ISO 27001:2022

GUÍA DE IMPLEMENTACIÓN DE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

nqa.

> ISO 27001:2022

GUÍA DE IMPLEMENTACIÓN

*UK and Ireland only

Contenido

INTRODUCCIÓN A LA NORMA

La mayoría de las empresas poseen o tienen acceso a información valiosa o sensible. No proteger adecuadamente esta información puede tener graves consecuencias operativas, financieras y jurídicas. En algunos casos, pueden llevar a la quiebra total de la empresa.

El reto al que se enfrentan la mayoría de las empresas es cómo ofrecer una protección adecuada. En concreto, ¿cómo se aseguran de haber identificado todos los riesgos a los que están expuestas y cómo pueden gestionarlos de forma proporcionada, sostenible y rentable?

ISO 27001 es la norma reconocida internacionalmente para Sistemas de Gestión de Seguridad de la Información (SGSI). Proporciona un marco sólido para proteger la información que puede adaptarse a todo tipo y tamaño de organizaciones. Las organizaciones que están muy expuestas a riesgos relacionados con la seguridad de la información optan cada vez más por implantar un SGSI que cumpla la norma ISO 27001.

La familia 27000

La serie de normas 27000 nació en 1995 como BS 7799 y fue redactada por el Departamento de Comercio e Industria (DTI) del Reino Unido. Las normas se denominan correctamente "ISO/IEC" porque son desarrolladas y mantenidas conjuntamente por dos organismos internacionales de normalización: ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional). Sin embargo, para simplificar, en el uso cotidiano se suele omitir la parte "IEC".

Actualmente hay 45 normas publicadas en la serie ISO 27000. De ellas, la ISO 27001 es la única norma destinada a la certificación. Todas las demás normas ofrecen orientación sobre la aplicación de las mejores prácticas. Algunas orientan sobre cómo desarrollar SGSI para sectores concretos; otras orientan sobre cómo implantar procesos y controles clave de gestión de riesgos para la seguridad de la información.

Revisiones y actualizaciones

Las normas ISO se revisan cada cinco años para evaluar si es necesario actualizarlas.

La actualización más reciente de la norma ISO 27001 tuvo lugar en 2022 y supuso una importante reestructuración del anexo SL, así como una serie de nuevos controles.

Tres de las normas son especialmente útiles para todo tipo de organizaciones a la hora de implantar un SGSI. Son las siguientes:

- **ISO 27000 Tecnología de la información - Visión general y vocabulario**
- **ISO 27002** Tecnología de la información - Técnicas de seguridad - Código de buenas prácticas para los controles de seguridad de la información. Este es el más comúnmente referenciado, relativo al diseño e implementación de los 93 controles especificados en el Anexo A de ISO 27001:2022.
- **ISO 27005** Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información.

BENEFICIOS DE LA IMPLANTACIÓN

La seguridad de la información tiene ahora una importancia fundamental para las organizaciones, y la adopción de la norma ISO 27001 es cada vez más común. Ya no se trata de si se verán afectadas por una violación de la seguridad, sino de cuándo y cómo responderán.

Implantar un Sistema de Gestión de la Seguridad de la Información (SGSI) y conseguir la certificación ISO 27001 es una empresa importante. Sin embargo, si se hace de forma eficaz, las organizaciones que necesitan proteger información valiosa o sensible obtienen importantes beneficios. Estas ventajas suelen clasificarse en tres ámbitos:

COMERCIAL

Contar con el aval de una tercera parte independiente para un SGSI puede proporcionar a una organización una ventaja competitiva frente a sus competidores. Los clientes expuestos a importantes riesgos de seguridad de la información exigen ahora la certificación ISO 27001 en las licitaciones.

Si el cliente también cuenta con la certificación ISO 27001, sólo elegirán trabajar con proveedores cuyos controles de seguridad de la información coincidan con sus propios requisitos contractuales.

Para las organizaciones que desean trabajar con este tipo de clientes, disponer de un SGSI con certificación ISO 27001 es un requisito clave para mantener y aumentar sus ingresos comerciales.

OPERATIVO

La obtención de la ISO 27001 favorece una cultura interna que es constantemente consciente de los riesgos para la seguridad de la información y tiene un enfoque coherente para hacerles frente. Esto conduce a controles que son más sólidos a la hora de hacer frente a las amenazas. También se minimiza el coste de su implantación y mantenimiento, y en caso de que estos controles fallen, las consecuencias se reducirán y mitigarán con mayor eficacia.

TRANQUILIDAD

Las organizaciones tienen información que es fundamental para sus operaciones, vital para mantener su ventaja competitiva o una parte inherente de su valor financiero.

Contar con un SGSI sólido permite a los directivos de las empresas dormir más tranquilos, sabiendo que están menos expuestos al riesgo de multas cuantiosas, interrupciones importantes de la actividad empresarial o un un atque cibernético.

ISO 27001 es un marco reconocido internacionalmente para un SGSI de mejores prácticas y su cumplimiento puede verificarse de forma independiente para mejorar la imagen de una organización y dar confianza a sus clientes.

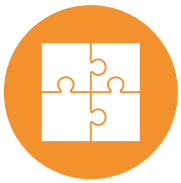
PRINCIPIOS CLAVE Y TERMINOLOGÍA

El objetivo principal de un SGSI es proteger la información sensible o valiosa. La información sensible suele incluir información sobre empleados, clientes y proveedores. La información valiosa puede incluir propiedad intelectual, datos financieros, registros legales, datos comerciales y datos operativos.

LOS TIPOS DE RIESGO A LOS QUE ESTÁ SUJETA LA INFORMACIÓN SENSIBLE PUEDEN AGRUPARSE GENERALMENTE EN 3 CATEGORÍAS:

Confidencialidad

cuando una o acceso no autorizado a la información.



Integridad

cuando se modifique el contenido de la información de modo que deje de ser exacta o completa.

Disponibilidad

cuando se pierda u obstaculice el acceso a la información.

Estos tipos de riesgo para la seguridad de la información forman lo que comúnmente se denomina la tríada CID.

Los riesgos en la seguridad de la información surgen normalmente de la presencia de amenazas y vulnerabilidades en los activos que procesan, almacenan, guardan, protegen o controlan el acceso a la información que pueden dar lugar a incidentes.

En el contexto de la norma ISO 27001, los activos suelen incluir información, personas, equipos, sistemas o infraestructuras.

La información es el conjunto o conjuntos de datos que una organización quiere proteger, como registros de empleados, registros de clientes, registros financieros, datos de diseño, datos de pruebas, etc.

Los incidentes son sucesos no deseados que provocan una pérdida de confidencialidad (por ejemplo, una violación de datos), integridad (por ejemplo, la corrupción de datos) o disponibilidad (por ejemplo, un fallo del sistema).

Las amenazas son las que provocan los incidentes y pueden ser malintencionadas (por ejemplo, un ciberataque), accidentales (por ejemplo, compartir accidentalmente información con la parte equivocada) o de fuerza mayor (por ejemplo, una inundación).

Vulnerabilidades como ventanas abiertas en las oficinas, errores de configuración del código fuente o la ubicación de edificios junto a ríos aumentan la probabilidad de que la presencia de una amenaza dé lugar a un incidente indeseado y costoso.

En seguridad de la información, el riesgo se gestiona mediante el diseño, la aplicación y el mantenimiento de controles como ventanas cerradas con llave, pruebas de software, configuraciones correctas, parcheado de software o ubicación de equipos vulnerables por encima del nivel del suelo.

Un SGSI que cumple con la norma ISO 27001 tiene un conjunto interrelacionado de procesos de mejores prácticas que apoyan el diseño, implementación y mantenimiento de controles, específicos para ese negocio.

Los procesos que forman parte de un SGSI suelen ser una combinación de los procesos empresariales básicos existentes (por ejemplo, contratación, inducción, formación, compras, diseño de productos, mantenimiento de equipos, prestación de servicios,) y los específicos para mantener y mejorar la seguridad de la información (por ejemplo, gestión de cambios, gestión de la configuración, control de acceso, gestión de incidentes, inteligencia de amenazas).

CICLO PDCA

La norma ISO 27001 se basa en el ciclo Planificar-Hacer-Verificar-Actuar (PDCA), también conocido como rueda de Deming o ciclo de Shewhart. El ciclo PDCA puede aplicarse no sólo al sistema de gestión en su conjunto, sino también a cada elemento individual para proporcionar un enfoque continuo en la mejora continua.

En resumen:

Planificar:

Establecer objetivos, recursos necesarios, requisitos de clientes y partes interesadas, políticas organizativas e identificar riesgos y oportunidades.

Hacer:

Aplicar lo previsto.

Verificar:

Supervisar y medir los procesos para establecer el rendimiento en relación con políticas, objetivos, requisitos y actividades planificadas, e informar de los resultados.

Actuar:

Tomar medidas para mejorar el rendimiento, según sea necesario.

Modelo PDCA ISO 27001

Planificar-Hacer-Verificar-Actuar es un ejemplo de sistema de bucle cerrado. Esto garantiza que el aprendizaje de las fases de "hacer" y "comprobar" se utiliza para informar las fases de "actuar" y "planificar" posteriores. En teoría, se trata de un sistema cíclico, pero es más bien una espiral ascendente, ya que el aprendizaje te hace avanzar cada vez que pasas por el proceso.

