MODUM
Gestión orientada a Resultados

Gestión de Riesgos
Un aporte práctico

John Miles

SERIE ESTRATEGIA

Gestión de Riesgos
Un aporte práctico

John Miles PhD

Gestión de Riesgos. Un aporte práctico

Por John Miles

Modum Srl.
Rincón 454
Email: contacto@modum.com.uy
www.modum.com-uy
Montevideo – Uruguay.

Contenido

PENSAMIENTO BASADO EN RIESGOS

Las normas ISO 31000 e ISO 9001:2015 define al riesgo como el "*efecto de la incerti*dumbre" sobre los objetivos, considerando que un efecto es una desviación respecto de un resultado esperado, sea positivo, negativo o ambos; y también que los objetivos pueden tener aspectos diferentes (por ejemplo: financieros, salud y seguridad, ambientales, calidad, etc.) y se pueden aplicar en niveles diferentes (estratégico, en toda la organización, en proyectos específicos, en productos o servicios o en procesos).

El riesgo está caracterizado por la referencia a eventos potenciales y a las consecuencias que pueden producir o una combinación de ambos. O sea, un riesgo se expresa en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y de la posibilidad de que suceda.

Todos los riesgos relacionados con la calidad, la seguridad, las finanzas, lo comercial o el medio ambiente etc., pueden ser tratados bajo un solo aspecto 'multidisciplinario' del sistema de gestión. La organización tiene que analizar su contexto y determinar los riesgos que deben abordarse para lograr los resultados planificado y prevenir y/o mitigar los efectos no deseados. En consecuencia, el pensamiento basado en riesgos es esencial para lograr un sistema de gestión eficaz enfocado en la prevención y la mejora continua.

CLASES DE RIESGOS

Las categorías de riesgos deben adaptarse en función de las características de cada organización. Sin embargo, tradicionalmente se distinguen entre riesgos de un nivel estratégico, que desarrollan una influencia a mediano y largo plazo en los objetivos de la organización, y los riesgos operacionales, que afectan la operación rutinaria y del día a día.

ALGUNOS EJEMPLOS DE FACTORES DE RIESGOS ESTRATÉGICOS

Riesgos políticos	Riesgos relacionados con los aspectos políticos / gubernamentales que pueden afectar a la organización en el desarrollo de su misión. Cambios de gobierno, de políticas públicas, de acuerdos internacionales.
Riesgos económicos	Riesgos relacionados con aspectos de la economía nacional, regional o mundial: factores como la macroeconomía, la política cambiaria, monetaria o fiscal, inflación, etc. Son riesgos del entorno que comprometen a la organización para responder a sus compromisos económico-financieros.
Riesgos sociales	Riesgos relacionados con los cambios demográficos, urbanísticos o socioeconómicos que afectan a la organización en el desarrollo de su misión.
Riesgos tecnológicos	Riesgos relacionados con la incapacidad de la organización para adaptarse al ritmo evolutivo, para adquirir, incorporar y utilizar las últimas

	tecnologías, o para responder a una nueva demanda generada por un importante cambio tecnológico.
Riesgos legislativos	Riesgos relacionados con cambios importantes en la legislación o en las normas aplicadas al campo de actividad de la organización (legislación sobre las condiciones de trabajo, legislación sobre protección de datos, legislación contra la discriminación...).
Riesgos medioambientales	Riesgos relacionados con las consecuencias que tiene para el medio ambiente la realización de los objetivos estratégicos de la organización (riesgos relacionados con la eficiencia energética, la contaminación, el reciclaje, el enterramiento de residuos...)
Riesgos asociados a los clientes	Riesgos relacionados con la incapacidad de la organización para responder a las expectativas y nuevas necesidades de sus clientes.

ALGUNOS EJEMPLOS DE RIESGOS FACTORES OPERACIONALES

Riesgo Estratégico	Riesgos asociados con la capacidad de comprender el contexto y desarrollar estrategias adecuadas. La clara definición de políticas, de la propuesta de valor, del diseño y conceptualización de la organización y sus procesos por parte de la alta dirección.
Riesgos de la actividad	Riesgos concretos del sector de actividad de la organización (riesgos sanitarios y clínicos dentro del sector de la salud; riesgos relacionados con el bienestar de los residentes en el sector del alojamiento, riesgos con la inocuidad de alimentos en la industria alimenticia, ...).
Riesgos de cumplimiento	Se asocian con la capacidad de la organización para cumplir con los requisitos legales, reglamentarios, contractuales, de ética y en general con su compromiso ante la comunidad.
Riesgos financieros	Riesgos relacionados con la planificación y el control financiero, con la gestión presupuestal, la elaboración de los estados financieros, las cobranzas y los pagos, la financiación de proyectos, el capital de trabajo, la cobertura de seguro, etc.
Riesgos de seguridad	Riesgos que atañen a la salud y seguridad de las personas y los bienes de la organización (incendio; accidentes laborales; fallos en el equipamiento...).
Riesgos contractuales	Riesgos relacionados con la incapacidad de las partes contratantes para entregar los productos /servicios en las condiciones técnicas y con los precios acordados.
Riesgos de reputación	Riesgos relacionados con la reputación de la organización y la percepción que tienen los clientes y el público en general de su calidad y comportamiento ético. Están relacionados con la percepción y la confianza por parte de los clientes, proveedores, socios y la sociedad en general hacia la organización.
Riesgos Operativos	Comprenden riesgos provenientes del funcionamiento y de las operaciones de la organización, de los sistemas de información, de la definición y ejecución de los procesos, de la estructura, de la articulación entre las distintas áreas o sectores.
Riesgos tecnológicos	Riesgos relacionados con la disfunción u obsolescencia del equipamiento tecnológico (IT; equipamientos...). Están relacionados con la capacidad tecnológica de la organización para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión

Riesgos medioambientales	Riesgos relacionados con la contaminación, el ruido, la eficiencia energética, etc. de las operaciones en curso de la organización

Como se establece en la ISO 9001:2015: *una organización necesita planificar e implementar acciones para abordar los riesgos y las oportunidades. Abordar tanto los riesgos como las oportunidades establece una base para aumentar la eficacia del sistema de gestión, alcanzar mejores resultados y prevenir los efectos negativos.*

Las oportunidades pueden surgir como resultado de una situación favorable para lograr un resultado previsto, por ejemplo, un conjunto de circunstancias que permita a la organización atraer clientes, desarrollar nuevos productos y servicios, reducir los residuos o mejorar la productividad.

