Gestión de riesgos

en la norma ISO 19011:2011

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
AEC

Foro CERPER 2010

Isaac Navarro:

Nueva ISO 19011

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
AEC

UNE-EN ISO 19011: 2002

"Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental."

ISO19011

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

AEC

UNE-EN ISO 19011: 2002

"Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental."

UNE-EN ISO 19011: 2011

"Directrices para la auditoría de los sistemas de gestión."

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
AEC

Las dos versiones tienen los mismos capítulos

Capítulo 1. Alcance.
Capítulo 2. Referencias normativas.
Capítulo 3. Términos y definiciones.
Capítulo 4. Principios de auditoria.
Capítulo 5. Gestión de un programa de auditoria.
Capítulo 6. Realización de la auditoria.
Capítulo 7. Competencia y evaluación de auditores.

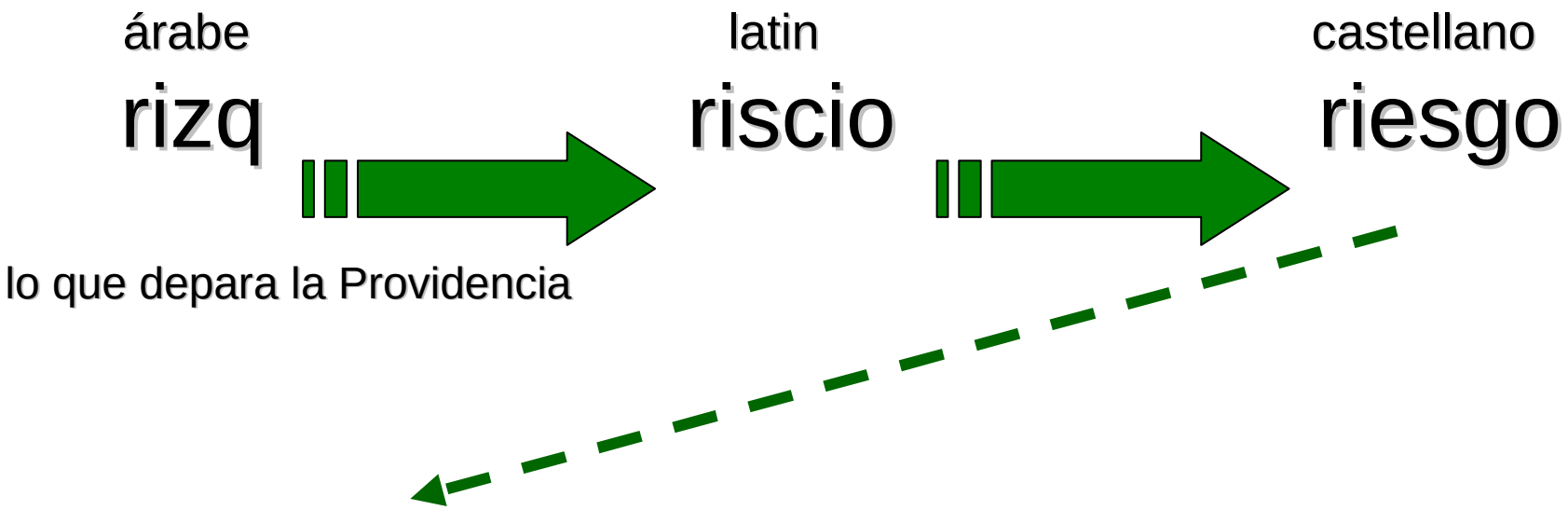
…. pero tienen diferencias sustanciales

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
AEC

Diferencias

Versión 2002	Versión 2011
Sistemas de gestión de calidad y/o MA	Todo tipo de sistemas de gestión
Auditorías de 1ª, de 2ª y de 3ª parte	Auditorías de 1ª y de 2ª parte (3ª parte, ISO 17021:2011)
No habla de gestión de riesgos	Incide en gestión de riesgos
Competencias de “líder” y “equipo”	Competencias “líder”, “equipo” y “gestor del programa de auditorías”
Implementación del programa ligera	Mayor profundidad y extensión
Revisión documentación, antes	Revisión documentación antes y durante
Sin anexos	Anexos A y B. Ejemplos de conocimientos y habilidades Guía planificación y ejecución auditorías

¿Qué es un riesgo?



ISO Guía 73:2009 (terminología en materia de riesgos):

Efecto de la incertidumbre sobre la consecución de objetivos.

Combinación de la probabilidad de ocurrencia y el impacto de un evento, considerando que las consecuencias posibles puedan ser tanto positivas como negativas.

