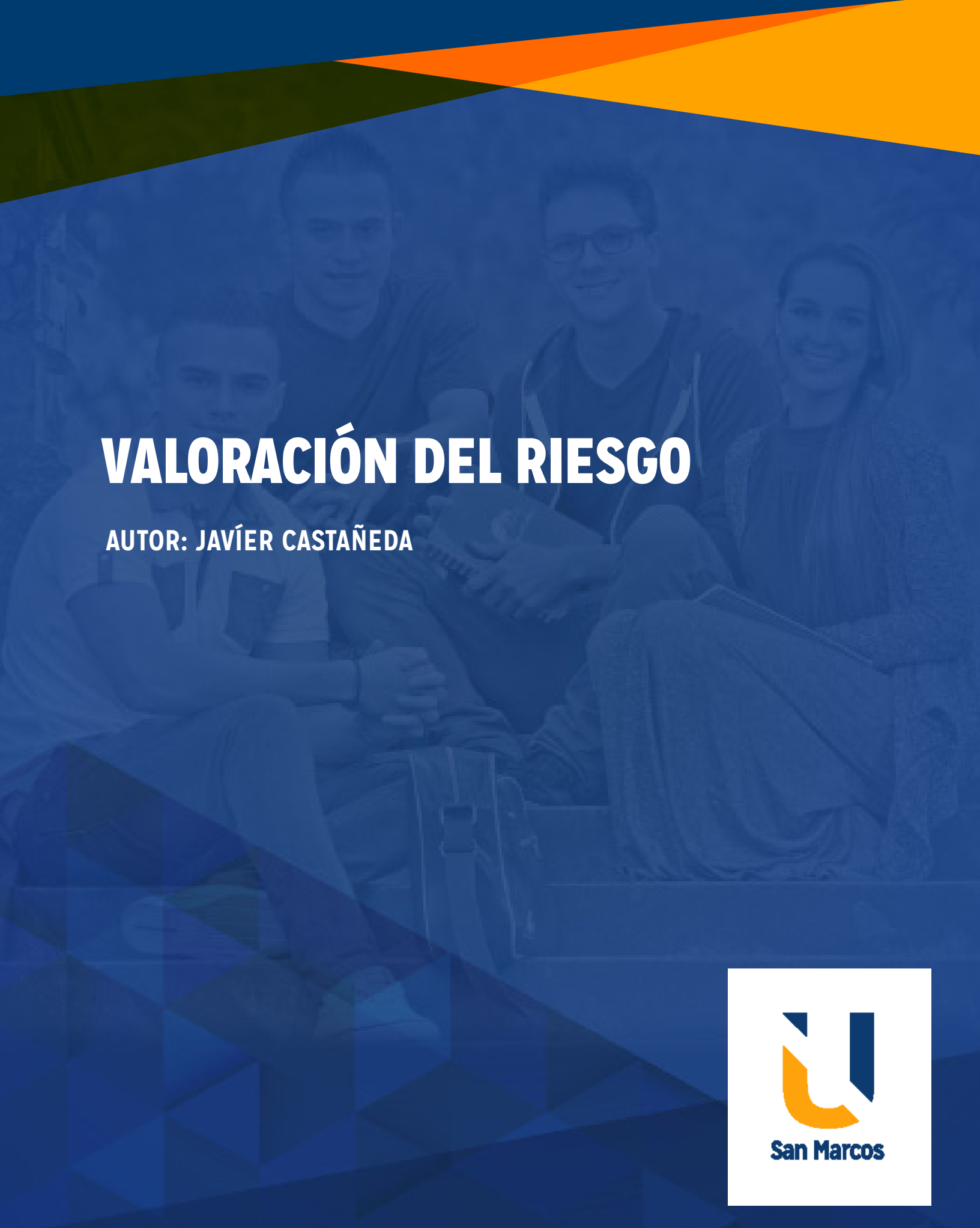
VALORACIÓN DEL RIESGO

AUTOR: JAVÍER CASTAÑEDA



San Marcos

ÍNDICE

INTRODUCCIÓN

En la gestión del riesgo, una de las etapas más importantes es la valoración del riesgo, donde a través de un proceso secuencial, sistemático e integral, se puede identificar, analizar, calificar y evaluar el riesgo, aspectos que son determinantes con el fin de poder tomar decisiones frente al mismo.

