

ISOTools



ISO 31000

¿Qué es la norma ISO 31000?

La **ISO 31000** es una norma internacional que ofrece las directrices y principios para gestionar el riesgo de las organizaciones.

Esta norma fue publicada en 2018 por la Organización Internacional de Normalización (ISO) en colaboración con IEC, y tiene por objetivo que organizaciones de todos los tipos y tamaños puedan gestionar los **riesgos** en la empresa de forma efectiva, por lo que recomienda que las organizaciones desarrollen, implanten y mejoren continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de **riesgos** en cada una de sus actividades.

Como complemento a esta norma se ha desarrollado otro estándar: la **ISO 31010** "Gestión del riesgo. Técnicas de evaluación de riesgos". Esta norma provee de una serie de técnicas para la identificación y evaluación de **riesgos**, tanto positivos como negativos.

¿Cómo beneficia a la empresa la ISO 31000?

La norma **ISO 31000 y sus beneficios**, fue establecida por la Organización Internacional de Normalización (ISO). Ofrece a las empresas un **marco integral para la gestión de riesgos**, brindando numerosos **beneficios que contribuyen al éxito y la sostenibilidad** de la organización, como los que se detallan a continuación:

Mejora la Toma de Decisiones

La implementación de la ISO 31000 proporciona a la empresa un **enfoque estructurado para identificar, evaluar y gestionar riesgos**. Esto facilita la toma de decisiones informadas, ya que los

Líderes tienen una comprensión más clara de los posibles riesgos asociados con diferentes acciones y estrategias empresariales.

Optimización de Recursos

Al identificar proactivamente los riesgos y establecer procesos para su gestión, las empresas pueden **optimizar la asignación de recursos**. Esto evita la pérdida de recursos valiosos en situaciones de crisis y ayuda a la empresa a centrarse en áreas que realmente generen valor.

Incremento de la Resiliencia Empresarial

La ISO 31000 ayuda a las empresas a desarrollar una **cultura de gestión de riesgos que promueve la resiliencia**. Al anticipar y prepararse para posibles desafíos, la empresa se vuelve más capaz de adaptarse y recuperarse rápidamente de situaciones adversas, garantizando así su continuidad operativa.

Fortalecimiento de la Confianza del Cliente y del Mercado

La adopción de estándares internacionales, como la ISO 31000, demuestra el **compromiso de la empresa con las mejores prácticas en gestión de riesgos**. Esto genera confianza tanto entre los clientes como en el mercado en general, lo que puede resultar en una ventaja competitiva y un fortalecimiento de la reputación de la empresa.

Cumplimiento Normativo y Legal

La ISO 31000 ayuda a las empresas a **cumplir con los requisitos legales y normativos relacionados con la gestión de riesgos**. Esto no solo reduce la exposición a posibles sanciones legales, sino que también promueve una cultura empresarial, ética y responsable.

Innovación y Oportunidades

Al comprender y gestionar los riesgos de manera efectiva, las empresas pueden estar **mejor posicionadas para identificar nuevas oportunidades**. La ISO 31000 no solo se trata de minimizar amenazas, sino también de capitalizar oportunidades que pueden surgir en un entorno empresarial dinámico.

Reducción de Pérdidas Financieras

La gestión efectiva de riesgos, según la ISO 31000, contribuye a la **reducción de pérdidas financieras derivadas de eventos imprevistos**. Al anticipar y planificar la respuesta a posibles crisis, la empresa puede minimizar el impacto económico negativo.

La implementación de la ISO 31000 no solo es un requisito esencial en un entorno empresarial cada vez más complejo, sino que también **aporta beneficios tangibles al proporcionar un marco sólido para la gestión de riesgos, fortaleciendo así la resiliencia y el rendimiento global de la empresa**.

Beneficio	Descripción
Mejora la toma de decisiones	Proporciona un enfoque estructurado para identificar, evaluar y gestionar riesgos, lo que permite decisiones más informadas y con mayor comprensión de las consecuencias potenciales.
Optimización de recursos	Al gestionar los riesgos de manera proactiva, la empresa evita pérdidas innecesarias y puede dirigir sus recursos a actividades que generan mayor valor.
Incremento de la resiliencia empresarial	La norma impulsa una cultura de anticipación y preparación ante posibles desafíos, permitiendo que la organización se adapte y recupere rápidamente ante eventos adversos.

