Introducción a los sistemas integrados de gestión

PID_00258883

Natalia Cebrián Mirallas

Tiempo mínimo de dedicación recomendado: 4 horas

Universitat Oberta de Catalunya

Natalia Cebrián Mirallas

Índice

Introducción

Al objeto de afrontar la preparación de un sistema integrado de gestión de calidad, ambiental y de seguridad y salud en el trabajo, es necesario adoptar una táctica determinada ya que, a pesar de que las normas correspondientes guardan actualmente la misma estructura, tienen ciertos aspectos que son específicos de cada norma.

Consideramos conveniente separar tres aspectos muy determinados de la gestión de la organización, como son los que podríamos agrupar bajo los epígrafes de: organizativos, dinámicos y estáticos.

Los aspectos organizativos son los referidos a la descripción de la empresa y a la preparación del sistema. Definen los procesos que han de llevarse a cabo para que la organización cumpla sus fines, los objetivos que debe alcanzar y la forma como está estructurado el personal y los cuadros directivos, así como las condiciones de competencia y formación de dicho personal y las relaciones de comunicación internas.

Los aspectos dinámicos contemplan la preparación y ejecución de los procesos y son característicos de la gestión de calidad, ya que definen las actividades del personal, tanto en la realización de los trabajos como en el control de los resultados.

Los aspectos estáticos son característicos de la gestión ambiental y de seguridad y salud en el trabajo. Describen, fundamentalmente, la situación en que deben encontrarse las instalaciones a fin de que no sean agresivas para el personal ni para el entorno circundante y las protecciones que han de ser utilizadas para eliminar o disminuir dicha agresividad.

A continuación, en este primer módulo vamos a conocer estos elementos comunes y específicos de estos tres sistemas de gestión; y conoceremos otras normas o modelos que podrían integrarse también con alguno de estos tres sistemas de gestión o con todos ellos. Nos detendremos en normas de sistemas de gestión comunes en todas las organizaciones, como son el sistema de gestión de seguridad de la información, responsabilidad social y *compliance* penal.

Y por último, daremos unas breves pinceladas de la Norma ISO 31000, que marca directrices para realizar la gestión de riesgos en todas las nuevas normas de estructura de alto nivel.

Objetivos

Este primer módulo pretende los siguientes objetivos:

1. Recordar el principio básico de los sistemas de gestión basado en el ciclo de Deming o de mejora continua.

2. Conocer los factores de éxito y fracaso en la integración de sistemas de gestión.

3. Exponer los objetivos y qué se entiende por un sistema de gestión de calidad.

4. Determinar las normas aplicables en un sistema de gestión de calidad.

5. Exponer los dos modelos para implantar un sistema de gestión ambiental teniendo en cuenta la Norma ISO 14001 y el Reglamento EMAS.

6. Determinar las normas aplicables en un sistema de gestión ambiental.

7. Especificar las necesidades de las organizaciones en implantar un sistema de gestión en seguridad y salud en el trabajo y los objetivos que persiguen este tipo de sistemas de gestión.

8. Determinar las normas aplicables en un sistema de gestión de seguridad y salud en el trabajo, y conocer la nueva estructura de la norma de alto nivel ISO 45001:2018, así como las diferencias de esta nueva norma con la Norma OHSAS 18001:2007.

9. Especificar los elementos comunes y específicos de cada sistema de gestión.

10. Conocer otras normas y modelos que son susceptibles de ser integrados con estos tres sistemas de gestión, profundizando en las normas de sistemas de seguridad de la información, de responsabilidad social y de *compliance* penal que son comunes en todas las organizaciones.

11. Comentar la norma de directrices ISO 31000, muy útil para realizar la gestión de riesgos de las nuevas normas de estructura de alto nivel.

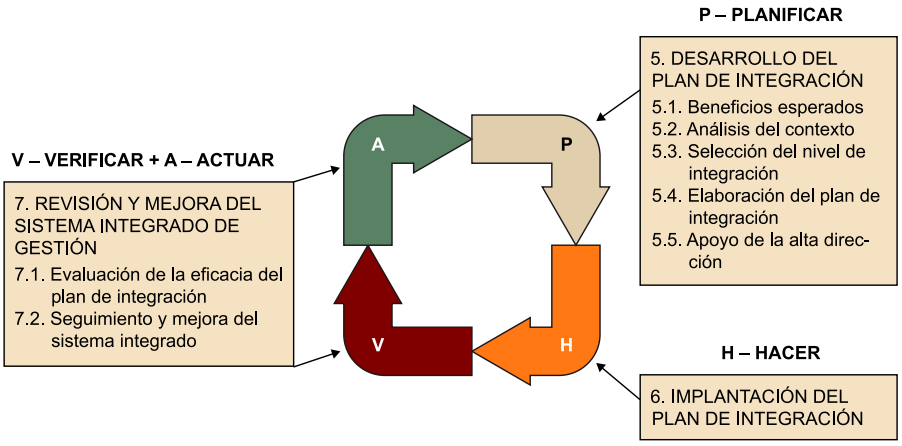
1. Principios de la gestión integrada en las organizaciones

Las organizaciones hoy desarrollan su actividad en un **entorno altamente competitivo**, en el que la globalización, el desarrollo sostenible y las tecnologías de la información y la comunicación son parámetros clave. Hoy nadie cuestiona este hecho. Pero sí se cuestiona cómo, de modo local e individual, puede una organización adaptarse a esa realidad.

En ese contexto, los **sistemas integrados de gestión** ayudan a las organizaciones a aplicar, de manera particular y local, unas necesidades identificadas en el ámbito global, de la mano de las organizaciones mundiales, por ejemplo de la salud, del comercio o del medio ambiente.

Un principio básico en la gestión por procesos y también en la integración de sistemas de gestión es la aplicación del **CICLO DEMING o PDCA** o en español PHVA (planificar + hacer + verificar + actuar). Se trata de un ciclo lógico que debe prevalecer en el diseño de las actividades, tanto con enfoque integrado o no.

Figura 1. Aplicación del ciclo PHVA en la implantación de un SIG



La Norma **UNE 66177:2005. «Sistemas de gestión. Guía para la integración de los sistemas de gestión»**, editada por la Asociación Española de Normalización (AENOR), establece cuatro aspectos o principios que la organización debería analizar para identificar el mejor método de integración posible y los recursos necesarios para su ejecución. Estos aspectos son los siguientes:

- Madurez
- Complejidad
- Alcance
- Riesgo

En módulos siguientes entraremos en profundidad en el conocimiento y aplicación de esta norma.

El sistema de gestión en la empresa debe ser solo uno.

Esta es una afirmación que, aunque algo exagerada o rigurosa, debe ser considerada un objetivo que debemos intentar lograr, aunque nunca lo logremos en realidad.

Las organizaciones hoy tienen una estructura con tendencia a crear sistemas diferentes, quizás uno o más por departamento; por ello es importante la visión NO departamental de la organización. Para así romper esas barreras que impiden la fluidez de la información, de la comunicación y de las actividades tanto departamentales como interdepartamentales.

Con el desarrollo e implantación de las normas de calidad, medio ambiente, seguridad laboral, seguridad alimentaria (si aplica) y, en los últimos tiempos, de la responsabilidad social y la ética empresarial, se han ido conformando diferentes áreas en la empresa. Ha ocurrido sobre todo en las medianas y grandes (más de cincuenta trabajadores), en las que las responsabilidades se han ido repartiendo a medida que el equipo directivo ha considerado introducir un nuevo concepto, una nueva norma, un nuevo sistema.

Pero esta actitud ha hecho, sobre todo, burocratizar el sistema de gestión y crear nuevos departamentos con sus respectivas barreras, y en según qué casos, más altas todavía que en el caso de los departamentos tradicionales, por la tendencia conocida de integración. Ese recelo ha hecho en algunas empresas que haya auténticas batallas de conservación de responsabilidades y competencias. Con todo, el sentido común está haciendo que el sistema se unifique, siendo el hilo conductor el **mapa de procesos y el sistema informático integral de gestión**.

La base del desarrollo de las actividades deben ser los procesos.

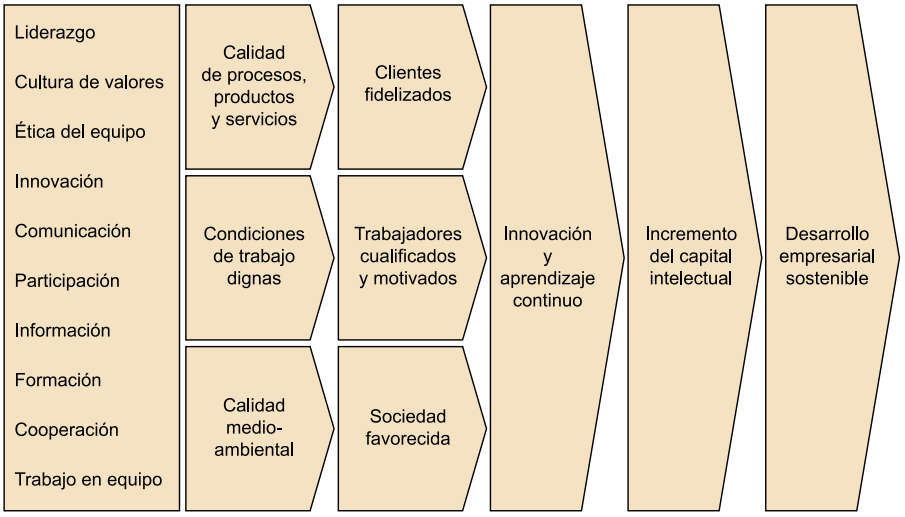
Esta es otra afirmación contundente pero indispensable para las organizaciones. Debe aceptarse que la integración basa su desarrollo en la gestión por procesos. Los departamentos deben dejar sus diferencias a un lado y centrarse en la eficiencia del sistema de gestión.