En la presente cartilla se desarrollará la metodología de la matriz de evaluación de riesgos, la cual es una de muchas otras herramientas y métodos para la identificación y posterior valoración del riesgo, siendo esta una de las más completas y efectivas.

Los temas considerados en el presente referente de pensamiento están desarrollados a partir de la estructuración e implementación de la gestión del riesgo, medidas de tratamiento y políticas, con el ánimo de generar en el estudiante pensamiento práctico, a partir de varias opciones de trabajo académico como actividades y recursos de aprendizaje que aportaran a profundizar en el conocimiento mediante la complementación de las ideas y material del referente, los invito a adentrarse en el campo de la gestión del riesgo y las posibilidades de aplicación en la empresa del siglo XXI.

Para consolidar y orientar el referente se estructuró la pregunta ¿De qué forma se aplica la prevención y gestión del riesgo para proteger las organizaciones de la materialización de riesgos y amenazas?, centrando el ejercicio en la valoración del riesgo, ello como un recurso que los gerentes competitivos manejan para llevar sus organizaciones a niveles de competitividad con fuertes vínculos y la prevención como garante de la salud e integridad organizacional.

Estructuración e implementación de gestión del riesgo, medidas de tratamiento y políticas

Figura 1.
Fuente: Shutterstock/322872056

Valoración del riesgo

Valorar el riesgo es de manera integral lograr una visión total del mismo, con el fin de poder tratarlo para lograr resultados positivos para la organización.

Identificación y análisis del riesgo

La identificación del riesgo consiste en reconocer todos aquellos aspectos que por su interacción con la organización pueden significar un riesgo, para ello se deben emplear herramientas y métodos que sean de reconocimiento por sus resultados y que permitan abarcar todo tipo de riesgos y con ello reducir la posibilidad de gestionarlos por errores u omisiones en su identificación.

Existen muchas herramientas y métodos para realizar este ejercicio, como se detalla en el siguiente cuadro de la Asociación Española de Gerencia de Riesgos y Seguros, donde hace una compilación de herramientas y métodos los cuales aportan al proceso de identificación, análisis y evaluación de riesgos, en la evaluación del riesgo se tratará algunas técnicas de evaluación de riesgos propuesto en la ISO 31010.

Herramientas y técnicas	Proceso de evaluación del riesgo					
	Identificación del riesgo	Análisis del riesgo			Evaluación del riesgo	
		Consecuencia	Probabilidad	Nivel de riesgo		
Tormenta de ideas (Brainstorming)	FA	NA	NA	NA	NA	B01
Entrevistas estructuradas o semiestructuradas	FA	NA	NA	NA	NA	B02
Delphi	FA	NA	NA	NA	NA	B03
Lista verificación (Check-lists)	FA	NA	NA	NA	NA	B04
Análisis preliminar de riesgos	FA	NA	NA	NA	NA	B05
Estudios de riesgos operacionales (HAZOP)	FA	FA	A	A	A	B06
Análisis de riesgos y puntos de control críticos (HACCP)	FA	FA	NA	NA	FA	B07
Valoración de riesgo medioambiental	FA	FA	FA	FA	FA	B08
Que pasaría si (What if)	FA	FA	FA	FA	FA	B09
Análisis de escenario	FA	FA	A	A	A	B10
Análisis del impacto en el negocio	A	FA	A	A	A	B11
Análisis de causa	NA	FA	FA	FA	FA	B12
Análisis modal de fallos potenciales y sus efectos (ANFE-FMEA)	FA	FA	FA	FA	FA	B13
Análisis de árbol de fallos	A	NA	FA	A	A	B14
Análisis de árbol de sucesos	A	FA	A	A	NA	B15
Análisis de causa consecuencia	A	FA	FA	A	A	B16
Análisis de causa efecto	FA	FA	NA	NA	NA	B17
Análisis de niveles de protección	A	FA	A	A	NA	B18
Árbol de decisión	NA	FA	FA	A	A	B19
Análisis de fiabilidad humana	FA	FA	FA	FA	A	B20
Análisis de la pajarita	NA	A	FA	FA	A	B21
Mantenimiento centrado en la confiabilidad	FA	FA	FA	FA	FA	B22
Análisis de errores de diseño (SNEAK)	A	NA	NA	NA	NA	B23
Análisis de Markov	A	FA	NA	NA	NA	B24
Simulación de Monte Carlo	NA	NA	NA	NA	FA	B25
Estadísticas y redes Bayesianas	NA	FA	NA	NA	FA	B26
Curvas FN	A	FA	FA	A	FA	B27
Índices de riesgos	A	FA	FA	A	FA	B28
Matriz de consecuencia/probabilidad	FA	FA	FA	FA	A	B29
Análisis coste/beneficio	A	FA	A	A	A	B30
Análisis de decisión multicriterio	A	FA	A	FA	A	B31

