

ISO 31000

Docente: Cynthia Sanabria

OBJETIVOS DE APRENDIZAJE

Al finalizar este módulo, el participante será capaz de:



01

COMPRENDER

Principios de la Gestión del Riesgo

- ✓ Demostrar comprensión de los principios de la gestión del riesgo, tal como se formulan en ISO 31000.



02

IMPLEMENTAR

Marco de Gestión del Riesgo

- ✓ Establecer, mantener y mejorar continuamente un marco de gestión del riesgo, de acuerdo con las directrices de ISO 31000.



03

APLICAR

Proceso de Gestión del Riesgo

- ✓ Aplicar el proceso de gestión del riesgo, de acuerdo con las directrices de ISO 31000.



SECCIÓN 2

Normas ISO



01

¿Qué es ISO?

Concepto, estructura y propósito de la Organización Internacional de Normalización.



02

La norma y la metodología

Fundamentos y enfoque metodológico de ISO.



03

ISO 31000, ISO/TR 31004 e ISO/IEC 31010

La familia de normas para la gestión del riesgo.



04

La historia de ISO 31000

Evolución y principales hitos de la norma.



05

AS/NZS 4360, la predecesora de ISO 31000

Antecedentes y transición hacia un estándar global.



06

Otras mejores prácticas de evaluación/gestión del riesgo

Modelos y metodologías complementarias.



07

¿Qué significa ISO 31000 para su organización?

Beneficios, valor estratégico e impacto en la toma de decisiones.



¿Qué es ISO?

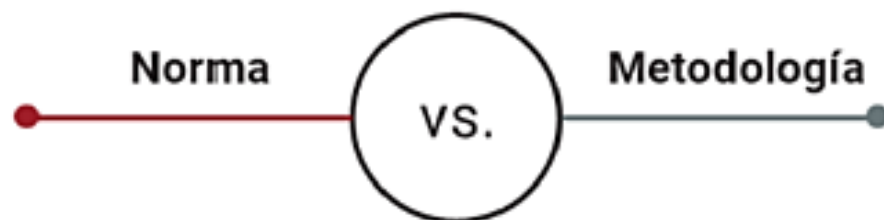
- ISO es una organización internacional de organismos nacionales de normalización de más de 160 países.
- Los resultados finales de los trabajos realizados por ISO son publicados como normas internacionales.
- ISO ha publicado más de 23,000 normas desde 1947.



Norma y Metodología

Diferencias

- Documento de referencia que cubre un amplio interés industrial
- Basada en un proceso voluntario, aprobada por una organización reconocida
- Especifica requisitos (normativos) o directrices (informativas) para determinadas actividades
- Responde principalmente a las preguntas "¿Por qué?" y "¿Qué?"



- Estructura rigurosa y formalizada
- Utiliza los recursos eficazmente para lograr el resultado deseado
- Depende de herramientas tales como cuestionarios o un software especializado
- Responde principalmente a la pregunta "¿Cómo hacer?"

ISO 31000

- ISO 31000 proporciona directrices sobre la gestión del riesgo a los que se enfrentan las organizaciones de cualquier industria o sector.
- Se puede aplicar a cualquier tipo de riesgo, cualquiera sea su naturaleza o sus consecuencias.
- Las organizaciones no pueden ser certificadas en esta norma.



ISO/TR 31004

- ISO/TR 31004 proporciona directrices para la implementación de ISO 31000.
- Este informe técnico está diseñado para ayudar a las organizaciones a aumentar la eficacia de sus actividades de gestión del riesgo alineándolas con ISO 31000.
- Puede ser utilizado por cualquier organización pública o privada, empresa, grupo o persona.