2. Factores de éxito y fracaso de un sistema integrado de gestión

Vamos a desarrollar una única visión sobre factores de éxito y de fracaso en el diseño, implantación y mejora de los sistemas de gestión integral. Y es que solo puede haber una línea de actuación exitosa, teniendo en cuenta factores clave. Si una organización no tiene en cuenta los factores clave en la gestión integral, inevitablemente pasarán a ser factores de fracaso.

Desarrollemos, por tanto, un listado ordenado de factores clave en la gestión integral, desde dos puntos de vista: uno teórico, basado en los criterios del modelo EFQM, y el otro práctico, basado en la opinión de varias empresas que han implantado exitosamente un sistema de gestión integral.

Figura 2



A continuación, veremos los factores clave en los sistemas integrados de gestión.

2.1. Factores relacionados con la dirección

La dirección de la empresa o entidad que se plantea implantar un sistema de gestión integral, generalmente, tiene una base sobre la que construir el resto del «edificio». Normalmente, se trata de empresas que han implantado como mínimo la Norma ISO 9001 y están certificadas. También puede darse el caso de que hayan realizado algunas mejoras e incluso incursiones relacionadas con la gestión ambiental, en línea con la Norma ISO 14001. Como mínimo también han desarrollado un sistema propio de gestión de la seguridad laboral, o bien lo tienen solucionado a través de una empresa subcontratada (hasta hace poco este servicio lo ofrecían las mutuas sanitarias).

La dirección tiene ciertas responsabilidades, unas determinadas por leyes reglamentarias y otras que son propias del buen hacer del equipo directivo. El sistema de gestión integral ayuda en parte a poner orden en esas obligaciones y también en los parámetros voluntarios que determinan el éxito empresarial, las buenas prácticas empresariales.

Por otro lado, el modelo EFQM determina un abanico amplio de criterios de buenas prácticas empresariales, que dependen directamente del equipo directivo. Vamos a relacionarlas a continuación, junto con los «factores clave» para el éxito del sistema de gestión integral:

1) Liderazgo, política y estrategia, gestión de recursos, gestión de personas y gestión de procesos

- El equipo directivo debe implicarse en la formación del personal, para conseguir que acepten los cambios.

- El equipo directivo debe planificar correctamente el proyecto de implantación del sistema de gestión integral, teniendo en cuenta los tiempos, dedicación y recursos asignados.

- El equipo directivo debe comunicar a todo el personal los avances y logros conseguidos gracias al sistema de gestión integral.

- El equipo directivo debe designar al coordinador del sistema de gestión entre las personas más valiosas de la empresa, tanto desde el punto de vista técnico como humano.

- El equipo directivo debe liderar el proyecto de diseño del sistema de gestión integral y revisar cada avance en su implantación y mejora.

- El equipo directivo debe definir una política integrada de gestión, adaptada a la realidad de la organización. Debe revisarla, actualizarla y comunicarla.

- El equipo directivo debe establecer las metas durante la implantación y los objetivos de calidad, medioambientales y de seguridad y salud laboral a conseguir en el desarrollo de los procesos integrados.

- El equipo directivo debe facilitar la necesaria formación en los diferentes ámbitos que cubre el sistema de gestión integral, de manera planificada y con seguimiento basado en el control de la eficacia de las acciones formativas.

- El equipo directivo debe realizar el seguimiento del sistema de gestión integral, a través de las reuniones periódicas de «revisión por la dirección» planificadas.

2.2. Factores relacionados con las personas

Las personas en la organización son la base del conocimiento, de la productividad, de la calidad y del futuro, ya que ellos son los que deben aplicar lo desarrollado en el sistema de gestión integral. De ellos depende que se cumplan los objetivos de calidad, medioambientales y de seguridad y salud laboral. Deben estar motivados, sin duda, pero también deben ser responsables de cada actividad que desarrollan, y tener siempre en cuenta los nuevos parámetros que se le han presentado y establecido en el sistema de gestión integral. A continuación, vamos a listar algunos «factores clave» para que la implantación y mejora del sistema de gestión integral sea posible, en lo que se refiere a las responsabilidades de las personas en la organización:

1) Resultados en las personas

- Las personas en la organización deben considerar la calidad, el medio ambiente y la seguridad y salud laboral como parámetros de gestión básicos que deben considerar en cada una de las actividades que desarrollan.

- Las personas deben conseguir los objetivos que se les proponen desde el ámbito directivo, y en caso de no hacerlo, averiguar cuál es la causa para llevar a cabo las acciones correctoras y preventivas necesarias.

- Las personas deben interactuar con el sistema de gestión integral, de manera que puedan seguir de manera correcta y eficiente los procesos determinados en él, y dado el caso, proponer mejoras que hagan del sistema una herramienta eficiente, más que eficaz.

- Las personas deben interactuar entre ellas, de manera asertiva y positiva, considerando la parte humana como la más importante. Gracias a este factor, pueden darse logros impensables en cualquier organización.

2.3. Factores relacionados con la sociedad

En un entorno cambiante, donde las organizaciones deben buscar siempre la reducción de costes, mediante la gestión de recursos tecnológicos que permiten más producción en menos tiempo, existe un elemento cada vez más importante y que es tenido cada vez más en cuenta a la hora de tomar decisiones que afectan al entorno en las organizaciones. La sociedad empieza a tomar protagonismo en sus diferentes áreas de influencia: el medio ambiente, el entorno social y el entorno económico. La capacidad que tenga la organización

para sopesar esas áreas de influencia, en relación con las decisiones estratégicas únicamente empresariales, va a determinar el nivel de **sostenibilidad** que tiene la organización.

Hoy, las organizaciones deben considerar que los recursos naturales son limitados, que el entorno social es importante y debe ser apoyado en algunas de sus necesidades, en las que la organización puede tener un papel importante. Debe también considerar que sus acciones tienen un peso en la sociedad, en lo económico, por lo que asuntos como invertir o desinvertir pueden afectar a ese entorno y deben ser tenidos en cuenta. A continuación, vamos a describir algunos de los «factores clave» relacionados con la sociedad y con los sistemas de gestión integral:

Resultados con la sociedad

- La organización debe relacionarse con su entorno, para conocer hasta qué punto lo afecta, ya sea positiva o negativamente. Por ejemplo, asociaciones de vecinos, culturales o de acción social.
- La organización debe tener en cuenta TODOS los reglamentos tanto en el ámbito nacional como local que le puedan afectar por su actividad, y ser absolutamente rigurosa con respecto a su cumplimiento. Este factor es especialmente importante por afectar especialmente al ámbito medioambiental y de seguridad y salud laboral.
- La organización debe colaborar con la Administración pública en todo aquello que pueda revertir en un bien para la sociedad.

2.4. Factores relacionados con los proveedores y clientes

Los clientes son la razón de ser de las empresas. Sin ellos, no tiene sentido la actividad empresarial. Por ello, son muy importantes en el desarrollo de un sistema de gestión integral. De qué puede servir ser riguroso con la prevención de riesgos laborales, con la seguridad alimentaria, con la calidad del producto o servicio o con la reducción de residuos, si nuestro cliente no valora ninguno de estos factores, ni los tiene en cuenta a la hora de llevar a cabo sus actividades, con alto nivel de despilfarro o accidentes laborales. E igualmente ocurre con los proveedores de nuestra organización. Ellos deben mantener nuestros mismos criterios de gestión, para así optimizar los resultados de tal esfuerzo.

A continuación, comentamos algunos de los «factores clave» para el éxito del sistema de gestión integral, relacionados en este caso con proveedores y clientes de nuestra organización:

Resultados en clientes y proveedores

- Los clientes y proveedores de la organización deben estar informados de cada uno de los logros conseguidos con nuestra gestión integral.
- Los clientes y proveedores deben ser invitados a visitar nuestras instalaciones, para que así puedan valorar la posibilidad de adoptar alguna de las medidas de gestión implantadas.
- Los proveedores, antes de su contratación, deben ser valorados por la organización para asegurar que cumple unos mínimos de gestión de calidad, medio ambiente y de seguridad y salud laboral.
- Los proveedores deben conocer las condiciones de entrega de productos o de prestación de servicios, para no afectar negativamente sobre el sistema de gestión integral.
- Los clientes deben recibir periódicamente algún tipo de cuestionario o entrevista que permita a la organización valorar si se están cumpliendo sus expectativas, no solo en cuanto a calidad y precio, sino en cuanto a otros parámetros como la gestión medioambiental, de seguridad y salud laboral o de seguridad alimentaria (dado el caso), por ejemplo.

3. Normas aplicables a los sistemas de gestión de la calidad

Los sistemas de gestión de la calidad son sistemas para establecer la política y objetivos y lograr dichos objetivos orientados a dirigir y controlar una organización con respecto a la calidad (adaptado de UNE-EN-ISO 9000:2015).

Los sistemas de gestión de la calidad son utilizados por las organizaciones para asegurar su capacidad de **proporcionar productos que cumplan los requisitos** de sus clientes, los requisitos legales y reglamentarios aplicables y **lograr la satisfacción del cliente** mejorando continuamente la eficacia.

La Norma ISO 9001 forma parte de la **serie de Normas ISO 9000**:

- **ISO 9000:2015**. Sistemas de gestión de la calidad. Fundamentos y vocabulario.
- **ISO 9001:2015**. Sistemas de gestión de la calidad. Requisitos.
- **ISO 9004:2018** Gestión de la calidad. Calidad en la organización. Directrices para alcanzar el éxito sostenido.
- **ISO 19011:2012**. Directrices para la auditoría de los sistemas de gestión.

En el desarrollo de la norma internacional ISO 9001 se han tenido en cuenta los principios de gestión de la calidad enunciados en las Normas ISO 9000 e ISO 9004.

