Nueva UNE-ISO 31000:2018
“Gestión del riesgo. Directrices”

Cómo implementar la Gestión del Riesgo con base en ISO 31000

Madrid 13 de junio de 2018

SOLUCIONES
ADMINISTRACIÓN
DE RIESGOS

SOLUCIONES
CONTINUIDAD
DE NEGOCIO

EDUCACIÓN

DRI
México

SOLUCIONES
GESTIÓN INTEGRAL
DE RIESGOS

RISK MÉXICO
Construyendo Resiliencia

Conferencista:

- **Ing. Jorge Escalera Alcázar,** MBA, MBCP, CT31000
- Director, Risk México, S.A. de C.V.
- Presidente del Spanish Translation Task Force (STTF) ISO 31000
- Presidente del Comité Mexicano ISO/TC 262 Gestión del Riesgo
- Coordinador del WG2 Continuidad de Negocio del Comité Mexicano ISO/TC 292 Seguridad y Resiliencia
- Primer Presidente (2004) de RIMS Capítulo México
- Líder de las prácticas de Administración de Riesgos, Continuidad de Negocio, Continuidad de Operaciones, Recuperación ante Desastres y Gestión Integral de Riesgos.
- Más de 23 años de experiencia.
- Desde hace más de 16 años es consultor para corporaciones en México y multinacionales del Sector Privado y asesor para Instituciones del Sector Público.

RISK MÉXICO
Construyendo Resiliencia

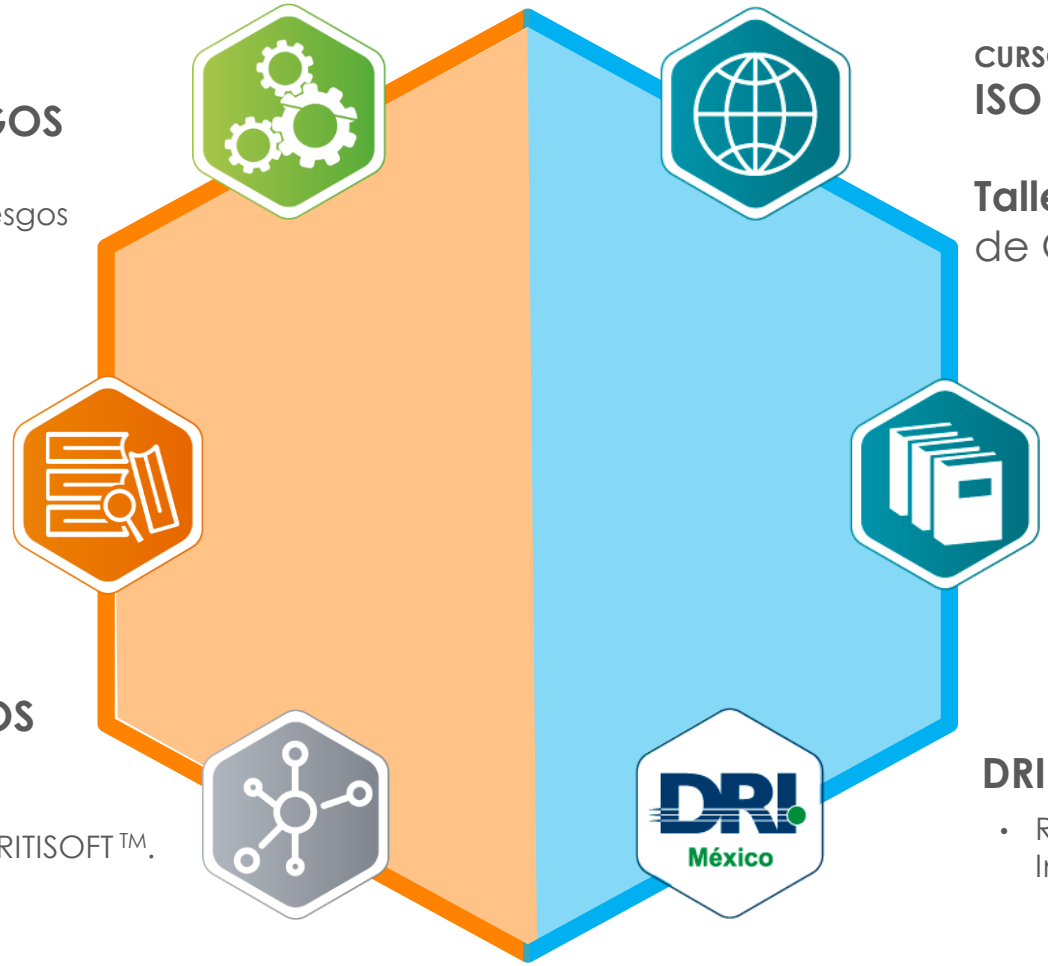
Somos una firma mexicana que ofrece soluciones de **educación**, **certificación** y **consultoría** en los sectores público y privado.

SERVICIOS DE CONSULTORÍA

SOLUCIONES
ADMINISTRACIÓN DE RIESGOS
Consultoría. Outsourcing. Mejora al Programa de Administración de Riesgos y/o Seguros.

SOLUCIONES
CONTINUIDAD DE NEGOCIO
- Planes BCP, DRP TI, COOP.
- Plan de Manejo de Crisis (CMP).
- Plan de Retirada de Productos (Product Recall Plan).

SOLUCIONES
GESTIÓN INTEGRAL DE RIESGOS
- Mapa de Riesgos
- Políticas y Marco de Referencia
- Gestión Integral de Riesgos con APERITISOFT™.



