ISO 31004 –Anexo A

FORO DE PRESENTACIÓN ISO 31004 – Guía para la implementación de ISO 31000

Fernando Redondo – Wilis
Inmaculada Ramírez – Willis

Madrid, 11 de Febrero de 2014

AGE(R)S
Asociación Española de Gerencia de Riesgos y Seguros

ESTRUCTURA ANEXO A

AGE(R)S

- A.1 GENERALIDADES
- A.2 RIESGO Y OBJETIVOS
- A.3 INCERTIDUMBRE
- A.4 TRATAMIENTO Y CONTROL DE RIESGOS
- A.5 MARCO DE TRABAJO DE GESTIÓN DEL RIESGO
- A.6 CRITERIOS DEL RIESGO
- A.7 GESTIÓN, GESTIÓN DEL RIESGO Y GESTIONAR EL RIESGO

AGE(R)S

- Términos y conceptos con un significado particular en la ISO 31000 y en ISO 31004, por ejemplo:

***Riesgo* = "*efecto de la incertidumbre sobre la consecución de los objetivos*".**

A.2. RIESGO Y OBJETIVOS & A.3. INCERTIDUMBRE

AGE(R)S

- **Incertidumbre: las organizaciones de todo tipo enfrentan factores e influencias internas y externas que hacen que sea incierto si lograrán o excederán sus objetivos, cuándo y en qué medida.**
  - Cambia con el tiempo.
  - El grado de percepción de la misma es variable entre las distintas partes de la organización.

- **Objetivos: resultados que la organización busca.**
  - Expresión de intención y propósito, metas explícitas e implícitas, valores e imperativos, obligaciones sociales y requisitos legales y de reglamentación.
  - La gestión del riesgo se facilita si los objetivos están expresados en términos mensurables.
  - Con frecuencia hay múltiples objetivos, y la inconsistencia entre ellos puede ser fuente de riesgo.

- **Riesgo: combinación de la posibilidad de un suceso (o peligro o fuente de riesgo) y su consecuencia.**
  - Puede tener consecuencias positivas o negativas: oportunidad Vs amenaza, o ambas al mismo tiempo.
  - Un riesgo se crea o se altera cuando se toman decisiones: la Alta Dirección, como responsable del logro de los objetivos, debe comprender el riesgo en el momento de la toma de decisión y decidir el modo de tratar el mismo.

- **Controles: medidas implementadas por las organizaciones para modificar los riesgos que posibilitan el logro de los objetivos. Los controles pueden modificar el riesgo actuando sobre:**
  - La incertidumbre (probabilidad de materialización del riesgo)
  - El impacto (rango de consecuencias posibles).

- **Tratamiento del riesgo: proceso previsto para cambiar o crear controles, incluyendo la retención del riesgo.**

A.5. MARCO DE TRABAJO DEL RIESGO

AGE(R)S

- **Marco de trabajo de gestión del riesgo: disposiciones (prácticas, procesos, sistemas, recursos y cultura) dentro del sistema de gestión de la organización, que permiten gestionar el riesgo.**
  - Las características de un marco de referencia, y la medida en la que está integrado en el sistema de gestión de la organización, a la larga determinarán la eficacia para gestionar el riesgo.
  - El marco de referencia incluye declaraciones claras de la alta dirección sobre la intención de la organización con respecto a la gestión del riesgo (descritas en la ISO 31000 como mandato y compromiso) y la capacidad necesaria (recursos y capacidad) para cumplir esta intención.
  - Capacidad: comprende numerosos elementos integrados a los procesos globales de gestión de la organización. Pueden ser exclusivos para la tarea de gestionar el riesgo (por ejemplo, un sistema de información especializado), o pueden ser aspectos del sistema de la organización para la gestión (por ejemplo, sus prácticas de recursos humanos).

A.6. CRITERIOS DEL RIESGO & A.7. GESTIÓN, GESTIÓN DEL RIESGO Y GESTIONAR EL RIESGO

AGE(R)S

- Criterios del riesgo: parámetros que permiten describir los riesgos y tomar decisiones acerca de la importancia del riesgo. Es la actitud de la organización frente al riesgo, en función de los criterios se evalúa el riesgo y se selecciona el tratamiento.

- **Gestión: actividades coordinadas que dirigen y controlan una organización en la búsqueda del logro de sus objetivos.**

- **Gestión del riesgo: actividades coordinadas relacionadas con el efecto de la incertidumbre sobre los objetivos. La gestión del riesgo tiene que estar integrada completamente en los sistemas y procesos de gestión de la organización. Es la arquitectura que usan las organizaciones (principios, marco de referencia y proceso) para gestionar el riesgo eficazmente.**

- **Gestionar el riesgo: aplicación de esa arquitectura (gestión del riesgo) a decisiones, actividades y riesgos particulares.**

GESTIÓN DEL RIESGO
ISO 31004 : GUÍA PARA LA IMPLEMENTACIÓN DE LA ISO 31000
ANEXO A (informativo) - CONCEPTOS Y PRINCIPIOS FUNDAMENTALES

AGE(R)S

Asociación Española de
Gerencia de Riesgos y Seguros