Beneficio	Descripción
Fortalecimiento de la confianza del cliente y del mercado	Adoptar estándares internacionales demuestra compromiso con las mejores prácticas, aumentando la confianza de clientes y stakeholders y fortaleciendo la reputación corporativa.
Cumplimiento normativo y legal	Facilita el cumplimiento de requisitos legales y regulatorios relacionados con la gestión de riesgos, reduciendo la exposición a sanciones y fomentando una cultura ética.
Impulso a la innovación y oportunidades	Una adecuada gestión de riesgos permite identificar y aprovechar oportunidades emergentes, no solo prevenir amenazas, impulsando así el crecimiento empresarial.
Reducción de pérdidas financieras	Al prever escenarios críticos y planificar respuestas efectivas, la empresa minimiza el impacto económico de eventos inesperados, reduciendo pérdidas financieras.

Norma ISO 31000

Estructura de la norma ISO 31000

La variedad y complejidad de los **riesgos** es muy diversa por lo que este estándar internacional desarrollado por la ISO (International Organization for Standardization) no está pensado para un sistema particular de gestión, más bien es una guía de buenas prácticas para las actividades relacionadas con la gestión de **riesgos**.

El diseño y la implantación de la gestión de **riesgos** dependerán de las diversas necesidades de cada organización, de sus objetivos concretos, contexto, estructura, operaciones, procesos, actividades, servicios, etc.

El estándar **ISO 31000** está estructurado en tres elementos claves para una efectiva gestión de riesgos:

Principios para la gestión de riesgos

Para una mayor eficacia, la gestión del riesgo en una organización debe basarse en un conjunto de principios fundamentales que garanticen su solidez y sostenibilidad en el tiempo. Estos principios, recogidos en normas como la ISO 31000, promueven un enfoque estructurado, adaptativo y alineado con los objetivos estratégicos de la organización. Entre los más relevantes destacan:

- **Integración:** la gestión del riesgo debe formar parte integral de todos los procesos organizacionales, desde la toma de decisiones hasta la planificación operativa.
- **Estructura y personalización:** debe adaptarse al contexto interno y externo de la empresa, considerando su cultura, objetivos, entorno regulatorio y partes interesadas.
- **Enfoque sistémico y proactivo:** se orienta a anticipar, detectar y responder eficazmente a riesgos y oportunidades, en lugar de reaccionar solo ante eventos negativos.
- **Basado en la mejor información disponible:** utiliza datos confiables, pero acepta la existencia de incertidumbre y limita las decisiones a lo que se conoce en ese momento.
- **Participación de las partes interesadas:** involucra a todos los niveles de la empresa y fomenta la transparencia en la identificación y evaluación de riesgos.
- **Mejora continua:** la gestión del riesgo no es estática; debe revisarse y actualizarse con base en los resultados obtenidos, los cambios en el contexto y la evolución de la compañía.

Estructura de soporte o marco de Trabajo

El objetivo de este elemento es integrar el proceso de gestión de **riesgos** con la dirección, para que esta adquiera un fuerte compromiso con la implantación de la **Gestión del Riesgo**. En este caso, la norma establece una serie de órdenes que debe cumplir la gerencia para asegurar la efectividad de la gestión de **riesgos**:

- **Diseñar la estructura de gobierno del riesgo:** definir responsabilidades claras, asignar recursos y establecer canales de comunicación efectivos.
- **Establecer políticas y objetivos:** la dirección debe aprobar una política de gestión de riesgos que oriente las acciones de todos los niveles de la empresa.
- **Desarrollar cultura de riesgo:** fomentar una mentalidad preventiva y analítica en todo el personal, promoviendo la concienciación sobre la importancia de identificar y tratar riesgos.
- **Integrar la gestión de riesgos en la planificación estratégica:** asegurar que las decisiones clave tengan en cuenta los posibles impactos positivos y negativos.
- **Asignar recursos y capacidades:** dotar de medios técnicos, financieros y humanos a las áreas responsables de identificar y controlar riesgos.
- **Monitorear y revisar el marco:** evaluar si la estructura es eficaz, realizando ajustes cuando cambian los contextos o se detectan deficiencias.

Proceso de gestión de riesgos

Este proceso consta de tres etapas: establecimiento del contexto, valoración de **riesgos** y tratamiento de los mismos. Cada fase tiene una función específica dentro del ciclo de gestión, permitiendo avanzar de lo general a lo específico en la toma de decisiones frente a la incertidumbre:

Establecimiento del contexto. En esta fase se analiza el entorno en el que opera la empresa, tanto externo como interno, así como los criterios que se utilizarán para evaluar los riesgos. También se identifican las partes interesadas, sus expectativas y la tolerancia al riesgo. Este paso es clave para asegurar que el análisis posterior se ajuste a la realidad de la organización y sea coherente con su estrategia.