SERVICIOS DE EDUCACIÓN

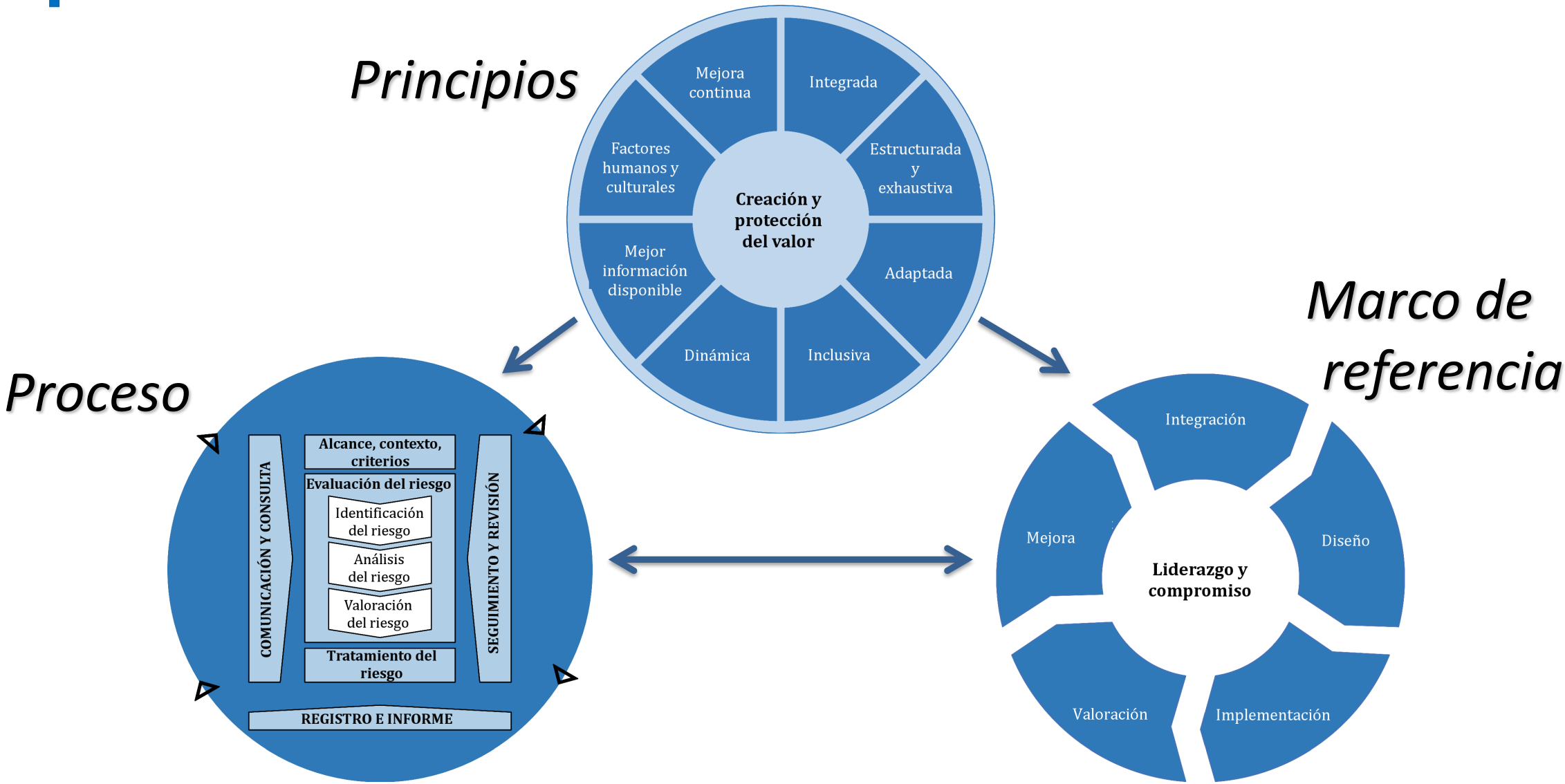
CURSO DE CERTIFICACIÓN
ISO 31000 GESTIÓN DEL RIESGO

Taller ISO 31010 - Técnicas de Evaluación de Gestión del Riesgo

DIPLOMADO
GERENCIA DE ADMINISTRACIÓN DE RIESGOS
- Módulo I: Fundamentos de la Administración de Riesgos.
- Módulo II: Técnicas e Implementación de la Administración de Riesgos.
- Módulo III: La Práctica y Tendencias de la Administración de Riesgos.

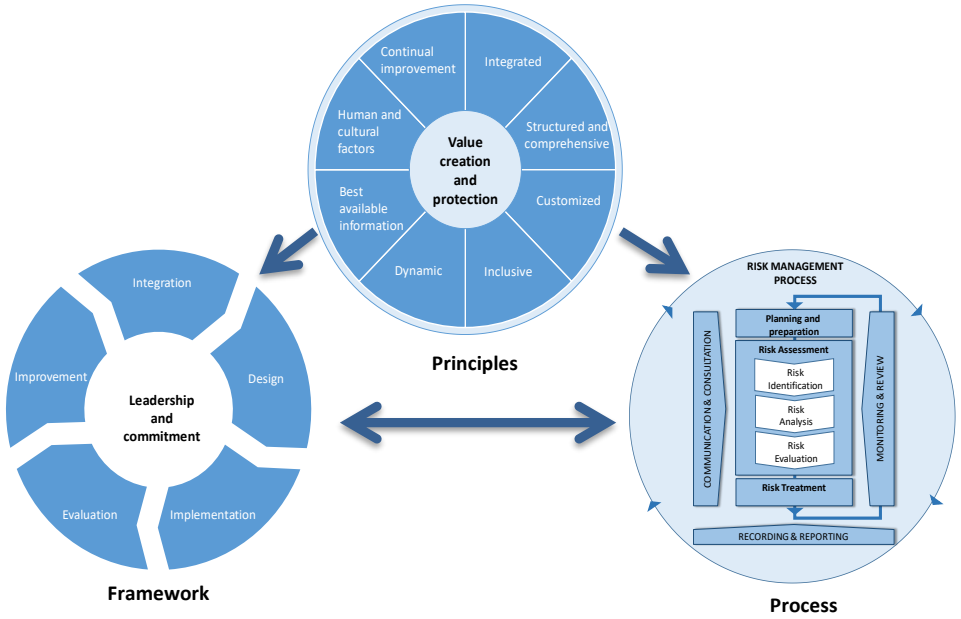
DRI MÉXICO
- Representante del Disaster Recovery Institute International.