Además de estas normas, otras muchas están relacionadas, tanto a escala internacional (Normas ISO) como nacional (Normas UNE).

La familia de Normas ISO 9000 se ha elaborado para asistir a las organizaciones, de todo tipo y tamaño, en la implantación y la operación de sus sistemas de gestión de la calidad, con el objetivo de que sean eficaces.

La adopción de un sistema de gestión de la calidad debería ser una **decisión estratégica de la organización**. El diseño y la implementación del sistema de gestión de la calidad de una organización están influenciados por el entorno de la organización, sus necesidades cambiantes, sus objetivos particulares, los productos que proporciona, los procesos que emplea, su tamaño y la estructura de la organización.

«Deberes» de la organización

- La organización deberá definir y gestionar los procesos necesarios para asegurar que el servicio esté conforme a los requisitos del cliente. Por lo tanto, debe elaborar los procedimientos del sistema de gestión de la calidad necesarios para describir los procesos requeridos. La extensión de los procedimientos dependerá, lógicamente, del tipo de organización que se trate.
- La organización debe establecer y mantener actualizado un **procedimiento** para identificar y tener acceso a los **requisitos legales** aplicables a la calidad de sus servicios.
- La organización tiene que establecer los objetivos de la calidad, para todas las funciones y niveles relevantes dentro de esta. Estos objetivos tienen que ser consistentes con la política de la calidad y con el compromiso para la mejora continua.

Resultados de la planificación de la calidad

La organización tiene que identificar las actividades y los recursos necesarios para alcanzar los objetivos de calidad. La planificación debe cubrir lo siguiente:

- Los procesos requeridos por el sistema de gestión de la calidad.
- La realización de los procesos y recursos necesarios, identificando las características de la calidad en las diferentes etapas, para llegar a los resultados deseados.
- Las actividades de verificación, los criterios de aceptación y los registros de la calidad necesarios.

4. Normas aplicables a los sistemas de gestión ambiental

Las normas que se encuentran vigentes actualmente en España para la implantación de un SGMA son las siguientes:

- **Norma UNE-EN-ISO-14001** sobre sistemas de gestión medioambiental: especificaciones y directrices para su utilización.

- **Reglamento 1221/2009(EMAS)**, por el que se permite que las empresas del sector industrial se adhieran con carácter voluntario a un sistema de gestión y auditoría medioambientales.

La filosofía de los dos sistemas es la misma: «Pretenden servir a aquellas organizaciones que están interesadas en conseguir y demostrar (mediante certificación por tercera parte) una **actuación ambiental correcta**». Aunque el **Reglamento EMAS tiene un mayor grado de compromiso y exigencia**, por tanto goza de un mayor reconocimiento público por parte de la Administración.

Por otro lado, la **familia de Normas ISO 14000** está compuesta por:

- ISO 14001:2015 Sistemas de gestión ambiental. Especificaciones y directrices para su utilización.

- ISO 14004:2016 Sistemas de gestión ambiental. Directrices generales sobre la implementación.

- ISO 14006: 2011 Sistemas de gestión ambiental. Directrices para la incorporación del ecodiseño.

- ISO 14010:1996 Directrices para la auditoría ambiental. Principios generales.

- ISO 14011:1996 Directrices para la auditoría ambiental. Procedimientos de auditoría. Auditoría de sistemas de gestión ambiental.

- ISO 14031:2013 Gestión ambiental. Evaluación del desempeño ambiental. Directrices

- ISO 14040:2006 Gestión ambiental. Evaluación del ciclo de vida. Principios y marco.

- ISO 14050:2009 Gestión ambiental. Vocabulario.

5. Normas aplicables a los sistemas de gestión de seguridad y salud en el trabajo

La nueva Norma ISO 45001:2018 es la **primera norma internacional de sistemas de gestión de seguridad y salud en el trabajo** que tiene por objeto sustituir en breve al estándar OHSAS 18001:2007. Esta norma concreta los requisitos necesarios para establecer un sistema de gestión de seguridad y salud en el trabajo, con orientación para su utilización, lo que permite a la empresa facilitar condiciones de trabajo seguras y saludables para la prevención de los daños y el deterioro de la salud de los empleados, además de **mejorar de forma proactiva el desempeño de la seguridad y salud en el trabajo**. Esto incluye el desarrollo e implementación de una política de la SST y objetivos que tengan en cuenta los requisitos legales aplicables y otros requisitos que la organización suscriba.

El objetivo global de la Norma ISO 45001:2018 es ayudar a las organizaciones a reducir esta carga al proporcionar un marco para mejorar la seguridad de los empleados, reducir los riesgos laborales y crear mejores condiciones de trabajo más seguras en todo el mundo.

Esta norma está destinada a ser aplicable a cualquier organización, independientemente de su tamaño, tipo y naturaleza, y todos sus **requisitos** están destinados a **integrarse en la gestión propia** de una organización. La International Organization for Standardization (ISO) ha desarrollado la Norma ISO 45001 con la finalidad de que **todas las organizaciones sean usuarios de la misma**. Así, no debería importar si una organización es una microempresa o un conglomerado global, si es una organización sin fines de lucro, una organización benéfica, una institución académica o un departamento gubernamental. Siempre y cuando la organización cuente con personas que trabajen en su nombre o que pueden verse afectadas por sus actividades, usar un enfoque sistemático para administrar la salud y la seguridad le reportará beneficios. Esta norma puede ser utilizada por pequeñas operaciones de bajo riesgo por igual, así como por alto riesgo y grandes organizaciones complejas. Si bien esta norma requiere que los riesgos de seguridad y salud en el trabajo sean abordados y controlados, también adopta un **enfoque basado en el riesgo** para el propio sistema de gestión de seguridad y salud en el trabajo, para garantizar:

1) que es efectivo, y

2) se mejora para cumplir con el siempre cambiante «contexto» de una organización.

Este enfoque basado en riesgo es coherente con la forma en que las organizaciones gestionan sus otros riesgos «comerciales» y, por lo tanto, fomenta la integración de los requisitos de la norma en el conjunto de procesos de gestión de las organizaciones.

La **implementación** de un sistema de gestión de seguridad y salud en el trabajo será una **decisión estratégica de una organización**, pudiendo respaldar así sus iniciativas de sostenibilidad, ya que si las personas están más seguras y saludables en el lugar de trabajo aumenta la rentabilidad de la organización.

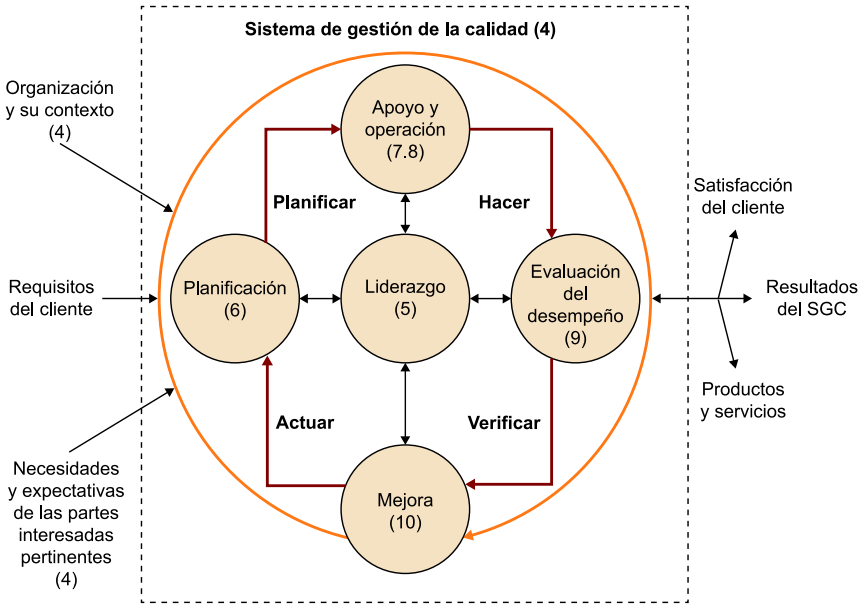
El sistema de gestión de seguridad y salud en el trabajo puede desempeñar un papel importante para garantizar que los riesgos se gestionen de manera efectiva. En este sentido, ISO 45001 enfatiza la necesidad de la participación de los trabajadores en el funcionamiento de una gerencia de seguridad y salud en el trabajo, además de exigir que una organización se asegure de que sus trabajadores sean competentes para hacer sus tareas asignadas de forma segura.

6. Elementos comunes y específicos en un sistema de gestión de calidad, ambiental y de seguridad y salud en el trabajo

Por integración de sistemas de gestión se entiende la acción y el efecto de aunar o fusionar los elementos de gestión comunes y semejantes, de las normas de referencia implicadas en los sistemas a integrar, tanto en lo que se refiere a la documentación aplicable como en la implementación de los mismos. Esto anterior implica que las organizaciones tienen que llevar a cabo acciones que permitan compartir herramientas, metodologías o sistemáticas para la gestión de diferentes áreas, y para dar cumplimiento a las diferentes normas o modelos por los que se rige esta gestión.

