Evolución de la Norma ISO 31000: Análisis de los Principales Cambios de la Edición 2009 a la Edición 2018

Esteban Tobon Tirado

etobon@asriesgos.com 300 8840190 asriesgos.com Bogotá D.C. - Colombia

1. Introducción

La gestión de riesgos es una piedra angular para la viabilidad y sostenibilidad de cualquier organización. La norma ISO 31000 ha sido durante mucho tiempo (y lo seguirá siendo) una referencia clave en este campo, proporcionando un marco sólido y reconocido internacionalmente. En esta publicación, exploraremos los principales cambios que han ocurrido en la norma ISO 31000 desde su edición de 2009 hasta la versión más reciente de 2018.

2. ISO 31000: Edición 2009 - Un Vistazo Retrospectivo:

La versión 2009 de la ISO 31000 estableció un marco robusto para la gestión de riesgos, centrándose en los principios fundamentales de identificación, evaluación y tratamiento de riesgos. Su enfoque estaba en proporcionar una guía para que las organizaciones personalizaran sus procesos de gestión de riesgos según sus necesidades específicas.

Sin embargo, algunos aspectos de la edición de 2009 se percibieron como ambiguos, y la implementación práctica varió en diferentes organizaciones. Las críticas señalaron la necesidad de una mayor claridad en la integración de la gestión de riesgos en la toma de decisiones estratégicas.

3. ISO 31000: Edición 2018 - Refinando la Efectividad:

La versión 2018 de la ISO 31000 representa un paso significativo hacia la mejora y refinamiento del enfoque de gestión de riesgos. Uno de los cambios más notables es la mayor integración de la gestión de riesgos en el proceso de toma de decisiones estratégicas de la organización.

Se ha hecho hincapié en la adaptabilidad y aplicabilidad de la norma a diferentes contextos y organizaciones. La estructura de alto nivel común a todas las normas ISO, conocida como Anexo SL[1], se ha incorporado, lo que facilita la integración de la gestión de riesgos con otros sistemas de gestión.

4. Enfoque Basado en Principios:

La ISO 31000:2018 mantiene los principios fundamentales establecidos en la edición anterior, pero ahora se presenta de una manera más clara y detallada. La adopción de un enfoque basado en principios busca proporcionar una base sólida para la gestión de riesgos y promover una cultura organizacional que valore la evaluación y gestión de riesgos como una parte integral de la toma de decisiones.

[1] El Anexo SL proporciona una nueva estructura, denominada de Alto Nivel, para los sistemas de gestión ISO- sustituye a la histórica Guía 83 de la ISO. Ha sido creada para introducir un texto base idéntico y unos términos y definiciones comunes. Esta medida, optimiza las normas, fomenta la certificación, facilita la integración de los sistemas de gestión.

5. **Enfoque Proactivo y Dinámico:**

La nueva edición enfatiza la necesidad de un enfoque proactivo y dinámico para la gestión de riesgos. Procura la anticipación de posibles cambios en el entorno y la adaptación inmediata a ellos. Este cambio refleja la comprensión de que la gestión de riesgos no debe ser un proceso estático, sino una función que evoluciona con el tiempo y las circunstancias cambiantes.

6. **Mejora Continua:**

La ISO 31000:2018 aborda explícitamente el concepto de mejora continua en la gestión de riesgos. Destaca la importancia de aprender de la experiencia, revisar y mejorar los procesos de gestión de riesgos de manera constante. Este énfasis en la mejora continua refleja la naturaleza evolutiva de los riesgos y la necesidad de una respuesta organizacional igualmente adaptable.

7. **Ejemplos de Sistemas de Gestión Implementados Bajo los Estándares de la ISO 31000:2018**

La ISO 31000:2018 proporciona un marco robusto y adaptable que puede aplicarse a diversas áreas y sectores. A continuación, se presentan algunos ejemplos de sistemas de gestión específicos que pueden implementarse bajo los estándares de esta norma:

Sistema de Gestión de Riesgos Empresariales (ERM): La ISO 31000 se presta naturalmente a la implementación de un Sistema de Gestión de Riesgos Empresariales (ERM) que abarque todos los aspectos de la organización. Este enfoque integral permite a las empresas identificar, evaluar y gestionar riesgos en todas las áreas funcionales, desde operaciones hasta finanzas y marketing.

Sistema de Gestión de la Calidad (QMS) con Enfoque en Riesgos: Integrar los principios de la ISO 31000 en un Sistema de Gestión de la Calidad (QMS) ayuda a las organizaciones a identificar riesgos que podrían afectar la calidad de los productos o servicios. Este enfoque proactivo facilita la anticipación de posibles problemas y la toma de medidas preventivas.