Arquitectura del nuevo ISO 31000:2018



Normas ISO 31000 e ISO/TC 262

ISO 31000:2018

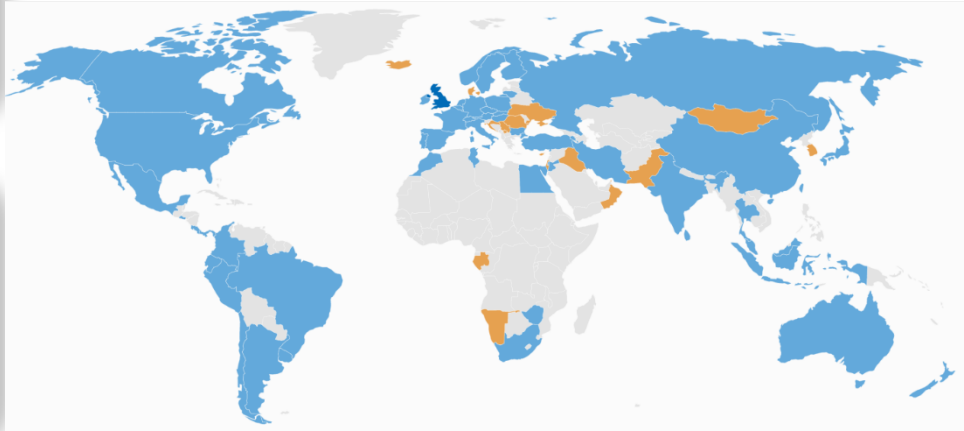


+ **ISO GUÍA 73**
GESTIÓN DEL RIESGO VOCABULARIO

+ **ISO 31010**
TÉCNICAS DE GESTIÓN DEL RIESGO

+ **ISO 31004**
GUÍA PARA LA IMPLEMENTACIÓN DE ISO 31000

- ISO/TC 262 - estándares/trabajos en desarrollo:
  - Revisión de la guía 73 / terminología estándar
  - ISO 31022, Lineamientos para la Implementación de la Gestión de Riesgos Jurídicos Empresariales
  - Manual de implementación de ISO 31000
- ISO/TC 262:
  - 55 países participantes
  - 18 Países Observadores