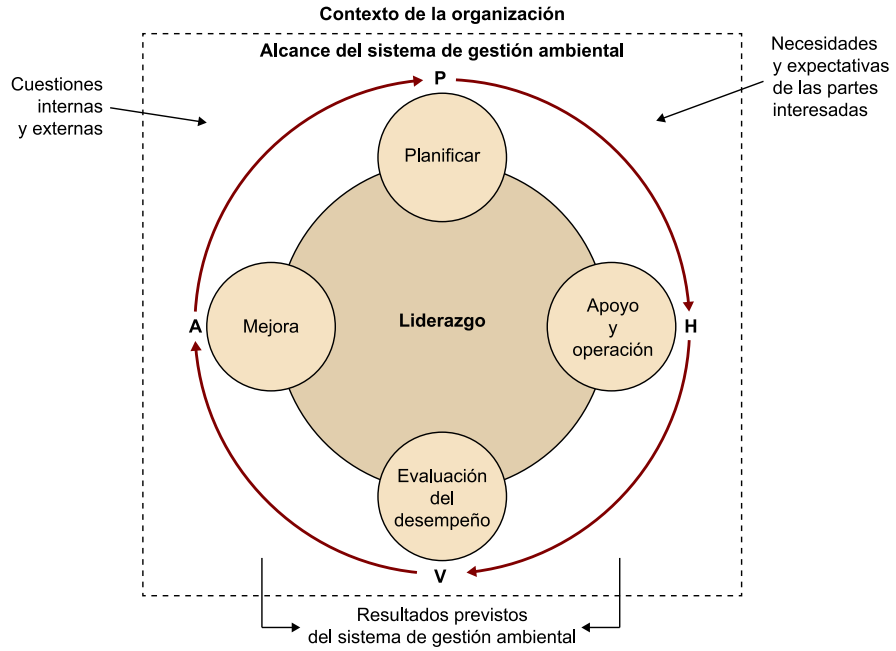
Así, por ejemplo, cuando se plantea la integración de la calidad, medio ambiente y la seguridad y salud en el trabajo en una organización, es posible identificar muchos elementos comunes y semejantes que pueden ser aunados o fusionados. En las siguientes figuras se puede apreciar.

Figura 3. Estructura de la Norma ISO 9001:2015



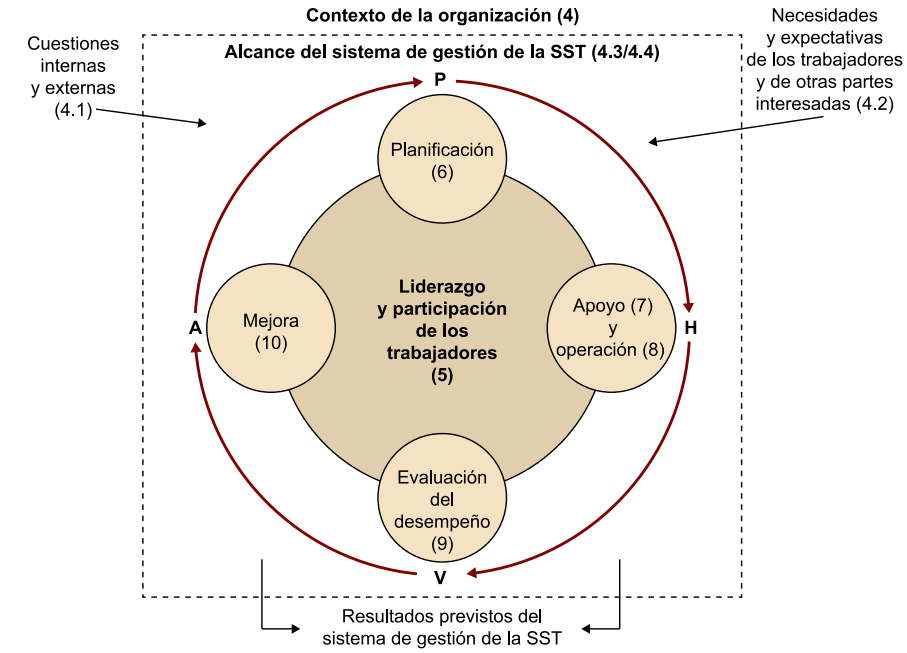
En la figura adjunta se aprecia cómo la organización (basada en sus líderes) planifica (P) el sistema y sus procesos, así como los recursos necesarios para generar y proporcionar los resultados de acuerdo a los requisitos del cliente y las políticas de la organización, y para identificar y abordar los riesgos y oportunidades. Se implementa (H) lo planificado anteriormente, se realiza el seguimiento y medición (V) de los procesos y los productos y servicios y se informa sobre los resultados. Finalmente, cabe tomar acciones para mejorar el desempeño (A).

Figura 4. Estructura de la Norma ISO 14001:2015



En esta figura se aprecia cómo la organización (basada en sus líderes) establece los objetivos ambientales y los procesos necesarios para generar y proporcionar los resultados de acuerdo a la política ambiental de la organización (P). Se implementan (H) los procesos según lo planificado, se realiza el seguimiento y medición (V) de los procesos. Finalmente, cabe tomar acciones para mejorar continuamente (A).

Figura 5. Estructura de la Norma ISO 45001:2018



En esta figura se aprecia que este nuevo sistema de gestión requiere de liderazgo, compromiso y participación de todos los niveles y funciones de la organización. Para ello es necesario establecer objetivos, programas y procesos necesarios para entregar resultados de acuerdo con la política de la organización

(P), implementar los procesos según lo planeado (D), monitorear y medir actividades y procesos con respecto a la política y los objetivos, e informar de los resultados (C) y tomar medidas para mejorar continuamente el rendimiento de seguridad y salud en el trabajo para lograr los resultados previstos (A).

Las tres normas con **estructura de alto nivel** adoptan un enfoque basado en el riesgo; se otorga relevancia a la gestión de competencias y la toma de conciencia del personal, se enfatiza la gestión del conocimiento de la organización y de su contexto y se da una mayor comprensión en las necesidades y expectativas de las partes interesadas.

Esta **estructura común** (estructura de norma de alto nivel) a estas tres normas en cuanto a requisitos responde a lo siguiente:

- Capítulo 4. Contexto de la organización.
- Capítulo 5. Liderazgo.
- Capítulo 6. Planificación.
- Capítulo 7. Soporte.
- Capítulo 8. Operaciones.
- Capítulo 9. Evaluación del desempeño.
- Capítulo 10. Mejora.
- Anexo de orientación.

A continuación, detallamos en rasgos generales los nuevos requisitos de estos capítulos:

- **Capítulo 4**: Se establece que las organizaciones deben conocer su entorno, conocer las necesidades de las partes interesadas y determinar el alcance del sistema de gestión. Otro punto destacable es que el sistema de gestión debe estar alineado con la dirección estratégica de la organización.

- **Capítulo 5**: Se establece que la alta dirección debe liderar el sistema de gestión y establecer la política del sistema, la definición de funciones y responsabilidades y de compromisos concretos con respecto al sistema de gestión.

- **Capítulo 6**: Sobre la planificación se establece cómo implementar acciones para gestionar el riesgo y las oportunidades que surgen cuando se planifican los sistemas de gestión. Por otra parte, los objetivos de la organización han de ser planificados de forma detallada.

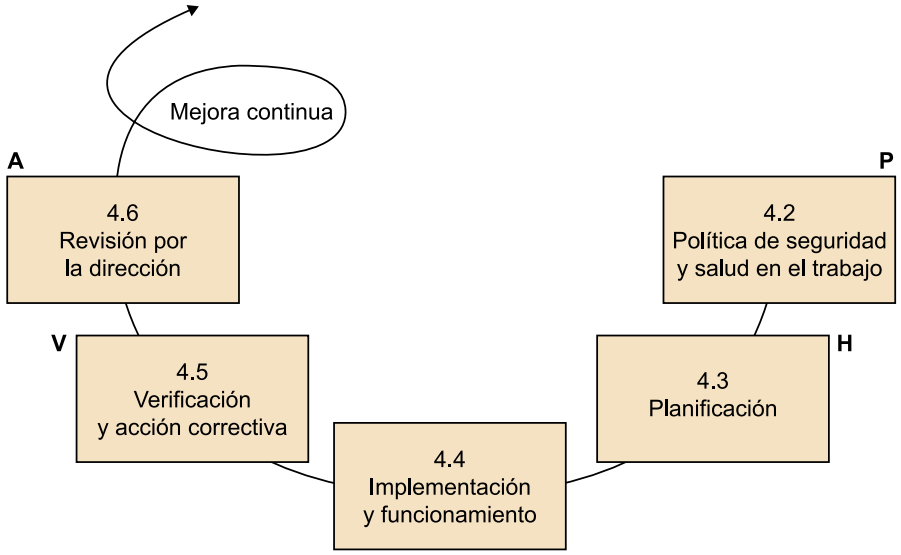
- **Capítulo 7**: Está basado en los recursos necesarios para implementar y gestionar el sistema de gestión; se refiere a los recursos (humanos y materiales). También se incluyen requisitos sobre la competencia y toma de conciencia del personal, sobre cómo ha de ser la comunicación y los controles a establecer sobre información documentada.

- **Capítulo 8**: Se refiere a la operación y está orientado a cómo se deben planificar, implementar y controlar los procesos del sistema de gestión. En este apartado, cada norma establece sus requisitos específicos que los diferencia del resto de las normas. Se establecen requisitos propios de la materia de estudio, como puede ser calidad, medioambiente, etc.

- **Capítulo 9**: Se aborda el seguimiento, la medición, el análisis y la evaluación del sistema de gestión y sus componentes, es decir, la evaluación del desempeño. También se establecen los requisitos para auditar el sistema y para la revisión del sistema por parte de la alta dirección.

- **Capítulo 10**: Se trata sobre la mejora, se desarrollan los requisitos referidos a las acciones correctoras y a la mejora continua.

Figura 6



De este modo se facilita la integración de los sistemas compartiendo la misma estructura. A continuación, se facilita un resumen de los **cambios más significativos**:

- El centro de la implementación de las normas son los procesos.

- No se requiere un manual obligatorio (requisito de ISO 9001).

- No se solicitan procedimientos documentados explícitos.

- Incorporación de la denominación e información documentada.

- Mantener información documentada (antiguos documentos).

- Conservar información documentada (antiguos registros).