Tabla 1.
Fuente: Asociación Española de Gerencia de Riesgos y Seguros (Agers), 2011

Herramientas de identificación

En el desarrollo del presente módulo, se tendrán en cuenta algunas de las herramientas más usadas como son los cuestionarios para la identificación y análisis de riesgos, listas de chequeo identificación y análisis de riesgos, diagramas de flujo de procesos, inspección e identificación en análisis de riesgos, análisis de los estados financieros de la empresa y combinación de herramientas.

Cuestionario de identificación y análisis de riesgos

El cuestionario consiste en realizar una serie de preguntas desde el contexto tanto interno como externo cuya finalidad es la de determinar la posibilidad de ocurrencia de algunos eventos que en caso de materializarse podrían generar daños y pérdidas a la organización, el cuestionario debe abarcar todos los tópicos posibles, su diseño debe ir acorde al tipo de organización y su objeto social.

El diseño del cuestionario debe responder a eventos que representen riesgo y no a la existencia de controles, esta área corresponde a la evaluación del riesgo, una vez estructuradas las preguntas estás deben responder de manera afirmativa o negativa a su materialización, de allí se pude inferir cuales son los riesgos más importantes, de ser necesario se puede ampliar las respuestas del cuestionario con la justificación tanto afirmativa como negativa de las personas que desarrollaron el mismo.

A continuación de se propone un modelo estándar con base a algunas consideraciones realizadas por MAFRE en el libro Gerencia de Riesgos y Seguros (1998, p. 151-154).

Cuestionario de identificación y análisis de riesgos					
No.	Preguntas	SI	NO	NO SABE	NECESITA MÁS INFOR-MACIÓN
	Riesgos Internos				
	Comerciales				
1	¿Posee productos terminados en instalacio-nes de terceros?				
2	¿Produce o utiliza materiales precederos?				
3	¿Vende a comprador único parte apreciable de la producción?				
4	¿Es su operación estacional?				
	Relacionamiento con grupos de interés				
1	¿Ha sido víctima de infidelidad grave de algún empleado?				
2	¿Tiene vecinos con alto índice de riesgo que pudieran afectarle?				
3	¿Desarrolla su operación en un ambiente insalubre o tóxico?				
	De gestión interna				
1	¿Ha sido objeto de sabotaje, huelga ilegal o vandalismo?				

2	¿Está su operación especialmente expuesta a errores de diseño?				
3	¿Posee automóviles u otros servicios para el uso de empleados?				
4	¿Puede su operación contaminar el ambiente?				
5	¿Es satisfactorio el índice de accidentalidad laboral en su operación?				
	Gestión directiva				
1	¿Regularmente viajan juntos varias personas claves en la organización?				
	Otros				
1	¿Posee maquinaria y/o instalaciones claramente obsoletas?				
	Riesgos Externos				
	Fenómenos de origen natural				
1	¿Está ubicado en una zona de alto riesgo sísmico?				
2	¿Está ubicado en un área de alta pluviosidad?				
3	¿Está situado en proximidades a la costa, o la rivera de un rio o lago?				
	Político				
1	¿Está situado en un país o región donde se desarrollan conflictos armados?				
2	¿El país o región donde está ubicada la organización tiene inestabilidad política, económica o social?				
	Social				
1	¿Está situado en un área de alta presencia de organizaciones delictivas?				
	Otros				
1	¿Existe una alta posibilidad de cortes súbitos de energía eléctrica?				