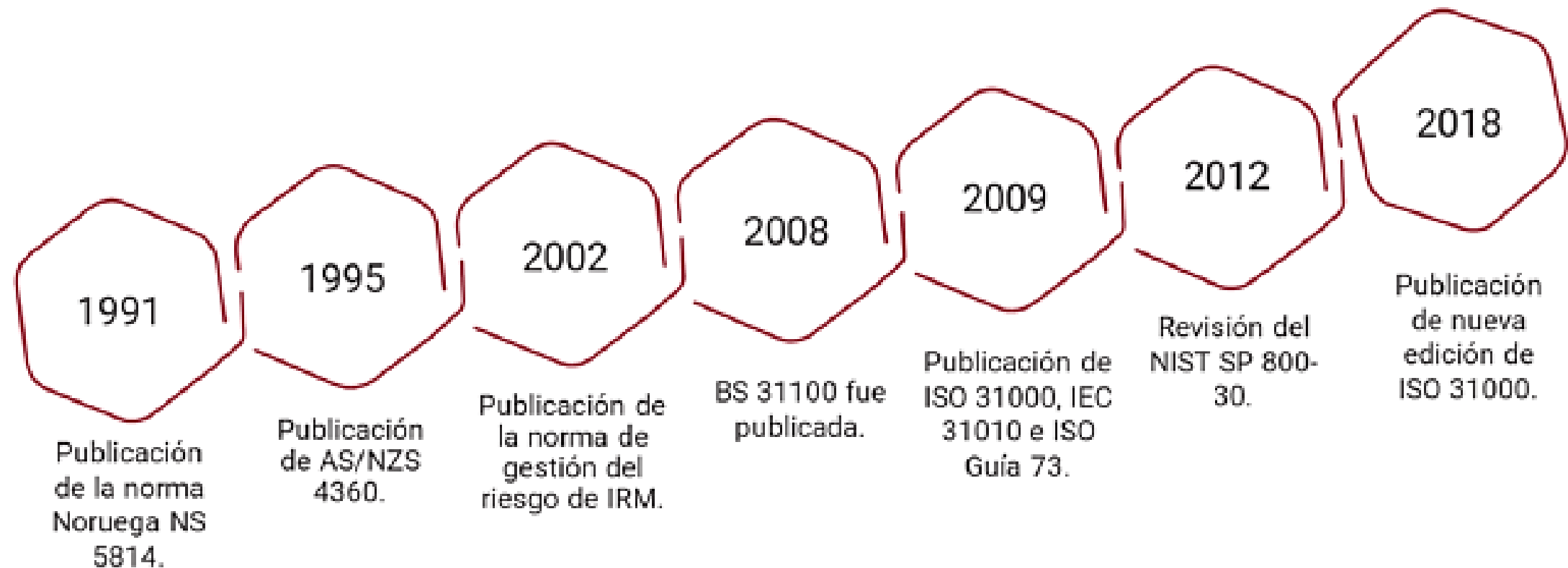
IEC 31010

- IEC 31010 es una norma de soporte de ISO 31000
- Proporciona orientación sobre la selección y aplicación de técnicas para evaluar el riesgo en una amplia gama de situaciones.
- Las organizaciones no pueden ser certificadas en esta norma.



La Historia de ISO 31000

1991–2018



¿Qué Significa ISO 31000 para su Organización?

ISO 31000 ofrece orientación sobre cómo las organizaciones pueden incorporar la toma de decisiones basada en el riesgo en su gobernanza, planificación, gestión, informes, políticas, valores y cultura.

ISO 31000 ayuda a las organizaciones a establecer una estrategia de gestión del riesgo para detectar y mitigar los riesgos de manera eficaz, aumentando así las posibilidades de alcanzar sus objetivos.

Ventajas de la Gestión del Riesgo

Introducción a ISO 31000

- *La gestión del riesgo es iterativa y asiste a las organizaciones a establecer su estrategia, lograr sus objetivos y tomar decisiones informadas.*
- *La gestión del riesgo es parte de la gobernanza y el liderazgo y es fundamental en la manera en que se gestiona la organización en todos sus niveles. Esto contribuye a la mejora de los sistemas de gestión.*



Propietario del Riesgo

Definiciones

1

ISO Guía 73, cláusula 3.5.1.5 Propietario del riesgo

Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo

2

Dueño del riesgo, la persona responsable de supervisar los riesgos y de seleccionar e implementar una estrategia de respuesta al riesgo adecuada. (PMBOK, 6ª edición, 2017)

3

Propietario del riesgo, la persona o entidad responsable de reconocer y supervisar el estado de un riesgo específico ("COSO Enterprise Risk Management", 2ª edición, 2011)

Amenaza

IEC 31010, cláusula 3.5

Fuente potencial de peligro, daño u otro resultado indeseable

Nota 1 a la entrada: Una amenaza es una situación negativa en la que la pérdida es probable y sobre la que uno tiene relativamente poco control.



Nota 2 a la entrada: Una amenaza para una de las partes puede representar una oportunidad para la otra.



Evento

ISO Guía 73, cláusula 3.5.1.3

Ocurrencia o cambio de un conjunto particular de circunstancias

¿Qué saber sobre los eventos?



NOTE 1

Un evento puede tener una o más ocurrencias y puede tener varias causas.

NOTA 2

Un evento puede consistir en algo que no sucede.

NOTA 3

A veces, un evento puede denominarse "incidente" o "accidente".

NOTA 4

Un evento sin consecuencias también puede denominarse "cuasi accidente", "incidente", "cuasi golpe" o "cercano a impacto".