Al desarrollar su sistema de gestión, la organización debe:

- Identificar los riesgos y oportunidades para cumplir con los requisitos exigidos para asegurar que el sistema de gestión pueda lograr los resultados previstos y que la organización pueda lograr de manera consistente la conformidad de los bienes y servicios, la satisfacción del cliente y de las otras partes interesadas. Mediante la evaluación de riesgos también se pretende prevenir, o reducir, los efectos no deseados, y lograr la mejora continua.
- Planificar, integrar y poner en práctica las acciones en los procesos del sistema para hacer frente a estos riesgos y oportunidades, y evaluar la eficacia de estas acciones.
- Revisar periódicamente el sistema para garantizar que los procesos de gestión de riesgos siguen siendo pertinentes y eficaces. Los factores que afectan a la probabilidad y las consecuencias de un evento pueden cambiar, al igual que los factores que afectan a la idoneidad de las opciones de tratamiento. El control de los procesos debe proporcionar información acerca de la eficacia del proceso de gestión de riesgos.

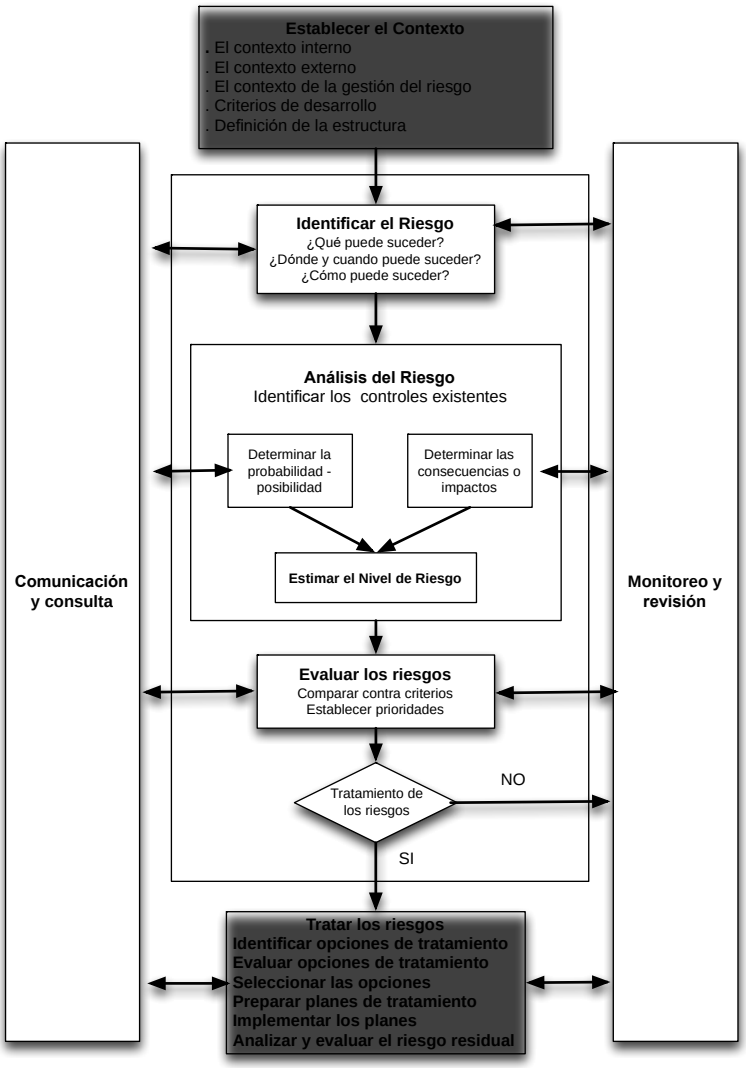
El riesgo se caracteriza a menudo por referencia a los "eventos" potenciales (con una probabilidad de ocurrencia) y "consecuencias" (impactos) o una combinación de ambos. En consecuencia, las medidas adoptadas para hacer frente a los riesgos y las oportunidades serán proporcionales a los impactos potenciales sobre la conformidad de los bienes y servicios, sobre la satisfacción del cliente y otras partes interesadas y se tomarán en función de la probabilidad de ocurrencia.

La adopción de pensamiento basado en el riesgo, con el tiempo, mejora la confianza de los clientes y su satisfacción al asegurar la consistencia de la calidad de los bienes y servicios producida por el desarrollo de una cultura proactiva de prevención y de mejora.

Es recomendable elaborar un procedimiento específico donde se explicite y especifique los criterios y conceptos de la evaluación de los riesgos que aplican a la organización, no solo los de calidad sino incluyendo otros aspectos como seguridad, ambientales, financieros, etc.

La ISO 9001:2015 no especifica ninguna herramienta para el análisis y la gestión de riesgo. Sin embargo, la norma ISO 31000 es una buena guía metodológica a efectos de la gestión de riesgos.

El esquema general de gestión de riesgo planteado por la ISO 31000 se representa en la siguiente figura:



Podemos asumir que la norma ISO 31000 plantea la gestión de riesgos desarrollada en cuatro grandes fases:

1. Definición del contexto.
2. Identificación, análisis y evaluación de los riesgos.
3. Tratamiento de los riesgos.
4. Monitoreo y verificación de efectividad de las acciones.

Veamos que implica cada una de estas fases.

1. ESTABLECIMIENTO DEL CONTEXTO

El análisis del contexto busca contestar la pregunta ¿qué factores externos e internos pueden generar riesgos y que por lo tanto atenten contra el cumplimiento de los objetivos de la organización? La definición del contexto consiste en determinar los parámetros fundamentales y el entorno de la organización en los que debe integrarse la gestión de riesgos. Se trata de analizar a la vez el entorno interno (cultura, protagonistas, recursos, procesos, objetivos) y el externo (económico, social, reglamentario, los factores y las tendencias que tienen un impacto sobre los objetivos de la organización, los criterios de apreciación de riesgos por las partes implicadas, etc.). Esta etapa debe encararse al mismo tiempo que se considera el contexto para la norma ISO 9001:2015 o las otras aplicables (14001, 18001…) con el objetivo de "*determinar las cuestiones externas e internas que son pertinentes para su propósito y su dirección estratégica y que afectan a su capacidad para lograr los resultados previstos en el sistema de gestión*".

La finalidad de esta etapa es determinar:

1. Las condiciones o factores internos y externos que puedan generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y estrategia de la organización. Es importante identificar las necesidades y expectativas de los clientes y otras partes interesadas que la organización se plantea satisfacer y los posibles factores (internos o externos) que podría comprometer esta misión.
2. Los diferentes criterios que se utilizarán para evaluar la importancia del riesgo (criterios financieros, de reputación, relacionados con la seguridad y la salud del personal y/o de los involucrados, etc.) así como el método y la escala para definir su verosimilitud (probabilidad de ocurrencia) y la gravedad de sus impactos. Los criterios deben reflejar los valores de la organización, sus objetivos y recursos. Algunos criterios pueden ser impuestos o derivarse de los requisitos legales, reglamentarios u otros a los que la organización suscriba.
   Al definir los criterios de riesgo se deben considerar los siguientes aspectos:
   - La naturaleza y los tipos de causas y consecuencias que pueden ocurrir y cómo se miden.
   - Las escalas para determinar los niveles de gravedad y probabilidad.
   - Los niveles de riesgo de acuerdo con gravedad y probabilidad.
   - El nivel en que un riesgo se convierte en aceptable o tolerable.
   - Las combinaciones de los múltiples riesgos que deben tenerse en cuenta para evaluarlos.
3. El alcance, los objetivos, las responsabilidades y los recursos del proceso de gestión de riesgos. La gestión de riesgos no es una actividad puntual, es un proceso estratégico de la organización, y como tal debe ser gestionado.

2. IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN DE LOS RIESGOS

El segundo paso es la identificación, análisis y evaluación de los riesgos pertinentes para la organización definidos como "el efecto de la incertidumbre sobre la consecución de objetivos", y verificar si están o no controlados. Esta etapa busca contestar las siguientes preguntas:

1. ¿qué podría salir mal?
2. ¿cuál es la probabilidad (posibilidad) de que salga mal?
3. ¿cuáles son las consecuencias (gravedad)?

A) IDENTIFICACIÓN DE LOS RIESGOS:

Identificar todos los posibles eventos o situaciones que pueden evitar el cumplimiento de los objetivos de los procesos, de las actividades o de las personas y, en consecuencia, de los objetivos de la organización.

Se busca responder las preguntas:

- ¿qué es lo que puede ocurrir? ¿qué puede salir mal?
- ¿dónde y cuándo puede suceder?
- ¿cómo puede ocurrir?
- ¿cuáles son las consecuencias?

Se debe identificar las fuentes de riesgo, los posibles eventos o acontecimientos (incluyendo los cambios en las circunstancias) sus causas, las zonas/lugares de impactos y las potenciales consecuencias.

El objetivo de este paso es generar una lista exhaustiva de los riesgos basados en los acontecimientos o eventos que puedan crear, mejorar, prevenir, degradar, acelerar o retrasar el logro de los objetivos. La identificación completa es fundamental porque el riesgo que no se identifica en esta etapa no será incluido en el análisis posterior.

Esta etapa puede desarrollarse en tres fases:

1. En un primer momento, es necesario realizar una lista del conjunto **factores** de riesgos internos (organización, empleados, proyectos, etc.) y externos (clientes, empresas, medio ambiente, situación política, etc.).
2. A continuación, se identifican, para cada uno de los factores, los eventos que generan riesgos y sus posibles **consecuencias** para la organización.
3. Identificar los **controles** que existen para reducir o mitigar los efectos del riesgo.

Es conveniente documentar la relación completa de riesgos identificados. Del mismo modo, también es importante identificar, si existen, los controles asociados a cada riesgo y su eficacia.

Al identificar los riesgos se debe tener en cuenta:

- Fuente: aquello que tiene potencial intrínseco para hacer daño o generar oportunidades. Una fuente de riesgo puede ser tangible o intangible.
- Evento: aquello que ocurre, de manera que la fuente de riesgo genera un impacto en la organización. Un evento a veces puede ser contemplado como un "incidente" o "accidente".

- Consecuencia: el resultado o impacto sobre un grupo de partes interesadas, recursos o actividad de la organización.
- Causa: lo que genera el evento que tiene impacto en la organización.
- Controles: los controles establecidos para prevenir un evento o mitigar una consecuencia.
- Cuando/ dónde: puede ocurrir el riesgo

La identificación de los riesgos es la etapa más laboriosa ya que se debe incluir la totalidad de posibles riesgos de la organización, abarcando cada uno de sus procesos. Por eso este es un trabajo a medida de cada organización; podrá haber pautas generales pero la determinación de los riesgos y sus consecuencias es específica de cada organización.

Importante: Para identificar los riesgos en los procesos es conveniente conformar equipos de "análisis de riesgos", constituidos por personas de distinto nivel y disciplinas, con experiencia en el proceso analizado, con el propósito de aprovechar el conocimiento colectivo del grupo y desarrollar con ellos la lista de acontecimientos relacionados.

b) Análisis de riesgo

El análisis de riesgo aspira comprender cómo se desarrolla el riesgo. Determinar sus causas raíz, así como a qué y a quién afecta, con qué intensidad y consecuencias.

Para analizar el riesgo identificado existen numerosos modelos y herramientas, como la tormenta de ideas, el análisis de peligros y puntos críticos de control (ACCPP), análisis de causa y efecto (Ishikawa) el análisis de Pareto, o el análisis modal de fallos y efectos (AMFE). Además, cuando se analiza el riesgo con un enfoque estratégico se puede utilizar el análisis de fortalezas, debilidades, amenazas y oportunidades (FODA) o las 5 fuerzas de Porter. Debemos escoger aquel modelo o herramienta que se adapte mejor a las necesidades de la organización. La norma ISO 31000 presenta un listado de algunos modelos útiles.

Una vez identificados y analizados los riesgos, debe estimarse la probabilidad de que realmente se materialicen y cuáles serían las posibles consecuencias. Esto orientará la clasificación del riesgo, con el fin de obtener información para establecer el nivel de riesgo y las acciones que deberían implementarse.

c) Valoración del riesgo

El propósito de la valoración de los riesgos es ayudar en la toma de decisiones sobre cuáles son los que necesitan ser tratados, con qué prioridad y las estrategias y métodos más adecuados para el tratamiento. La evaluación de riesgos tiene como objetivo determinar las prioridades y los recursos que deberán movilizarse en función de los diferentes niveles de riesgo.

El nivel de cada riesgo se mide generalmente en función de la probabilidad de que ocurra y de la gravedad de su consecuencia; las cuales se establecen con la ayuda de escalas determinadas en el momento de definir el contexto. Los niveles de riesgo se establecen

gracias a los criterios de aceptabilidad previamente definidos, tales como niveles de control; nivel u origen del impacto; objetivos políticos...

El valor del riesgo resultará de multiplicar la "probabilidad" por la "consecuencia o impacto", acorde a la siguiente formula:

R = P x I (riesgo =probabilidad x Impacto)

Para esta valoración, podemos tomar las siguientes definiciones, que se establecen durante el análisis del contexto:

PROBABILIDAD O FRECUENCIA DE OCURRENCIA

Por probabilidad se entiende la posibilidad de ocurrencia del riesgo, que puede ser medida con criterios de frecuencia, si el riesgo se ha materializado (número de veces en un tiempo determinado), o de factibilidad, teniendo en cuenta la presencia de factores externos o internos que pueden propiciar el riesgo, aunque éste no se haya materializado.