Tabla 2.
Fuente: Castañeda, (2016)

Lista de chequeo identificación y análisis de riesgos

Son herramientas que emplean las aseguradoras para considerar de manera general todos los riesgos que pueden afectar a una empresa, y con base a ella ofertar las diferentes coberturas que por su naturaleza cada empresa puede necesitar para cubrir sus necesidades de transferencia del riesgo, este recurso tiene una limitación y es que su enfoque es a riesgos que son asegurables, sin embargo, es muy útil pues permite tener un amplio panorama del riesgo en el entorno empresarial.

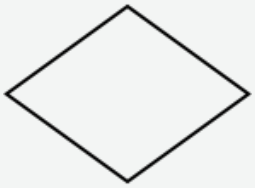
Lista de chequeo de las pólizas de seguros	
Grupo	Riesgo
Riesgos de la naturaleza	Terremoto, maremoto, tsunami, erupción volcánica, emanación natural de gas o vapor , lluvia torrencial, nieve, granizado, caída de rayo, desbordamiento de ríos, lagos, inundación, alud, avalancha, ola de calor o de frío, sequía, alimañas, roedores, moho, hongos, etc.
Riesgos tecnológicos	Incendio, explosión, humo, polvo, derrame de productos químicos, escape de gases, y vapores, contaminación súbita, avería mecánica o eléctrica de maquinaria, corte súbito de energía eléctrica, desmoronamiento de material apilado, etc.
Riesgos marítimos de aviación y transporte	Avería de medio de transporte aéreo, marítimo o terrestre, colapso de artefacto espacial, naufragio, colisión de automóvil matriculado, pérdida o deterioro de mercancía, error de conducción de automóvil, de vehículo de transporte terrestre o en operación de transporte aéreo.
Riesgos Políticos -sociales	Guerra civil o internacional, acto bélico, levantamiento militar, civil revolución, asonada, motín, huelga legal, confiscación, etc.
Riesgos antisociales	Terrorismo, sabotaje, huelga ilegal, acto vandálico, piromanía, asesinato, atentado, secuestro, robo, hurto, desaparición misteriosa, mermas, infidelidad de empleados, falsificación, desfalco, fraude, intrusión y espionaje industrial.
Riesgos indirectos	Daños a bienes arrendados a terceros, o bajo dominio de terceros, o bajo su responsabilidad civil.
Riesgos consecuenciales	Demolición necesaria de partes ilesas, pérdida de uso, desempleo temporal de mano de obra, pérdida de persona clave, gastos financieros extraordinarios, etc.
Responsabilidad civil empresarial	Daño a edificio o local arrendado, daño a bien de terceros en: depósito, proceso de transformación, mezcla o ensamble, incumplimiento de contrato, difamación, calumnia, piratería industrial o comercial, competencia desleal, etc.
Responsabilidad civil patronal	Incumplimiento de normas de higiene, de seguridad, de convenio colectivo, de contrato individual, daños a bienes de empleados, etc.
Responsabilidad automóviles	Daños materiales a ocupantes o a terceros, daños corporales a ocupantes o a terceros.

Responsabilidad civil profesional	Error técnico, de diseño o cálculo, error administrativo, error médico, abandono de funciones profesionales, negligencia, dolo de personal directivo, etc.
Responsabilidad civil ecológica	Contaminación gradual del ambiente, contaminación súbita o accidental, delito ecológico, contaminación radioactiva, lluvia ácida.
Riesgos personales	Muerte por accidente laboral, muerte por accidente no laboral, invalidez permanente, incapacidad profesional, incapacidad laboral transitoria, secuestro, asesinato, atentado, desempleo, etc.
Riesgos financieros	Riesgos de créditos, riesgo de inversión en el exterior, riesgo de caución, riesgo de cambio.