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
AEC

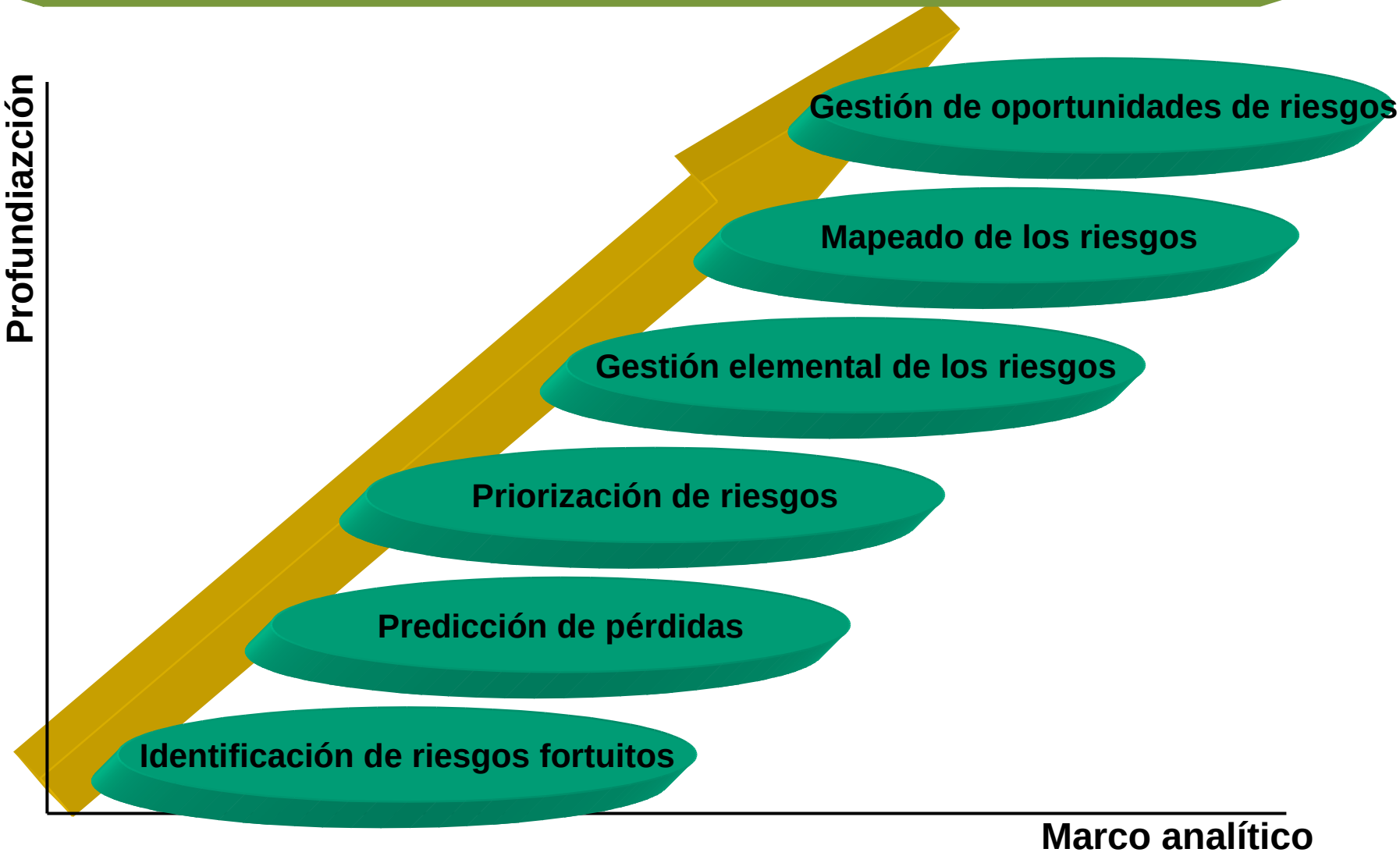
Atributos del riesgo

Posibilidad: no existe certeza absoluta de la materialización de un riesgo.

Variabilidad: las consecuencias pueden variar dentro de un abanico de resultados.

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
AEC

Evolución de la gestión de los riesgos



ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
AEC

Tipos de riesgos según su impacto

Tipo 1: Se produce el daño de manera muy rápida

Ocasionan pérdidas inmediatas y potencialmente significativas.

Tipo 2: Se produce el daño de manera más lenta.

Ocasionan pérdidas graduales y crecientes.

Tipo 3: Se produce el daño de manera espaciada y continua.

Ocasionan pérdidas crecientes y potencialmente significativas.

Tipo 4: Eventos catastróficos.