- Incorporación de la gestión de riesgos.

- Incorporación de la gestión de cambios.

Por otro lado, también existen **elementos específicos** de cada norma, que son los que detallamos en la siguiente tabla:

Numerales Anexo SL	Diferencias
1. Objeto y campo aplicación	Similar forma enfocada a cada norma.
2. Referencias normativas	Manejo específico para cada norma.
3. Términos y definiciones	Manejo específico para cada norma.
4. Contexto de la organización	• ISO 9001 requiere una planeación estratégica; las otras dos no. • En ISO 9001 se pueden hacer exclusiones; en las otras dos no.
5. Liderazgo	• La ISO 45001 tiene un requisito específico 5.4 Consulta y participación de los trabajadores, las otras dos no.
6. Planificación	• La ISO 14001 e ISO 45001 tienen un requisito específico 6.1.3 para lo legal y otros requisitos. • ISO 9001 tiene un requisito para el control de cambios 6.3; las otras dos no.
7. Apoyo	• En ISO 9001 el requisito 7.1 de recursos es muy amplio; en las otras dos normas no. • En ISO 45001 el requisito de comunicación 7.4.1 es más específico que en las otras dos.
8. Operación	• El capítulo 8 en la ISO 9001 es muy extenso y es el centro de esta norma (diseño, compras, producción, control de calidad). En ISO 14001 e ISO 45001 es puntual al control operacional y las emergencias. • En ISO 45001 incluye gestión de cambio, compras, contratistas. • ISO 14001 e ISO 45001 tienen un requisito para emergencias; ISO 9001 no. • No hay en ISO 14001 e ISO 45001 un requisito explícito para el control de no conformidades (8.7) como lo hay en ISO 9001.
9. Evaluación y desempeño	• ISO 9001 tiene un requisito específico para el análisis de datos 9.1.3; las otras dos no. • ISO 14001 e ISO 45001 manejan la metrología en este capítulo; ISO 9001 lo hace en el numeral 7.1.5.
10. Mejora	• La ISO 45001 usa la palabra específica «incidentes».

7. Presentación de otros sistemas de gestión. Normas y modelos

Otros modelos y normas se han editado con el fin de **satisfacer las necesidades de algunos sectores**, que por el tipo de producto que fabrican o servicio que prestan se ha considerado más adecuado un desarrollo específico.

En el siguiente cuadro vamos a analizar algunas de estas normas y modelos desarrollados para **sectores específicos**:

Norma-modelo	Sector	Organismo/descripción	Portal web
ISO 22000:2005	Agroalimentario	ISO. Norma creada para desarrollar e implantar sistemas de gestión de seguridad alimentaria, cuya intención final es conseguir una armonización en las normas existentes relacionadas con la calidad de la cadena alimentaria.	www.iso.org
IATF 16949:2016	Automoción	IATF (International Automotive Task Force). Norma creada con el fin de armonizar las diferentes evaluaciones y sistemas de certificación en la cadena de suministro global del sector automotriz.	www.iatfglobaloversight.org/
ISO 13485:2016	Sanitario	ISO. Norma creada para establecer un conjunto de requisitos regulatorios armonizados para los sistemas de gestión de la calidad dentro del sector de los productos sanitarios.	www.iso.org
ISO 27001:2013	Seguridad de la información	ISO. Norma creada para conseguir la preservación de la confidencialidad, integridad y disponibilidad de la información, así como de los sistemas implicados en su tratamiento, dentro de una organización.	www.iso.org
ISO 20000:2011	Servicios de TI	ISO. Define los requerimientos necesarios para realizar una entrega de servicios de tecnologías de la información (TI) alineados con las necesidades de negocio, con la máxima calidad y seguridad.	www.iso.org
UNE 166002:2014	Investigación, desarrollo e innovación tecnológica, I +D+i	UNE. Norma española que proporciona directrices con el fin de considerar tanto la eficacia como la eficiencia del sistema de gestión de I+D+i y, por lo tanto, el potencial de mejora de los resultados, así como la mejora de los procedimientos de transferencia interna de estos resultados para optimizar los procesos de innovación tecnológica de la organización. (Es una norma de directrices. No es certificable).	www.aenor.es
ISO 26000:2010	Responsabilidad social	ISO. Norma que pretende ayudar a las organizaciones a contribuir al desarrollo sostenible. Tiene como propósito fomentar que las organizaciones vayan más allá del cumplimiento legal, reconociendo que el cumplimiento de la ley es una obligación fundamental para cualquier organización y una parte esencial de su responsabilidad social. (Es una norma de directrices. No es certificable).	www.iso.org www.globalreporting.org
IQNet SR10: 2015		IQNet. Norma que establece los requisitos de un sistema de gestión de la responsabilidad social para organizaciones comprometidas con los principios y recomendaciones sobre responsabilidad social existentes y, en particular, los contenidos en la norma internacional ISO 26000. Es una norma certificable.	www.iqnet-certification.com

Norma-modelo	Sector	Organismo/descripción	Portal web
UNE 19601:2017	Administrativa y legal	UNE. Norma española creada para prevenir la comisión de delitos y reducir el riesgo penal en las organizaciones y, con ello, favorecer una cultura ética y de cumplimiento. (Sistema de gestión de *compliance* penal).	www.aenor.es

7.1. Sistemas de gestión comunes en las organizaciones

Muchos de los sistemas de gestión mencionados anteriormente hacen referencia a sectores específicos, pero algunos de estos sistemas de gestión son comunes en muchas organizaciones y por ello consideramos necesario profundizar en ellos. Estas normas son las que a continuación mencionamos:

7.1.1. Norma ISO 27001:2013

Esta norma proporciona los requisitos relacionados con los sistemas de gestión de seguridad de la información con el fin de permitir a una organización evaluar el riesgo y aplicar controles adecuados para **preservar la confidencialidad, integridad y disponibilidad de los activos de información**. El objetivo fundamental es proteger la información de su organización para que no caiga en las manos equivocadas o se pierda para siempre.

La dependencia en los servicios y sistemas de información hace que las organizaciones se vean cada vez más vulnerables frente a las amenazas de seguridad. La información constituye un activo que, al igual que otros activos importantes de negocio, es de gran valor para una empresa y por tanto necesita contar con medidas de seguridad adecuadas. Mediante una correcta identificación y clasificación de estos activos y una sistemática evaluación de riesgos por amenazas y vulnerabilidades, su empresa puede demostrar a clientes, consumidores, accionistas, autoridades y a la sociedad en general que se mantiene la confidencialidad, integridad y disponibilidad de los activos de información.

Es **aplicable** esta norma **a todas las organizaciones**, ya que todas las organizaciones disponen de activos y sistemas de información. La Norma ISO 27001 cubre todos los aspectos del tratamiento e intercambio de la información (sin importar el soporte), incluyendo la seguridad del perímetro físico y las personas. Esta norma ayuda a asegurar la continuidad del negocio en casi todas las circunstancias, tales como incendios, inundaciones, piratería, pérdida de datos, violación de la confidencialidad e incluso el terrorismo.

Ha sido desarrollada **sobre la base del Anexo SL**, en la que se proporciona un formato y un conjunto de alineamiento que siguen el desarrollo documental de un sistema de gestión sin que le importe el enfoque empresarial; se alinean bajo la misma estructura todos los documentos que se relacionan con el sistema de gestión de seguridad de la información y así se evitan problemas de

integración con otros marcos de referencia. Además, la nueva estructura (estructura de alto nivel) queda así (comparándola con la anterior norma del año 2005):

0) Introducción

En la Norma ISO 27001:2013 el cambio más significativo es la eliminación de la sección «Enfoque del proceso» que sí contenía la versión 2005, donde se describía el modelo PHVA, considerándose el corazón del sistema de gestión de seguridad de la información (SGSI).

1) Alcance

En la Norma ISO 27001:2013 se establece como obligatorio el cumplimiento de los requisitos especificados entre los capítulos 4 a 10 de dicho documento, para poder obtener una conformidad de cumplimiento y así poder certificase.

2) Referencias normativas

El estándar ISO 27002 ya no será referencia normativa para la Norma ISO 27001:2013, aunque se puede considerar necesario el desarrollo de una declaración de aplicabilidad. La Norma ISO 27001:2013 se convierte en una referencia normativa obligatoria y única, ya que contiene todos los nuevos términos y definiciones.

3) Términos y definiciones

Los términos y las definiciones que se encontraban en la ISO 27001:2005 fueron trasladados y agrupados en la sección 3 de la Norma ISO 27001:2013 «Fundamento y vocabulario», con el fin de contar con una sola guía de términos y definiciones que sea consistente.

4) Contexto de la organización

Se identifican todos los problemas externos e internos que rodean a la empresa:

- Se intuyen todos los requisitos para definir el contexto del SGSI sin importar el tipo de empresa que sea y el alcance que tenga.

- Se introduce una nueva figura como un elemento primordial para definir el alcance del SGSI.

- Se establece la prioridad de identificar y definir todas las necesidades de las partes interesadas con relación a la seguridad de la información y las expectativas creadas por el sistema de gestión de seguridad de la informa-

ción, ya que esto determinará las políticas de seguridad de la información y todos los objetivos a seguir para el proceso de gestión de riesgos.

5) Liderazgo

Se realiza un ajuste de la relación y las responsabilidades de la gerencia de la organización con respecto al sistema de gestión de seguridad de la información, destacando cómo se deberá demostrar el compromiso, como por ejemplo:

- Garantizar que los objetivos del SGSI y la política de seguridad de la información antes se conocían como la política del SGSI.
- Se debe garantizar la disponibilidad de todos los recursos para la implantación del SGSI.
- Se garantiza que los roles y las responsabilidades para la seguridad de la información se asignan y se comunican de forma adecuada.