Tabla 3. Lista de chequeo de pólizas de seguro
Fuente: Business Alliance for Secure Commerce (BASC)

Diagramas de flujo de proceso

Es la graficación de un proceso de manera secuencial, este aspecto se logra conociendo el procedimiento como se desarrolla, para ello se emplea una simbología estándar que permite de manera progresiva graficar paso a paso el procedimiento, facilitando entender los momentos del proceso y en él los riesgos que se presentan.

Función	Símbolo	Descripción
Inicio – fin		Representa el inicio o fin del procedimiento.
Proceso u operación		Representa una instrucción o tarea que debe ejecutarse. Operación.
Toma de decisiones		Elección. Representa una pregunta e indica el destino del flujo de información con base en respuestas alternativas de sí y no.
Preparación		Preparación o acondicionamiento. Implica un proceso predefinido. Puede ser parte o un todo de otro sistema.

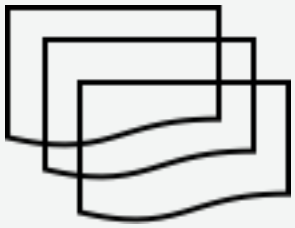
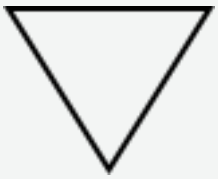
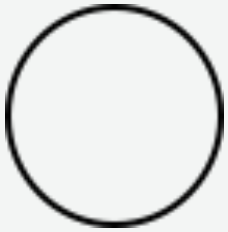
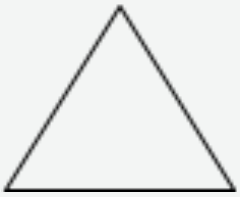
Documento		Indica lectura de algún documento. Casi siempre se refiere a un producto impreso.
Documento con varias copias		Representa la preparación de un documento con varias copias.
Entrada / Salida		Trámite u operación burocrática de rutina. Implica entrada o salida de información por cualquier parte del sistema.
Archivo		Implica archiva, guardar o almacenar documentos, productos, materiales u otros.
Conector de página		El total de páginas se registra en la parte inferior derecha y el número correspondiente a la página.
Conector interno		Permite conectar actividades o formatos con otras actividades dentro del diagrama de flujo.
Extracción De archivo		Significa "sacar del archivo" productos, materiales u otros.
Flechas		Representan flujo de información. Indica la dirección que sigue el flujo en el procedimiento.

Tabla 4.
Fuente: Castañeda, (2016)

A continuación, un ejemplo de un diagrama de flujo.