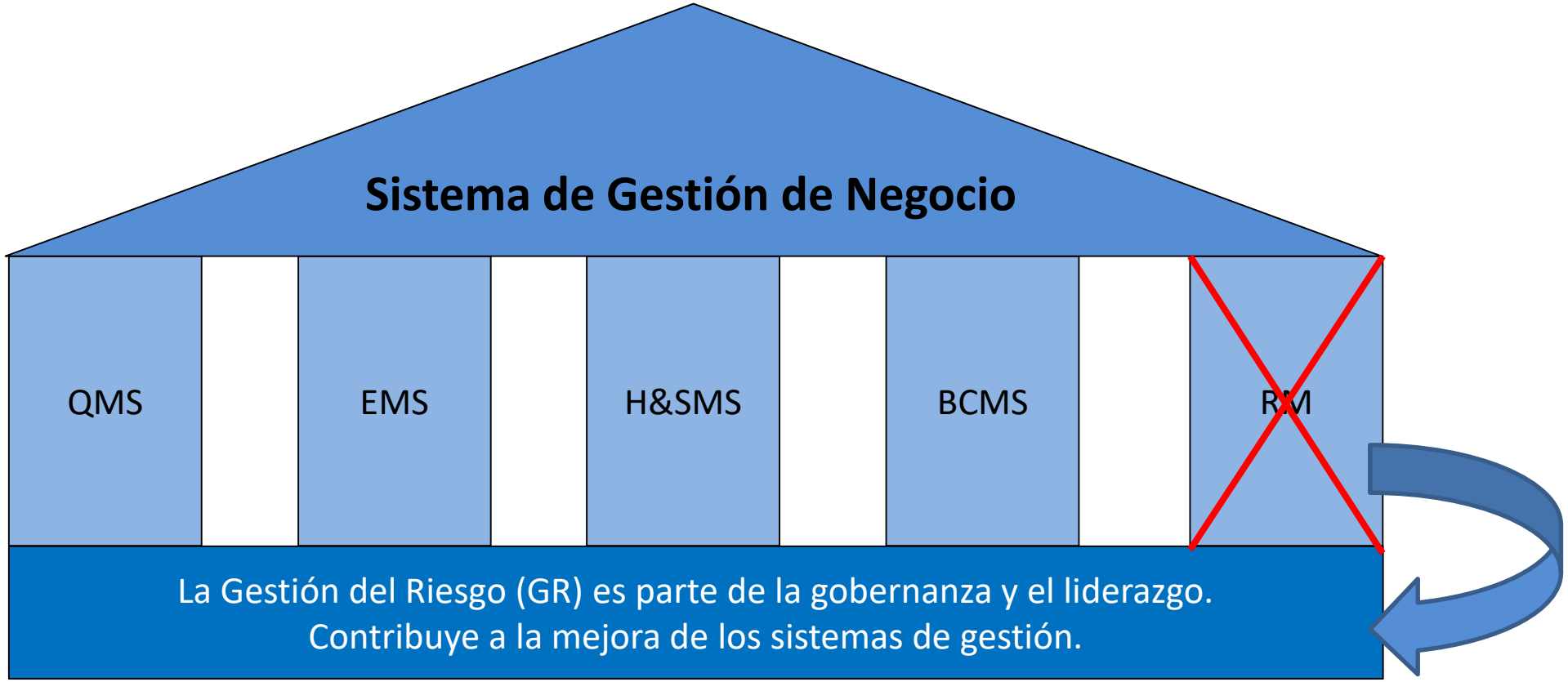


- ISO 31000:2018: Inglés, Francés, Español (STTF 12 países) y pronto: Ruso, Portugués, Alemán, Árabe, etc.

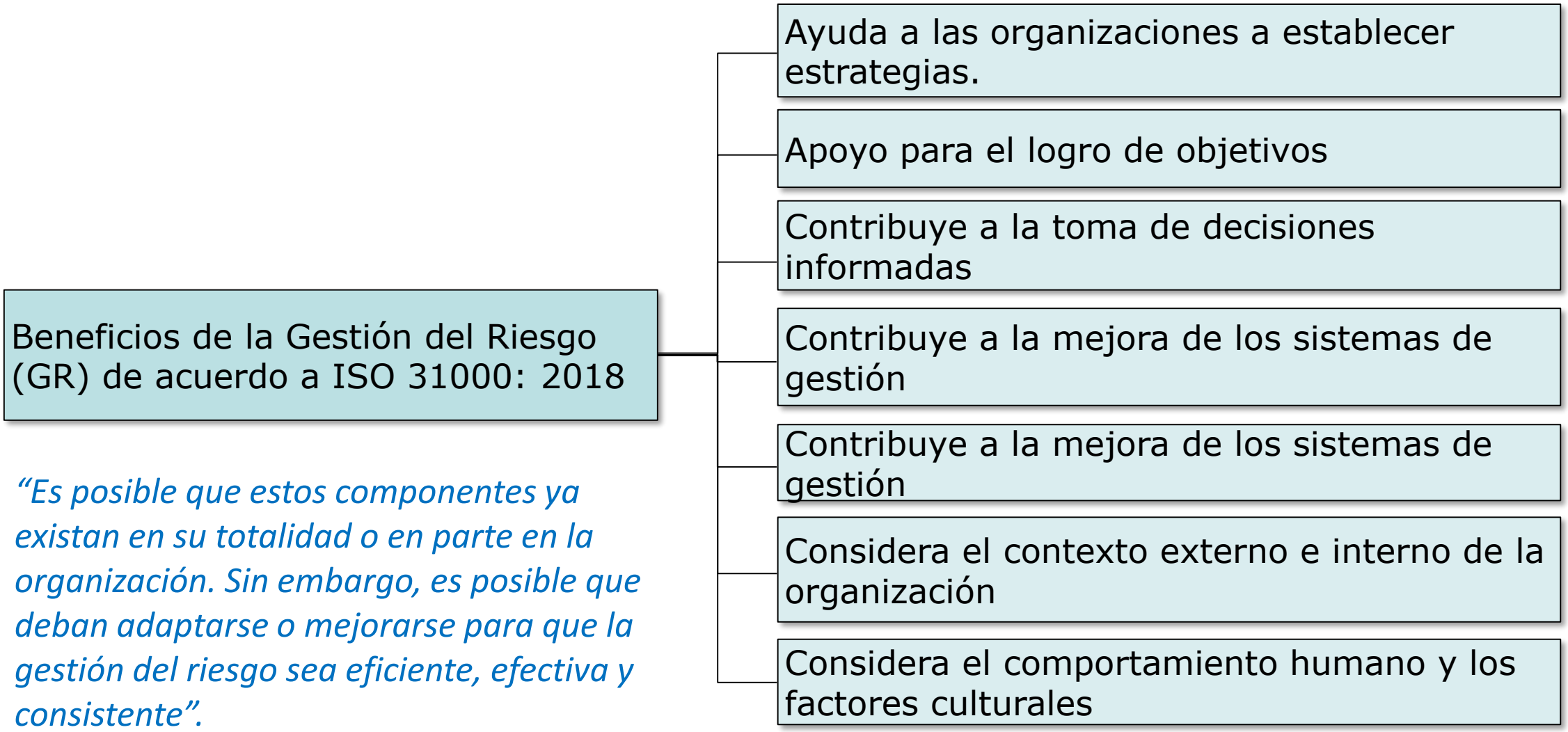
ISO/TC 262: RM Technical committee of the International Organization for Standardization

¿Por qué es tan especial el estándar ISO 31000?

- Son directrices que integran la toma de decisiones con base en riesgos en el gobierno, planificación, administración, reporteo, políticas, valores y culturas de la organización.



Beneficios de la Gestión del Riesgo con base en el estándar ISO 31000: 2018



"Es posible que estos componentes ya existan en su totalidad o en parte en la organización. Sin embargo, es posible que deban adaptarse o mejorarse para que la gestión del riesgo sea eficiente, efectiva y consistente".