Valoración de riesgos. Aquí se lleva a cabo la identificación, análisis y evaluación de los riesgos:

- **Identificación:** se detectan los eventos que podrían afectar el logro de los objetivos.
- **Análisis:** se estima la probabilidad de ocurrencia y el impacto de cada riesgo.
- **Evaluación:** se priorizan los riesgos en función de su criticidad y se determina si es necesario actuar sobre ellos.

Tratamiento del riesgo. Consiste en decidir y aplicar medidas para modificar los riesgos. Entre las opciones se encuentran: evitar el riesgo, reducirlo mediante controles o mejoras, transferirlo por ejemplo, a través de seguros o contratos, o aceptarlo si está dentro del umbral tolerable. Además, se debe planificar el seguimiento y establecer indicadores de control para verificar la eficacia de las acciones implementadas.

¿Por qué es tan valiosa la ISO 31000?

Hay que empezar comentando que esta norma no tiene un poder legal ni es regulada directamente sobre las organizaciones. Es decir, **no es obligatoria**. Pero quienes deciden implementarla, **reconocen el impacto y sus valiosos beneficios en la cultura organizativa**.

Y estas son algunas las razones o *principios* por lo que es tan valiosa su implementación:

- 01. Enfoque integral:** Con la implementación de esta norma, las organizaciones pueden evaluar cualquier tipo de riesgo (Positivo o negativo) porque no solo únicamente evalúa pérdidas, también propende evaluar las oportunidades.
- 02. Adaptabilidad:** Se puede adaptar a cualquier organización al proporcionarle un enfoque específico a sus requerimientos normativos. Incluso es de fácil integración con normas como 9001, 14001, entre otras.
- 03. Estructurada:** Gestiona los riesgos de manera coherente e integral en todas y cada una de las operaciones de la organización.
- 04. Incluye partes interesadas:** Ayuda a conocer la perspectiva y estado actual de las partes interesadas en el contexto relacionado a los riesgos inherentes con los que puedan estar asociados.
- 05. Promueve la mejora continua:** Al ser este uno de sus principios fundamentales, su enfoque garantiza la gestión del cambio en la empresa. Evalúa sus amenazas y oportunidades potenciales. Además, al tener un seguimiento continuo, aprende de la experiencia identificando lo que funciona bien y lo que puede mejorar.

06. Optimiza los procesos: La ISO 31000 promueve que las organizaciones optimicen sus procesos de riesgos, asegurando la utilización de los recursos de forma eficiente.

07. Es de reconocimiento global: Al ser norma internacional, su implementación genera competitividad y confianza en el mercado.

08. Facilita toma de decisiones: Al identificar los riesgos, evaluarlos y gestionarlos, la alta gerencia puede actuar en consecuencia, logrando disminuir las brechas hacia sus objetivos estratégicos.

¿Es certificable la norma ISO 31000?

La norma ISO 31000 no es certificable. A diferencia de otras normas ISO como ISO 9001 o ISO 27001, que establecen requisitos formales para la certificación de sistemas de gestión, la ISO 31000 proporciona **principios y directrices** para gestionar el riesgo de manera eficaz, pero **no contiene requisitos específicos de cumplimiento** que puedan ser auditados con fines de certificación.

El propósito principal de la ISO 31000 es **orientar a las empresas en el diseño, implementación y mejora continua de su proceso de gestión de riesgos**, adaptándolo a su contexto, naturaleza, tamaño y complejidad. Sin embargo, aunque no sea certificable, su aplicación permite **alinear la gestión de riesgos con las decisiones estratégicas**, fortalecer la gobernanza y aumentar la resiliencia organizacional.

Muchas empresas utilizan ISO 31000 como **referencia clave** para integrar la gestión de riesgos en sus sistemas certificados bajo otras normas, y como **marco base para modelos sectoriales** (como COSO o ERM), así como para responder a expectativas regulatorias y de stakeholders.

¿Cómo garantizar una implementación exitosa?