Nivel Probabilidad	Probabilidad /factibilidad	Ocurrencia /frecuencia	Comentario
1	Muy baja /raro	Remota	Excepcionalmente puede ocurrir. Poco común o frecuente.
2	Baja /improbable	Aislada	Es raro o difícil que suceda. No hay buenas razones para creer que sucederá.
3	Moderada/ posible	Ocasional	Es posible que ocurra unas pocas veces. Este evento sucede en forma esporádica.
4	Alta / probable	Recurrente	Muy probable, se repite con periodicidad. Este evento sucederá algunas veces. Hay buenas razones para creer que sucederá.
5	Muy alta / casi seguro	Frecuente	Ocurre seguro, con regularidad. Este evento está previsto que se produzca en la mayoría de las circunstancias.

IMPACTO O SEVERIDAD O CONSECUENCIA

Por impacto se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Impacto	Valor	Descripción	Descripción
1	Muy baja	Insignificante / marginal	Si el hecho llegara a presentarse tendría consecuencias o efectos mínimos sobre la organización.
2	Baja	Pequeño /menor	Si el hecho llega a presentarse tendrá un bajo impacto sobre la organización.
3	Moderada	Moderado	Si el hecho llega a presentarse tendrá medianas consecuencias o efectos sobre la organización.
4	Alta	Mayor /grave	Si el hecho llega a presentarse tendrá altas consecuencias o efectos sobre la organización.
5	Muy Alta	Catastrófico	Si el hecho llega a presentarse tendría desastrosas consecuencias o efectos sobre la organización.

MATRIZ DE RIESGO

La matriz de riesgo es una herramienta que permite clasificar y visualizar los riesgos mediante la combinación del impacto y de su probabilidad de ocurrencia. Los riesgos jerarquizados permiten establecer el orden de atención para las medidas de prevención, protección y control a adoptar.

A partir de las definiciones de los grados de probabilidad e impacto elaboramos la matriz de riesgos:

Probabilidad	**Impacto**				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Casi seguro (5)	5	10	15	20	25
Probable (4)	4	8	12	16	20
Posible (3)	3	6	9	12	15
Improbable (2)	2	4	6	8	10
Raro (1)	1	2	3	4	5

Al valorar cada uno de los riesgos se los puede ubicar en la matiz de riesgos. A partir de su ubicación, podemos clasificarlos en función de su gravedad. Se puede utilizar el siguiente criterio para la clasificación:

Tipo de riesgo	Nivel de riesgo	Probabilidad x impacto
A	Riesgo muy alto	15 - 25
B	Riesgo alto	9-14
C	Riesgo medio	4-8
D	Riesgo bajo	1-3

DESCRIPCIÓN DE LOS NIVELES DE RIESGO

Riesgo Muy Alto, Intolerable o Inadmisible (tipo A): el riesgo requiere de una acción inmediata, de la suspensión de la actividad hasta tanto no pueda ser controlado. El costo no debe ser una limitación y el no hacer nada no es una opción aceptable. Un riesgo de tipo A representa una situación de emergencia y deben establecerse controles temporales inmediatos. La mitigación debe hacerse por medio de controles de ingeniería y/o por factores humanos hasta reducirlo a uno tipo C o preferentemente de tipo D en un periodo breve de tiempo, por ejemplo, inferior a 60 días (este período debe establecerse en función del contexto de la organización). En caso de que se requiera correr este riesgo deberá ser con la autorización la más alta autoridad de la organización.

Riesgo Alto, Indeseable o Inaceptable (tipo B): el riesgo debe ser reducido y hay margen para investigar y analizar con más detalle. No obstante, la acción correctiva debe darse en los primeros 60 días (este período debe establecerse en función del contexto de la organización). Si la situación se demora más tiempo deben establecerse controles temporales inmediatos para reducir el riesgo. Son riesgos que se podrían "correr" con un adecuado aseguramiento de los controles y bajo la autorización y supervisión de la dirección de la organización.

Riesgo Medio, Tolerable, o Aceptable con controles (tipo C): el riesgo es significativo, pero se pueden acompañar las acciones correctivas con el paro de las actividades programadas; no requiere la suspensión inmediata de la actividad. Los medios de solución para atender los hallazgos deben darse en los próximos 18 meses (este período debe establecerse en función del contexto de la organización). La mitigación debe enfocarse en la disciplina operativa y en la confiabilidad de los sistemas de protección. Son riesgos que se podrían "correr" con un adecuado aseguramiento de los controles y bajo la autorización y supervisión, por ejemplo, del responsable del área.

Riesgo Bajo, Admisible razonablemente aceptable (tipo D): el riesgo requiere de acción, pero es de bajo impacto y puede programarse su atención y reducción juntamente con otras mejoras operativas. No debe ser intervenido, pues se considera un “riesgo seguro” ó “normal” para que una organización pueda lograr sus objetivos estratégicos. Deben continuarse con los controles existentes.

D) ANÁLISIS DE LOS CONTROLES EXISTENTES

En general las organizaciones implementan controles para reducir o mitigar los riesgos. Al valorar los riesgos hay que analizar la probabilidad e impacto cuando los controles actuales se están ejecutando, para saber si es necesario encarar acciones adicionales. Los controles, al igual que las acciones que se implementan para el tratamiento del riesgo, pueden clasificarse en:

- Preventivos: aquellos que actúan para eliminar las causas del riesgo, para prevenir su ocurrencia o materialización.
- Correctivos: aquellos que permiten el restablecimiento de la actividad después de ser detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia.

En el análisis de riesgo se deben incluir las siguientes actividades vinculadas a los controles:

1. Identificar los controles existentes: esto es, las practicas ó dispositivos existentes que puedan actuar para minimizar el riesgo bajo análisis. Se deberá considerar la totalidad de los controles existentes que actúan sobre el asunto de riesgo que se está considerando. Algunos ejemplos de control son:

Controles de gestión	Políticas claras aplicadas
	Seguimiento de planes estratégicos y operativos
	Indicadores de gestión – Cuadros de Mandos
	Seguimiento de cronogramas
	Evaluaciones de desempeño
	Informes de gestión
	Revisiones de la dirección
	Monitoreo de riesgos
Controles operativos	Verificación de firmas
	Listas de chequeos
	Registros controlados
	Segregación de funciones
	Niveles de autorización
	Procedimientos formales y documentados aplicados
	Sistemas y equipos de seguridad personal
	Personal capacitado
	Aseguramiento de calidad
	Supervisión definida
Controles legales	Normas claras y aplicadas
	Códigos de ética
	Seguimiento de la legislación aplicable

2. Calificar la efectividad e implementación del conjunto de controles actuales. Establecer el nivel de eficacia de los controles actuales. Los mismos pueden estar ejecutándose en forma óptima o ser totalmente inservibles para reducir o mitigar el riesgo.