Aspectos relevantes del nuevo ISO 31000:2018

Cambios ISO 31000: 2018 vs 2009

Arquitectura

Principios

Centrado en la creación de valor y la protección

ISO 31000: 2018

Arquitectura

Marco de referencia

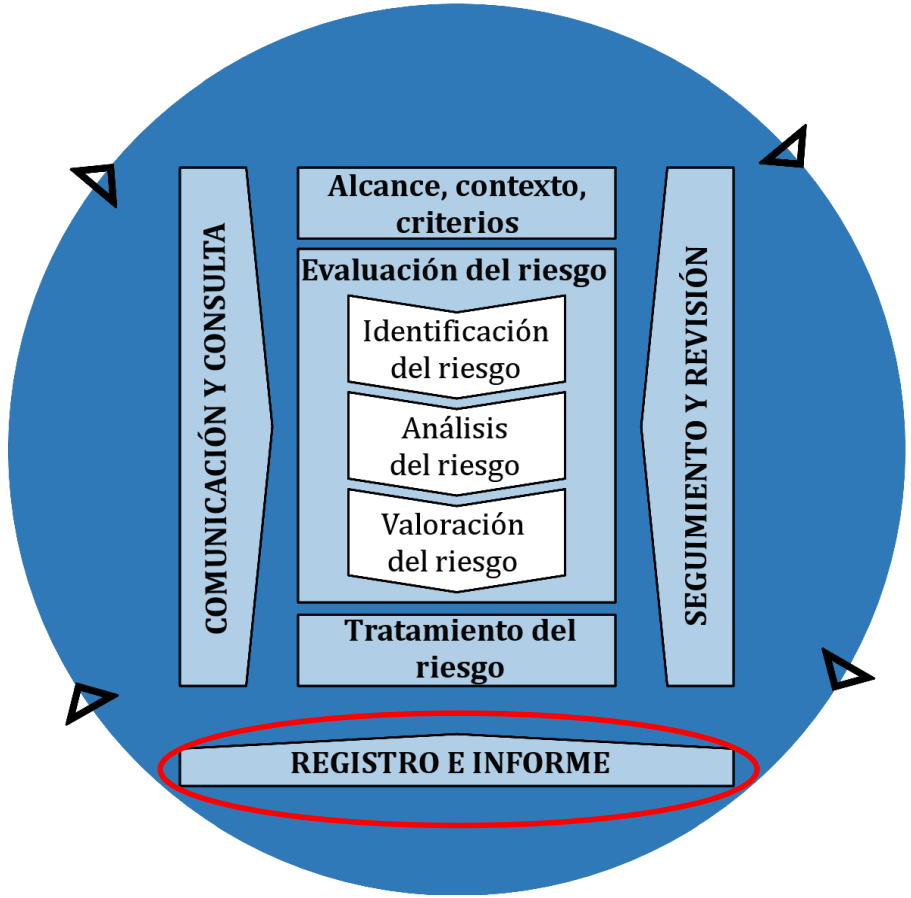
Liderazgo vs. Dirección

ISO 31000: 2018

Arquitectura

Proceso

Incluye
"Registro e Informe"



ISO 31000 / GUÍA 73 – Términos y Definiciones

- COMUNICACIÓN Y CONSULTA
- **CONSECUENCIA**
- **CONTROL**
- ESTABLECIMIENTO DEL CONTEXTO
- **EVENTO**
- EXPOSICIÓN
- CONTEXTO EXTERNO
- FRECUENCIA
- PELIGRO (HAZARD)
- CONTEXTO INTERNO
- NIVEL DE RIESGO
- **PROBABILIDAD (LIKELIHOOD)**
- MONITOREO
- PROBABILIDAD (PROBABILITY)
- RIESGO RESIDUAL
- RESILIENCIA
- REVISIÓN
- **RIESGO**
- ACEPTACIÓN DEL RIESGO
- AGRUPACIÓN DE RIESGOS
- ANÁLISIS DEL RIESGO
- APETITO POR EL RIESGO
- VALORACIÓN DEL RIESGO
- ACTITUD HACIA EL RIESGO
- AVERSIÓN AL RIESGO
- EVITAR DEL RIESGO
- CRITERIOS DE RIESGO
- DESCRIPCIÓN DEL RIESGO
- EVALUACIÓN DEL RIESGO
- FINANCIACIÓN DEL RIESGO
- IDENTIFICACIÓN DEL RIESGO
- **GESTIÓN DEL RIESGO**
- AUDITORÍA DE GESTIÓN DEL RIESGO
- MARCO DE REFERENCIA DE LA GESTIÓN DEL RIESGO
- PLAN PARA LA GESTIÓN DEL RIESGO
- POLÍTICA PARA LA GESTIÓN DEL RIESGO
- PROCESO DE GESTIÓN DEL RIESGO
- MATRIZ DE RIESGO
- **DUEÑO DEL RIESGO**
- PERCEPCIÓN DEL RIESGO
- PERFIL DE RIESGO
- REGISTRO DE RIESGOS
- REPORTE DEL RIESGO
- RETENCIÓN DEL RIESGO
- COMPARTIR EL RIESGO
- **FUENTE DE RIESGO**
- TOLERANCIA AL RIESGO
- TRATAMIENTO DEL RIESGO
- **PARTE INTERESADA**
- VULNERABILIDAD

ISO 31000:2018: solo 8 definiciones

vs.