Consecuencia

ISO Guía 73, cláusula 3.6.1.3

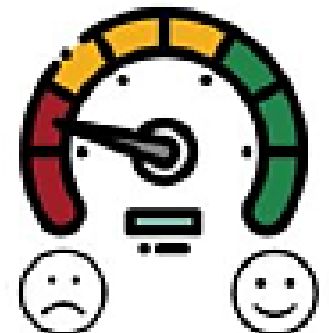
Resultado de un evento que afecta a los objetivos

NOTA 1 Un evento puede provocar una serie de consecuencias.

NOTA 2 Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos sobre los objetivos.

NOTA 3 Las consecuencias se pueden expresar de manera cualitativa o cuantitativa.

NOTA 4 Las consecuencias iniciales pueden intensificarse a través de reacciones en cadena.



Probabilidad

ISO Guía 73, cláusula 3.6.1.1

Posibilidad de que algo suceda



"Según nuestras previsiones,
mañana habrá un 50% de
probabilidad de lluvia".



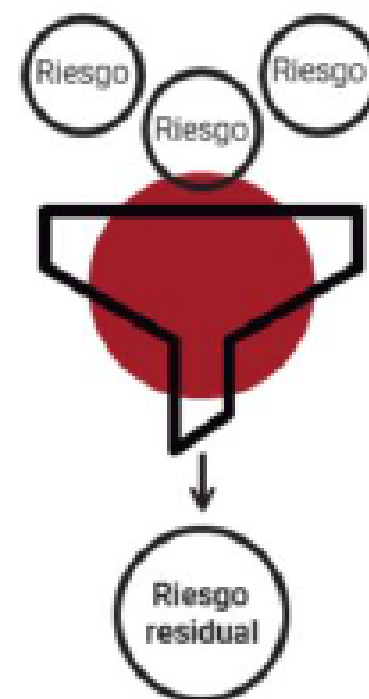
Riesgo Residual

ISO Guía 73, cláusula 3.8.1.6

Riesgo remanente después del tratamiento del riesgo

NOTA 1 El riesgo residual puede contener riesgos no identificados.

NOTA 2 El riesgo residual también se puede conocer como "riesgo retenido".



Nivel de Riesgo

ISO Guía 73, cláusula 3.6.1.8

Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de consecuencias y su probabilidad

PROBABILIDAD	CONSECUENCIAS				
	Insignificante (1)	Menor (2)	Moderada (3)	Mayor (4)	Extrema (5)
Rara (1)	Bajo	Bajo	Bajo	Bajo	Bajo
Poco probable (2)	Bajo	Bajo	Bajo	Medio	Medio
Posible (3)	Bajo	Bajo	Medio	Medio	Medio
Probable (4)	Bajo	Medio	Medio	Alto	Alto
Casi segura (5)	Bajo	Medio	Medio	Alto	Extremo

→ El Nivel de Riesgo 1 es Bajo

→ El Nivel de Riesgo 2 es Medio

→ El Nivel de Riesgo 3 es Alto

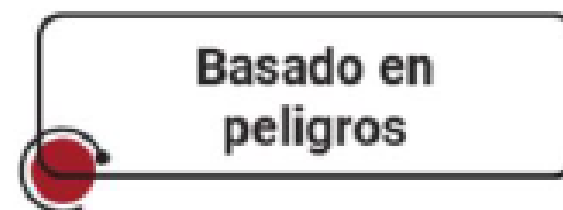
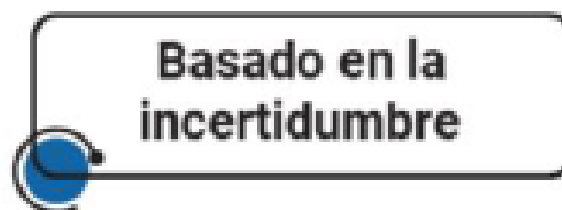
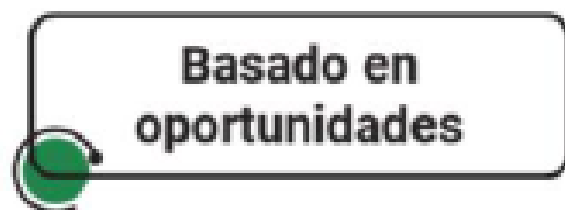
Tipos de Riesgo

- Los tipos de riesgo a los que se enfrenta una organización dependen en gran medida del contexto de esa organización, su sector industrial y el entorno en el que opera.
- Por lo tanto, es difícil definir una lista universal de todos los tipos de riesgo, tal vez con la excepción de un riesgo que afecta a todas las organizaciones: el riesgo operativo.
- El riesgo operativo implica cualquier evento que interrumpa las operaciones normales de la organización. Las pérdidas resultantes del riesgo operacional suelen originarse en una gestión deficiente, procesos inadecuados o fallidos, personas, sistemas o factores externos.

