de los productos y servicios		No hay cláusula similar en ISO 27001
8.7 Control de las salidas no conformes		No hay cláusula similar en ISO 27001
9 Evaluación del desempeño	**9 Evaluación del desempeño**	
9.1 Seguimiento, medición, análisis y evaluación	9.1 Seguimiento, medición, análisis y evaluación	La efectividad del sistema debe monitorearse utilizando los parámetros que la organización ha identificado para la realización del proceso. ISO 9001 también controla la satisfacción del cliente (9.1.2).
9.2 Auditoría interna	9.2 Auditoría interna	Se puede aplicar el mismo procedimiento a ambas normas en materia de auditorías internas.
9.3 Revisión por la dirección	9.3 Revisión por la dirección	La cláusula y los requisitos son los mismos, sin embargo, ambas normas tienen diferentes elementos de entrada. Se puede utilizar la misma documentación, sin embargo, deben incluirse los elementos de entrada separados.
10 Mejora	**10 Mejora**	
10.1 Generalidades		No hay cláusula similar en ISO 27001
10.2 No conformidad y acción correctiva	10.1 No conformidad y acción correctiva	Se puede utilizar el mismo proceso para cumplir con los requisitos similares de ambas normas.
10.3 Mejora continua	10.2 Mejora continua	Como ocurre con todos los sistemas de gestión, se hace hincapié en la mejora continua que se puede conseguir mediante un procedimiento conjunto de acciones correctivas.

Si ya cuenta con un sistema de gestión de calidad según la norma ISO 9001:2015, los beneficios de implementar un sistema de gestión de seguridad de la información son innumerables. No solo ayuda a demostrar el cumplimiento del nuevo RGPD, sino que también demueestra a sus clientes, empleados y partes interesadas que se toma en serio la seguridad de la información y los datos. Puede que ya haya adelantado más de lo que cree.



JOIN IN

InTouch
Boletín de noticias de NQA, que ofrece una variedad de información práctica.
Es gratis. **www.nqa.com/signup**

NQA Movies
Obtenga información comercial sobre cómo ayudamos a nuestros clientes.
www.youtube.com/nqamovies

Twitter
Manténgase al día con las últimas noticas de NQA
www.twitter.com/NQAGlobal

Linkedin
Conéctese con NQA en Linkedin, interactúe con nuestra red profesional.
www.linkedin.com/company/nqa-certificacion

Contacto

NQA Global Assurance, S.L. Calle Mayor 73, 3º. 34001 Palencia.
T: 979 70 19 12 **E: administracion@nqa.com** **www.nqa.com/es**

nqa.

NEVER STOP IMPROVING