Ocasionan pérdidas inmediatas sin posibilidad de recuperación.

Tipos de riesgos según su naturaleza

Riesgos financieros.
Ocasionados por fluctuaciones en los mercados.

Riesgos de crédito.
Ocasionados por dificultades de los deudores.

Riesgos estratégicos.
Derivados de la posición estratégica de la organización.

Riesgos operacionales.
Derivados de fallos en los procesos y/o recursos.

Proceso de gestión de riesgos

Diversos estándares.

Difieren muy poco entre ellos.

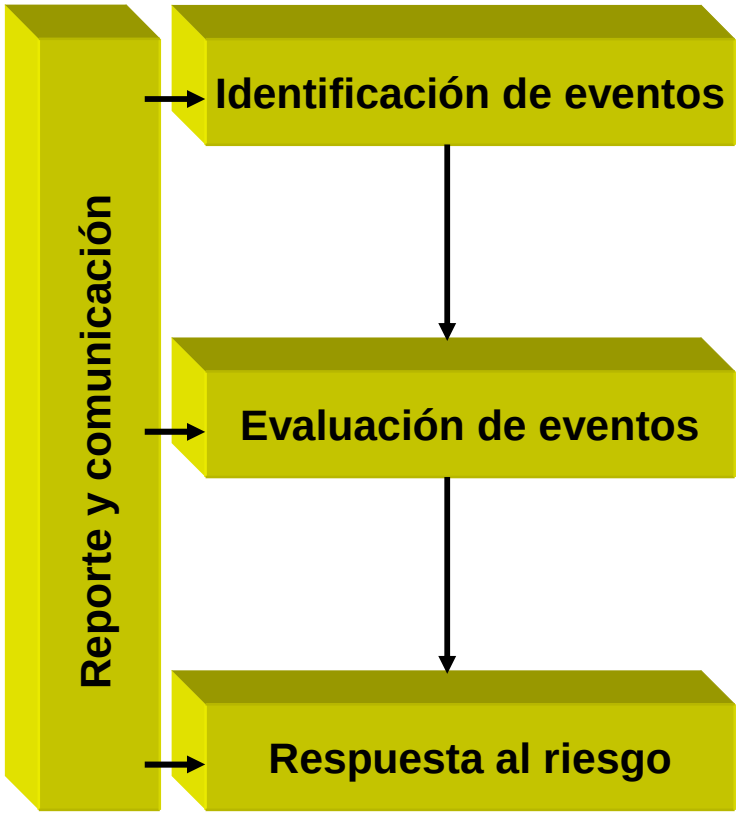
UNE-EN ISO 31000:2009

"Gestión del riesgo. Principios y directrices"