Tipos de Riesgo (continuación)

Considerando que los tipos de riesgo a los que se enfrenta una organización dependen en gran medida del contexto de esa organización, su sector industrial y el entorno en el que opera, tal vez sería más apropiado utilizar un enfoque diferente para definir los tipos de riesgo a los que se enfrentan las organizaciones.

A continuación se presenta una clasificación de los tipos de riesgo por parte del gobierno australiano:



Proceso de Gestión del Riesgo Según ISO 31000

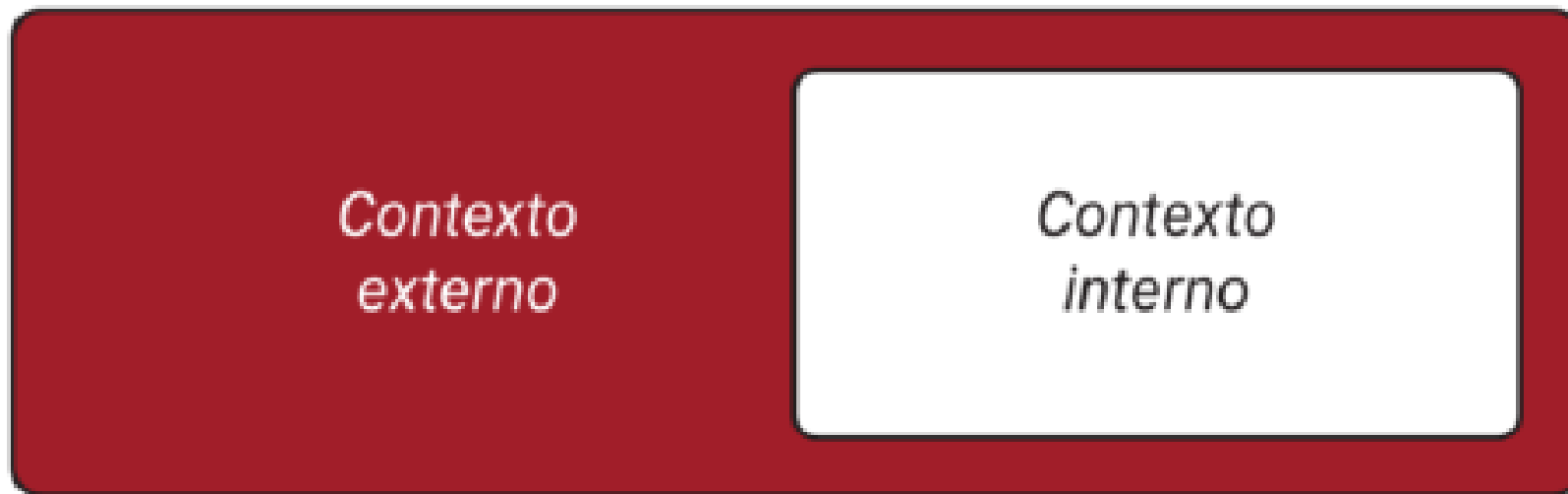
ISO 31000, Figura 4



Comprender la Organización y su Contexto

ISO 31000, cláusula 5.4.1

La organización debería analizar y comprender cuando diseñe el marco de referencia para gestionar el riesgo:

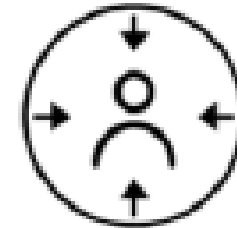


Contexto Interno de la Organización

ISO Guía 73, cláusula 3.3.1.2

Definición:

Entorno interno en el que la organización busca alcanzar sus objetivos



ISO 31000, cláusula 5.4.1 Comprensión de la organización y su contexto

El análisis del contexto interno de la organización puede incluir, pero no limitarse a:

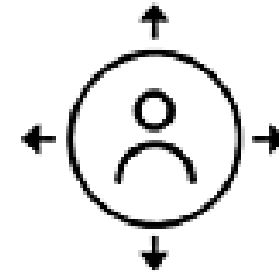
- la visión, la misión y los valores;
- la gobernanza, la estructura de la organización, los roles y la rendición de cuentas;
- la estrategia, los objetivos y las políticas;
- la cultura de la organización;
- las normas, las directrices y los modelos adoptados por la organización;
- las capacidades, entendidas en términos de recursos y conocimiento (por ejemplo, capital, tiempo, personas, propiedad intelectual, procesos, sistemas y tecnologías);*
- los datos, los sistemas de información y los flujos de información;
- las relaciones con partes interesadas internas, teniendo en cuenta sus percepciones y valores;
- las relaciones contractuales y los compromisos;
- las interdependencias e interconexiones.