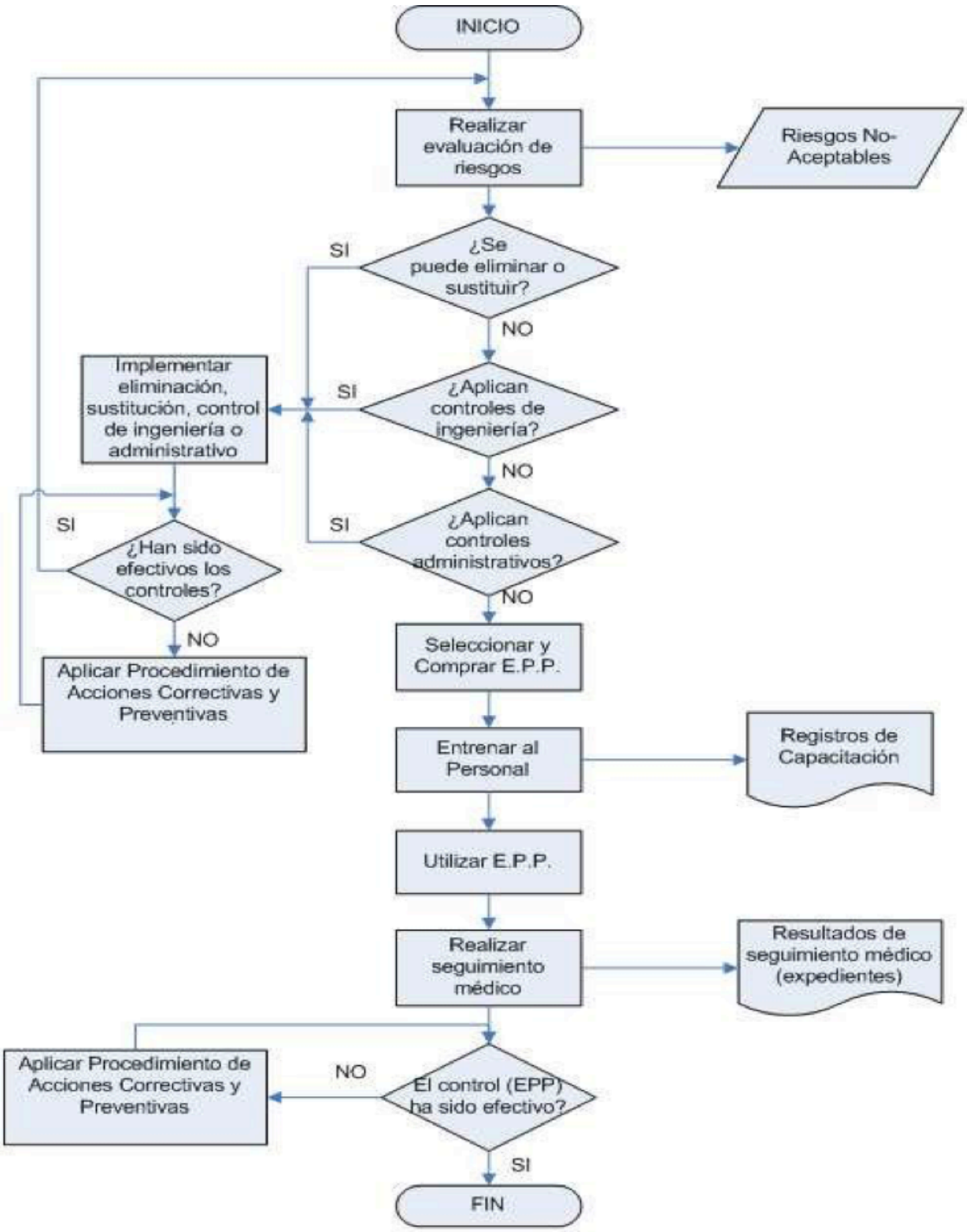


Figura 2.
Fuente: Central Hidroeléctrica Lorena, (2010)

Análisis de los estados financieros de la empresa

La función principal de la alta gerencia es el conocimiento amplio y profundo de la organización, de allí se desprende la apreciación integral de la situación de la empresa, donde se puede de manera precisa establecer la situación y los indicadores financieros, donde están factores de riesgo definitivos en la integridad de la organización, aspectos como:

- Rentabilidad.
- Liquidez.
- Nivel de endeudamiento.
- Rotación de inventarios.
- Cartera.

Otros aspectos como el análisis de los balances y resultados de manera vertical y horizontal, análisis de activos, pasivos, pérdidas y ganancias, etc.

Análisis de información documental, políticas, informes, etc.

Otra fuente de información que permite apreciar riesgos, es el estudio de documentos como informes de auditoría, quejas y reclamos, procesos contractuales, siniestralidad de contratos, manuales de operación, publicidad, etc.

Inspección e identificación en análisis de riesgos

Complementario a las anteriores herramientas es indispensable la verificación física, "nada reemplaza la percepción directa", es decir, que se requiere hacer inspecciones que permitan un cotejo con la recolección de información a través de documentos, para ello el inspector deberá tener un conocimiento de la documentación, los procesos, procedimientos y actividades de la dependencia o proceso que se va revistar.

La actividad de inspección en lo posible debe ser realizada por una persona con conocimientos profundos y técnicos sobre el proceso o dependencia, debe ser una inspección sistemática y secuencial, en lo posible se debe emplear una lista de verificación o de chequeo para no dejar espacios vacíos en la misma.

La inspección debe iniciar con una revisión general y luego específica del proceso o dependencia, finalizada se debe realizar una reunión de resultados con los dueños del proceso o encargados de la dependencia, para confrontar los resultados y finalmente debe haber un informe de los encontrado y de los riesgos detectados en la actividad.

Combinación de herramientas

Para finalizar este capítulo, la recomendación es aplicar la mayor cantidad de herramientas para la identificación y análisis de riesgos, de manera integrada, todo ello enfocado a minimizar la posibilidad de que se queden sin considerar riesgos potencialmente dañinos para la organización.