2009: 29 definiciones

Rojo / negrita = Utilizado en ISO 31000

ISO 31000 – Términos y Definiciones

3.1. RIESGO = Efecto de la incertidumbre sobre los objetivos.

3.2. Gestión del riesgo = actividades coordinadas para dirigir y controlar la organización con relación al riesgo (3.1).

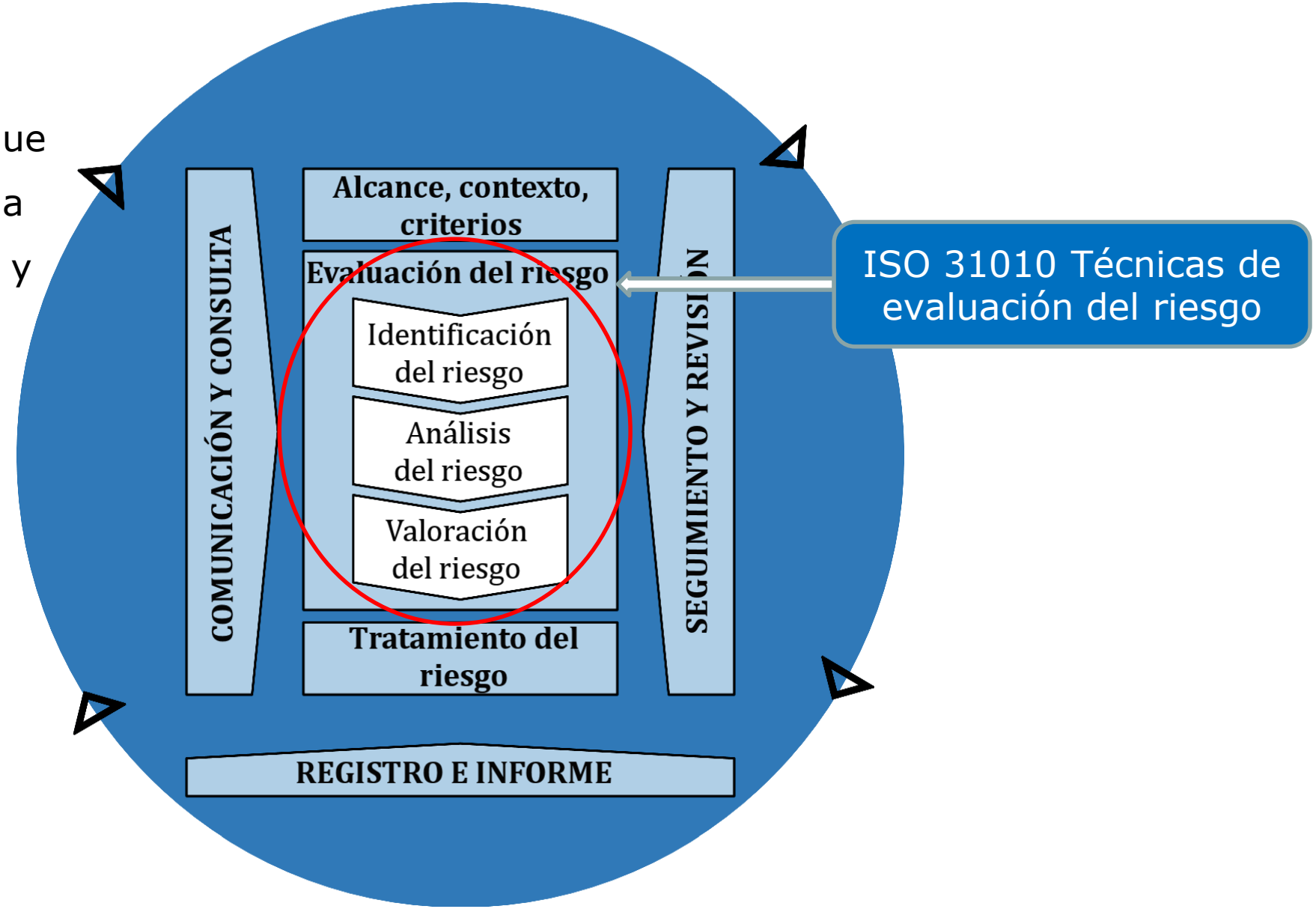
ISO 31000 – Términos y Definiciones

Dueño del riesgo = Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

- + **Recursos** (humanos, tecnológicos, información, financieros, colaboradores).
- + **Competencia** (programa de entrenamiento y capacitación).

Evaluación del riesgo y la ISO 31010 – Técnicas

- Suele requerir un enfoque multidisciplinario dado la amplia gama de causas y consecuencias.



Objeto y campo de aplicación de la norma ISO 31010

- "Esta norma está prevista para reflejar **las buenas prácticas actuales** en la selección y utilización de las técnicas de evaluación del riesgo"

- ISO 31010 es:
  - Una norma de apoyo a la norma ISO 31000
  - Una norma genérica
  - Ofrece orientaciones sobre distintas técnicas

- ISO 31010:
  - **No** establece criterios específicos para determinar si una evaluación de riesgos es necesaria, ni el método o técnica a utilizar según la aplicación particular
  - **No** cataloga TODAS las técnicas existentes
  - **No** impone métodos o técnicas particulares
  - **No** es certificable