Contexto Externo de la Organización

ISO Guía 73, cláusula 3.3.1.1

Definición:

Entorno externo en el que la organización busca alcanzar sus objetivos



ISO 31000, cláusula 5.4.1 Comprensión de la organización y su contexto

El análisis del contexto externo de la organización puede incluir, pero no limitarse a:

- los factores sociales, culturales, políticos, legales, reglamentarios, financieros, tecnológicos, económicos y ambientales ya sea a nivel internacional, nacional, regional o local;*
- los impulsores clave y las tendencias que afectan a los objetivos de la organización;*
- las relaciones, percepciones, valores, necesidades y expectativas las partes interesadas externas;*
- las relaciones contractuales y los compromisos;*
- la complejidad de las redes y dependencias;*

Comprensión de la Misión, Objetivos, Valores y Estrategias de la Organización



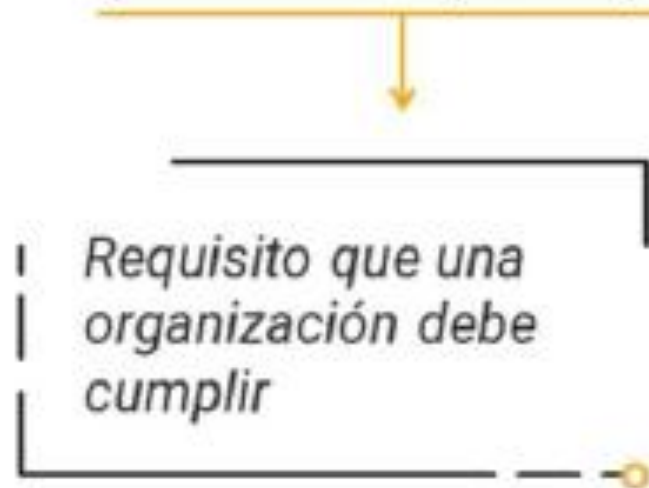
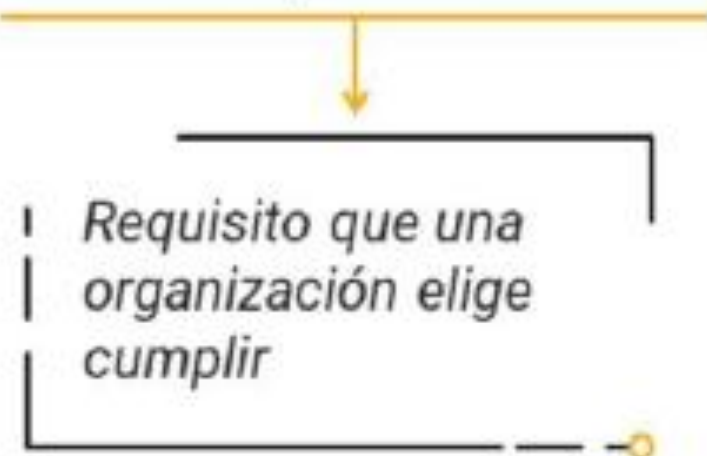
Identificación y Análisis de Requisitos Relacionados con la Gestión del Riesgo



Identificación de las Obligaciones de *Compliance*

ISO 19600, cláusulas 3.14, 3.15 y 4.5.1

Las fuentes de las obligaciones de compliance deberían incluir requisitos de compliance y pueden incluir compromisos de compliance.



Política de Gestión del Riesgo y Manual de Gestión del Riesgo

Política de gestión del riesgo

- Normalmente es un documento corto (2 páginas)
- Es un documento informativo organizacional destinado a las partes interesadas internas y externas de la organización
- Describe brevemente su propósito y los objetivos de la organización sobre la gestión del riesgo



Manual de la gestión del riesgo:

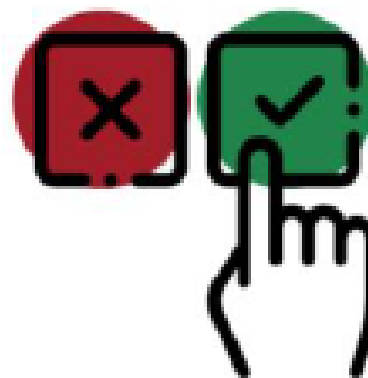
- Es más extenso (10 -15 páginas) que una política de gestión del riesgo
- Proporciona información sobre el alcance, el propósito, la declaración de la política, los objetivos y las funciones y responsabilidades de la organización
- Describe en detalle el proceso de gestión del riesgo sobre cómo identificar, evaluar y tratar el riesgo
- Puede contener apéndices, anexos y otros documentos de apoyo