6) Planificación

Este apartado de la Norma ISO 27001:2013 se enfoca a la definición de los objetivos de seguridad como un todo; estos objetivos deben estar claros y se deben contar con planes específicos para conseguirlos.

Se pueden presentar grandes cambios en el proceso de evaluación de riesgos:

- El proceso para evaluar los riesgos ya no se encuentra enfocado a los activos, las vulnerabilidades y las amenazas.
- La metodología se enfoca con el objetivo de identificar todos los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información.
- El nivel de riesgos se determina por la probabilidad de que ocurra un riesgo y las consecuencias generadas, si el riesgo se materializa.
- Se elimina el término propietario del activo y se adopta el término propietario del riesgo.
- Los requisitos no han sufrido transformaciones significativas.

7) Soporte

Los requisitos del soporte para el establecimiento de la implementación y mejora del SGSI, que incluye:

- Recursos.
- Personal competente.
- Conciencia y comunicación de todas las partes interesadas.

Se incluye una nueva definición que es «información documentada»; esta sustituye a los términos «documentos y registros», establece el proceso de documentar, mantener, controlar y conservar la documentación que corresponde al sistema de gestión de seguridad de la información. La Norma ISO 27001:2013 se enfoca en el contenido de los documentos y no en que existe un determinado número de estos.

8) Operación

Establece todos los requisitos para medir el funcionamiento del sistema de gestión de seguridad de la información, todas las expectativas de la gerencia de la organización y la retroalimentación sobre estas, además de cumplir con la Norma ISO 27001:2013. Además, la organización se plantea y controla las operaciones y los requisitos de seguridad; el pilar de este proceso se centra en realizar las evaluaciones de riesgos de seguridad de la información de forma periódica por medio de un programa elegido. Todos los activos, las vulnerabilidades y las amenazas ya no son la base principal de la evaluación de riesgos. Solo se requiere para realizar la identificación de los riesgos, que están asociados a la confidencialidad, la integridad y la disponibilidad.

9) Evaluación del desempeño

La base para poder realizar la identificación y la medición de la eficiencia y el desempeño que realiza el sistema de gestión de seguridad de la información continúa siendo las auditorías internas y las revisiones del SGSI.

Se tiene que considerar el estado en el que se encuentran los planes de acción para poder atender las no conformidades como es debido; además, se establece la necesidad de definir quién y cuándo realiza las evaluaciones, además de quién tiene que analizar la información que se ha recolectado.

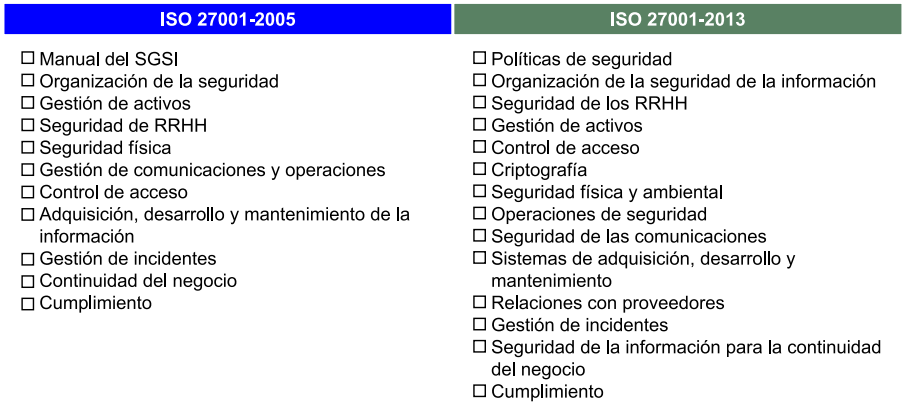
10) Mejora

El principal elemento del proceso de mejora son las no conformidades identificadas, las cuales tienen que contabilizarse y compararse con las acciones correctivas para asegurarse de que no se repitan y que las acciones correctoras que se realicen sean efectivas.

Cabe añadir también que se han realizado cambios en su contenido, agregando y eliminando controles, reestructurando especialmente el Anexo «A», donde se aumenta a 14 los dominios de control y se reduce en 20 la cantidad de controles, quedando en 113.

Dentro de los nuevos dominios de control aparece Criptografía, que se separa del dominio Adquisición, desarrollo y mantenimiento de la información. El segundo dominio de control adicional es Relación con proveedores, y el tercero es resultado de la división del dominio Gestión de comunicaciones y operaciones en dos nuevos dominios: Operaciones de seguridad y Seguridad de las comunicaciones. Las diferencias entre los dominios de control entre las dos versiones de norma son las siguientes:

Figura 7



Como hemos dicho en el Anexo A de la Norma ISO 27001, se reflejan **los dominios de control y mecanismos de control** que están descritos en la Norma **ISO-IEC 27002** (la Norma ISO 27002 es un documento complementario a la Norma ISO 27001). Lo interesante es que las empresas que quieran certificarse con esta norma **ya no están obligadas** a implementar todos los controles de este anexo, por lo que este se convierte en una guía para **evitar que se omitan controles importantes** por parte de la organización en el momento de implementar su sistema de gestión (SGSI). Esta nueva característica brinda mayor flexibilidad a las empresas para implementar de la manera más adecuada el sistema de gestión.

La **información documentada** (documentos y registros) **que es requerida** en esta norma es la siguiente:

Documentos	Capítulo ISO 27001:2013
Alcance del SGSI	4.3
Políticas y objetivos de seguridad de la información	5.2 - 6.2
Metodología de evaluación y tratamiento de riesgos	6.1.2

Documentos	Capítulo ISO 27001:2013
Declaración de aplicabilidad	6.1.3.d
Plan de tratamiento del riesgo	6.1.3.e - 6.2
Informe sobre evaluación y tratamiento de riesgos	8.2 - 8.3
Definición de funciones y responsabilidades de seguridad	a.7.1.2 - a.13.2.4
Inventario de activos	a.8.1.1
Uso aceptable de los activos	a.8.1.3
Política de control de acceso	a.9.1.1
Procedimientos operativos para gestión de TI	a.12.1.1
Principios de ingeniería para sistema seguro	a.14.2.5
Política de seguridad para proveedores	a.15.1.1
Procedimiento para gestión de incidentes	a.16.1.5
Procedimientos de la continuidad del negocio	a.17.1.2
Requisitos legales, normativos y contractuales	a.18.1.1
Registros de capacitación, habilidades, experiencia y calificaciones	7.2
Resultados de supervisión y medición	9.1
Programa de auditoría interna	9.2
Resultados de las auditorías internas	9.2
Resultados de la revisión por parte de la dirección	9.3
Resultados de acciones correctivas	8.2 - 8.3
Definición de funciones y responsabilidades de seguridad	10.1
Registros sobre actividades de los usuarios, excepciones y eventos de seguridad	a.12.4.1 - a.12.4.3

Esta es la información documentada mínima, ya que la norma permite que se agregue cualquier otro documento que pueda mejorar el nivel de seguridad de la información. La mayoría de los documentos son los documentos habituales de cualquier sistema de gestión, pero hay algunos documentos específicos de esta norma que a continuación pasamos a detallar en profundidad:

- **Declaración de aplicabilidad**: Se redacta sobre la base de los resultados del tratamiento del riesgo; es un documento clave dentro del SGSI porque describe no solo qué controles del Anexo A son aplicables, sino también cómo se implementarán y su estado actual. También deberíamos considerar la declaración de aplicabilidad como un documento que describe el perfil de seguridad de su empresa.

- **Plan de tratamiento del riesgo**: Este es, básicamente, un plan de acción sobre cómo implementar los diversos controles definidos por la declaración de aplicabilidad. Este documento se desarrolla en función de la declaración de aplicabilidad y se utiliza y actualiza activamente a lo largo de toda la implementación del SGSI. A veces, se puede fusionar con el plan del proyecto.

- **Uso aceptable de los activos**: Habitualmente, este documento se confecciona bajo la forma de una política y puede cubrir un amplio rango de temas porque la norma no define muy bien este control.

- **Política de control de acceso**: En este documento se puede cubrir solo la parte comercial de la aprobación de acceso a determinada información y sistemas; también se puede incluir el aspecto técnico del control de acceso. Además, podemos optar por definir reglas para acceso lógico únicamente o también para acceso físico. Este documento se debería redactar después de finalizado el proceso de evaluación y tratamiento de riesgos.

- **Principios de ingeniería para sistemas seguros**: Este es un nuevo control en ISO 27001:2013 y requiere que se documenten los principios de ingeniería de seguridad bajo la forma de un procedimiento o norma y que se defina cómo incorporar técnicas de seguridad en todas las capas de arquitectura: negocio, datos, aplicaciones y tecnología. Estos principios pueden incluir validación de datos de entrada, depuración, técnicas para autenticación, controles de sesión segura, etc.

- **Política de seguridad para proveedores**: Este también es un control nuevo en ISO 27001:2013, y una política de este tipo puede abarcar un amplio rango de controles: cómo se realiza la selección de potenciales contratistas, cómo se ejecuta la evaluación de riesgos de un proveedor, qué cláusulas incluir en el contrato, cómo supervisar el cumplimiento de cláusulas contractuales de seguridad, cómo modificar el contrato, cómo cerrar el acceso una vez cancelado el contrato, etc.

- **Procedimiento para gestión de incidentes**: Este es un procedimiento importante que define cómo se informan, clasifican y manejan las debilidades, eventos e incidentes de seguridad. Este procedimiento también define cómo aprender de los incidentes de seguridad de la información para que se puedan evitar en el futuro. Un procedimiento de esta clase también puede invocar al plan de continuidad del negocio si un incidente ha ocasionado una interrupción prolongada.