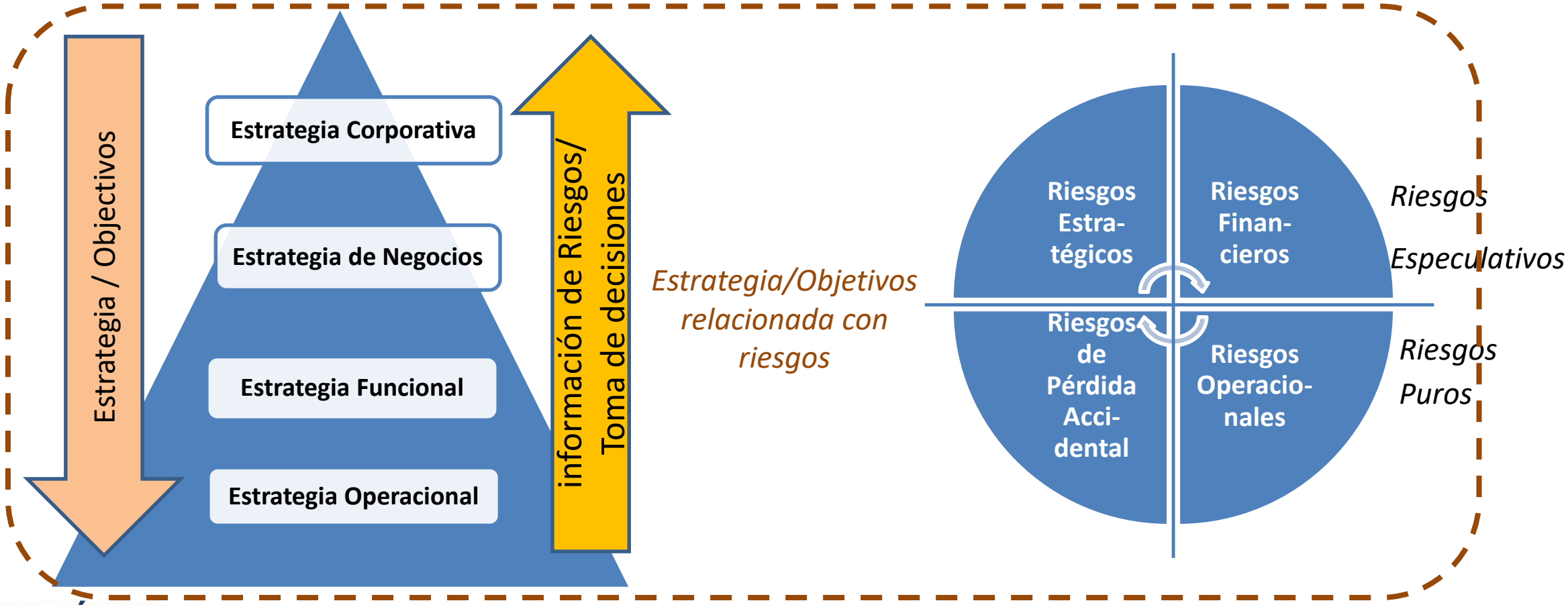
¿Cómo ISO 31000 puede ayudar a mejorar la eficiencia operacional y la gobernanza?

- Ayuda a desarrollar una estrategia de MR que vincule objetivos y riesgos.
- Es un componente activo para mejorar el rendimiento de una organización.
- Es un sistema abierto basado en principios.
- Permite una toma de decisiones más informada y efectiva.
- Ayuda a desarrollar una cultura para gestionar el riesgo.

- A través de Comunicación y Consulta con todos las partes interesadas internas y externas:
  - Unifique múltiples esfuerzos para gestionar los riesgos.
  - Integra el proceso de RM en procesos entre empresas.
  - Habilita la aplicación "operacional" de múltiples procesos de GR.

¿Cómo ISO 31000 puede ayudar a mejorar la eficiencia operacional y la gobernanza?

- Guía ISO 31000 nos da una guía para vincular la estrategia (y los objetivos) con la gestión del riesgo a todos los niveles, establecer una comunicación y consulta de riesgos y un proceso de registro y presentación de informes.



Metodología de Risk México para implementar un programa de RM basado en ISO 31000

- **Nuestra Metodología en Tres Fases:**

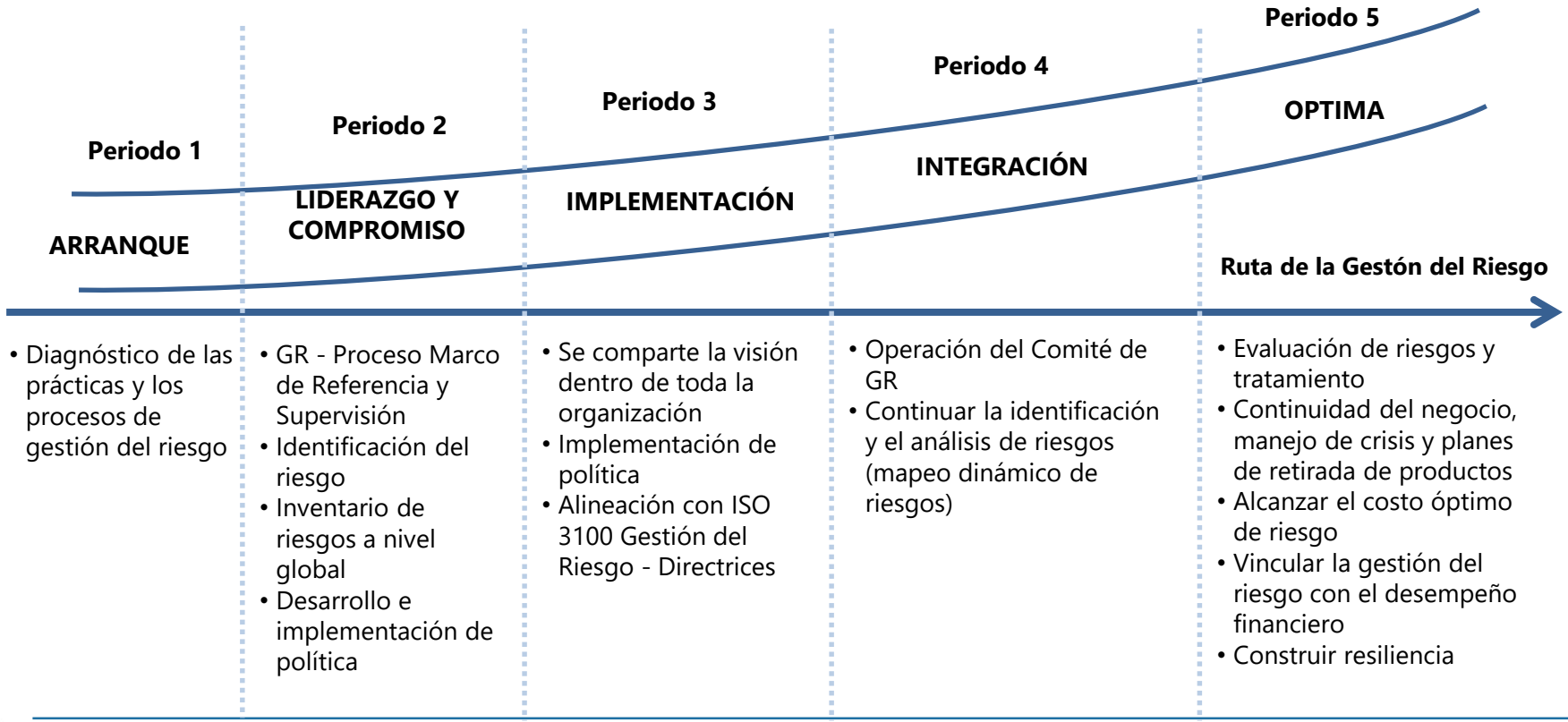
- **Fase de Descubrimiento:**
  - La organización debería evaluar sus prácticas y procesos de RM existentes, evaluar las brechas existentes frente a ISO 31000 y abordar esas brechas dentro del marco de referencia.
  - Todos los componentes del marco de referencia y la forma en que trabajan juntos deben adaptarse a las necesidades de la organización.