   Se puede utilizar la tabla siguiente para calificar el grado de control actual:

Calificación	Estado de control
Fuerte	Se han aplicado todos los controles económicos factibles acorde a las mejores prácticas de la industria. Las políticas y los procedimientos están establecidos y documentados. EL control es revisado continuamente, Nada más que hacer excepto revisar y monitorear los controle existentes.
Moderado	Hay establecidos programas y procedimientos. Los controles implantados son insuficientes para prevenir o mitigar el riesgo. El control actual no es muy efectivo o algunos de los controles no aparecen bien diseñados en cuanto a que no atacan la causa raíz.
Débil	Acciones informales con procedimientos escasos o no sistemáticos. Se desconoce el riesgo o la necesidad de controles asociados.
Incontrolables	Fuera de control de la organización

3. Determinar que desplazamiento en la matriz de riesgo produce la aplicación de los controles existentes. Esto es, analizar el nivel de riesgo al que queda expuesto el proceso luego de que se aplican los controles que tiene en marcha la organización y que están actuando sobre la posibilidad de ocurrencia o sobre el impacto. Esto permitirá tener la posición de partida para evaluar si es necesario implementar acciones adicionales.

En consecuencia, el riesgo se analiza mediante la combinación de estimaciones de probabilidad y las consecuencias de que el evento ocurra, en el contexto de las medidas de control existentes para ese evento.

E) Evaluación de riesgo desde las perspectivas

Los riesgos pueden afectar de forma diferente a distintas dimensiones o perspectivas de la organización. Por eso, es conveniente analizar el impacto que tiene cada riesgo en cada una de las perspectivas relevantes para la organización. Estas perspectivas estarán definidas durante la fase de análisis del contexto y pueden ser:

Perspectiva	Posible impacto
Financiera	Pérdida o ganancia económica
Clientes	Afectación en el cliente, actuales y potenciales
Procesos	Influencia del riesgo en los procesos de la empresa
Personal	Impacto en la capacitación, aprendizaje, crecimiento, seguridad o salud y rotación del personal

Proveedores	Impacto en los proveedores y socios de negocio
Sociedad	Impacto en la sociedad en general
Otras partes interesadas	Afectación a las partes interesadas
Producto / servicio	Afectación de la calidad / precio /entrega del producto / servicio
Medio ambiente	Impacto en el medio ambiente

Por lo tanto, deberemos primero identificar cada uno de los riesgos de la empresa y, posteriormente, de forma individualizada evaluar la probabilidad que ocurra un riesgo y el impacto en cada perspectiva. Esto permitirá tomar acciones más focalizadas y eficaces.

Puede ser difícil lograr un entendimiento compartido de la aplicación de la gestión de riesgos entre las distintas partes interesadas ya que cada interesado puede percibir diferentes daños potenciales, colocar una probabilidad diferente en cada daño que se produzca y atribuir distintos niveles de gravedad a cada daño.

3. TRATAMIENTO DEL RIESGO

Luego de realizada la evaluación, se deben definir las acciones que se tomarán para responder a los riesgos que se han identificado y ponderado, integrándolas en los procesos del sistema de gestión. El tratamiento del riesgo es el proceso que se realiza para modificar el riesgo llevándolo a un nivel aceptable. La cantidad de esfuerzo utilizada en el tratamiento de riesgos debe ser proporcional a la importancia del riesgo.

Esta fase implica la identificación y evaluación de las opciones existentes para tratar los riesgos considerados como prioritarios. También es en esta fase cuando se determinan y ponen en marcha los planes de acción correspondientes. Como punto de partida deberá tenerse claro que tan solo se gestionará aquella porción de riesgos que este por fuera del rango de aceptabilidad definido en la etapa de análisis del contexto.

En función de la valoración del riesgo se tomarán acciones que buscan eliminar la fuente de riesgo, en caso de que sea posible, o sino disminuir la "posibilidad" del riesgo (medidas de prevención) o disminuir las "consecuencias" del riesgo (medidas de protección), o una combinación de ambas.

En definitiva, el tratamiento del riesgo puede centrarse en las siguientes preguntas:

1. ¿El riesgo está por encima del nivel aceptable?
2. ¿Qué se puede hacer para reducir o eliminar el riesgo?
3. ¿Cuál es el equilibrio adecuado entre los beneficios, riesgos y recursos?
4. ¿Se introducen nuevos riesgos como consecuencia de las acciones que se implementen para tratar el riesgo?
5. ¿Cuál es el plan de acción para tratar el riesgo?

La selección de la opción de tratamiento de riesgo más adecuada consiste en equilibrar los costos y los esfuerzos de la implementación con los beneficios esperados y en función a los requisitos legales, reglamentarios y otros como la responsabilidad social y la protección del medio ambiente.

Diferentes formas de tratar los riesgos pueden ser:

Tipo de tratamiento	Descripción
Evitar ó eliminar el riesgo	Tomar medidas encaminadas a prevenir la materialización del riesgo. Consiste en decidir no realizar la actividad que probablemente genera el riesgo. Evitar el riesgo no iniciando o continuando con la actividad. Evitar supone salir de las actividades que generen riesgos, puede incluir acciones como: • Retirar la fuente de riesgo. • Prescindir de una unidad de negocio, línea de producto o segmento geográfico. • Decidir no emprender nuevas iniciativas/ actividades que podrían dar lugar a riesgos. • Cambios sustanciales en los procesos por mejoramiento, rediseño o eliminación de actividades (utilización de distintos insumos o materias primas, cambio de tecnología, eliminación de etapas). Debe ser siempre la primera alternativa a considerar, aunque no siempre es posible.
Reducción del riesgo	Implica llevar a cabo acciones para reducir la probabilidad (medidas de prevención) o el impacto (medidas de protección) del riesgo o ambos conceptos a la vez. • Eliminando la causa raíz que produce el riesgo. • Modificando (minimizando) su probabilidad de ocurrencia. • Actuando sobre las consecuencias del correspondiente riesgo. • Optimizando procedimientos o implementando controles. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles.