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

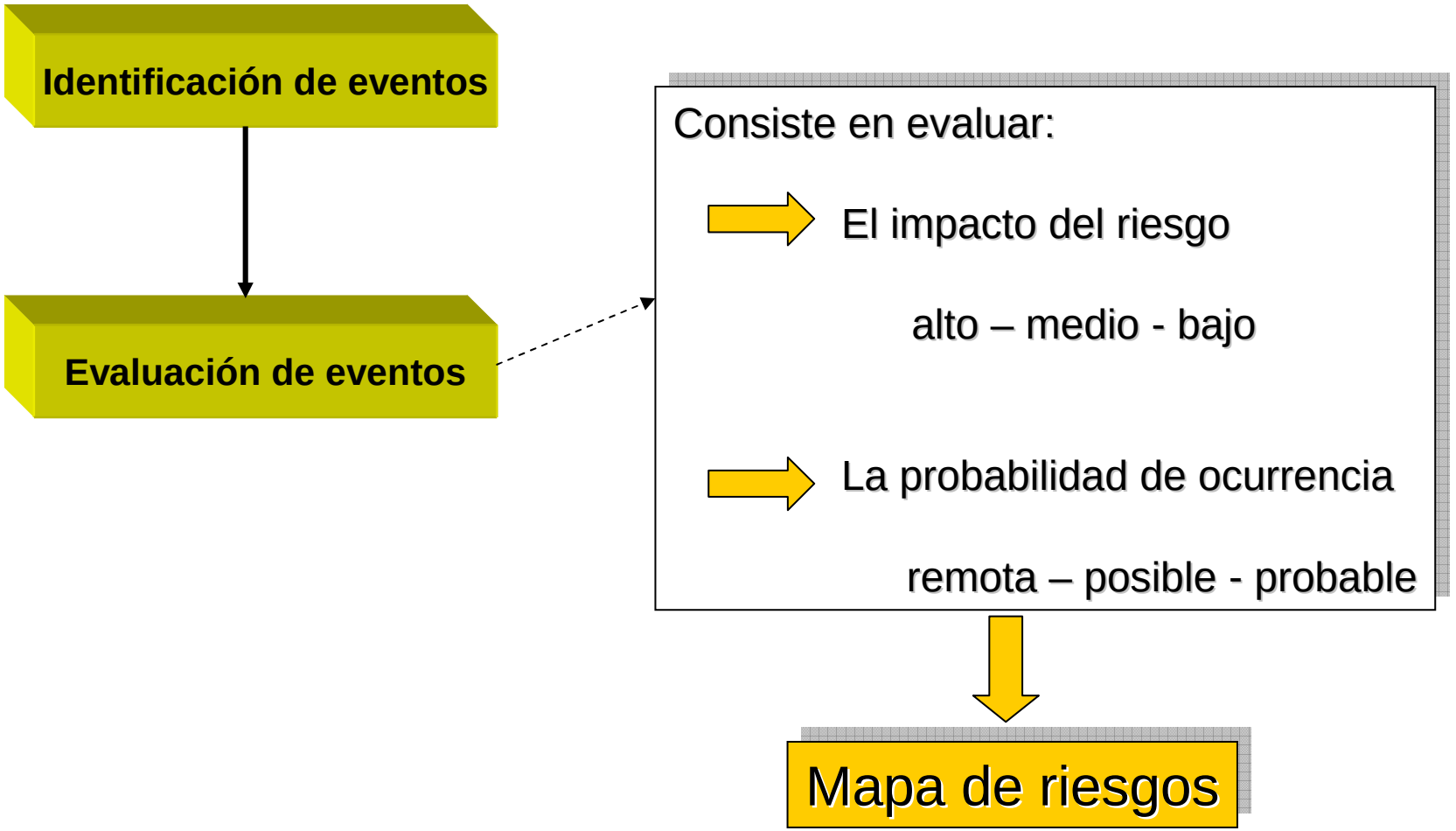
AEC

Proceso de gestión de riesgos



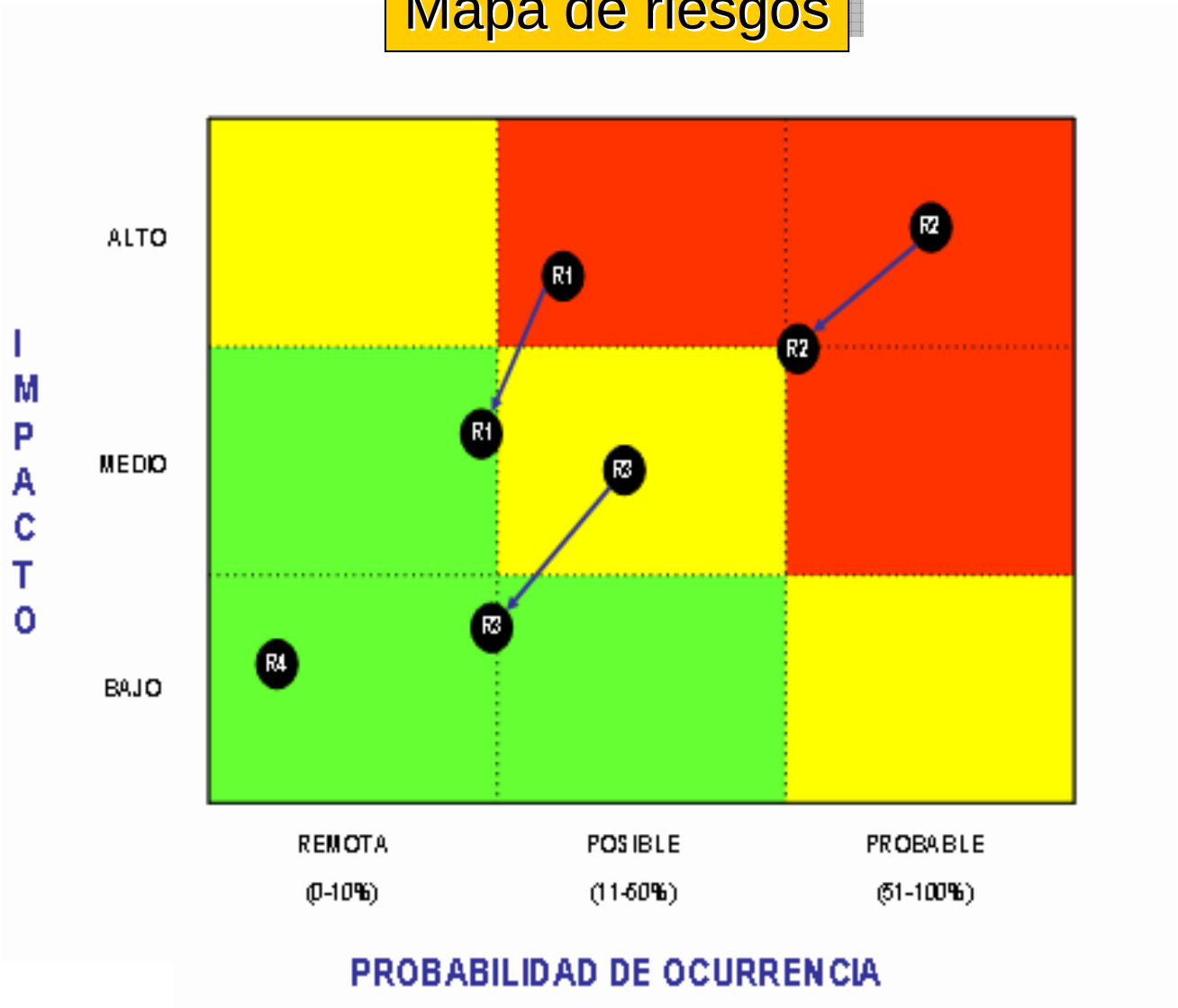
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
AEC