PENSAMIENTO BASADO EN EL RIESGO/AUDITORÍAS

Las auditorías son un enfoque sistemático, basado en pruebas y en procesos para evaluar su Sistema de Gestión de la Seguridad de la Información. Se realizan interna y externamente para verificar la eficacia del SGSI. Las auditorías son un ejemplo brillante de cómo se adopta el pensamiento basado en el riesgo dentro de la Gestión de la Seguridad de la Información.

Auditorías de 1ª parte - Auditorías internas

Las auditorías internas son una gran oportunidad para aprender dentro de su organización. Proporcionan tiempo para centrarse en un proceso o departamento concreto y evaluar realmente su rendimiento. El objetivo de una auditoría interna es garantizar el cumplimiento de las políticas, procedimientos y procesos determinados por usted, la organización, y confirmar la conformidad con los requisitos de la norma ISO 27001.

Planificación de auditorías

Elaborar un calendario de auditorías puede parecer un ejercicio complicado. Dependiendo de la escala y complejidad de sus operaciones, puede programar auditorías internas desde cada mes hasta una vez al año.

Pensamiento basado en riesgo

La mejor manera de considerar la frecuencia de las auditorías es examinar los riesgos que entraña el proceso o la actividad que se está auditando. Cualquier proceso de alto riesgo, ya sea porque tiene un alto potencial de salir mal o porque las consecuencias serían graves si saliera mal, debe auditarse con más frecuencia que un proceso de bajo riesgo.

La forma de evaluar los riesgos depende exclusivamente de usted. La norma ISO 27001 no dicta ningún método concreto de evaluación o gestión de riesgos.

Las organizaciones deben aplicar una metodología de evaluación de riesgos y un plan de tratamiento con criterios adecuados de aceptación de riesgos y los criterios necesarios para llevar a cabo una evaluación de riesgos en primer lugar. Este proceso debe estar plenamente integrado en su sistema de gestión. Los riesgos deben priorizarse para su tratamiento y tratarse adecuadamente.

Para tratar el riesgo, las organizaciones pueden seleccionar y aplicar los controles aplicables del anexo A, así como aplicar cualquier otro control al margen de éste para gestionar sus riesgos hasta un nivel aceptable. En consecuencia, debe elaborarse una Declaración de Aplicabilidad y cada control del Anexo A debe justificarse, tanto si se aplica como si no. La gestión de riesgos es fundamental en un SGSI y tan importante como la identificación y valoración de activos.

2a parte - Auditorías externas

Las auditorías de segunda parte suelen ser realizadas por los clientes o por terceros en su nombre, o usted puede llevarlas a cabo con sus proveedores externos. Las auditorías de segunda parte también pueden ser realizadas por reguladores o cualquier otra parte externa que tenga un interés formal en una organización.

Es posible que tenga poco control sobre el momento y la frecuencia de estas auditorías, pero si establece su propio SGSI se asegurará de estar bien preparado cuando se produzcan.

3a parte - Auditoría certificación

Las auditorías de terceros corren a cargo de organismos de certificación externos acreditados por UKAS, como NQA.

El organismo de certificación evaluará la conformidad con la norma ISO 27001:2022, para lo cual un representante visitará la organización y evaluará el sistema pertinente y sus procesos. El mantenimiento de la certificación también implica reevaluaciones periódicas.

La certificación demuestra a los clientes su compromiso con la calidad, la seguridad y las crecientes amenazas a las empresas en este mundo digital.

LA CERTIFICACIÓN ASEGURA:

- Evaluación periódica para supervisar y mejorar continuamente los procesos.
- Credibilidad de que el sistema puede lograr los resultados previstos.
- Reducción del riesgo y la incertidumbre y aumento de las oportunidades de mercado.
- Coherencia en los resultados diseñados para satisfacer las expectativas de las partes interesadas.

PENSAMIENTO BASADO EN PROCESOS/ AUDITORÍA

Un proceso es la transformación de entradas en salidas, que tiene lugar como una serie de pasos o actividades que dan lugar al objetivo u objetivos previstos. A menudo, la salida de un proceso se convierte en una entrada para otro proceso posterior. Muy pocos procesos funcionan de forma aislada.

"Proceso: conjunto de actividades interrelacionadas o en interacción que utiliza o transforma insumos para obtener un resultado".

Fundamentos y vocabulario de ISO 27001:2022

Un proceso es la transformación de entradas en salidas, que tiene lugar como una serie de pasos y da lugar al objetivo u objetivos previstos. A menudo, la salida de un proceso se convierte en entrada de otro proceso posterior. Muy pocos procesos funcionan de forma aislada.

Incluso una auditoría tiene un enfoque de proceso. Comienza con la identificación del alcance y los criterios, establece un curso de acción claro para lograr el resultado y tiene un producto definido (el informe de auditoría). Utilizar el enfoque por procesos para auditar también garantiza que se asignan a la auditoría el tiempo y las competencias correctos. Esto la convierte en una evaluación eficaz del rendimiento del SGSI.

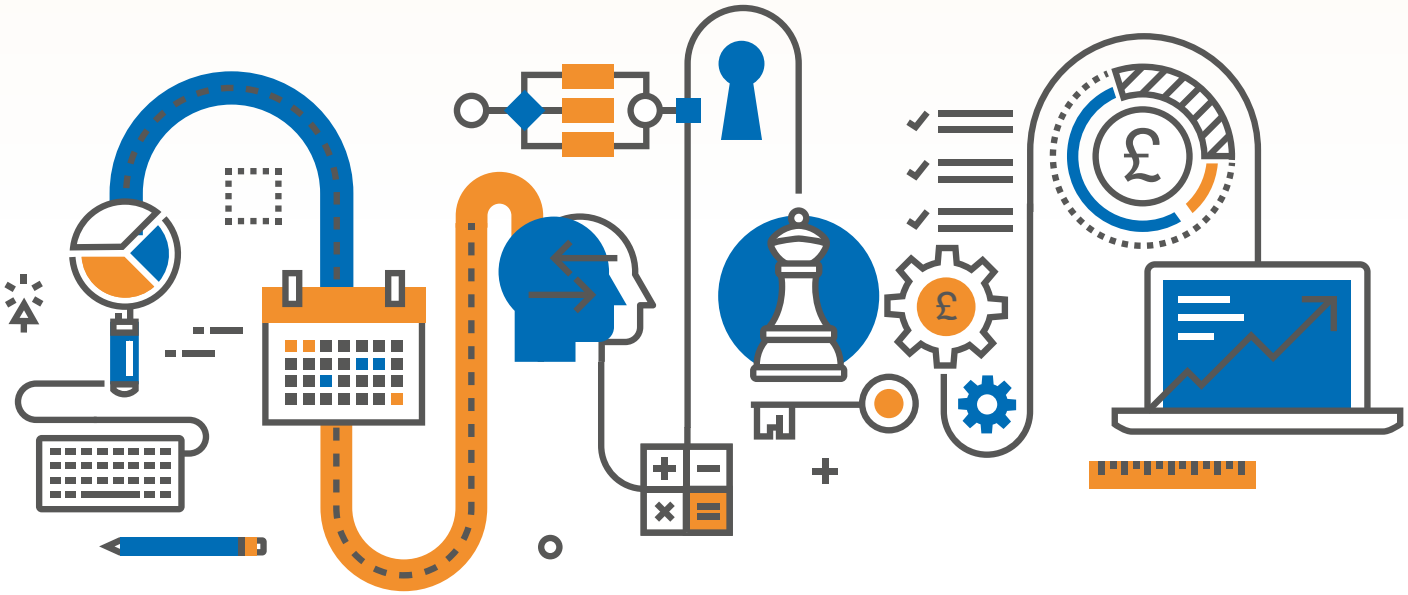
"Se consiguen resultados coherentes y predecibles con mayor eficacia y eficiencia cuando las actividades se entienden y gestionan como procesos interrelacionados que funcionan como un sistema coherente."

ISO 27001:2022 Fundamentos y vocabulario

Comprender cómo se interrelacionan los procesos y producen resultados puede ayudarle a identificar oportunidades de mejora y optimizar el rendimiento global. Esto también es aplicable cuando los procesos, o parte de ellos, se externalizan.

Comprender cómo afecta o podría afectar esto al resultado, y comunicarlo claramente a la empresa que presta el servicio externalizado, garantiza la claridad y la responsabilidad en el proceso.