Compartir o transferir el riesgo	La probabilidad o el impacto del riesgo se reduce trasladando o compartiendo el riesgo para que otras partes soporten una porción de este. • Compartiendo las consecuencias del riesgo con otras partes o departamentos de la organización. • Adoptar seguros contra perdidas inesperadas y significativas. • Entrar en sociedad compartida (joint venture). Establecer acuerdos con otras empresas. • Establecer contratos de servicio, producción ó maquila con terceros. • Protegerse contra los riesgos utilizando instrumentos de mercado de capital. • Tercerizar procesos de negocio. • Descentralizar el almacenamiento de la información vital para la empresa. En este caso hay que pensar en qué nuevos riesgos ocasiona este cambio.
Aceptar o asumir	Aceptar el riesgo inherente, pero conociéndolo. Consiste en retener el riesgo dentro de la organización para perseguir una oportunidad y establecer un plan apropiado de mitigación del riesgo. • Provisionar las posibles pérdidas. • Confiar en las compensaciones naturales existentes dentro de un portafolio. • Aceptar el riesgo si se adapta a la tolerancia al riesgo existente.
Prevención	Consiste en cambiar (reducir) la probabilidad de ocurrencia del riesgo. Esto puede incluir acciones como: • Programas de auditorías y cumplimiento. • Revisiones formales de requerimientos, especificaciones, diseño de ingeniería y operaciones. • Controles de inspección y de procesos. • Verificaciones y pruebas. • Mantenimiento preventivo. • Aseguramiento de la calidad, administración y estándares. • Establecer límites operacionales. • Entrenamiento estructurado.
Protección	Consiste en cambiar (reducir) la gravedad de las consecuencias. Esto podría incluir acciones tales como: 1) Características del diseño. 2) Barreras de ingeniería y estructurales. 3) Planeamiento de control de fraudes. 4) Equipos de protección personal. 5) Minimización la exposición a fuentes de riesgo.

La selección de la acción a implementar implica equilibrar los costos y los esfuerzos para su implementación, así como los beneficios finales. Por lo tanto, se deben considerar aspectos de viabilidad como: técnicos, legales, institucionales, financieros, costos-beneficios.

Es muy probable que, una vez tratado el riesgo, continúe existiendo una probabilidad residual de ocurrencia de este. En general, el riesgo residual resultante, será entendido y aceptado por las correspondientes partes interesadas que estén afectadas por el mismo. El nivel de riesgo residual aceptable debe definirse en la fase de análisis del contexto.

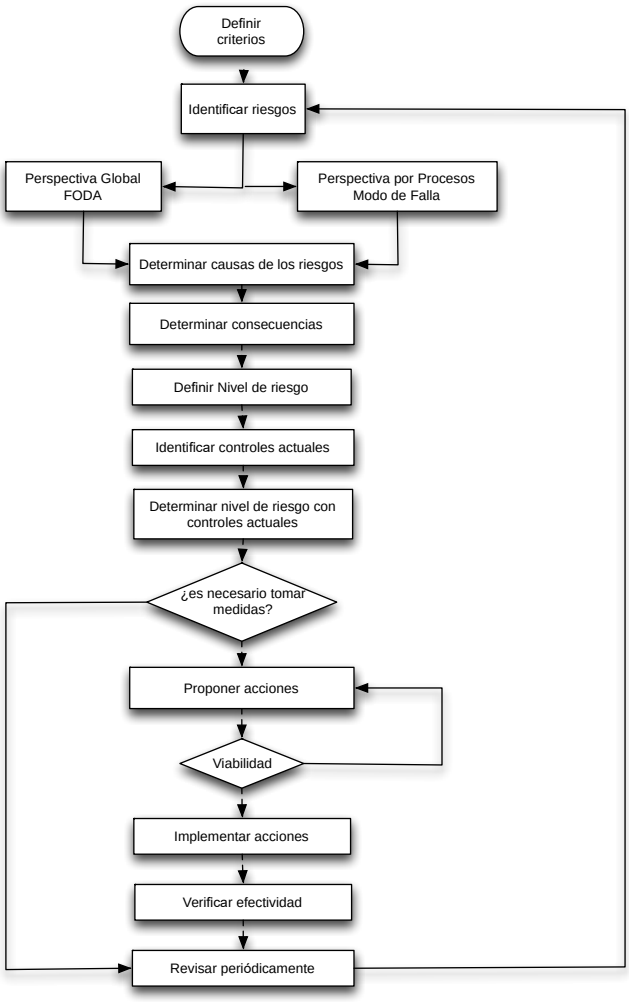
4. MONITOREO Y REVISIÓN

La fase final de la gestión de riesgos consiste en evaluar la eficacia de las acciones tomadas mediante el seguimiento y la revisión periódica. Esta representa la última etapa del Ciclo PDCA de la mejora continua, que deberá seguir desarrollándose.

En la revisión periódica que realiza la dirección del sistema de gestión se deberá incorporar un informe con el análisis de la gestión de riesgos de la organización y su efectividad.

RESUMEN: PASOS PARA EL DESARROLLO DE LA GESTIÓN DE RIESGOS

En el siguiente diagrama se presentan los pasos para la ejecución de la gestión de riesgos en la organización:



Las actividades de gestión de riesgos deberían ser ejecutadas por equipos interdisciplinarios, para tener una visión integral. Los equipos deben incluir a expertos de las áreas correspondientes (calidad, operaciones, finanzas, legales o regulatorios, ventas,

etc.), además de personas que conozcan y puedan facilitar el proceso de gestión de riesgos.

Una vez integrado el equipo, los pasos del proceso son los siguientes:

1. Definir criterios para:
    a. Evaluación de probabilidad.
    b. Evaluación de impacto.
    c. Niveles de riesgo y nivel de riesgo aceptable.
    d. Perspectivas de análisis.
    e. Responsable y recursos asignados al proceso de gestión de riesgos.
2. Identificar y listar los riesgos
    a. Perspectiva global (del contexto u operativa general del negocio): utilizando la matiz FODA.
    b. Perspectiva de procesos: analizando el modo de falla. Identificar los posibles puntos tanto de origen como de materialización de riesgos:
        i. ¿qué puede suceder?
        ii. ¿dónde y cómo puede suceder?
        iii. ¿por qué puede suceder?
3. Identificar las causas de los riesgos, los elementos disparadores del riesgo:
    a. ¿Cuáles son los elementos claves que favorecen la ocurrencia del riesgo?
    b. ¿Cómo se están monitoreando estos elementos?
    c. ¿Quién reporta sobre estos elementos?
    d. ¿Con qué frecuencia se reporta?
4. Determinar consecuencias / impactos de los riesgos. Determinar cuáles son las perspectivas más afectadas, sobre estas se enfocará la intervención.
5. Definir nivel de riesgo presente:
    a. Determinar probabilidad.
    b. Determinar impacto.
    c. Determinar nivel del riesgo.
6. Identificar controles existentes y su efectividad.
7. Definir nivel de riesgo con la aplicación de los controles actuales.
8. Definir si es necesarios tomar acciones adicionales:
    a. Mejorar /cambiar controles actuales
    b. Implementar nuevos controles
    c. Implementar otras acciones
9. Priorizar los riesgos para los cuáles se debe tomar acciones, iniciando con el escenario de mayor criticidad, de acuerdo con la evaluación realizada.
10. Proponer acciones a implementar:
    a. Establecer las posibles acciones de intervención que puedan ser factibles de utilizar para mitigar la consecuencia sobre la perspectiva escogida para el análisis.
    b. Realizar la estimación del impacto de la acción. Cada acción de intervención tiene la capacidad potencial de disminuir el nivel de riesgo hasta un determinado punto. El impacto de la acción es el porcentaje en el cual es capaz de reducir el nivel.
    c. Identificar la rentabilidad de la acción a través de un análisis de “costos-beneficios”.