Proceso de gestión de riesgos



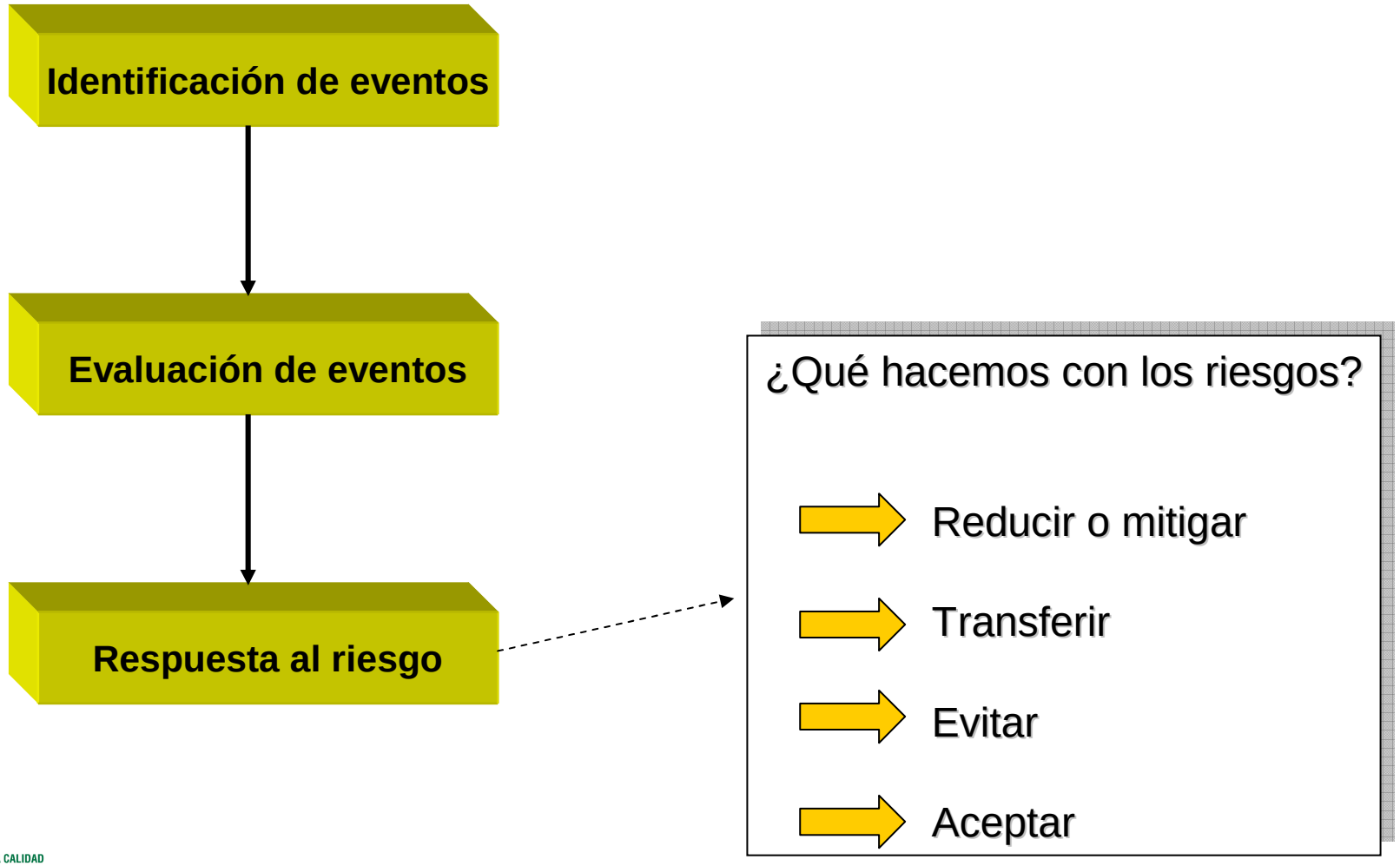
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
AEC

