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.

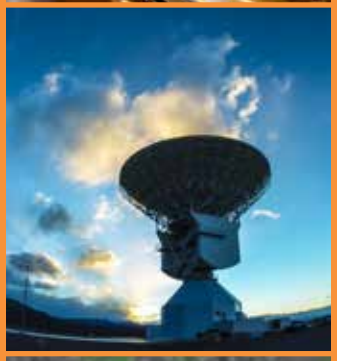
ESQUEMATIZACIÓN

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

ISO 9001:2015	ISO 27001:2013	ORIENTACIÓN
6 Planificación	**6 Planificación**	
6.1 Actions to address risks and opportunities	**6.1 Actions to address risks and opportunities**	Both standards specifically require the identification of risks and opportunities arising from the context of the organization in terms of quality and information security. The only difference with ISO 27001 is that the standard provides a list of control measures which can be used to mitigate these risks in the form of Annex A.
6.2 Quality objectives and plans to achieve them	**6.2 Information security objectives and planning to achieve them**	Both standards stipulate a need to establish objectives and their plans for realisation. These can be separate documents or placed together.
6.3 Planning of changes		No similar clause in ISO 27001.
7 Support	**7 Support**	
7.1 Resources	**7.1 Resources**	The standards require the organization to determine and provide the necessary resources for process execution. This means the same processes can be used, such as; a purchasing process to fulfil requirements.
7.1.1 General		No similar clause in ISO 27001.
7.1.2 People		No similar clause in ISO 27001.
7.1.3 Infrastructure		No similar clause in ISO 27001.
7.1.4 Environment for the operation of processes		No similar clause in ISO 27001.
7.1.5 Monitoring and measuring resources		No similar clause in ISO 27001.
7.1.5.2 Measurement Traceability		No similar clause in ISO 27001.
7.1.6 Organizational knowledge		No similar clause in ISO 27001.
7.2 Competence	**7.2 Competence**	Both standards require the organization to identify and provide training for the necessary competencies of employees and also to keep records regarding those competencies.
7.3 Awareness	**7.3 Awareness**	A requirement of both standards is that employees are aware of the relevant policies and procedures. This also includes awareness of the role they play within the management system and how they impact the organizations performance with regards to quality and information security.
7.4 Communication	**7.4 Communication**	Both standards require the same thing and can be met via the same methods or processes.
7.5 Documented information	**7.5 Documented information**	The requirement is the same and the same processes/ procedures can be applied.

ISO 9001:2015	ISO 27001:2013	GUIDANCE
8 Operation	**8 Operation**	
8.1 Operational planning and control	8.1 Operational planning and control	Although the clause names are the same they have different scopes between the standards. ISO 9001 – focuses on defining and controlling process ISO 27001 – focuses on establishing information security controls.
8.2 Requirements for products and services		No similar clause in ISO 27001.
8.3 Design and development of products and services	A.6.1.5 Information security in project management	A.6.1.5 is a control measure from ISO 27001 Annex A and can be part of the procedure for design and development.
8.4 Control of externally provided processes, products and services	A.15 Supplier relationships	Although different clause numbers – very similar requirements. Contracts entered into with suppliers should include a consideration of information security clauses. Indeed, information security can be used as criteria for the evaluation of suppliers.
8.5 Production and service provision	A.12 Operations security	Any IT processes that support the production and service provision should have the information security requirements taken into account.
8.6 Release of products and services		No similar clause in ISO 27001.
8.7 Control of nonconforming outputs		No similar clause in ISO 27001.
9 Performance evaluation	**9 Performance evaluation**	
9.1 Monitoring, measurement, analysis and evaluation	9.1 Monitoring, measurement, analysis and evaluation	The effectiveness of the management system must be monitored using the parameters that the organization has identified as being important for the process realization. ISO 9001 also monitors customer satisfaction (9.1.2).
9.2 Internal Audit	9.2 Internal Audit	The same procedure can be applied to both standards regarding internal audits.
9.3 Management review	9.3 Management review	The clause and requirements are the same however both standards have different input elements. The same documentation can be used however the separate input elements must be contained.
10 Improvement	**10 Improvement**	
10.1 General		No similar clause in ISO 27001.
10.2 Nonconformity and corrective action	10.1 Nonconformity and corrective action	The same process can used to meet the similar requirements of both standards.
10.3 Continual improvement	10.2 Continual improvement	As with every management system an emphasis is placed on continual improvement which can be conducted via a joint procedure for corrective action.

If you already have a robust Quality management system in place under ISO 9001:2015, the benefits of implementing an Information Security Management System as well are countless. Not only does it help to demonstrate compliance to the new GDPR but it also highlights to your customers, employees and stakeholders that you take information security and data security seriously. You may already be doing more than you think.



JOIN IN

InTouch
Access NQA's knowledge hub, giving a range of practical information. It's FREE.
www.nqa.com/signup

NQA Movies
Gain commercial insight into how we help our customers never stop improving.
www.youtube.com/nqamovies

Twitter
Keep up-to-date with NQA's latest news.
www.twitter.com/NQAGlobal

Linkedin
Connect with NQA on Linkedin, engage with our professional network, access knowledge, gain insights and opportunities.
www.linkedin.com/company/nqa-global

Contact us

NQA, Warwick House, Houghton Hall Park, Houghton Regis, Dunstable,
Bedfordshire LU5 5ZX, United Kingdom
T: 0800 052 2424 **E: info@nqa.com** **www.nqa.com**

nqa.

NEVER STOP IMPROVING