A continuación se detallan los elementos a tener en cuenta para la **implementación de un Sistema de Gestión de Riesgos con ISO 31000:**

- **Compromiso:** Entendiendo estas ventajas organizativas y competitivas, el **éxito al implementar ISO 31000** dependerá primero (como toda norma) del compromiso de la alta dirección. Y más concretamente a la asignación de recursos, ya sean humanos, financieros y tecnológicos, pero, sobre todo, a la aceptación de los resultados como parte de aprendizaje y al compromiso con la ejecución de acciones de mitigación que las evaluaciones de los riesgos ameriten.
- **Contexto organizacional:** Si la organización tomó la decisión de implementar la ISO 31000, se debe identificar el terreno. Es decir, definir los objetivos, incluir partes interesadas y evaluar las condiciones internas y externas que son clave en la evaluación de los riesgos y que influyen en la gestión.
- **Desarrollo del marco integral:** Estructura un marco integral para que la gestión se alinee con los principios y se adapte a los requerimientos. Puede contemplar las políticas y procedimientos de la plataforma estratégica.
- **Aprendizaje:** Capacitaciones al recurso y partes interesadas para que comprendan la importancia de la gestión y contribuyan en la implementación, siendo conscientes de las ventajas que esto implica.
- **Gestión de los riesgos:** Implementa ordenadamente una estructura que permita gestionar los riesgos mediante metodologías y herramientas ágiles, de forma que tenga el control en todo momento.



Los principios para la gestión de riesgos de la Norma Internacional ISO 31000

Según la norma **ISO31000**, los **principios de la gestión de riesgos** son los siguientes:

- Crear y proteger el valor. Contribuye a la consecución de objetivos, así como la mejora de ciertos aspectos tales como la **seguridad** y salud laboral, cumplimiento de los requisitos legales, protección ambiental, etc.
- Estar integrada en los procesos de una organización. No debe ser entendida como una actividad aislada, sino como parte de las actividades y procesos principales de una organización.

- Formar parte de la toma de decisiones. La gestión del riesgo ayuda a la toma de decisiones evaluando la información sobre las distintas alternativas.
- Tratar explícitamente la incertidumbre. La gestión del riesgo trata aquellos aspectos de la toma de decisiones que son inciertos, la naturaleza de esa incertidumbre y como puede tratarse.
- Ser sistemática, estructurada y adecuada. Contribuye a la eficiencia y, consecuentemente, a la obtención de resultados fiables.
- Basarse en la mejor información disponible. Los inputs del proceso de gestión del riesgo están basados en fuentes de información como la propia experiencia, la observación y la opinión de expertos.
- Estar hecha a medida. La gestión del riesgo está alineada con el contexto externo e interno de la organización y con su perfil de riesgo.
- Tener en cuenta factores humanos y culturales. Reconoce la capacidad y percepción de los empleados y personas interesadas, esto puede facilitar o dificultar la consecución de los objetivos de la organización.
- Ser transparente e inclusiva. La apropiada y oportuna participación de los grupos de interés (stakeholders) y, en particular, de los responsables a todos los niveles, asegura que la gestión del riesgo permanece relevante y actualizada.
- Ser dinámica, iterativa y sensible al cambio. La organización debe velar para que la gestión del riesgo detecte y responda a los cambios de la empresa y de su entorno.

- Facilitar la mejora continua de la organización. Las organizaciones deberían desarrollar e implementar estrategias para mejorar continuamente, tanto en la gestión del riesgo como en cualquier otro aspecto de la organización.

Software para ISO 31000

La Plataforma ISOTools facilita la automatización de la ISO31000

La **Plataforma Tecnológica ISOTools** facilita la **implementación, automatización y mantenimiento** de las actividades de la gestión de riesgos según **ISO 31000:2009**.

Sobre la base de los procesos y la lógica del **ciclo PHVA (Planear - Hacer - Verificar - Actuar)** ISOTools está diseñado para hacer más efectivo el manejo de la documentación, mejorar la comunicación y reducir tiempos y costos. De esta forma se consigue un impacto real sobre la eficiencia, los costos y los resultados de la organización.

Este software permite optimizar su **Gestión de Riesgos** basada en la **ISO 31000** como camino hacia la excelencia e integrar la norma ISO-31000 con otras normas, como ISO 9001, ISO 45001 e ISO 14001, de una forma sencilla gracias a su estructura modular.

Referencias bibliográficas:

- International Organization for Standardization. (2018). *ISO 31000:2018 – Risk management — Guidelines*. ISO.
- International Organization for Standardization. (s. f.). *ISO 31000 family — Risk management*. Recuperado de <https://www.iso.org/cms/render/live/es/sites/isoorg/home/standards/popular-standards/iso-31000-risk-management.html>
- Wikipedia. (s. f.). *ISO 31000*. Recuperado de https://es.wikipedia.org/wiki/ISO_31000

ISOTools