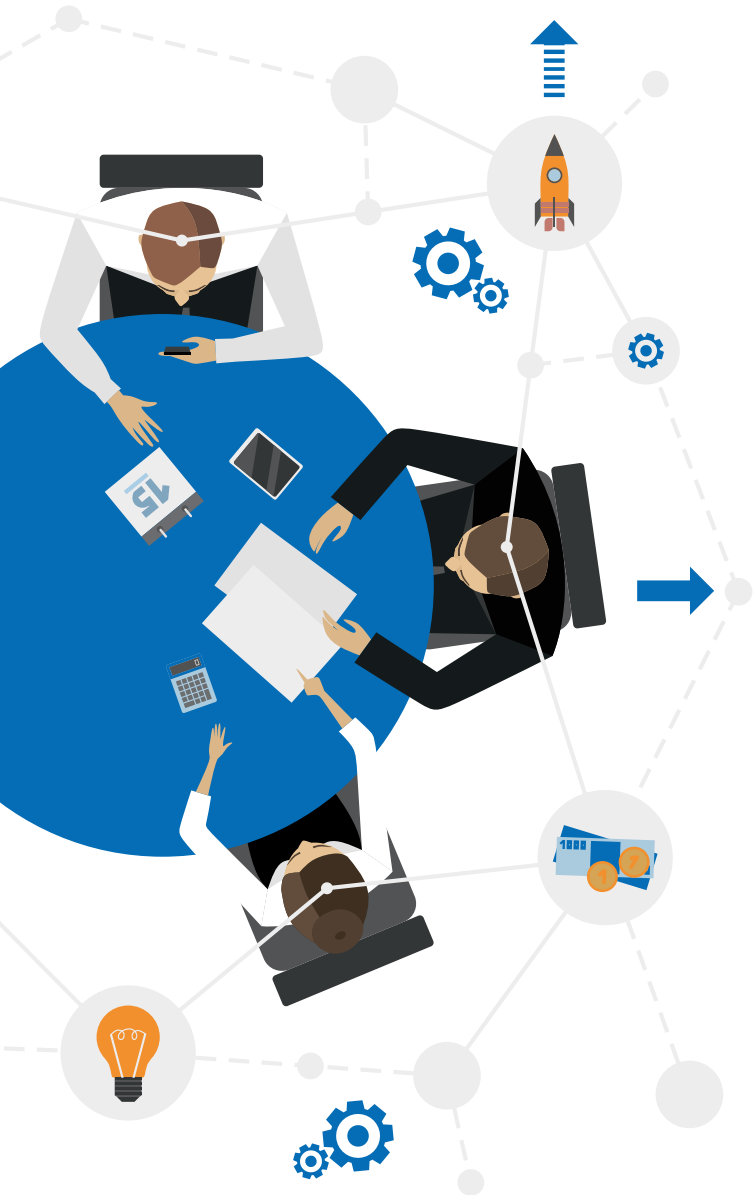
El último paso del proceso consiste en revisar el resultado de la auditoría y asegurarse de que la información obtenida se utiliza correctamente. Una revisión formal de la gestión es la oportunidad de reflexionar sobre el rendimiento del SGSI y de tomar decisiones sobre cómo y dónde mejorar. El proceso de revisión por la dirección se trata con mayor profundidad en la Sección 9 - Evaluación del desempeño.



ANEXO SL

La norma ISO 27001 ha adoptado el anexo SL, y esta estructura también se utiliza para las normas ISO 14001 (norma de sistemas de gestión medioambiental) e ISO 45001 (norma de sistemas de gestión de la salud y la seguridad).

Antes de la adopción del anexo SL había muchas diferencias entre las estructuras de las cláusulas, los requisitos y los términos y definiciones utilizados en las distintas normas de sistemas de gestión. Ello dificultaba a las organizaciones la integración de la aplicación y gestión de varias normas, entre las que las más comunes eran las de medio ambiente, calidad, salud y seguridad, y seguridad de la información.



Estructura de alto nivel

El anexo SL consta de 10 cláusulas:

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

De estas cláusulas, los términos comunes y las definiciones básicas no pueden modificarse. Los requisitos no pueden suprimirse ni modificarse, pero sí pueden añadirse requisitos y recomendaciones específicos de una disciplina.

Todos los sistemas de gestión requieren tener en cuenta el contexto de la organización (más información al respecto en la sección 4); un conjunto de objetivos pertinentes para la disciplina, en este caso la calidad, y alineados con la dirección estratégica de la organización; una política documentada que respalde el sistema de gestión y sus objetivos; auditorías internas y revisión por parte de la dirección. Cuando existen varios sistemas de gestión, muchos de estos elementos pueden combinarse para abordar más de una norma.

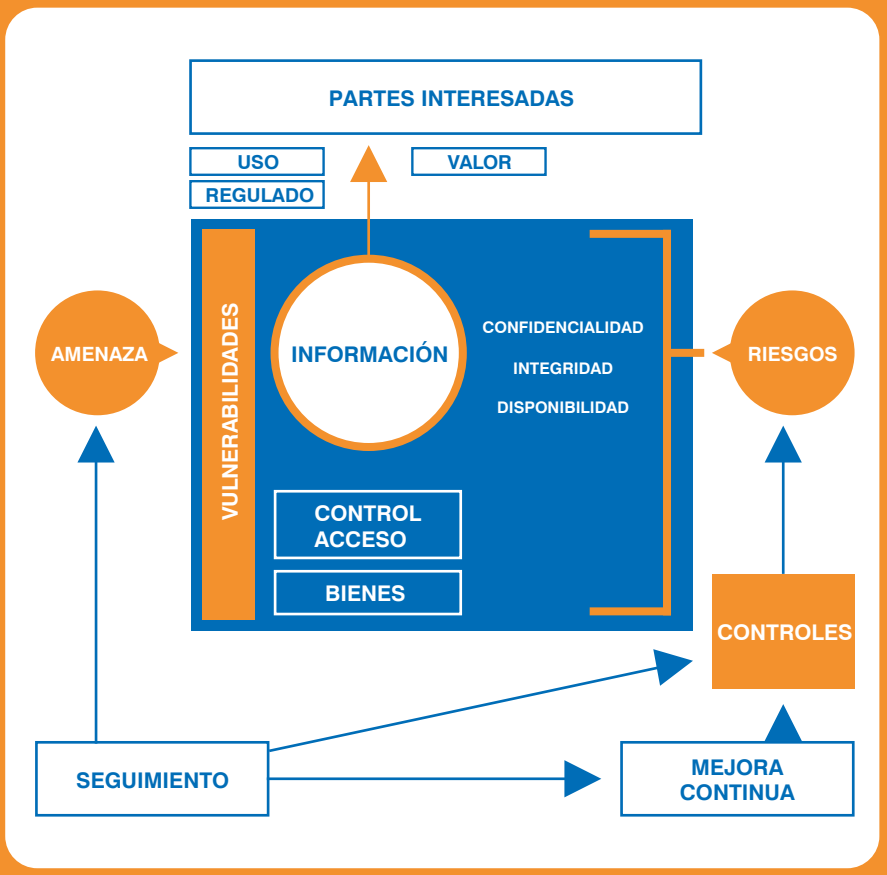
10 CLÁUSULAS DE ISO 27001:2022

La norma ISO 27001 consta de 10 secciones conocidas como cláusulas.

Los requisitos de la norma ISO 27001 que deben cumplirse se especifican en las cláusulas 4.0 a 10.0. La organización debe cumplir con todos los requisitos de las cláusulas 4.0 - 10.0. No pueden declarar una o más cláusulas como no aplicables a ellos. No pueden declarar que una o más cláusulas no les son aplicables.

En la norma ISO 27001, además de las cláusulas 4.0 a 10.0, hay un conjunto adicional de requisitos detallados en una sección denominada Anexo A, a la que se hace referencia en la cláusula 6.0.

El Anexo A contiene 93 controles de seguridad de la información. Es necesario tener en cuenta cada uno de estos 93 controles. Para cumplir con la norma ISO 27001, la organización debe implementar estos controles, o se debe dar una justificación aceptable para no implementar un control en particular.



SECCIÓN 1: ALCANCE

La sección Alcance de la norma ISO 27001 establece:

- la finalidad de la norma.
- Los tipos de organizaciones a las que se aplica; y
- Las secciones de la norma (denominadas cláusulas) que contienen los requisitos que debe cumplir una organización para que se certifique su "conformidad" con la misma (es decir, que es conforme).

La norma ISO 27001 está diseñada para ser aplicable a cualquier tipo de organización. Independientemente de su tamaño, complejidad, sector industrial, finalidad o madurez, su organización puede implantar y mantener un SGSI que cumpla la norma ISO 27001.

SECCIÓN 2: REFERENCIAS NORMATIVAS

En las normas ISO, la sección Referencias normativas enumera cualquier otra norma que contenga información adicional relevante para determinar si una organización cumple la norma en cuestión. En la norma ISO 27001, solo se enumera un documento: ISO 27000 Tecnología de la información - Visión general y vocabulario.

Algunos de los términos y requisitos detallados en la norma ISO 27001 se explican con más detalle en la norma ISO 27000. La referencia a la norma ISO 27000 es muy útil para comprender mejor un requisito o identificar la mejor forma de cumplirlo.

CONSEJO - Los auditores externos esperarán que haya tenido en cuenta la información contenida en la norma ISO 27000 en el desarrollo e implantación de su SGSI.

SECCIÓN 3: TÉRMINOS Y DEFINICIONES

La norma ISO 27001 no contiene términos ni definiciones. En su lugar, se hace referencia a la versión más actual de ISO 27000 Sistemas de Gestión de Seguridad de la Información - Visión General y Vocabulario. La versión actual de este documento contiene 81 definiciones de términos que se utilizan en la norma ISO 27001.

Además de los términos explicados anteriormente en la sección "Principios clave y terminología", otros términos importantes son:

Controles de acceso

Garantizar que el acceso físico y lógico a los activos está autorizado y restringido en función de los requisitos de seguridad de la empresa y de la información.

Activo de información

Un conjunto de información, definido y gestionado como una sola unidad, para que pueda ser comprendido, compartido, protegido y explotado. Los activos de información deben identificarse y su valor establecerse asignando su valor a la organización, basándose en los impactos reputacionales y/o financieros que pueden causar si se ven comprometidos.

Riesgo

Combinación de la probabilidad de que se produzca un suceso relacionado con la seguridad de la información y las consecuencias resultantes.

Evaluación de riesgos

Proceso de identificación de riesgos, análisis del nivel de riesgo que plantea cada uno de ellos y evaluación de la necesidad de adoptar medidas adicionales para reducirlos a un nivel más aceptable.

Tratamiento del riesgo

Procesos o acciones que reducen los riesgos identificados a un nivel aceptable.