Mapa de riesgos



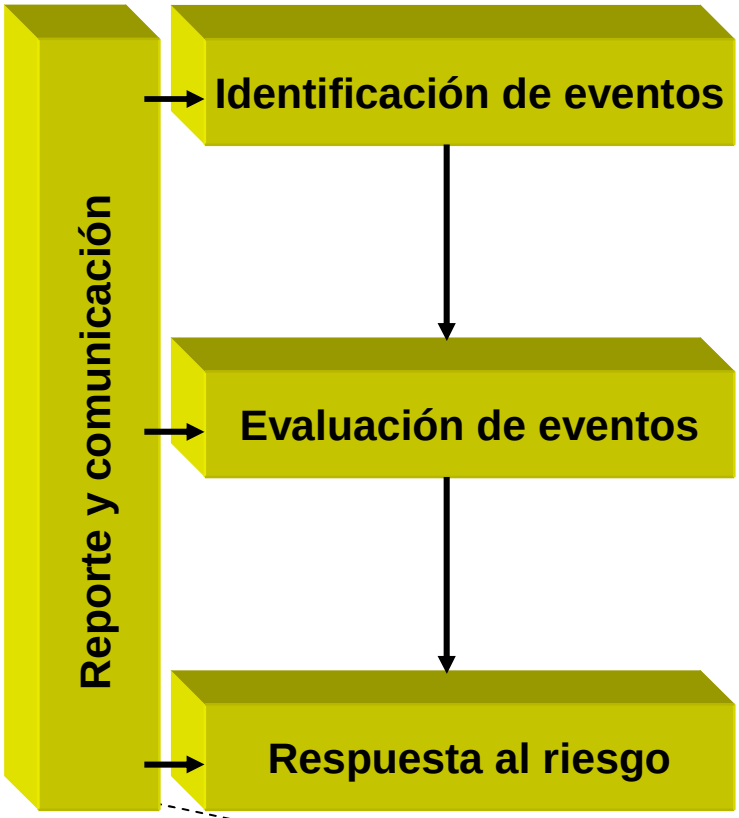
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
AEC

Proceso de gestión de riesgos



ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
AEC

Proceso de gestión de riesgos



Seguimiento adecuado de los riesgos

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
AEC

Los riesgos en la ISO 19011:2011

Recordemos

Capítulo 1. Alcance.
Capítulo 2. Referencias normativas.
Capítulo 3. Términos y definiciones.
Capítulo 4. Principios de auditoria.
Capítulo 5. Gestión de un programa de auditoria.
Capítulo 6. Realización de la auditoria.
Capítulo 7. Competencia y evaluación de auditores.