11. Verificar la viabilidad de las acciones propuestas. La rentabilidad nos indica la opción optima desde el punto de vista de la inversión y de los resultados posibles a obtener con una acción de intervención. Sin embargo, las acciones de intervención pueden tener otras implicaciones o efectos adversos, que deben ser considerados en el momento de tomar la decisión final. Los aspectos o factores adicionales a la "rentabilidad" que deben tenerse en cuenta para la toma de decisiones sobre las medidas de intervención a adoptar son del tipo: sociales, políticos, legales/reglamentarios, organizacionales, culturales, etc.
12. Definición de las medidas de intervención: una vez considerados los aspectos de viabilidad que afectan o podrían afectar a las acciones en consideración, se debe tomar la decisión de cuáles serán las medidas de intervención a implantar para el tratamiento del riesgo, comenzando por aquellas que, siendo adecuadamente rentables, son política, legal, social, o culturalmente viables de aplicar.
13. Implementar las acciones, realizar un plan de acción.
14. Verificar la efectividad de las acciones.
15. Revisar y comenzar nuevamente el proceso.

Nota: hay que tener en cuenta que siempre existirá algún nivel de riesgo residual, no solo por las limitaciones de los recursos, sino también por la incertidumbre del futuro y demás limitaciones inherentes a todas las actividades

ANEXO I: TABLA DE REGISTRO Y TRATAMIENTO DE RIESGOS

A modo de ejemplo presentamos las siguientes tablas que se pueden utilizar para el registro de los riesgos y para el seguimiento del tratamiento.

Se puede utilizar la siguiente tabla para realiza el registro

Aspecto evaluado	Riesgo	Causa	Consecuencia	Nivel de riesgo	Controles actuales	Nivel de riesgo con controles	Necesidad de acción
Rotación del personal	Personal con experiencia abandona la organización	Organizaciones similares ofrecen mejores condiciones laborales	Altos costos de contratación e inducción de nuevo personal	Alto	Política de calidad de vida en el trabajo implementada	Medio	si
Atención al cliente	Generación de respuestas inadecuadas. Respuestas sin la competencia técnica o no acorde a lo requerido.	Personal poco capacitado	Aumento de nivel de quejas	Medio	Proceso de selección	Medio	si
		No existe documentación de apoyo para las respuestas	Pérdida de imagen		Capacitación solo en el momento de inducción		

Cuando se requiera una acción, se desarrollará el plan de acción correspondiente.

Aspecto	Riesgo	Acción para implementar	Responsable	Plazos	Recursos necesarios	Nivel de riesgo resultante	Verificación de eficacia

ANEXO II: PLANILLA PARA ANÁLISIS DE RIESGOS

Esta planilla se puede utilizar para identificar y describir los riesgos de la organización, a nivel de un proceso, de un proyecto, de un departamento o general de toda la organización.

Definiciones

Columna	Definición
Evento / riesgo	En esta columna se identifica el evento o riesgo que se está analizando
Descripción	Se describe el riesgo/ evento identificado. Se debe describir cuales son las consecuencias si el riesgo no es tratado.
Impacto	Se coloca el impacto que puede tener en la organización: 1 – bajo, 5- muy alto
Probabilidad	Se coloca la probabilidad de que el evento/riesgo efectivamente ocurra: 1 – poco probable, 5- muy probable.
Nivel de riesgo	Es la multiplicación del impacto por la probabilidad. Cuanto mayor sea este número mayor será el riesgo para la organización.
Responsable	Identifica la persona u organización que es responsable de gestionar/tratar el riesgo. Puede ser tanto interna o como externa a la organización.
Controles actuales	Identifica como el riesgo está siendo gestionado/ controlado actualmente. Posibles controles son políticas y procedimientos, revisiones, tecnologías para tratar el riesgo, …
Monitoreo	Describir qué se está haciendo para monitorear o realizar el seguimiento del riesgo para asegurar que el mismo está siendo tratado.

Pasos para realizar el análisis de riesgo

1. Integrar un equipo de personas multidisciplinaria – que aporten distintas visiones – pero que tengan conocimiento del proceso/área que se va a analizar.
2. A través de una lluvia de ideas para identificar los eventos, amenazas y posibles riesgos. No es necesario preocuparse, en esta etapa, por la probabilidad de ocurrencia. Se listan todos los riesgos en la primera columna de la planilla.
3. Revisar cada uno de los riesgos identificados y describirlos brevemente. A medida que se describen, considerar las amenazas, consecuencias e impactos si el riesgo no se trata. Poner esta información en la columna de descripción.
4. Considerar el impacto del riesgo en la organización si el mismo no se gestiona. Asignarle un valor de 1 (bajo) a 5 (alto).
5. Considerar la probabilidad de que ocurran las consecuencias negativas identificadas con los controles que actualmente están implementados (las políticas, procedimientos, tecnología, etc.). Asignar un valor: 1 (muy poco probable) a 5 (muy probable).
6. Calcular el nivel de riesgo multiplicando el impacto por la probabilidad. A mayor nivel de riesgo peor será el mismo para la organización.
7. Identificar quién o qué organización está gestionando/tratando el riesgo actualmente.

8. Identificar cómo el riesgo se está gestionando/tratando actualmente. Considerar las políticas, los procedimientos, los controles, las tecnologías, las prácticas. Ponerlas en la columna de controles actuales.
9. Identificar cómo y quién está realizando el monitoreo/seguimiento de los controles o tratamientos actuales para asegurarse que el riesgo está efectivamente siendo gestionado.
10. Finalmente, revisar la lista. Comenzando por los riesgos de mayor nivel definir qué acciones adicionales se deben tomar para gestionarlo y reducir su nivel.

Evento/ riesgo	Descripción	Impacto	Probabilidad	Nivel	Responsable	Controles actuales	Monitoreo	Observaciones

ANEXO III: ANÁLISIS FMEA (FAILURE MODE AND EFFECTS ANÁLISIS)

El Análisis de Modo de Falla y Efecto (FMEA por las siglas en ingles de Failure Mode Analysis and Effects) es una herramienta simple, versátil y poderosa que ayuda al equipo a identificar los posibles defectos en el proceso que deberían ser eliminados o reducidos. El FMEA es un proceso sistemático para la identificación de las fallas potenciales del diseño de un producto o de un proceso antes de que estas ocurran, con el propósito de eliminarlas o de minimizar el riesgo asociado con las mismas.