Alta dirección

El grupo de personas que toman las decisiones de más alto nivel en una organización. Es probable que sean responsables de establecer su dirección estratégica y de determinar y alcanzar los objetivos de las partes interesadas.

Cuando redacte la documentación de su sistema de gestión de la seguridad de la información, no tiene por qué utilizar estos términos exactos. Sin embargo, puede ayudar a aclarar el significado y la intención si puede definir los términos que ha utilizado. Puede ser útil incluir un glosario en la documentación del sistema.

Junto al "Riesgo" hay otros dos componentes fundamentales de la norma ISO 27001, que son:

Mejora continua (CI)

La idea de que los cambios pequeños, continuos y bien calculados pueden dar lugar a mejoras importantes con el tiempo. En ISO, la CI se refiere al esfuerzo de la empresa por mejorar constantemente su sistema de gestión para cumplir los requisitos de la norma ISO.

SECCIÓN 4: CONTEXTO DE LA ORGANIZACIÓN

El propósito de su SGSI es proteger los Activos de Información de su organización, para que pueda alcanzar sus objetivos.

La forma de hacerlo y las áreas específicas de prioridad dependerán del contexto en el que opere su organización. organización:

- Internamente: las cosas sobre las que la organización tiene cierto control.
- Externamente: las cosas que la organización no controla directamente.

Un análisis cuidadoso del entorno en el que opera su organización es fundamental para identificar los riesgos inherentes a la seguridad de sus activos de información. El análisis es la base que le permitirá evaluar qué procesos debe considerar añadir o reforzar para construir un SGSI eficaz.

Contexto interno

Los siguientes son ejemplos de las áreas que pueden tenerse en cuenta al evaluar las cuestiones internas que pueden influir en los riesgos del SGSI:

- Madurez: ¿Es una empresa ágil con un lienzo en blanco en el que trabajar, o una institución con procesos y controles de seguridad establecidos?
- Cultura organizativa: ¿Es su organización relajada en cuanto a cómo, cuándo y dónde trabaja la gente, o extremadamente reglamentada?
- Gestión: ¿Existen canales y procesos de comunicación claros entre los principales responsables de la toma de decisiones y el resto de la organización?
- Tamaño de los recursos: ¿Trabaja con un equipo de seguridad de la información o lo hace todo una persona?
- Madurez de los recursos: ¿Los recursos disponibles están informados, plenamente formados, son fiables y constantes, o el personal carece de experiencia y cambia constantemente?
- Formatos de los activos de información: ¿Sus activos de información se almacenan principalmente en formato impreso o electrónicamente en un servidor o en sistemas remotos basados en la nube?
- Sensibilidad/valor de los activos de información: ¿Su organización tiene que gestionar activos de información muy valiosos?
- Coherencia: ¿Dispone de procesos uniformes en toda la organización o de una multitud de prácticas operativas diferentes con poca coherencia?
- Sistemas: ¿Tiene su organización muchos sistemas que funcionan con versiones de software que ya no son compatibles con el fabricante, o mantiene la tecnología más actualizada y mejor disponible?
- Complejidad del sistema: ¿Utiliza un sistema principal que hace todo el trabajo pesado, o varios sistemas departamentales con una transferencia de información limitada entre ellos?
- Espacio físico: ¿Disponen de una oficina propia y segura, o trabajan en un espacio compartido con otras organizaciones, o son una organización exclusivamente remota?

Contexto externo

Los siguientes son ejemplos de las áreas que pueden tenerse en cuenta al evaluar las cuestiones externas que pueden influir en los riesgos del SGSI:

- La competencia: ¿Opera en un mercado innovador y en evolución, que requiere actualizaciones de los sistemas para seguir siendo competitivo, o en un mercado maduro y estable con pocas innovaciones?
- Propietario: ¿Necesita aprobación para mejorar la seguridad física?
- Reguladores: ¿Existe en su sector la obligación de realizar cambios reglamentarios con regularidad, o hay poca supervisión por parte de los organismos reguladores?
- Económico/político: ¿Influyen las fluctuaciones monetarias en su organización? ¿Cómo afectan las situaciones geopolíticas a su organización?
- Consideraciones ambientales: ¿Están sus instalaciones en una llanura inundable y los servidores en un sótano? ¿Existen factores que hagan de sus instalaciones un posible objetivo de robo o atentado terrorista (por ejemplo, en un lugar céntrico o cerca de un posible objetivo)?
- Prevalencia de los ataques a la seguridad de la información: ¿Su organización opera en un sector que sufre ciberataques?
- Accionistas: ¿Están muy preocupados por la vulnerabilidad de la organización a las violaciones de datos? ¿Hasta qué punto les preocupa el coste de los esfuerzos de la organización por mejorar su seguridad de la información?

Partes interesadas

Una parte interesada es cualquiera que esté, pueda estar o se perciba afectado por una acción u omisión de su organización. Las partes interesadas se irán aclarando a lo largo del proceso de análisis exhaustivo de los problemas internos y externos.

Probablemente incluirá a accionistas, propietarios, reguladores, clientes, empleados y competidores. Dependiendo de su empresa, pueden incluir al público en general y al medio ambiente. No tiene que intentar comprender o satisfacer todos sus caprichos, pero sí determinar cuáles de sus necesidades y expectativas son relevantes para su SGSI.

Alcance del SGSI

Para cumplir con la norma ISO 27001, debe documentar el alcance de su SGSI. Los alcances documentados suelen describir:

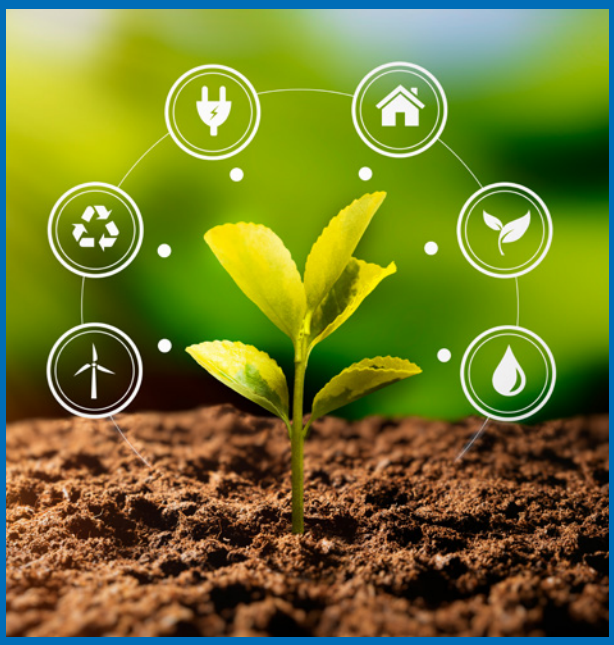
- Los límites del lugar o lugares físicos incluidos (o no incluidos).
- Los límites de las redes físicas y lógicas incluidas (o no incluidas).
- Los grupos de empleados internos y externos incluidos (o no incluidos)
- Los procesos, actividades o servicios internos y externos incluidos (o no incluidos).
- Interfaces clave en los límites del ámbito de aplicación.

Si quiere priorizar recursos creando un SGSI que no cubra toda su organización, seleccionar un ámbito limitado a la gestión de los intereses de las partes interesadas clave es un enfoque pragmático. Esto se puede hacer incluyendo sólo sitios, activos, procesos y unidades de negocio o departamentos específicos. Algunos ejemplos son:

- **"Todas las operaciones realizadas por el Dpto. IT."**
- **"Soporte y gestión del correo electrónico".**
- **"Todos los equipos, sistemas, datos e infraestructuras del centro de datos de la organización, situado en la sede de Basingstoke".**

CONSEJO: Documente o mantenga un archivo de toda la información recopilada en el análisis del contexto de su organización y de las partes interesadas, como por ejemplo

- Conversaciones con un alto representante de la organización, por ejemplo, un director general, CFO, CTO...
- Actas de reuniones o planes de negocio.
- Un documento específico que identifica los problemas internos/externos y las partes interesadas, así como sus necesidades y expectativas; por ejemplo, un análisis DAFO, un estudio PESTLE o una evaluación de riesgos empresariales de alto nivel.



Nueva consideración para el cambio climático

ISO ha introducido cambios en la norma ISO 27001 para subrayar la importancia de abordar los efectos del cambio climático en el marco de los sistemas de gestión de las organizaciones.

Para mejorar la concienciación y la respuesta de las organizaciones al cambio climático, ISO ha introducido dos cambios fundamentales en la cláusula 4:

Cláusula original 4.1:
"Comprensión de la organización y su contexto. La organización debe determinar las cuestiones externas e internas que son relevantes para su propósito y que afectan a su capacidad para lograr el resultado o resultados previstos de su sistema de gestión de XXX."

Esta cláusula incluye ahora explícitamente la afirmación "La organización determinará si el cambio climático es una cuestión relevante".

Cláusula original 4.2:
"Comprender las necesidades y expectativas de las partes interesadas. La organización debe determinar:

- Las partes interesadas que son relevantes para el sistema de gestión XXX.
- Los requisitos pertinentes de estas partes interesadas.
- Cuáles de estos requisitos se abordarán a través del sistema de gestión XXX".

La cláusula ahora también dice: "Nota: Las partes interesadas pertinentes pueden tener requisitos relacionados con el cambio climático".