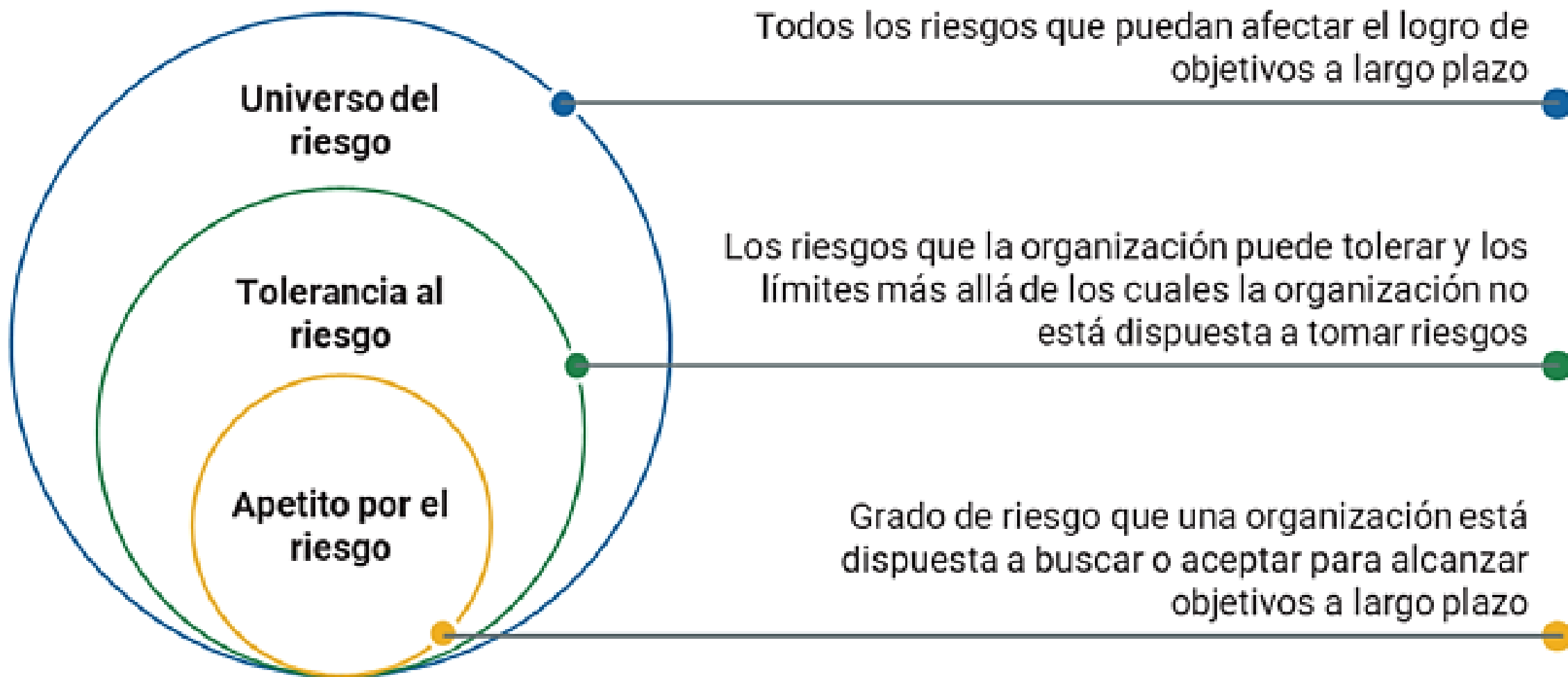
Apetito por el Riesgo

ISO Guía 73, cláusula 3.7.1.2

Cantidad y tipo de riesgo que una organización está dispuesta a conseguir o conservar