- **Procedimientos de la continuidad del negocio**: Generalmente se trata de planes de continuidad del negocio, planes de respuesta ante incidentes, planes de recuperación para el sector comercial de la organización y planes de recuperación ante desastres (planes de recuperación para infraestructura de TI). Estos procedimientos se describen con mayor detalle en

la Norma ISO 22301, la principal norma internacional para continuidad del negocio.

- **Resultados de supervisión y medición**: La forma más sencilla de describir cómo se miden los controles es a través de políticas y procedimientos que definan a cada control. En general, esta descripción puede ser realizada al final de cada documento, y cada descripción tiene que definir los tipos de ICD (indicadores clave de desempeño) que es necesario medir para cada control o grupo de controles. Una vez que se establece este método de control, se debe realizar la medición en función de dicho método. Es importante reportar los resultados de esta medición de forma regular a las personas que están a cargo de la evaluación.

- **Registros sobre actividades de los usuarios, excepciones y eventos de seguridad**: Habitualmente, se llevan de dos formas. Primero, en formato digital, generados en forma automática o semiautomática como registros de diversas TI y de otros sistemas, y segundo, en papel, donde cada registro se hace manualmente. Procedimiento para control de documentos. En general, este es un procedimiento independiente y ya se implementa en otras normas como ISO9001, ISO14001, ISO45001 o similares; podemos utilizar el mismo procedimiento para todos estos sistemas de gestión.

- **Controles para gestión de registros**: La forma más sencilla es redactar el control de registros en cada política o procedimiento (u otro documento) que requiera la generación de un registro. Estos controles, normalmente, son incluidos hacia el final de cada documento y se confeccionan bajo el formato de una tabla que detalla dónde se archiva el registro, quién tiene acceso, cómo se protege, por cuánto tiempo se archiva, etc.

La **información documentada no obligatoria de uso frecuente** en la Norma ISO 270001:2013 es la siguiente:

Documentos	Capítulo ISO 27001:2013
Procedimiento para control de documentos	7.5
Controles para gestión de registros	7.5
Procedimiento para auditoría interna	9.2
Procedimiento para medidas correctivas	10.1
Política trae tu propio dispositivo (BY OD)	a.6.2.1
Política sobre dispositivos móviles y teletrabajo	a.6.2.1
Política de clasificación de la información	a.8.2.1 / 2 / 3
Política de claves	a.9.2.1 / 2 / 4, a.9.3.1, a.9.4.3
Política de eliminación y destrucción	a.8.3.2, a.11.2.7

Documentos	Capítulo ISO 27001:2013
Procedimiento para trabajo en áreas seguras	a.11.1.5
Política de pantalla y escritorio limpio	a.11.2.9
Política de gestión de cambio	a.12.1.2, a.14.2.4
Política de creación de copias de seguridad	a.12.3.1
Política de transferencia de la información	a.13.2.1 / 2 / 3
Análisis del impacto en el negocio	a.17.1.1
Plan de prueba y verificación	a.17.1.3
Plan de mantenimiento y revisión	a.17.1.3

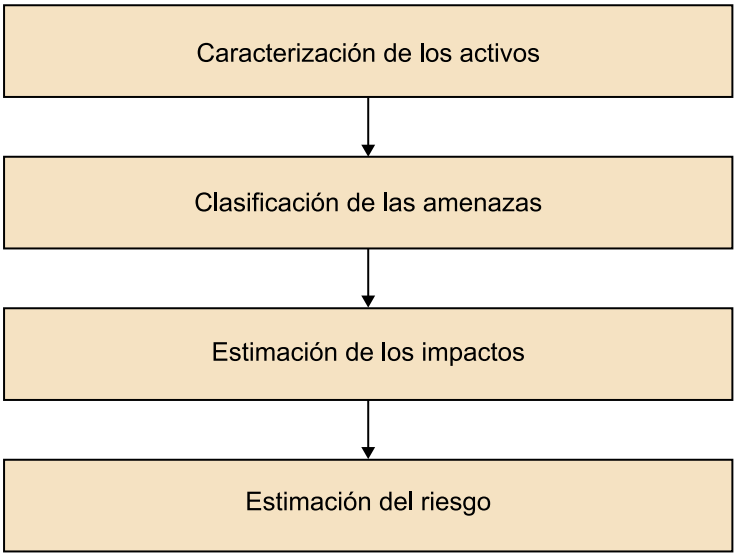
En resumen, los **requisitos adicionales** de la Norma ISO 27001, respecto a las normas ISO 9001, ISO 14001 e ISO 45001, están presentes en los apartados 6 y 8 y son los siguientes:

- **Evaluación de los riesgos de seguridad de información**: La organización tiene que desarrollar una metodología para la identificación y evaluación de riesgos de seguridad de la información. Este proceso no debe ser mezclado con abordar los riesgos y oportunidades en las normas ISO 9001, ISO 14001 e ISO 45001. Pues el segundo tiene menos requisitos y aplicar la misma metodología puede ser abrumador e improductivo en estas tres normas.

- **Información sobre el tratamiento de riesgos de seguridad**: Este proceso no tiene un elemento común en la ISO 9001, ISO 14001 e ISO 45001, por lo que se puede hacer de forma independiente. Esto requiere que la organización aplique uno o varios controles de seguridad de la información catalogados en el Anexo A de la ISO 27001.

Nos tiene que quedar claro en esta norma que el proceso de gestión de los riesgos asociados a la seguridad de la información es el siguiente:

Figura 8



Y teniendo claro este esquema, cabe implantar los requisitos específicos de esta norma.

No entraremos en más detalle en esta norma porque no consideramos en esta asignatura conveniente profundizar en ello.

7.1.2. Normas de responsabilidad social

1) Norma ISO 26000:2010

Es una **guía voluntaria** de responsabilidad social; ofrece orientación armonizada, pertinente a escala mundial para las **organizaciones del sector público y privado de todo tipo** sobre la base de un consenso internacional entre expertos representantes de los principales grupos de interés, y de esa manera fomenta la aplicación de **mejores prácticas de la responsabilidad social en todo el mundo**. Es una norma de directrices, no de requisitos; por lo tanto, es importante tener en cuenta que **no es certificable**.

Hay que tener en cuenta que un negocio sostenible para las organizaciones significa no solo el suministro de productos y servicios que satisfagan al cliente, y hacerlo sin poner en peligro el medio ambiente, sino también funcionar de una manera socialmente responsable.

ISO 26000 es una herramienta poderosa de responsabilidad social para ayudar a las organizaciones a pasar de las buenas intenciones a las buenas acciones.

La percepción y la realidad del desempeño de una organización sobre la responsabilidad social pueden influir, entre otras cosas, en:

- Su ventaja competitiva.
- Su reputación.
- Su capacidad para atraer y retener a trabajadores o miembros de la organización, clientes o usuarios.
- Mantener la motivación, compromiso y productividad de los empleados.
- La percepción de los inversionistas, propietarios, donantes, patrocinadores y la comunidad financiera, y sus relaciones con empresas, gobiernos, medios de comunicación, proveedores y organizaciones.

En la aplicación de la ISO 26000, es recomendable que una organización tenga en cuenta la sociedad, la diversidad medioambiental, jurídica, cultural, política y organizativa, así como las diferencias en las condiciones económicas, mientras que está siendo compatible con las normas internacionales de comportamiento.

Los **capítulos** que presenta la Norma ISO 26000:2010 a través de su índice son los siguientes:

- Objetivo y campo de aplicación.
- Términos y definiciones.
- Comprender la responsabilidad social.
- Principios de la responsabilidad social.
- Reconocer la responsabilidad social e involucrarse con las partes interesadas.
- Orientación sobre materias fundamentales de responsabilidad social.
- Orientación sobre la integración de la responsabilidad social en toda la organización.
- ANEXO A. Ejemplos de iniciativas voluntarias y herramientas para la responsabilidad social.
- ANEXO B. Referencias útiles para la implementación de la responsabilidad social.

- Abreviaturas y bibliografía.

Hay que diferenciar que los **fundamentos de la responsabilidad social** son siete:

1) Gobernanza de la organización

2) Derechos humanos

3) Prácticas laborales

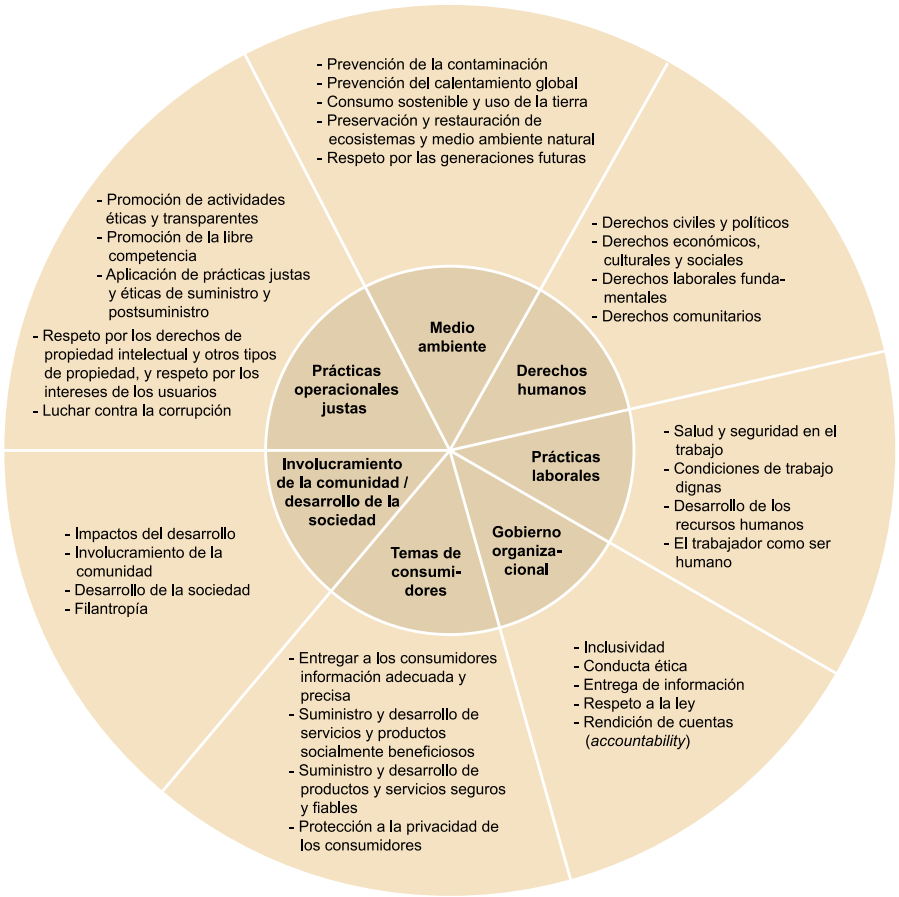
4) Medio ambiente

5) Prácticas justas de operaciones

6) Asuntos de consumidores

7) Participación activa y desarrollo de la comunidad

Figura 9



Por otro lado, los **principios de la responsabilidad social** proporcionan a la organización directrices para aceptar, rechazar o modificar sus estrategias, políticas, prácticas y procesos de implementación. Las acciones de una organización deberían ser llevadas a cabo de manera consistente con los principios relevantes.