SECCIÓN 5: LIDERAZGO

La importancia del liderazgo

El liderazgo en este contexto significa la participación en el establecimiento de la dirección del SGSI, su aplicación y provisión de recursos. Esto incluye:

- Garantizar que los objetivos del SGSI sean claros y estén alineados con la estrategia general.
- Claridad en las responsabilidades y la rendición de cuentas.
- El pensamiento basado en el riesgo está en el centro de toda toma de decisiones
- Comunicación clara de esta información a todas las personas dentro del ámbito de su SGSI.

La norma ISO 27001 concede gran importancia al compromiso activo de la Dirección en el SGSI, partiendo de la base de que el compromiso de la Dirección es crucial para garantizar la implantación efectiva y el mantenimiento de un SGSI eficaz por parte de los empleados.

Política de seguridad info.

Una responsabilidad vital de la dirección es establecer y documentar una Política de Seguridad de la Información (PSI) que esté alineada con los objetivos clave de la organización. Debe incluir objetivos o un marco para establecerlos. Para demostrar que está alineada con el contexto de la organización y los requisitos de las principales partes interesadas, se recomienda que haga referencia o contenga un resumen de los principales problemas y requisitos que debe gestionar. También debe incluir el compromiso de:

- Cumplir los requisitos aplicables en materia de seguridad de la información, como los requisitos legales, las expectativas de los clientes y los compromisos contractuales.
- La mejora continua de su SGSI.

El PSI puede hacer referencia a, o incluir sub-políticas que cubran, los controles clave del SGSI de la organización. Algunos ejemplos son: la selección de proveedores críticos para la seguridad de la información, la contratación y formación de los empleados, clear desk y clear screen, controles criptográficos, controles de acceso, etc.

Para demostrar la importancia del PSI, es aconsejable que lo autorice el miembro de mayor rango de su Alta Dirección o cada uno de los miembros del equipo de Alta Dirección.

CONSEJO: Para asegurarse de que su PSI está bien comunicado y a disposición de las partes interesadas, recomendamos:

- IInclúyala en los paquetes de iniciación y en las presentaciones para nuevos empleados y contratistas.
- Publique la declaración clave en los tablones de anuncios internos, las intranets y el sitio web de su organización.
- Haga que su cumplimiento y/o apoyo sea un requisito contractual para empleados, contratistas y proveedores críticos para la seguridad de la información.

Funciones y responsabilidades

Para que las actividades de seguridad de la información formen parte de las actividades de la mayoría de las personas de la organización, las responsabilidades y las obligaciones de rendir cuentas deben definirse y comunicarse claramente.

Aunque la norma no exige la designación de un representante de seguridad de la información, puede ser útil para algunas organizaciones nombrar a uno que dirija un equipo de seguridad de la información para coordinar la formación, supervisar los controles e informar sobre el funcionamiento del SGSI a la alta dirección. Es posible que esta persona ya sea responsable de la protección de datos.

Sin embargo, para desempeñar su función con eficacia, lo ideal es que forme parte del equipo de alta dirección y que tenga sólidos conocimientos técnicos sobre gestión de la seguridad de la información.

Evidenciar liderazgo al auditor

La Dirección serán aquellos que establecen la dirección estratégica y aprueban la asignación de recursos para la organización o área de negocio con el alcance de su SGSI. Dependiendo de cómo esté estructurada su organización, estas personas pueden ser el equipo directivo diario. Un auditor normalmente pondrá a prueba el liderazgo mediante una entrevista, y evaluará su nivel de implicación en el:

- Evaloración de riesgos y oportunidades.
- Establecimiento y comunicación de políticas.
- Fijación y comunicación de objetivos.
- Revisión y comunicación del rendimiento del sistema.
- Asignación de recursos, responsabilidades y obligaciones adecuadas.

CONSEJO: Antes de su auditoría externa, identifique quién de la alta dirección se reunirá con el auditor externo. Prepárelos con un simulacro de entrevista que incluya las preguntas que espera que les hagan.

SECCIÓN 6: PLANIFICACIÓN

La norma ISO 27001 es una herramienta de gestión de riesgos que orienta a una organización para que identifique las causas de sus riesgos para la seguridad de la información. Como tal, el propósito de un SGSI es:

- **Identificar los riesgos importantes, los obvios y los ocultos pero peligrosos.**
- **Garantizar que las actividades y los procesos operativos de una organización estén diseñados, dirigidos y dotados de recursos para gestionar intrínsecamente esos riesgos.**
- **Responder y adaptarse automáticamente a los cambios para hacer frente a los nuevos riesgos y reducir continuamente la exposición al riesgo de la organización.**

Disponer de un plan de acción detallado que se supervise de forma alineada y se apoye en revisiones periódicas es crucial, y proporciona al auditor la mejor prueba de que la planificación del sistema está claramente definida.

Evaluación de riesgos

La evaluación de riesgos es el núcleo de cualquier SGSI eficaz. Ni siquiera la organización mejor dotada de recursos puede eliminar la posibilidad de que se produzca un incidente de seguridad de la información. Para todas las organizaciones, la evaluación de riesgos es esencial:

- Aumentar la probabilidad de identificar todos los riesgos potenciales mediante la participación de personas que utilicen técnicas de evaluación.
- Asignar recursos para abordar las áreas más prioritarias.
- Tomar decisiones estratégicas sobre cómo gestionar los riesgos que permitan alcanzar con mayor probabilidad sus objetivos.

La mayoría de los marcos de evaluación de riesgos consisten en una tabla que contiene los resultados de los elementos 1-4 con una tabla o matriz suplementaria que cubre el punto 5.

Un auditor externo esperará ver un registro de su evaluación de riesgos, un propietario asignado para cada riesgo identificado y los criterios que ha utilizado.

CONSEJO: El anexo A (5.9) contiene el requisito de mantener una lista de los activos de información, los activos asociados a la información (por ejemplo, edificios, archivadores, ordenadores portátiles, licencias) y las instalaciones de procesamiento de la información. Si completa su evaluación de riesgos evaluando sistemáticamente los riesgos que plantea cada elemento de esta lista, habrá cumplido dos requisitos en el mismo ejercicio.

La norma ISO 27005 - Gestión de riesgos para la seguridad de la información ofrece orientación sobre el desarrollo de una técnica de evaluación de riesgos para su organización. Sea cual sea la técnica que elija, debe incluir los siguientes elementos:

1. Proporcionan un impulso para la identificación sistemática de los riesgos (por ejemplo, revisando los activos, grupos de activos, procesos, tipos de información) uno a uno, comprobando en cada uno la presencia de amenazas y vulnerabilidades comunes, y registrando los controles que tiene actualmente para gestionarlos.
2. Proporcionar un marco para evaluar la probabilidad de que se produzca cada riesgo de forma sistemática (por ejemplo, una vez al mes, una vez al año).
3. Proporcionar un marco para evaluar las consecuencias de que se produzca cada riesgo sobre una base coherente (por ejemplo, pérdida de 1.000 £, pérdida de 100.000 £).
4. Proporcione un marco para clasificar cada riesgo identificado sobre una base coherente teniendo en cuenta su evaluación de la probabilidad y las consecuencias.
5. Establecer criterios documentados que especifiquen, para cada puntuación o categoría de riesgo, el tipo de acción que debe emprenderse y el nivel o prioridad que se le asigna.

Tratamiento del riesgo

Para cada riesgo identificado en su evaluación de riesgos, debe aplicar criterios coherentes para determinar si debe:

- **Aceptar el riesgo, o**
- **Tratar el riesgo ("Tratamiento del riesgo").**

Las opciones de Tratamiento de Riesgos disponibles suelen ser una de las siguientes:

- Evitar - Dejar de realizar la actividad o de procesar la información expuesta al riesgo.
- Eliminación - Eliminar la fuente del riesgo.
- Cambiar la probabilidad - Implantar un control que haga menos probable que se produzca un incidente de seguridad de info.
- Cambiar las consecuencias - Implantar un control que disminuya el impacto si se produce un incidente.
- Transferir el riesgo - Externalizar la actividad o el proceso a un tercero que tenga mayor capacidad para gestionar el riesgo.
- Aceptar el riesgo - Si la organización no dispone de un tratamiento práctico del riesgo, o si el coste del tratamiento del riesgo se considera superior al coste del impacto, puede tomar la decisión informada de aceptar el riesgo. Esta decisión deberá ser aprobada por la alta dirección.

Un auditor externo esperará ver un Plan de Tratamiento de Riesgos que detalle las acciones de tratamiento de riesgos que ha implementado o planea implementar. El plan debe ser lo suficientemente detallado como para permitir verificar el estado de ejecución de cada acción. También deberá haber pruebas de que este plan ha sido aprobado por los responsables y la Dirección.

Anexo A y declaración de aplicabilidad

Todas las opciones de Tratamiento del Riesgo (excepto la "aceptación") implican la implantación de uno o más controles. El Anexo A de la norma ISO 27001 contiene una lista de 93 controles de seguridad de la información. Tendrá que considerar si implantar e estos controles en su Plan de Tratamiento de Riesgos.

La descripción de los 93 controles es bastante vaga, por lo que se recomienda encarecidamente revisar la norma ISO 27002, que contiene más información sobre las formas de aplicarlos.

Como prueba de la realización de esta evaluación, se le pedirá que elabore un documento denominado Declaración de Aplicabilidad (SoA). En él, deberá registrar cada uno de los 93 controles:

- Si es aplicable a sus actividades, procesos y riesgos de seguridad de la información..
- Tanto si lo ha aplicado como si no.
- JJustificación de la inclusión o exclusión del control.

Para la mayoría de las organizaciones, la mayoría de los 93 controles serán aplicables, y es probable que ya hayan implantado varios de ellos en cierta medida.