Sistema de Gestión Ambiental (EMS) con Enfoque en Riesgos Ambientales: Para organizaciones comprometidas con la sostenibilidad, la ISO 31000 puede ser aplicada en la gestión de riesgos ambientales. Un Sistema de Gestión Ambiental (EMS) que adopta este enfoque facilita la identificación y mitigación de riesgos relacionados con impactos ambientales y eventos adversos.

Sistema de Gestión de Seguridad de la Información (ISMS): En el ámbito de la ciberseguridad, un Sistema de Gestión de Seguridad de la Información (ISMS) puede beneficiarse enormemente de los principios de la ISO 31000. Este enfoque permite una evaluación integral de riesgos relacionados con la seguridad de la información y establece medidas para proteger la confidencialidad, integridad y disponibilidad de los datos.

Sistema de Gestión de la Continuidad del Negocio (BCMS): La continuidad del negocio es esencial en un entorno empresarial impredecible. Integrar la ISO 31000 en un Sistema de Gestión de la Continuidad del Negocio (BCMS) ayuda a las organizaciones a identificar y gestionar riesgos que

podrían interrumpir sus operaciones. Esto incluye eventos como desastres naturales, pandemias u otras amenazas.

Sistema de Administración de Riesgos Antilavado de Dinero (ALD) y Contra la Financiación del Terrorismo (CFT): Integrar los principios de la ISO 31000 en un Sistema de Administración de Riesgos ALD/CFT permite a las empresas de cualquier sector (financiero, solidario, Real, APNFD, identificar y evaluar de manera integral los riesgos asociados con actividades de lavado de dinero y financiamiento del terrorismo. Este enfoque proactivo facilita el diseño e implementación de controles efectivos para mitigar tales riesgos, asegurando el cumplimiento normativo y la integridad de las empresas.

Sistema de Gestión de Riesgos en Programas de Transparencia y Ética Empresarial (PTEE): Un Sistema de Gestión de Riesgos en Programas de Transparencia y Ética Empresarial utiliza la ISO 31000 para identificar y gestionar riesgos éticos y de integridad. Este enfoque contribuye a la creación de una cultura organizacional ética al anticipar y abordar posibles desafíos relacionados con la transparencia, corrupción y comportamiento ético. Facilita la implementación de programas PTEE sólidos y eficaces.

Sistema Integrado de Gestión de Riesgos y Ética Empresarial: La integración de la ISO 31000 en un sistema que abarque riesgos generales, así como riesgos específicos de ALD, CFT, y ética empresarial, ofrece una visión completa y coherente de la gestión de riesgos. Este enfoque permite a las organizaciones abordar los desafíos multifacéticos alineando estratégicamente sus esfuerzos en riesgos financieros, legales, éticos y de reputación.

Sistema de Administración de Riesgos en Cumplimiento Normativo: En el ámbito del cumplimiento normativo, la ISO 31000 puede ser aplicada para desarrollar un Sistema de Administración de Riesgos que se centre en identificar y mitigar riesgos asociados con el incumplimiento normativo. Este enfoque aborda los riesgos legales y regulatorios, incluyendo aquellos relacionados con ALD, CFT, y prácticas comerciales éticas.

Estos ejemplos ilustran la versatilidad de la ISO 31000:2018 al adaptarse a diferentes contextos organizativos y áreas de enfoque. La norma brinda un marco que no solo es aplicable a la gestión de riesgos en general, sino que también se integra eficazmente con otros sistemas de gestión, potenciando así la capacidad de las organizaciones para enfrentar los desafíos en un mundo empresarial en constante cambio.

La ISO 31000:2018 puede ser adaptada para satisfacer las necesidades específicas de la gestión de riesgos en áreas críticas como ALD, CFT, y ética empresarial, al proporcionar un enfoque estructurado y basado en principios, facilitando la identificación proactiva y la gestión efectiva de los riesgos, fortaleciendo así la resiliencia y la integridad de las organizaciones en un entorno empresarial complejo.

8. Conclusiones:

En resumen, la transición de la ISO 31000 de 2009 a 2018 ha sido significativa. Los cambios introducidos reflejan la evolución en la comprensión de la gestión de riesgos y buscan abordar las críticas y mejorar la aplicabilidad práctica de la norma. La ISO 31000:2018 se posiciona como un instrumento valioso para las organizaciones que buscan fortalecer sus capacidades de gestión de riesgos en un entorno empresarial cada vez más complejo y dinámico.

ESTEBAN TOBÓN TIRADO
Socio Consultor
ASRIESGOS SAS.