Instrucción

Apreciado estudiante lo invito a consultar el recurso: organizador gráfico, acerca de las herramientas de identificación de riesgos. Lo encuentra disponible en la página principal de este eje.

Métodos de identificación

Como se mencionó anteriormente existen varios métodos de identificación de riesgos, normalmente se parte de lo general a lo particular, aunque algunas inician de lo particular a lo general, de los métodos existentes en el presente capítulo se va a trabajar el Método de Análisis de Vulnerabilidad, propuesto por César Duque, así:

- Método análisis de vulnerabilidad.

Método Matriz de análisis de vulnerabilidad

El análisis de vulnerabilidad se emplea en empresas tanto del sector público como privado, fue estructurada por César Duque bajo el Modelo del Sistema Gestión Integral del Riesgo en las Organizaciones "GIRO", el desarrollo de la metodología del sistema que se adelantará a continuación es de su autoría, se trabajará la escala y pasos más representativos de método.

Descripción del método

Inicialmente en el desarrollo del análisis de vulnerabilidad se deben tener en cuenta los siguientes pasos:

1. Definición del equipo evaluador.
2. Determinación del sistema de referencia y ámbito de aplicación.
3. Determinación de factores de vulnerabilidad.
4. Definición de nivel de riesgo aceptable.
5. Identificación de los recursos, procesos o actividades amenazadas.
6. Identificación y selección de amenazas.
7. Determinación de consecuencias reales del sistema.
8. Cálculo de porcentaje de vulnerabilidad.
9. Evaluación.

Definido el equipo evaluador, el cual debe estar integrado por personas que por su experiencia y conocimiento de la organización pueden realizar un proceso sistemático e integral de la situación y los riesgos que pueden afectar la organización, a continuación, se procede trabajar el numera 2.

El sistema de referencia se refiere a una organización, empresa, unidad de negocio, departamento o unidad administrativa, a la cual se le va a adelantar el estudio y análisis de riesgos y con ello establecer las vulnerabilidades a las que está expuesto. Determinado el sistema de referencia que en conclusión es la estructura que será afectada en caso de materializarse cualquier riesgo, luego se debe precisar el ámbito de aplicación, el cual se encuadra en el recurso, proceso, instalación, etc., al cual se va a realizar el análisis de riesgos.

Posteriormente y mediante un proceso o herramienta de diagnóstico se procede a identificar las amenazas que se pueden manifestar en el ámbito de aplicación cuya clasificación en el presente método se circunscribe a 4 grandes grupos como son: naturales, tecnológicas, sociales y operacionales. Con dicha información se procede a evaluar que tan representativas son para el sistema de referencia, su importancia se denomina “significancia” y se determina mediante el grado de significancia de las amenazas (Duque, 1999, p. 49), representada en siguiente cuadro:

Grado de significacia de la amenaza				Potencial de daño de la amenaza (P)		
				Bajo	**Medio**	**Alto**
				Escala		
				1	**2**	**3**
Tamaño relativo de la amenaza (T)	**Bajo**	**Escala**	1	1	2	3
	Medio		2	2	4	6
	Alto		3	3	6	9
				Grado de significancia de la amenaza (S)		

Tabla 5. Grado de significancia de las amenazas
Fuente: propia

El grado de significancia de las amenazas para el sistema de referencia, se obtiene de la multiplicación de dos variables:

Tamaño relativo de la amenaza (T), el cual se refiere en una escala cualitativa de bajo, medio y alto, a que tan representativa es dicha amenaza, su apreciación se realiza desde la experiencia y conocimiento del equipo evaluador, teniendo un componente importante de subjetividad, por ello se busca de manera colegiada y a través de una apreciación desde la intersubjetividad del equipo, la escala cualitativa tiene un valor cuantitativo de 1 a 3 de bajo a alto respectivamente.

El potencial de daño (P) que la amenaza puede causar en el sistema de referencia, al igual que la anterior variable, se mide cualitativamente en tres niveles de la escala (bajo, medio y alto) y cuantitativamente de 1 a 3.