CONSEJO: Su Declaración de Aplicabilidad (DdA) no tiene por qué ser un documento complejo. Bastará con una simple tabla con los siguientes encabezados de columna:

- Control - ¿Aplicable? - ¿Implementado? - Justificación

También es aconsejable registrar alguna información sobre cómo se ha aplicado el control para ayudarle a responder más fácilmente a cualquier pregunta de su auditor externo.

CONSEJO: Aunque no es obligatorio, puede que desee incluir atributos en su evaluación de riesgos y/o SoA. Estos atributos pueden ayudarle a registrar y recuperar información empresarial para tomar decisiones basadas en el riesgo.

Objetivos de SI y planificación para conseguirlos

En los niveles de su organización, debe disponer de un conjunto documentado de objetivos relacionados con la seguridad de la información. Estos objetivos pueden ser de alto nivel y aplicarse a toda la organización o a un departamento.

Cada objetivo que fijes debe ser

- Mensurable.
- Alineado con su ISP.
- Tener en cuenta los requisitos de seguridad de la información de la organización.
- Tener en cuenta los resultados del proceso de evaluación y tratamiento de riesgos.

Los objetivos típicos que son relevantes para la seguridad de la información incluyen:

- Responder, contener y erradicar los efectos de los incidentes de seguridad de la información en un plazo determinado, para reducir el impacto y los efectos del incidente.
- Lograr un nivel mensurable de cumplimiento de los controles de seguridad de la información.
- Ofrecer una disponibilidad definida de servicios de información.
- No superar un número apreciable de errores de datos.
- Mejorar los recursos disponibles mediante contratación, formación o adquisición.
- Aplicación de nuevos controles.
- Lograr el cumplimiento de las normas relacionadas con la seguridad de la información.

Cada objetivo debe comunicarse al personal pertinente. Los objetivos deben actualizarse cuando sea necesario para mantener su pertinencia y evaluar los resultados en función de ellos.

Para cada uno de los objetivos debe planificar cómo va a alcanzarlos. Esto incluye determinar:

- Lo que hay que conseguir.
- Qué recursos se asignan.
- Quién es el propietario o el principal responsable de la consecución del objetivo.
- Tanto si hay una fecha límite para la finalización como si se trata de un requisito continuo.
- El método de evaluación de los resultados con respecto al objetivo (es decir, cuál es su medida).
- Registro de los resultados.

SUGERENCIA: Entre las formas eficaces de comunicar los objetivos de seguridad de la información se encuentran incluirlos en la formación inicial, fijarlos como objetivos de los empleados o incluirlos en las evaluaciones de los empleados, establecerlos en los acuerdos de nivel de servicio con los proveedores.

ISO 27001
Guía del Anexo A

ISO 27001:2022 es la norma internacional que describe las mejores prácticas para un Sistema de Gestión de la Seguridad de la Información (SGSI). Si está familiarizado con nuestra anterior guía de implantación, ya habrá examinado las cláusulas contenidas en la norma. También habrá aprendido que esta norma sigue un enfoque basado en el riesgo a la hora de considerar la seguridad de la información de una organización. Esto requiere la identificación de los riesgos de seguridad y, a continuación, la selección de los controles adecuados para reducir, eliminar o gestionar dichos riesgos.

En el Anexo A de la norma figuran los controles necesarios para cumplir esos requisitos de riesgo. En total, hay 93 controles subdivididos en cuatro grupos de control diferentes. Al considerar estos controles, es importante tener en cuenta que se trata simplemente de posibilidades u opciones.

Al llevar a cabo el proceso de riesgos, el riesgo identificado debe contar con los controles adecuados que se hayan seleccionado de la lista del Anexo A. No se pueden aplicar todos los controles. Por ejemplo, si su organización no dispone de locales y opera a distancia, no sería adecuado utilizar algunos controles del ámbito de la seguridad física.

Del mismo modo, el paso a soluciones basadas en la nube exige una nueva mirada a los controles existentes en los ámbitos de la seguridad de las operaciones y las comunicaciones.

Categorías de controles

CONTROLES ORGANIZATIVOS | **CONTROL DE PERSONAS** | **CONTROLES FÍSICOS** | **CONTROLES TECNOLÓGICOS**

Otras consideraciones

Antes de la auditoría de certificación, una organización debe haber elaborado una Declaración de Aplicabilidad (SoA).

Este requisito se describe en la cláusula 6 de la norma ISO 27001. El SoA debe contener al menos 93 entradas con cada una de las Categorías y Controles enumerados. Una vez hecho esto, cada control debe ser seleccionado y justificado o excluido con una justificación similar. Todos los documentos de SoA deben poder demostrar que se ha tenido en cuenta cada control. Esto significa que una SoA debe contener todas las entradas señaladas. No basta con enumerar los controles seleccionados. Los controles seleccionados formarán parte de las pruebas del tratamiento del riesgo y deberán registrarse.

Esta información se incluirá en un registro de riesgos y podrá conservarse como documentación. La metodología variará de una organización a otra, aunque la demostración de que los controles del Anexo A están implantados es una necesidad constante.

Las disposiciones de seguridad de la norma no son algo a lo que deba atenerse únicamente el equipo informático o de seguridad de una organización. La norma exige que se tengan en cuenta todos los aspectos de la organización a la hora de examinar los riesgos y su tratamiento.

Las personas mejor situadas para poner remedio a los problemas no siempre se encuentran en el Departamento de TI. La ubicación exacta del tratamiento de riesgos variará de una organización a otra. La propiedad del riesgo es vital para garantizar que los controles están sujetos a revisión.

Por último

Los controles del Anexo A son sólo algunas de las opciones de que dispone una organización. Se pueden utilizar controles de seguridad adicionales no descritos específicamente en el Anexo A para dar tratamiento a un riesgo identificado. Siempre que las cláusulas y los controles de la norma se aborden de forma adecuada, el SGSI funcionará y proporcionará buenos niveles de seguridad de la información.

SECCIÓN 7: SOPORTE

La cláusula 7 se refiere a los recursos. Se refiere tanto a las personas, la infraestructura y el entorno como a los recursos físicos, materiales, herramientas, etc. También se presta una atención renovada al conocimiento como recurso importante dentro de su organización. A la hora de planificar sus objetivos de calidad, una consideración importante será la capacidad actual de sus recursos, así como los que pueda necesitar de proveedores o socios externos.

Para implantar y mantener un SGSI eficaz es necesario disponer de recursos de apoyo. Estos recursos deberán ser:

- Capaces - Si son equipos o infraestructuras.
- Competentes - Si son personas.
- Incluidos en las reuniones de revisión de la gestión.

Competencia

La aplicación de controles eficaces de seguridad de la información depende en gran medida de los conocimientos y competencias de sus empleados, proveedores y contratistas. Para tener la certeza de contar con una base adecuada de conocimientos y competencias, es necesario:

- Definir qué conocimientos y competencias se requieren.
- Determinar quién debe poseer los conocimientos y competencias necesarios.
- Establecer cómo puede evaluar o verificar que las personas adecuadas tienen los conocimientos y las competencias adecuadas.

Su auditor esperará que disponga de documentos que detallen sus requisitos en materia de conocimientos y competencias. Cuando considere que se cumplen los requisitos, deberá demostrarlo con documentos como certificados de formación, registros de asistencia a cursos o evaluaciones internas de competencias.

CONSEJO: La mayoría de las organizaciones que ya utilizan herramientas como matrices de formación/habilidades, valoraciones o evaluaciones de proveedores pueden satisfacer el requisito de registros de competencias ampliando las áreas cubiertas para incluir la seguridad de la información.

Concienciación

Además de garantizar la competencia específica del personal en relación con la seguridad de la información, el grupo más amplio de empleados, proveedores y contratistas deberá conocer los elementos básicos de su SGSI. Esto es fundamental para establecer una cultura de apoyo dentro de la organización. Todo el personal, proveedores y contratistas deben ser conscientes de lo siguiente

- Que tiene un SGSI y por qué lo tiene.
- Que tiene una Política de Seguridad de la Información y qué elementos de la política son relevantes para ellos.
- Cómo pueden contribuir a proteger información valiosa y qué deben hacer para ayudar a la organización a alcanzar sus objetivos.
- Qué políticas, procedimientos y controles les afectan y qué consecuencias tiene su incumplimiento.

CONSEJO: La comunicación de esta información puede realizarse normalmente a través de los procesos y documentos existentes, como las inducciones, los contratos de trabajo, las charlas, los acuerdos con proveedores...

Comunicación

Para que los procesos de su SGSI funcionen eficazmente, deberá asegurarse de que las actividades de comunicación están bien planificadas y gestionadas. La norma ISO 27001 las detalla de forma concisa al exigirle que las determine:

- Lo que hay que comunicar.
- Cuando hay que comunicarlo.
- A quién hay que incluir en las comunicaciones.
- Cuáles son los procesos de comunicación.

CONSEJO: Si sus requisitos de comunicación están bien definidos en sus procesos, políticas y procedimientos, entonces no necesita hacer nada más para satisfacer este requisito. Si no son suficientes, entonces debería considerar documentar sus actividades clave de comunicación en forma de tabla o procedimiento que incluya los epígrafes detallados anteriormente.
Recuerde que también hay que comunicar el contenido de estos documentos.

Información documentada

Para que sea útil, la información documentada que utilice para implantar y mantener su SGSI debe serlo:

- Exacto.
- Comprensible para las personas que lo utilizan.
- Apoyo para cumplir los requisitos legales, gestionar los riesgos de seguridad de la información y alcanzar sus objetivos.