- **Fase de Mejora:**
  - Definir, en conjunto con los líderes del riesgo, las necesidades actuales de GR de la organización y establecer el proceso de GR, incluida la comunicación y la consulta con las partes interesadas internas y externas.

- **Fase de Estandarización:**
  - Entrenamiento sobre el proceso de GR: Establecimiento del contexto, identificación, análisis, valoración y tratamiento del riesgo, seleccionando las mejores prácticas de evaluación de riesgos. (ISO 31010 - Técnicas de GR).
    Estandarizar la Gestión del Riesgo dentro de la organización / UEN / Funciones a través de los "**dueños del riesgo**".

Metodología de Risk México para implementar un programa de RM basado en ISO 31000

- Definimos el nivel de madurez de la gestión del riesgo de la organización y desarrollamos un plan para lograr una práctica y un proceso de gestión del riesgo óptimos, que incluyen:
  - Centralizar la información de GR
  - Desarrollo de una política y directrices globales de GR
  - Implementación de un Comité Corporativo de GR
  - Definir el soporte corporativo para desarrollar la capacidad de recuperación del negocio y el logro del costo óptimo del riesgo



Metodología de Risk México

- Ejemplo de un entregable al final de la Fase de Descubrimiento:
  - Informe sobre una revisión crítica de los componentes de Gestión del Riesgo frente a ISO 31000.

- **Revisión de 15 componentes de la GR**

No.	Componentes de la GR	Grado de Alineación
1	Política para la GR	
2	Plan para la GR	
3	Riesgos	
4	Nivel del riesgo	
5	Fuente del riesgo	
6	Propietario del riesgo	
7	Identificación del riesgo	
8	Análisis del riesgos	
9	Criterios del riesgo	
10	Evaluación del riesgo	
11	Tratamiento del riesgo	
12	Perfil del riesgo	
13	Comunicación y consulta	
14	Monitoreo del riesgo	
15	Revisión del riesgo	

Grado de Alineación vs. ISO 3100

Grado de Alineación con ISO 31000	Rango de Calificación	Color
Muy Alto	≥ 80%	
Alto	60-79%	
Moderado	40-59%	
Bajo	20-39%	
Muy Bajo	<20%	

Metodología de Risk México

- Ejemplo de un entregable al final de la Fase de Descubrimiento:
  - Informe sobre una revisión crítica de los componentes de Gestión del Riesgo frente a ISO 31000.

- **Revisión de 5 atributos para una gestión mejorada de los componentes de la GR**

No.	Componentes de la GR	Grado de Alineación
A.1	Mejora continua	
A.2	Rendición total de cuentas con respecto a los riesgos	
A.3	Aplicación de la gestión del riesgo en la toma de decisiones	
A.4	Comunicaciones continuas	
A.5	Integración completa en la estructura de gobierno de la organización	

Grado de Alineación vs. ISO 3100

Grado de Alineación con ISO 31000	Rango de Calificación	Color
Muy Alto	≥ 80%	
Alto	60-79%	
Moderado	40-59%	
Bajo	20-39%	
Muy Bajo	<20%	

Información de Contacto

Para conocer mas información sobre alguno de los productos o servicios de Risk México, por favor contáctese con nuestro equipo de trabajo.

Ing. Jorge Escalera Alcázar, MBCP, CT31000
Director
jorge.escalera@riskmexico.com
Ext. 101

Lic. Eduardo Escalera Balderas, CBCP, C31000
Gerente de Servicios
eduardo.escalera@riskmexico.com
Ext. 106
Cel: (81)15993477

www.riskmexico.com

Número Telefónico: 01 800 725 RISK (7475), +52 (81) 86763401, 04 y 05
info@riskmexico.com