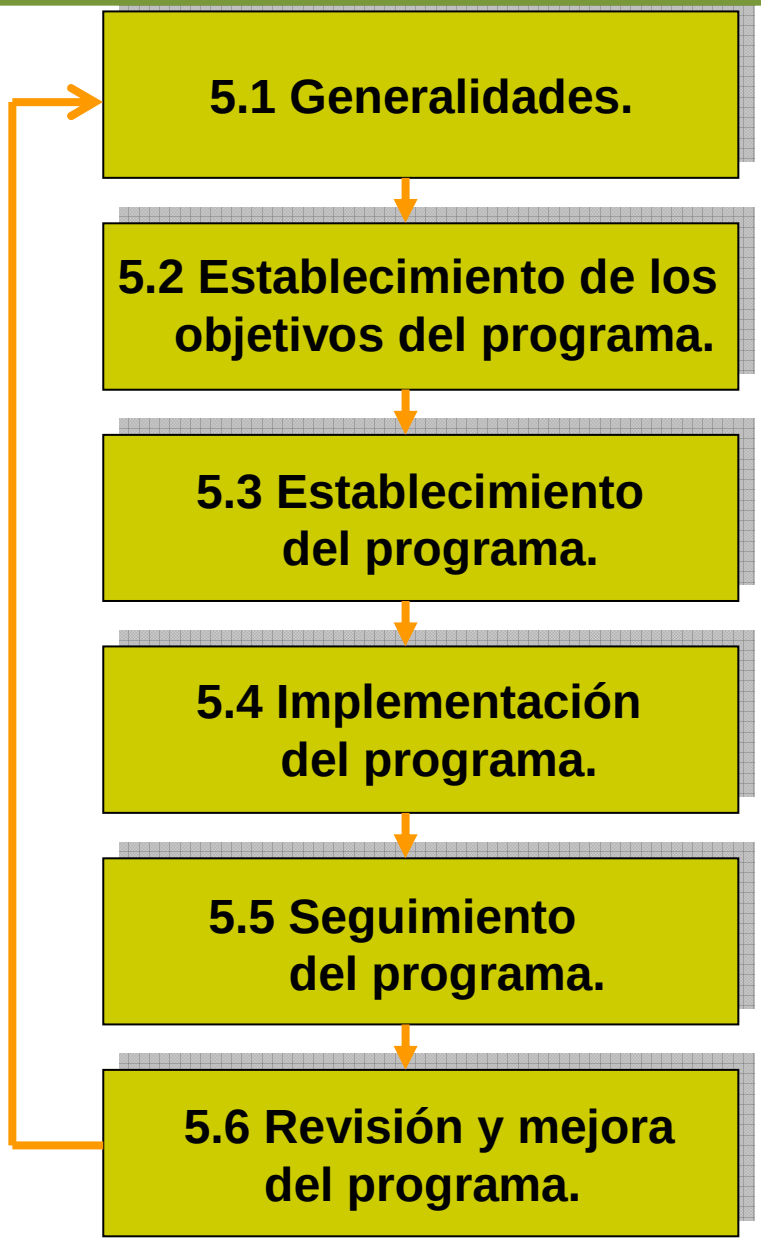
Se trata de riesgos operacionales

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
AEC

Los riesgos en la ISO 19011:2011

Capítulo 5

Gestión del programa



ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
AEC

Gestión del programa de auditoría

Punto de la norma	Aparecen los riesgos
5.1 Gestión del programa de auditoría. Generalidades	
5.2 Establecimiento de los objetivos del programa de auditoría	Evaluar los riesgos que pueden impedir que se implemente el programa de manera efectiva.
5.3.1 Roles y responsabilidades de la persona responsable del programa	Tener en cuenta los riesgos asociados al programa.
5.3.2 Competencia de la persona responsable del programa	La necesaria para gestionar los riesgos asociados al programa.
5.3.3 Determinación de la extensión del programa	
5.3.4 Identificación y evaluación de los riesgos del programa de auditoría	Riesgos asociados a la planificación
5.3.5 Establecimiento de procedimientos para el programa de auditoría	Tener en cuenta los riesgos identificados en 5.3.4
5.3.6 Identificación de los recursos del programa de auditoría	Tener en cuenta los riesgos identificados en 5.3.4
5.4.1 Implementación del programa de auditoría. Generalidades	
5.4.2 Determinación de los objetivos, alcance y criterios	
5.4.3 Selección de los métodos de auditoría	
5.4.4 Selección de los miembros del equipo auditor	Asegurar su independencia para evitar conflictos de interés.
5.4.5 Asignación de responsabilidades al líder del equipo auditor	El responsable del programa le debe proveer de la información necesaria para abordar los riesgos
5.4.6 Gestión de los resultados del programa de auditoría	
5.4.7 Gestión y mantenimiento de los registros del programa de auditoría	Entre ellos, los relativos a los riesgos.
5.5 Seguimiento del programa de auditoría	
5.6 Revisión y mejora del programa de auditoría	Revisar eficacia de las medidas tomadas para hacer frente a los riesgos asociados al programa: - Riesgos que se han materializado pero que no fueron identificados originalmente. - Riesgos que no se han materializado pero que han sido identificados en el transcurso del desarrollo del programa.

Los riesgos en la ISO 19011:2011

Capítulo 6

Realización de la auditoría

- **6.1 Generalidades.**
- **6.2 Inicio de la auditoría.**
- **6.3 Preparación de las actividades de auditoría.**
- **6.4 Desarrollo de las actividades de auditoría.**
- **6.5 Preparación y distribución del informe.**
- **6.6 Finalización de la auditoría.**
- **6.7 Actividades de seguimiento.**