Para que su información documentada satisfaga siempre estos requisitos, deberá disponer de procesos que garanticen que:

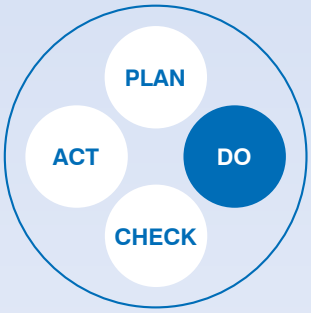
- La información documentada es revisada, en su caso, por las personas adecuadas antes de su difusión general.
- El acceso a la información documentada se controla para que no pueda modificarse accidentalmente, corromperse, borrarse o ser consultada por externos.
- La información se elimina de forma segura o se devuelve a su propietario cuando es necesario.
- Puede realizar un seguimiento de los cambios en la información para garantizar el control del proceso.

La fuente de la información documentada puede ser interna o externa, por lo que los procesos de control deben gestionar la información documentada de ambas fuentes.

CONSEJO: Las organizaciones que tienen un buen control de los documentos suelen contar con uno o varios de los siguientes elementos:

- Una sola persona o un pequeño equipo responsable de garantizar que los documentos nuevos/modificados se revisan antes de su publicación, se almacenan en el lugar adecuado, se retiran de la circulación cuando son sustituidos y que se mantiene un registro de cambios.
- Un sistema de gestión electrónica de documentos que contiene flujos de trabajo y controles automáticos.
- Sólidos procesos de copia de seguridad de datos electrónicos y de archivo/almacenamiento de archivos en papel.
- Gran conocimiento por parte de los empleados de los requisitos de control de documentos, mantenimiento de registros y acceso/conservación de la información.

SECCIÓN 8: OPERACIÓN



Así que, después de toda la planificación y evaluación de riesgos, estamos listos para pasar a la fase de "hacer". La cláusula 8 trata de tener un control adecuado sobre la creación y entrega de su producto o servicio.

La gestión de los riesgos para la seguridad de la información y la consecución de sus objetivos requieren la formalización de sus actividades en un conjunto de procesos claros.

Es probable que muchos de estos procesos ya existan (por ejemplo, la iniciación y la formación) y que simplemente haya que modificarlos para incluir elementos relevantes para la seguridad de la información. Otros procesos pueden tener lugar de manera ad hoc (por ejemplo, aprobación de proveedores), mientras que algunos pueden no existir en absoluto (por ejemplo, auditoría interna).

Para aplicar procesos eficaces son cruciales las siguientes prácticas:

1. Los procesos se crean adaptando o formalizando las actividades habituales de una organización.
2. Identificación sistemática de los riesgos de seguridad de la información pertinentes para cada proceso.
3. Definición y comunicación claras del conjunto de actividades necesarias para gestionar los riesgos asociados a la seguridad de la información cuando se produce un evento (por ejemplo, la incorporación de un nuevo empleado a la empresa).
4. Asignación clara de las responsabilidades para llevar a cabo las actividades relacionadas.
5. Asignación adecuada de recursos para garantizar que las actividades relacionadas puedan llevarse a cabo como y cuando sea necesario.
6. Evaluación rutinaria de la coherencia con la que se sigue cada proceso y su eficacia en la gestión de los riesgos pertinentes para la seguridad de la información.

CONSEJO: Para cada proceso, designe a una persona responsable de garantizar que se lleven a cabo los pasos 2 a 6. Esta persona suele denominarse propietario del proceso. A esta persona se la suele denominar propietario del proceso.

Evaluación de riesgos para la seguridad de la información

Los métodos y técnicas de evaluación de riesgos descritos en la cláusula 6 deben aplicarse a todos los procesos, activos, información y actividades dentro del alcance del SGSI de la organización.

Dado que los riesgos no son estáticos, los resultados de estas evaluaciones deben revisarse frecuentemente, al menos una vez al año, o con mayor frecuencia si la evaluación identifica la presencia de uno o más riesgos significativos. Los riesgos también deben revisarse siempre que:

- Se completan todas las acciones de Tratamiento de Riesgos (véase más abajo).
- Se producen cambios en los activos, la información o los procesos de la organización.
- Se identifican nuevos riesgos.
- La experiencia o nueva información indican que la probabilidad y las consecuencias de cualquier riesgo identificado han cambiado.

CONSEJO: Para asegurarse de que su proceso de evaluación de riesgos cubre los tipos de eventos que requerirían una revisión, también debe tener en cuenta los controles del Anexo A.

Tratamiento de los riesgos para la seguridad de la información

El plan de tratamiento de riesgos que elabore no puede quedarse simplemente en una declaración de intenciones: debe aplicarse. Cuando sea necesario introducir cambios para tener en cuenta nueva información sobre riesgos y cambios en los criterios de evaluación de riesgos, el plan debe actualizarse y volver a autorizarse.

También se debe evaluar el impacto del plan y registrar los resultados de esta evaluación. Esto puede hacerse como parte de la revisión de la gestión o de los procesos de auditoría interna, o utilizando evaluaciones técnicas como pruebas de penetración en la red, auditorías de proveedores o auditorías de terceros sin previo aviso.

SECCIÓN 9: EVALUACIÓN DEL DESEMPEÑO

Existen tres formas principales de evaluar el rendimiento de un SGSI. Éstas son:

- Supervisar la eficacia de los controles del SGSI.
- Mediante auditorías internas.
- Reuniones de revisión por la dirección.

Seguimiento, medición, análisis y evaluación

Su organización tendrá que decidir qué necesita supervisar para asegurarse de que el proceso del SGSI y los controles de seguridad de la información funcionan según lo previsto. No es práctico para una organización supervisar manualmente todo en todo momento. Si intentara hacerlo, es probable que el volumen de datos fuera tan grande que resultara prácticamente imposible utilizarlo con eficacia. Por lo tanto, tendrá que tomar una decisión informada sobre qué supervisar. Las siguientes consideraciones serán importantes:

- ¿Qué procesos y actividades están sujetos a las amenazas más frecuentes y significativas?
- ¿Qué procesos y actividades presentan las vulnerabilidades inherentes más importantes?
- ¿Qué resulta práctico controlar y generar información significativa y oportuna?
- ¿Está automatizando su supervisión?
- Con cada proceso de supervisión que ponga en marcha, para que sea eficaz debe definirlo claramente:
  - Cómo se lleva a cabo el seguimiento
  - Cuando se emprende.
  - Quién es responsable de llevarla a cabo.
  - Cómo se comunican los resultados, cuándo, a quién y qué hacen con ellos.
  - Si los resultados de la supervisión identifican un rendimiento inaceptable, ¿cuál es el proceso o procedimiento de escalada para hacer frente a esta situación?

Para demostrar a un auditor que dispone de un proceso de supervisión adecuado, deberá conservar registros de los resultados de la supervisión, los análisis, las revisiones de evaluación y cualquier actividad de escalado.

Auditorías internas

El objetivo de las auditorías internas es comprobar los puntos débiles de los procesos del SGSI e identificar oportunidades de mejora. También son una oportunidad para que la alta dirección compruebe la eficacia del SGSI. Si se hacen bien, las auditorías internas pueden garantizar que no haya sorpresas en las auditorías externas.

Las auditorías internas que realice deben comprobar

- La coherencia con que se siguen y aplican los procesos, procedimientos y controles.
- Hasta qué punto sus procesos, procedimientos y controles generan los resultados previstos.
- Si su SGSI sigue cumpliendo la norma ISO 27001 y los requisitos de las partes interesadas.

Para garantizar que las auditorías se llevan a cabo con un calidad y de forma que aporten valor añadido, es necesario que las realicen personas que sean:

- Respetadas.
- Competentes.
- Familiarizadas con los requisitos de la norma ISO 27001.
- Capaces de interpretar su documentación y conocedores de técnicas y comportamientos de auditoría sólidos.

Lo más importante es que se les asigne tiempo suficiente para completar la auditoría y se les garantice la cooperación de los empleados pertinentes. Debe mantener un plan para llevar a cabo sus auditorías internas. Un auditor externo esperará que este plan garantice que todos los procesos de su SGSI se auditan en un ciclo de tres años y que cuentan con procesos que:

- Mostrar pruebas de un rendimiento deficiente (por ejemplo, a través de auditorías previas, o resultados de supervisión o incidentes de seguridad de la información).
- Gestionar los riesgos más importantes para la seguridad de la información.
- Se auditan con mayor frecuencia.

El auditor externo también esperará que las acciones identificadas en las auditorías se registren, sean revisadas por los empleados adecuados y se apliquen a tiempo para rectificar cualquier problema significativo. En el plazo de cierre de las auditorías, los auditores deben tener en cuenta las oportunidades de mejora identificadas que requieran una inversión significativa de recursos.

Revisión por la dirección

cLa revisión por la dirección es un elemento esencial de un SGSI. Es el punto formal en el que la Alta Dirección revisa la eficacia del SGSI y asegura su alineación con la dirección estratégica de la organización. Las revisiones por la dirección deben tener lugar a intervalos planificados y el programa general de revisión (es decir, una reunión o varias reuniones) debe cubrir como mínimo una lista de áreas básicas especificadas en la cláusula 9.3 de la norma.