Existen tres tipos de principios: generales, sustantivos y operacionales.

a) Principios generales. Son principios primordiales que se aplican en todas las circunstancias. Se aplican tanto para los principios sustantivos como para los generales. Estos principios deberían trascender a cualquier área temática en particular. Los principios generales forman la base de los principios sustantivos y operacionales que le siguen. Incluyen:

- Respeto de convenciones y declaraciones internacionalmente reconocidas y de instrumentos ampliamente reconocidos, derivados de ellas.

- Respeto a la ley.

- Reconocimiento del derecho de las partes interesadas de ser escuchadas y el deber de una organización de responder.

b) Los principios sustantivos se aplican a resultados por los cuales la organización es responsable. Ellos:

- Vienen de instrumentos intergubernamentales relevantes y autorizados, y/o de instrumentos aprobados reconocidos ampliamente por organismos intergubernamentales desarrollados a través de un proceso multipartes interesadas (*multi-stakeholder*). Abierto y transparente.

- Son expresamente aplicables a actores no-estatales.

- No están limitados geográficamente.

Los principios sustantivos se relacionan con los impactos por los cuales las organizaciones son responsables. Incluyen, pero no se limitan a:

- El medioambiente
- Derechos humanos
- Prácticas laborales
- Gobierno de la organización
- Prácticas de negocios justo
- Involucramiento de la comunidad
- Temas de consumidores

c) Los principios operacionales se aplican a la naturaleza y calidad de los procesos. Se aplican al proceso de implementación de los principios sustantivos. Estos son principios que:

- Han llegado a través de un proceso multipartes-interesadas (*multi-stakeholder*) abierto y transparente.
- Son expresamente aplicables a actores no-estado.
- No están limitados geográficamente.

Los principios operacionales guían cómo las organizaciones actúan. Incluyen:

- Rendición de cuentas (*accountability*)
- Límites
- Integración
- Materialidad
- Enfoque multipartes-interesadas (*multi-stakeholder*)
- Transparencia
- Enfoque de ciclo de vida

2) Norma IQNet SR10

Es el primer estándar que establece requisitos **certificables** sobre sistemas de gestión de responsabilidad social que están respaldados por una red internacional de certificación de reconocido prestigio como es **IQNet**. Se trata de una entidad certificadora, de ámbito internacional, que agrupa a las principales entidades certificadoras de diferentes países. Este estándar sustituye a las especificaciones RS10 de origen español. Establece los requisitos de un sistema de gestión de la responsabilidad social **de acuerdo fundamentalmente con la norma internacional ISO 26000** sobre sistemas de gestión de responsabilidad social.

La **estructura de alto nivel** que conforma la Norma IQNet SR10 es idónea para empresas que ya cuentan con sistemas de gestión de calidad ISO 9001, sistemas de gestión ambiental ISO 14001 y/o EMAS, así como sistemas de gestión de prevención de riesgos laborales ISO 45001. Favorece de esta forma la integración de los aspectos financieros y de buen gobierno, sociales y ambientales de la empresa.

Además de con sistemas de estructura de alto nivel ISO (estructura HLS), IQNet es **complementaria** a los Convenios Fundamentales de la Organización Internacional del Trabajo (OIT), la Declaración Universal de los Derechos Humanos, ISO 26000, SA8000, Global Reporting Iniciative (GRI) y el modelo de Empresa Familiarmente Responsable (EFR).

Entre los requisitos del estándar IQNet SR10 destacan el liderazgo, el compromiso y la exigencia de códigos de conducta, para aumentar el alcance del buen gobierno. Establece valores y los utiliza como guía en la toma de decisiones, acreditando el comportamiento apropiado de la organización. Los **principios básicos** son:

- Mejora continua, siguiendo el ciclo PDCA
- Transversalidad
- Voluntariedad
- Enfoque a los intereses de todos los grupos de interés
- Rendición de cuentas
- Transparencia
- Comportamiento ético
- Respeto al principio de legalidad
- Respeto de la normativa internacional de comportamiento
- Respeto de los derechos humanos
- Liderazgo
- Adicionalidad
- Eficiencia

No entraremos en más detalle porque en la plataforma de dicha asignatura se dispone de dicha norma para su consulta.

3) Norma UNE 19601:2017

Estándar **nacional** de mejores prácticas **para prevenir delitos**, reducir el riesgo y fomentar una cultura empresarial ética y de cumplimiento con la ley.

Este estándar establece los requisitos de un sistema de gestión para:

- Prevenir la comisión de delitos que puedan llevar aparejada responsabilidad penal para la misma.

- Difundir la cultura de prevención y cumplimiento en la organización.

- Establecer medidas de vigilancia y control idóneas para prevenir delitos y para reducir de forma significativa el riesgo de cometerlos.

- Mejorar la gestión, ayudar a reducir el riesgo penal y dar una mayor garantía de seguridad y confianza ante órganos de gobierno, accionistas e inversores, entre otros grupos de interés.

La Norma UNE 19601 desarrolla **requisitos que responden a lo indicado por el Código penal** para los modelos de gestión y prevención de delitos, pero también va más allá, incorporando las buenas prácticas en materia de *compliance*, mundialmente aceptadas.

El sistema que establece la Norma UNE 19601 presenta la denominada **estructura de alto nivel**, con lo que es integrable con otros sistemas de gestión.

La mera implantación de la Norma UNE 19601 **no conllevará la exoneración o atenuación automática de la responsabilidad penal de la persona jurídica**, pero sí puede constituir un elemento fundamental para acreditar que esta actuó de forma diligente antes de la comisión del delito y que empleó las mejores prácticas, conforme a modelos estandarizados y consensuados para crear una cultura de prevención que redujera de forma significativa el riesgo de su comisión.

Esta norma será **certificable** por una tercera parte independiente; un modo de asegurar que se aplica eficazmente. La Circular 1/2016 de la Fiscalía General del Estado sobre la reforma del Código penal considera que **las certificaciones podrán ser valoradas como un elemento adicional** de la eficacia de los modelos a la hora de eximir de responsabilidad penal a las personas jurídicas que hayan implantado modelos para la prevención de delitos.

7.2. Sistema de gestión del riesgo ISO 31000:2018

El nuevo enfoque en la gestión de riesgos de las nuevas normas publicadas con estructura de alto nivel obliga a tener en cuenta la metodología en la evaluación de riesgos desarrollada en la Norma ISO 31000:2018.

Por este motivo, es importante tener en cuenta esta norma.

La norma se centra, de forma exhaustiva, en la atención de la gestión del riesgo, como una herramienta para minimizar, de forma anticipada, las posibles inseguridades que pudieran producirse. Por tanto, la Norma ISO 31000 da respuesta, con eficiencia y seguridad, a los riesgos y peligros actuales a los que se enfrentan las organizaciones y empresas en su día a día.

Esta norma **contiene directrices** sobre la gestión de los riesgos a los que se enfrentan las organizaciones. La implementación de estas directrices puede personalizarse según la organización y su contexto, ya que **no es específica de ningún sector de actividad**. Es una norma que puede utilizarse durante toda la vida de la organización y aplicarse a cualquier actividad, incluyendo la toma de decisiones a todos los niveles.

Es el primer estándar que establece la **gestión de riesgos sociales y ambientales**, desarrollando nuevos estándares y procedimientos para la prevención de posibles peligros. El liderazgo, el compromiso y la integración de las posibles amenazas dentro de la estructura de una empresa u organización cobran especial relevancia en esta nueva versión.

La **estructura** de esta norma es la siguiente:

1. Objeto y campo de aplicación.

2. Referencias normativas.

3. Términos y definiciones.

4. Principios.

5. Marco de trabajo.

5.1. Generalidades.

5.2. Liderazgo y compromiso.

5.3. Integración.

5.4. Diseño.

5.5. Implementación.

5.6. Evaluación.

5.7. Mejora.

6. Proceso.

6.1. Generalidades.

6.2. Comunicación y consulta.

6.3. Alcance, contexto y criterios.

6.4. Apreciación del riesgo.

6.5. Tratamiento del riesgo.

6.6. Seguimiento y revisión.

6.7. Registro y presentación de informes.

No entraremos en más detalle en esta norma porque no corresponde a esta asignatura, pero tendremos que tener en cuenta que de la gestión de riesgos exigida en las normas ISO 9001, ISO 14001 e ISO 45001 podremos extraer la metodología de la Norma ISO 31000.