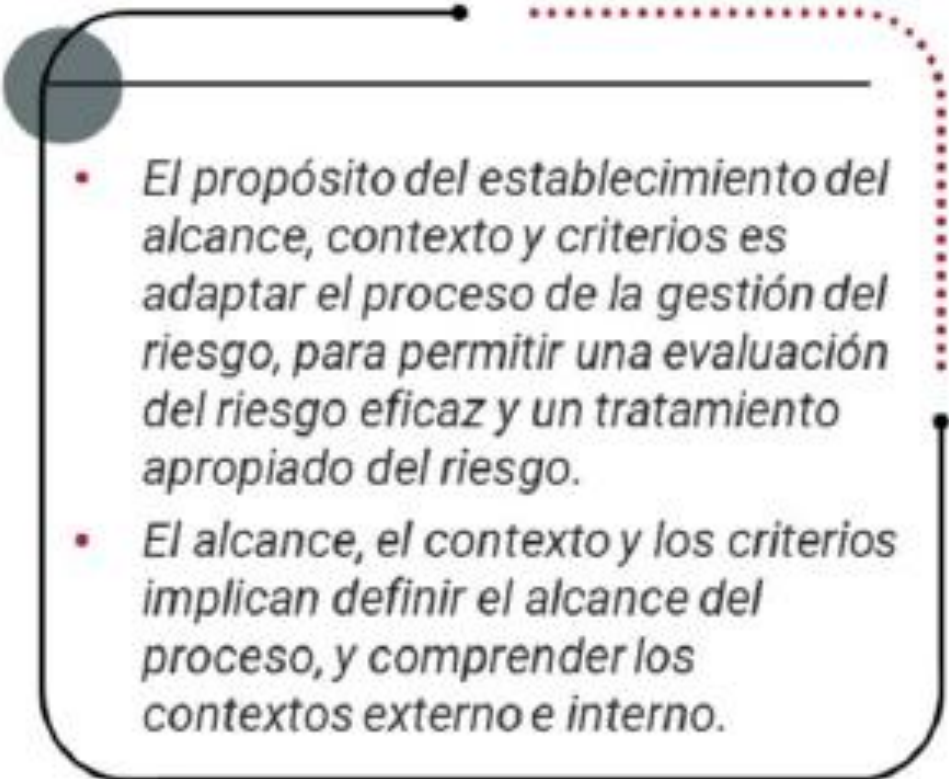


Universo, Tolerancia y Apetito por el Riesgo

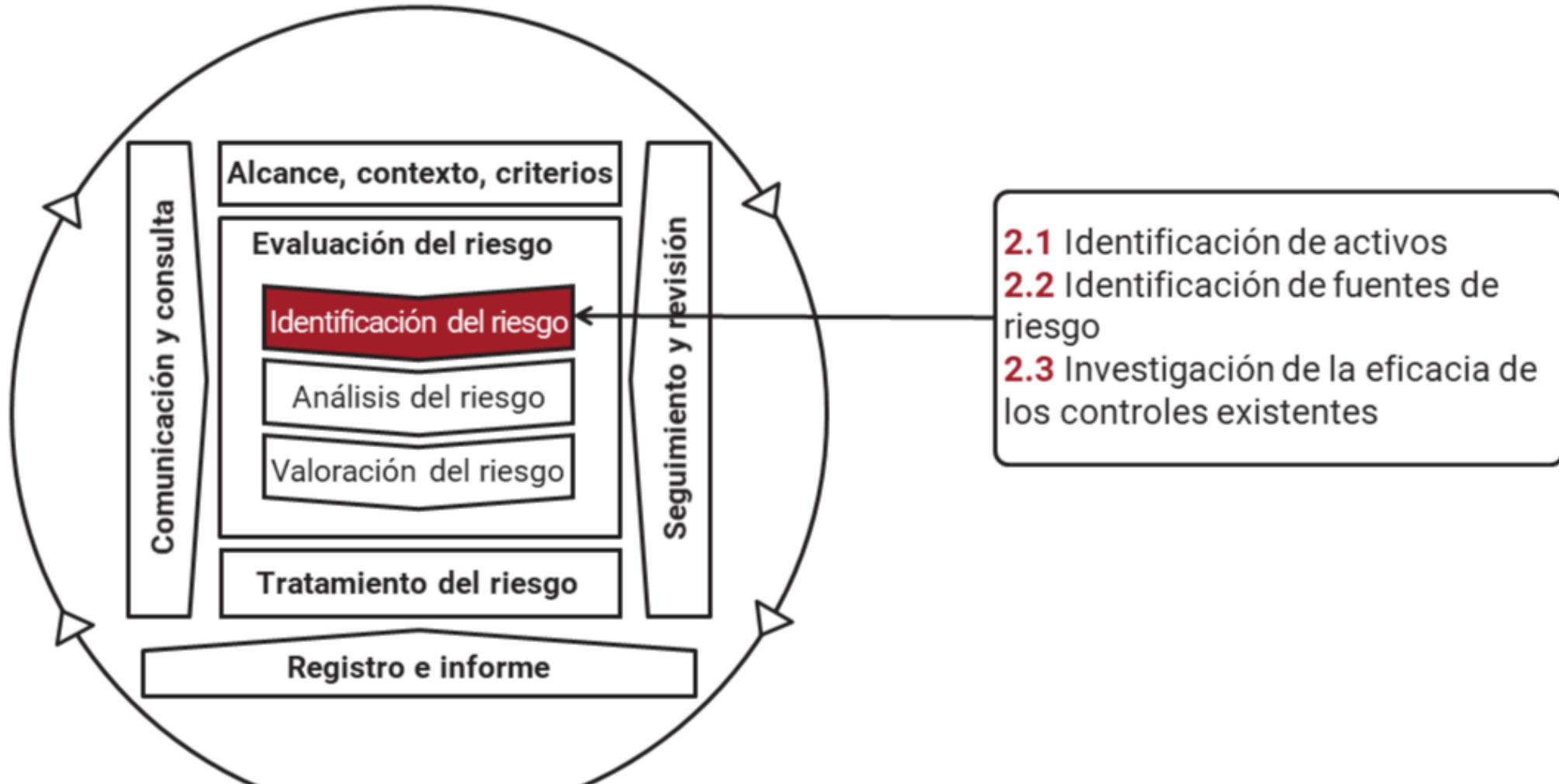


Alcance, Contexto, Criterios

ISO 31000, cláusula 6.3.1

- 
- *El propósito del establecimiento del alcance, contexto y criterios es adaptar el proceso de la gestión del riesgo, para permitir una evaluación del riesgo eficaz y un tratamiento apropiado del riesgo.*
 - *El alcance, el contexto y los criterios implican definir el alcance del proceso, y comprender los contextos externo e interno.*

2. Identificación del Riesgo



Recomendaciones de ISO 31000

ISO 31000, cláusula 6.4.2

- | | |
|--|--|
| <ul style="list-style-type: none">• <i>Para la identificación de los riesgos es importante contar con información pertinente, apropiada y actualizada.</i> | <ul style="list-style-type: none">• <i>La organización debería identificar los riesgos, tanto si sus fuentes están o no bajo su control. Se debería considerar que puede haber más de un tipo de resultado, que puede dar lugar a una variedad de consecuencias tangibles o intangibles.</i> |
|--|--|

Identificación del Riesgo

IEC 31010, cláusula 6.3.2

La identificación del riesgo permite que la incertidumbre se tenga explícitamente en cuenta. Todas las fuentes de incertidumbre y los efectos beneficiosos y perjudiciales podrían ser pertinentes, según el contexto y el alcance de la evaluación.



IEC 31010, cláusula 6.3.2 Identificar el riesgo (continuación)

Las técnicas para la identificar el riesgo generalmente hacen uso del conocimiento y la experiencia de una variedad de partes interesadas. Incluyen considerar:

- *qué incertidumbre existe y los efectos que podría tener;*
