Comunidad AEC
CALIDAD

Gestión de Riesgos

Introducción

A partir de la publicación UNE-EN ISO 9001:2015, se introduce el "Pensamiento basado en el riesgo", concepto de "riesgo" que no era considerado en los Sistemas de Gestión de Calidad hasta ese momento. Es un gran avance pues no es meramente la aplicación aislada del concepto del riesgo sino que abarca un concepto más amplio, un concepto de cultura para las organizaciones.

La situación de partida, antes de la publicación de la norma, era la siguiente:

- Concepto "No conformidad potencial" difícil comprender.
- No existe metodología gestión "no conformidades potenciales"
- Sistemas de gestión centrados en la corrección.

Es cierto que el concepto de "riesgo", en el ámbito de calidad, sí era tratado en alguno de los sectores más importantes a nivel industrial desde hace ya tiempo, como los sectores de automoción, aeroespacial, agroalimentario, financiero, etc. En estos sectores el concepto de "riesgo" está contenido también en diversa normativa específica sectorial.

Por ello, ante la nueva situación marcada por la ISO 9001, se sustituye la ´´no conformidad potencial´´ por ´´riesgo´´ y se cuenta con diversas metodologías para la Gestión del Riesgo:

- **COSO.** Es la más utilizada. Edición actual: COSO IV 2017, Gestión del Riesgo empresarial. Integración de la estrategia y el desempeño.
- **OCEG** (Open Compliance and Ethics Group) que lanzó la metodología GRC (Gobierno, Riesgo, Cumplimiento). GRC es un conjunto de capacidades que facilitan a una organización el logro de sus objetivos.
- **ISO 31000...**

Además de los principios para la gestión del riesgo y del marco de trabajo, aporta un proceso para la gestión del riesgo:

- Ámbito, contexto, criterios
- Tratamiento
- Identificación
- Comunicación y consulta
- Análisis
- Reporte y registro
- Evaluación
- Seguimiento y revisión

Normativa de referencia

- UNE- EN ISO 31000:2018 para la Gestión del Riesgo de una manera transversal y global en las organizaciones sea cual sea el tipo de riesgo al que se enfrenta la organización, certificable.
- ISO 22301:2019 sobre continuidad del negocio

Existen otras normas generales y especificas sectoriales.

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Comunidad AEC
CALIDAD

Gestión de Riesgos

1. Concepto de Gestión de Riesgos

Riesgo: Incertidumbre de que ocurra un evento en el futuro y que afecte adversamente a la consecución de los objetivos de la organización.

Factores de riesgo
Condición que favorece que se produzca un evento de riesgo

▼

Evento
Suceso o cambio de circunstancias, inesperado o imprevisto, que genera consecuencias

▼

Consecuencias
Resultados del suceso de un evento que afecta a objetivos de la organización

← Acciones que eliminan o mitigan los factores de riesgo (equivalente a acciones preventivas)

← Acciones que eliminan o mitigan las consecuencias (equivalente a acciones correctivas)

2. Metodologías

Dentro de las diferentes metodologías existentes para la gestión de riesgos, lo importante es cómo las empresas las implantan en sus organizaciones. De todas las aportaciones realizadas por los miembros de la Comisión de Gestión de Calidad pueden distinguirse las siguientes diferencias a la hora de la identificación de los riesgos:

- Gestión de riesgos transversales/organizacionales/corporativos.
- Gestión de riesgos operacionales y riesgos de gestión.
- Gestión de riesgos estratégicos, operacionales y de procesos.
- Gestión de riesgos generales, transversales (por proyectos/programas).
- Gestión de riesgos de contexto y riesgos de procesos.

Se indica lo siguiente:

- Muchas de las empresas poseen su **propia metodología** en la gestión de riesgos, más allá de las tres anteriormente mencionadas (OCEG, COSO e ISO 31000) y, en algunos casos, se utilizan las metodologías que se usan para la identificación de riesgos laborales.
- En algunas organizaciones existe un **Comité** dentro de la organización **para el seguimiento de la gestión de riesgos.** Por lo que se identifica un responsable de la gestión de riesgos por unidad/proceso/área para su reporte al comité.
- Las organizaciones dotan, en función de los riesgos identificados y su impacto, **provisione**s para hacer frente a estos riesgos si se materializan. De igual forma que se dota de esta provisión económica frente a posibles riesgos, hay que valorar económicamente las oportunidades que se deriven de la identificación y gestión de los riesgos.
- Se señala que la identificación de riesgos debe realizarse con un **equipo de personas que formen parte y conozcan suficientemente los diferentes procesos de la empresa**.