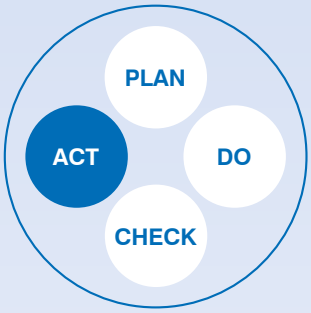
No es imprescindible que se celebre una única reunión de revisión de la gestión que abarque todo el orden del día.

Si actualmente celebra una serie de reuniones que cubren las aportaciones entre ellas, no hay necesidad específica de duplicarlas.

Deberá conservar información documentada sobre sus revisiones de gestión. Normalmente se trata de las actas de las reuniones o, tal vez, de las grabaciones de las conferencias telefónicas. No es necesario que sean notas extensas, pero deben contener un registro de las decisiones tomadas y las acciones acordadas, idealmente con responsabilidades y plazos.

CONSEJO: Si decide adaptar su programa actual de reuniones de gestión y estas reuniones cubren varias áreas, puede considerar la posibilidad de resumir las áreas que cubren estas reuniones en forma de tabla o procedimiento, de modo que tanto usted como un auditor tengan claro qué reuniones cubren cada una de las áreas de revisión requeridas.

SECCIÓN 10: MEJORA



El objetivo clave de la implantación de un SGSI debe ser reducir la probabilidad de que se produzcan sucesos relacionados con la seguridad de la información y su impacto. Ningún SGSI será perfecto. Sin embargo, un SGSI eficaz mejorará con el tiempo y aumentará la resistencia de la organización a los ataques contra la seguridad de la información.

No conformidad y acción correctiva

Uno de los principales motores de la mejora es aprender de los incidentes de seguridad, los problemas detectados en las auditorías, los problemas de rendimiento detectados en la supervisión, las quejas de las partes interesadas y las ideas generadas en las revisiones de la gestión.

Para cada oportunidad de aprendizaje identificada debe mantener un registro de:

- Qué ocurrió.
- Si el suceso tuvo consecuencias indeseables, qué medidas se adoptaron para contenerlas y mitigarlas.
- La causa raíz del suceso (si se determina).
- Las medidas adoptadas para eliminar la causa raíz.
- Una evaluación de la eficacia de las medidas adoptadas.
- Un análisis de tendencias de resultados similares puede ayudar a su empresa, pero no es un requisito.

Análisis de las causas

Para identificar medidas correctivas eficaces, es muy aconsejable realizar un análisis de la causa raíz del problema. Si no se llega al fondo de la cuestión, es probable que cualquier solución que se aplique no sea del todo eficaz. Un planteamiento sencillo, como el de los "cinco porqués", es una buena herramienta de análisis de las causas profundas: se empieza por el problema y luego se pregunta "por qué" suficientes veces para llegar a la causa profunda. Suele bastar con preguntar 5 veces, pero se puede profundizar.

Ejemplo:

Planteamiento del problema:

La organización fue infectada por el virus Wannacry.

¿Por qué?

Alguien hizo clic en un enlace de correo electrónico, se descargó el virus e infectó su PC.

¿Por qué?

No habían recibido ninguna formación para hacer clic en enlaces de correos electrónicos no deseados.

¿Por qué?

El responsable de formación está de baja por maternidad y la organización no ha implementado una cobertura para ellos.

¿Por qué?

El proceso de baja por maternidad no está contemplado en el Procedimiento de Gestión de Cambios, por lo que no se completó una evaluación de riesgos para identificar cualquier riesgo para la seguridad de la información.

CONSEJO: Puede que no disponga de recursos suficientes para realizar un análisis de causa raíz de cada suceso. Para priorizar sus esfuerzos, considere la posibilidad de realizar en primer lugar una evaluación sencilla del riesgo de un suceso y, a continuación, emprender el análisis de la causa raíz solo para aquellos que presenten un riesgo medio o alto.

SAQUE EL MÁXIMO PARTIDO A SUS SISTEMAS DE GESTIÓN

Consejos para implantar con éxito un SGSI

1. "¿Por qué? Asegúrese de que las razones para implantar un SGSI son claras y están alineadas con su dirección estratégica; de lo contrario, puede no obtener la aceptación de la dirección.

2. Considere "¿Para qué?" Implantar y mantener un SGSI requiere un compromiso importante, así que asegúrate de que su alcance es lo suficientemente amplio como para cubrir la información crítica que hay que proteger, pero no tan amplio como para no disponer de recursos suficientes.

3. Consiga que todas las partes interesadas participen. La dirección para establecer el contexto, los requisitos, la política y los objetivos; los directivos y empleados para la evaluación de riesgos, el diseño de procesos y la redacción de procedimientos.

4. Comunique ampliamente todo el proceso a todas las partes interesadas. Hágales saber lo que está haciendo, por qué lo está haciendo, cómo piensa hacerlo y cuál será su participación. Actualice periódicamente los avances.

5. Busca ayuda externa. No fracase por falta de conocimientos técnicos internos. La gestión de los riesgos de seguridad de la información requiere a menudo conocimientos especializados. Sin embargo, asegúrese de comprobar las credenciales de un tercero antes de contratarlo.

6. Los procesos y la documentación de apoyo deben ser sencillos. Puede ampliarse con el tiempo si es necesario.

7. Diseñar y aplicar normas en la práctica. No cometa el el error de documentar una norma demasiado elaborada que nadie pueda cumplir. Es mejor aceptar un riesgo y seguir buscando formas de gestionarlo.

8. Recuerde a sus proveedores. Algunos proveedores le ayudarán a mejorar su SGSI, otros aumentarán su riesgo. Debe asegurarse de que los proveedores de alto riesgo tengan controles al menos tan buenos como los suyos. Si no es así, busque alternativas.

9. Formar, formar y volver a formar. Es probable que la seguridad de la información sea un concepto nuevo para la mayoría de sus empleados. Es posible que tengan que cambiar hábitos arraigados durante muchos años. Es poco probable que baste con una sola sesión de concienciación.

10. No olvide asignar recursos suficientes para probar sus controles de forma rutinaria. Las amenazas a las que se enfrenta su organización cambian constantemente y debe comprobar si es capaz de responder a ellas.

PASOS TRAS LA IMPLEMENTACIÓN

1 FORMACIÓN DE SENSIBILIZACIÓN

- Su organización debe dar a conocer las distintas normas que abarca el SGI.
- Debe celebrar reuniones de formación separadas para la alta dirección, los mandos intermedios y los directivos de nivel inferior, lo que contribuirá a crear un entorno motivador, listo para la aplicación.

2 POLÍTICA Y OBJETIVOS

- su organización debe desarrollar una Política Integrada de Calidad/Política Medioambiental/ Política de Salud y Seguridad/Política de Seguridad de la Información y los objetivos pertinentes para ayudar a cumplir los requisitos.
- En colaboración con la alta dirección, la empresa debe organizar talleres con todos los niveles del personal directivo para perfilar los objetivos integrados.

3 ANÁLISIS INTERNO DE DEFICIENCIAS

- su organización debe identificar y comparar el nivel de cumplimiento de los sistemas existentes con los requisitos de las normas de su nuevo SGI.
- Todo el personal pertinente debe comprender las operaciones de la organización y elaborar un mapa de procesos para las actividades de la empresa.

4 DOCUMENTACIÓN / DISEÑO DE PROCESOS

- La organización debe crear documentación de los procesos conforme a los requisitos de las normas pertinentes.
- debe redactar y aplicar un manual, un cuaderno de procedimientos funcionales, instrucciones de trabajo, procedimientos de sistema y proporcionar los términos asociados.

5 DOCUMENTACIÓN / APLICACIÓN DE PROCESOS

- Los procesos y documentos elaborados en el paso 4 deben aplicarse en toda la organización y abarcar todos los departamentos y actividades.
- La organización debe organizar un taller sobre la aplicación de los requisitos de la norma ISO.

6 AUDITORÍA INTERNA

- Es esencial que la organización cuente con un sólido sistema de auditoría interna. Se recomienda la formación de auditores internos y NQA puede proporcionar formación de auditores internos para la(s) norma(s) que esté aplicando.
- Es importante aplicar medidas correctoras para mejorar cada uno de los documentos auditados, a fin de colmar las lagunas y garantizar la eficacia del SGI..

7 ORGANIZAR UNA REUNIÓN DE REVISIÓN DEL "SISTEMA" DE GESTIÓN

- TLa dirección de primer nivel debe revisar varios aspectos oficiales de la organización que son relevantes para las normas que se están implantando.
- Revisar la política, objetivos, resultados de la auditoría interna, del rendimiento de los procesos, de las quejas/recomendaciones/cumplimiento legal, de la evaluación de riesgos/incidentes y desarrollar un plan de acción tras la reunión, con acta.

8 ANÁLISIS EXHAUSTIVO DE LAS DEFICIENCIAS DE LOS SISTEMAS APLICADOS

- Debe realizarse un análisis formal de las deficiencias previo a la certificación para evaluar la eficacia y el cumplimiento de la implantación del sistema en la organización.
- Este análisis final de deficiencias preparará a su organización para la auditoría final de certificación.

9 ACCIONES CORRECTIVAS

- La organización debe estar preparada para la auditoría de certificación final, siempre que la auditoría de análisis de deficiencias realizada en el último paso y todas las no conformidades (NC) se hayan asignado acciones correctivas.
- Comprobar que todas las NC significativas están cerradas y que la organización está preparada para la auditoría final de certificación.

10 AUDITORÍA FINAL DE CERTIFICACIÓN

- Una vez completado, es de esperar que se recomiende a su organización que se registre según la norma exigida.
- ¡ENHORABUENA!

nqa.

www.nqa.com