- *qué circunstancias o cuestiones (tangibles o intangibles) tienen el potencial para futuras consecuencias;*
- *qué fuentes de riesgo están presentes o pudieran desarrollarse;*
- *qué controles están vigentes y si son eficaces;*
- *qué, cómo, cuándo, dónde y por qué pueden producirse sucesos y consecuencias;*
- *qué ha ocurrido en el pasado y cómo esto podría relacionarse de forma razonable con el futuro;*
- *qué aspectos humanos y factores organizativos podrían aplicar.*

2.2 Identificación de las Fuentes del Riesgo

ISO 31000, cláusula 6.4.2

La organización puede utilizar un rango de técnicas para identificar incertidumbres que pueden afectar a uno o varios objetivos. Se deberían considerar los factores siguientes y la relación entre estos factores:

<i>fuentes de riesgo tangibles e intangibles;</i>	<i>causas y eventos;</i>	<i>amenazas y oportunidades;</i>
<i>vulnerabilidades y capacidades;</i>	<i>cambios en los contextos externo e interno;</i>	<i>indicadores de riesgos emergentes;</i>
<i>naturaleza y valor de los activos y recursos;</i>	<i>consecuencias y sus impactos en los objetivos;</i>	<i>limitaciones de conocimiento y confiabilidad de la información;</i>
<i>factores relacionados con el tiempo;</i>	<i>sesgos, supuestos y creencias de las personas involucradas.</i>	

Determinación de Fuentes, Causas e Impulsores de Riesgo

IEC 31010, cláusula 6.3.3

La identificación de causas, fuentes e impulsores de riesgo puede:

contribuir a estimar la probabilidad de un evento o consecuencia;

ayudar a determinar los indicadores de alerta temprana y sus umbrales de detección;

ayudar a identificar los tratamientos que modificarán el riesgo;

determinar las causas comunes que pueden ayudar a desarrollar prioridades para tratar el riesgo.