- Se recomienda **incluir el concepto de´´ oportunidad´´** en la gestión de riesgos, de forma que se hable de ´´**Gestión de riesgos y oportunidades**´´, reforzando el alineamiento con las normas ISO, que rigen los principales sistemas de gestión y para fortalecer la gestión de oportunidades en las organizaciones.
- Se subraya la importancia de **delimitar claramente los objetivos de la gestión de riesgos y oportunidades** (por ejemplo: calidad del producto o servicio, mantener o aumentar el mercado, seguridad y salud de los trabajadores, continuidad del negocio, seguridad de la infraestructura, seguridad de los productos, inocuidad, etc.).
- Las acciones definidas para tratar los riesgos y oportunidades deberían **alinearse con el plan estratégico de la organización.**

3. Premisas de la implantación de una gestión de riesgos

- La multiplicidad de normas supone una descentralización de su gestión.
- Cumplir una metodología o Norma no debe ser el fin.
- No analizar riesgos sin un diseño previo de los procesos.
- La interiorización de la cultura del riesgo es fundamental para el éxito de la implantación, con la participación de los afectados en grupos de trabajo para su definición, así como su ulterior gestión. La gestión de riesgos debe hacerse desde el punto de vista del conocedor del proceso y la actividad.
- Debe ser inherente al desempeño de la función.
- Debe integrarse en la gestión y alinearse desde el vértice.
- Debe servir para desplegar los objetivos de la organización y su consecución.
- Los riesgos deben materializarse mediante su cuantificación.
- Debe establecerse clasificaciones o niveles de riesgo (al menos, de contexto e internos), sin constituir ´´etiquetas´´, tomando como referencia metodologías existentes.

- Debe implantarse progresivamente mediante proyectos piloto.

4. Fuentes de riesgos generales aplicables a cualquier sistema de gestión y con estructura común de acuerdo al Anexo SL.

Las fuentes de riesgos generales aplicables a cualquier sistema de gestión con base en ISO y con estructura de acuerdo al Anexo SL (estructura de Alto Nivel para todos los sistemas de gestión de las Normas ISO) pueden ser, entre otras, las siguientes:

- Contexto de la organización:
  - Debilidades y/o amenazas identificadas en la comprensión de la organización y su contexto.
  - Incumplimiento de requisitos y expectativas de partes interesadas.
  - Incumplimiento de requisitos legales o reglamentarios aplicables.
- Incumplimiento de los objetivos del sistema de gestión o de los procesos.
- Falta, ausencia, debilidad de liderazgo y compromiso.
- Fallas en la planificación o en el cumplimiento del ciclo de la mejora continua.
- Metodología seleccionada para la gestión de riesgos y oportunidades; por ejemplo: excesivamente compleja o débil, no alineada con el objetivo de la gestión de riesgos y oportunidades.
- Subjetividad de los procesos de evaluación de competencias del personal.
- Falta de sensibilización, conciencia, motivación, etc., del personal.
- Falla o debilidad en los procesos de comunicación.
- Desactualización de la información documentada.
- Falla o debilidad en la gestión de los cambios.
- Subjetividad en los procesos de evaluación de proveedores.

- Auditorías internas: riesgos por no independencia de auditores, tiempos planificados, redacción de no conformidades, etc. Oportunidades para desarrollo de competencias, optimización de recursos, etc...

A continuación, se muestra un **listado de posibles acciones o de acciones más comunes o típicas que pueden tomarse para tratar riesgos y oportunidades**, por ejemplo:

Riesgos:

- **Evitar:** no permitir que ocurra, renunciar a la actividad que se ve afectada o que puede generar el riesgo. Esta decisión puede tomarse ante riesgos inaceptables y cuyas consecuencias supondrían un grave peligro.
- **Asumir:** después de la evaluación, se considera que el riesgo no es lo suficientemente importante o que el tratamiento puede resultar excesivamente costoso en relación a la mejora que aportaría. En estos casos la acción sería:
  - **Asumir y aceptar:** no tomar acciones
  - **Asumir y mitigar:** corregir una vez ocurrido
  - **Eliminar la fuente que genera el riesgo:** eliminar la causa o evitar que se produzca la causa que da lugar al efecto no deseado
  - **Reducir:** Cambiar la probabilidad o las consecuencias
  - **Compartir el riesgo:** transferir a otro responsable que pueda manejar las consecuencias.

Oportunidades:

- **Innovar:** nuevos productos o servicios, estrategias comerciales novedosas, nuevos mercados o líneas de negocio, etc.
- **Cambiar:** actualización de tecnologías, reestructuración o automatización de procesos, etc.
- **Mejorar:** reingeniería de procesos, desarrollo de competencias del personal, desarrollo de proveedores, etc.

5. Los principales beneficios de la implantación de la gestión de riesgos.

Las fuentes de riesgos generales aplicables a cualquier sistema de gestión con base en ISO y con estructura de acuerdo al anexo SL pueden ser, entre otras, las siguientes:

- Buscar la **mejora**, identificando aspectos de la organizacion que no funcionan o van mal, asegurando el negocio.
- Convertir el análisis de riesgos en **oportunidades** de negocio.
- Analizar problemas **cuantificándolos**.
- Analizar **posibles ventajas**.
- Conseguir **objetivos ambiciosos**.
- Evitar objetivos **inasumibles**.
- Servir para una **correcta toma de decisiones**, disminuyendo fallos e incrementando las posibilidades de éxito.
- Los **riesgos** deben **cuantificarse** hasta donde se pueda llegar (provisiones/reservas de eficacia de la gestión, etc.). La matriz de riesgos debe tener asignado un presupuesto.