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
AEC

Realización de la auditoría

Punto de la norma	Aparecen los riesgos
6.1 Desarrollo de la auditoría. Generalidades	
6.2.1 Inicio de la auditoría. Generalidades	
6.2.2 Establecimiento del contacto inicial con el auditado	
6.2.3 Determinación de la viabilidad de la auditoría	Debe generar confianza de que se pueden alcanzar los objetivos de la auditoría, teniendo en cuenta los factores que los pueden poner en peligro.
6.3.1 Revisión de la documentación para preparar la auditoría	
6.3.2 Preparación del plan de auditoría	El responsable del equipo auditor debe evaluar los riesgos que la realización de la auditoría puede generar en la organización.
6.3.3 Asignación de tareas al equipo auditor	
6.3.4 Preparación de los documentos de trabajo	
6.4.1 Realización de las actividades de auditoría. Generalidades	
6.4.2 Realización de la reunión inicial	El responsable del equipo auditor debe exponer al auditado los riesgos identificados que pueden generarse al realizar la auditoría y las medidas adoptadas para paliarlos. Contrastar estos riesgos.
6.4.3 Revisión de documentación durante la auditoría	
6.4.4 Comunicación durante la auditoría	
6.4.5 Asignación de roles y responsabilidades de guías observadores	
6.4.6 Recogida y verificación de información	Se pueden identificar circunstancias que supongan un riesgo inmediato para el auditado. El equipo auditor debe informar al auditado y, en su caso, al cliente de la auditoría.
6.4.7 Generación de hallazgos de auditoría	
6.4.8 Preparación de las conclusiones de auditoría	
6.4.9 Realización de la reunión de cierre	
6.5.1 Preparación del informe de auditoría	
6.5.2 Distribución del informe de auditoría	
6.6 Finalización de la auditoría	
6.7 Realización de actividades de seguimiento de la auditoría	

Competencia y evaluación de los auditores

Punto de la norma	Aparecen los riesgos
7.1 Competencia y evaluación de los auditores. Generalidades	
7.2.1 Determinación de la competencia de los auditores. Generalidades	
7.2.2 Atributos personales	
7.2.3.1 Conocimientos y habilidades. Generalidades	
7.2.3.2 Conocimientos genéricos y habilidades de los auditores de sistemas de gestión	
7.3.3.3 Conocimientos y habilidades de los auditores de sistemas en la disciplina y el sector	
7.2.3.4 Conocimientos y habilidades genéricos de los líderes de equipos auditores	
7.2.3.5 Conocimientos y habilidades para llevar a cabo auditorías de sistemas de gestión en múltiples disciplinas	
7.2.4 Logro de competencia como auditor	
7.2.5 Líderes de los equipos de auditoría	
7.3 Establecimiento de los criterios de evaluación de auditores	
7.4 Selección del método adecuado para la evaluación de auditores	
7.5 Evaluación del auditor	
7.6 Mantenimiento y mejora de la competencia	
Anexo A. Orientaciones y ejemplos sobre habilidades y conocimientos específicos para los auditores	En cada ámbito específico se incluyen elementos necesarios para la cualificación de auditores. Los riesgos se encuentran presentes en todos ellos.
Anexo B. Orientaciones adicionales para la planificación y realización de auditorías	

ASOCIACIÓN AEC

La gestión de riesgos en los sistemas de gestión

Todos los sistemas de gestión tienen relación con la gestión de riesgos:

- O tienen en cuenta los riesgos relacionados con el objeto del sistema
- O se trata de un sistema ideado para gestionar algún tipo de riesgo

Gestión de la calidad (ISO 9001)

Se utiliza para lograr la satisfacción del cliente mediante el cumplimiento de sus requisitos.

La gestión de riesgos se aplica a evitar circunstancias que afecten a la conformidad
- en definición
- en prestación

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
AEC

La gestión de riesgos en los sistemas de gestión

Gestión ambiental (ISO 14001)

Concebido para gestionar un tipo particular de riesgo.

El proceso de gestión establecido por la norma obedece a un proceso de gestión de riesgos……pero no toma necesariamente en cuenta la probabilidad de ocurrencia sino únicamente la gravedad.

Gestión de la prevención de riesgos laborales (OSHAS 18001)

Concebido para gestionar un tipo particular de riesgo.

El proceso de gestión establecido por la norma obedece a un proceso de gestión de riesgos.

La gestión de riesgos en los sistemas de gestión

Gestión de la seguridad de la información (ISO 27001)

Concebido para gestionar un tipo particular de riesgo.

El proceso de gestión establecido por la norma obedece a un proceso de gestión de riesgos.

Gestión de la continuidad del negocio (BSI 25999, UNE 71599)

Concebido para gestionar riesgos de tipo 1.

El proceso de gestión establecido por las normas obedece a un proceso de gestión de riesgos.

Muchas gracias

José Rial

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

AEC