El FMEA permite:

- Identificar las formas en que un proceso puede fallar para cumplir con los requisitos críticos del cliente.
- Estimar el impacto y la probabilidad de ocurrencia de esa falla.
- Evaluar el plan de control actualmente utilizado para prevenir que ocurran las fallas.
- Priorizar las acciones que tienen que llevarse a cabo para evitar que las fallas ocurran o solucionar el problema ocasionado.

Cómo se ejecuta un FMEA

1) Integrar un equipo multifuncional de personas con experiencia en el producto o servicio que se va a analizar y con conocimiento de las necesidades del cliente.
2) Para cada etapa del proceso el equipo debe identificar.
   a) Modos de falla: son las formas con las cuales el requerimiento o el proceso puede fallar para cumplir con lo especificado por el cliente.
   b) Causas potenciales: son las deficiencias que pueden resultar en un modo de falla.
   c) Efectos potenciales: es el impacto en el cliente si el modo de falla no es corregido o prevenido.
3) Una vez que el equipo ha identificado el modo se falla se calcula el **RPN (Risk Priority Number**) para cada modo de falla. Este número combina la probabilidad de ocurrencias, la severidad de su impacto y la posibilidad de detección.

$$\mathbf{RPN = P \times S \times D}$$

Componente	Definición	Calificación	
		1 (min)	10 (max)
Probabilidad	¿es probable que la causa del modo de falla ocurra?	Probablemente no ocurra	Seguramente ocurra
Severidad	¿qué tan significativo será el impacto de efecto del modo de falla en el cliente?	Menos grave	Muy grave
Detección	¿es probable que el sistema pueda detectar	Probablemente se detecte	Probablemente no se detecte

	la causa o el efecto si ocurre?		

Cada uno de estos componentes se mide en una escala de 1 a 10; en consecuencia, el máximo valor del RPN es 1000.

Pasos para la ejecución del FMEA:

1) Integrar el equipo.
2) Determinar el alcance del análisis. ¿es para un concepto, un sistema, un diseño, un proceso o un servicio?
3) Identificar las funciones del alcance: ¿cuál es el propósito de este sistema, proceso o servicio? ¿qué es lo que esperan / requieren los clientes? Podrá ser necesario dividir el alcance en subsistemas, partes o subprocesos; en tal caso hay que determinar el objetivo de cada parte.
4) Desarrollar un mapa del proceso identificando todos los pasos de este.
5) Listar las entradas y salidas clave para satisfacer los requisitos de los clientes internos y externos.
6) Para cada paso del proceso, listar las formas en que puede variar (causas) e identificar los **posibles modos de falla** asociados a estas variaciones. Estas fallas afectarán la función / objetivo del alcance analizado.
7) Para cada modo de falla identificar todas las consecuencias en el sistema, sistemas relacionados, proceso, procesos relacionados, producto servicio, cliente, regulaciones, etc. ¿qué puede suceder si esta falla ocurre? ¿cómo impacta en el cliente? ¿qué requisitos se dejan de cumplir? Estos son los **potenciales efectos de la falla**.
8) Para cada consecuencia determinar su **severidad (S).**
9) Para cada modo de falla determinar todas las **potenciales causas raíz**. Usar las herramientas para análisis de problemas y detección de causas.
10) Para cada causa determinar la **probabilidad de ocurrencia (P).**
11) Para cada causa identificar los **controles que existen actualmente**. Son las medidas que previenen que ocurra el modo de falla o detectan el modo de fala en caso de que ocurra. Estos pueden ser procedimientos, políticas, mecanismos de medición, etc. que están en marcha para evitar que las fallas lleguen al cliente. Estos controles pueden prevenir que la causa ocurra, reducir su probabilidad de ocurrencia o detectar la falla luego de que ha ocurrido, pero antes de que el cliente se vea afectado.
12) Para cada control determinar la **capacidad de detección (D)**, esto es que tan bien los controles son capaces de detectar la causa o el modo de falla luego de que ha ocurrido, pero antes de que afecte al cliente.
13) Calcular el **RPN para cada escenario de modo de falla potencial**.
14) Ordenar de acuerdo con el RPN, priorizando dónde se debe actuar.
15) Determinar las acciones a seguir para reducir la gravedad o probabilidad de ocurrencia.
16) Después de que se haya completado una acción se estiman y registran los grados de probabilidad, gravedad y detección finales y se calcula el **RPN resultante**.

Tabla de FMEA

Proceso	Modo de la Falla Potencial	Efectos Potenciales de la falla	S	Causa Raiz potencial de la falla	P	Controles actuales	D	RPN	Acción a tomar	Resp.	Plazo Fecha	Resultados de las acciones tomadas				
												Acción Realizada fecha	S	P	D	RPN final

ANEXO IV: ANÁLISIS RIESGO DE UN PROCESO

La siguiente tabla se puede utilizar para evaluar y tratar los riesgos en un proceso. Se analiza, para cada una de las etapas del proceso, las potenciales fallas, las consecuencias que pueden provocar, las causas potenciales de estas fallas, la severidad del impacto y probabilidad de ocurrencia de las fallas. De acuerdo con el nivel de riesgo se recomiendan acciones para mitigarlo, definiendo responsables y plazos para su implementación.

DESCRIPCIÓN DEL RIESTO					CALIFICACION RIESGO			TRATAMIENTO		
Nº	ETAPA DEL PROCESO	FALLA POTENCIAL	CONSECUENCIAS POSIBLES	CAUSAS POTENCIALES	SEVERIDAD (S)	PROBABILIDAD (P)	IR (SxP)	ACCIONES RECOMENDADAS	RESP.	PLAZOS
1							0			
2							0			
3							0			

SOBRE EL AUTOR

John Miles es Doctor en Competitividad Empresarial y Desarrollo Económico. Máster en Administración y Dirección de Empresas, Ingeniero Industrial.

Más de 20 años de experiencia en consultoría empresarial en estrategia y modelos de negocios, reingeniería y mejora de procesos, implantación de sistemas de gestión.

Integrante del Sistema Nacional de Investigadores del Uruguay y docente universitario en las áreas de Dirección Estratégica, Dirección de Operaciones y Sistemas de Gestión, a nivel nacional e internacional. Ocupó cargos gerenciales en empresas nacionales e internacionales. Ha sido Decano de la Facultad de Ciencias Empresariales, Vicerrector de Desarrollo y Administrativo de la Universidad Católica del Uruguay. Ha sido Miembro del Consejo Asesor Honorario del Instituto Nacional de Calidad. Juez y Evaluador del Premio Nacional de Calidad del Uruguay y del Premio Iberoamericano de Calidad. Miembro de Consejo Nacional de Ciencia y Tecnología.

Rincón 454 – Montevideo, Uruguay
www.modum.com.uy