El grado de significancia (S), es el producto del tamaño relativo por el potencial de daño de la amenaza.

Para ello se puede establecer el siguiente cuadro, que puede ayudar a hacer de manera ordenada el ejercicio de la identificación de las amenazas más significativas, la metodología propuesta determina que se deben tener en cuenta aquellas que por su importancia tengan un valor superior a 2, en el cuadro para el manejo de la información se le debe dar un código a la amenaza, así;

Amenaza	A
Amenaza	B
Amenaza	C
Amenaza	D
Amenaza	E

Tabla 6.
Fuente: propia

Una vez el equipo evaluador ha establecido las amenazas y les ha asignado un código se procede a hacer la evaluación de las mismas por su grado de significancia, empleando el siguiente cuadro:

Amenaza	Código	Significancia			Selección	
		Tamaño relativo de la amenaza (T)	Potencial de daño (P)	Significancia (S)	SI	NO
Amenaza	A					
Amenaza	B					
Amenaza	C					
Amenaza	D					
Amenaza	E					

Tabla 7.
Fuente: propia

Luego se deben establecer los recursos o actividades amenazadas que se consideran en el ámbito de aplicación, también se les debe asignar un código de manejo diferente al de las amenazas, así;

Recurso	Código
Recurso	1
Recurso	2
Recurso	3
Recurso	4
Recurso	5

Tabla 8.
Fuente: propia

Una vez se tiene establecidas las amenazas y los recursos amenazados se procede a establecer lo que Duque (1999), denomina Escenario de Riesgos, el cual se configura cuando un recurso está expuesto a una amenaza, se debe tener en cuenta que un recurso no necesariamente está expuesto a todas las amenazas, ni tampoco que una amenaza afecte a todos los recursos, ya que en ocasiones las amenazas no tienen la posibilidad de afectar el recurso.

Para su identificación y manejo, normalmente cada escenario de riesgo tiene un código único y diferenciador, el cual normalmente corresponde a la adición del código del recurso a la de la amenaza, este código se ubica en la casilla del escenario de riesgos donde se da la intersección entre el recurso y la amenaza.

Por ejemplo, el recurso 1 que puede ser existencias, puede ser afectado en el proceso de inventario por la amenaza A, denominada hurto, la codificación del escenario se codificaría como A-1 y su denominación sería Hurto de existencias.

Sistema de referecnia	Empresa de insumos para computador		
Ámbito de aplicación	Proceso - inventarios		
	Amenaza		
Recurso	Hurto	Amenaza B	Amenaza C
Existencias	**A-1** (Hurto de existencias)	B-1	C-1
Recurso 2	A-2	B-2	C-2
Recurso 3	A-3		

Tabla 9.
Fuente: propia

Una vez se definido los posibles escenarios de riesgo dentro de los ámbitos de aplicación, se puede crear un catálogo que contenga esta clasificación, se consignan los códigos de los escenarios establecidos con sus respectivos significados.

Aquí concluye el proceso de identificación de amenazas y riesgos, en el siguiente numeral se trabaja la calificación del riesgo.

Calificación del riesgo (método)

Calificación en el Método Matriz de análisis de vulnerabilidad

En la mayoría de los procesos de valoración del riesgo se tiene en cuenta dos variables la frecuencia o probabilidad y la consecuencia o impacto, en cualquiera de los casos se busca establecer a través de manera cualitativa y cuantitativa las veces que se presenta el evento crítico y la intensidad de su manifestación sobre el recurso considerado, con el fin de poder tratarlo en cuanto a las veces que se presenta y también a la intensidad con que se manifiesta.

Las escalas de frecuencia o probabilidad, así como de consecuencias o impacto, son específicas de cada organización o empresa, que por su complejidad y estructura tiene particularidades, sin embargo se han establecido algunas escalas con base a la experiencia alcanzada a través del estudio de diferentes organizaciones teniendo en cuenta la historia de las mismas y sumándole a ello datos prospectivos entorno a actividad empresarial, a continuación se planteará la propuesta de César Duque, donde se da una gradación de los eventos por su frecuencia o probabilidad de ocurrencia y también se plantean siete tablas que abarcan los factores de vulnerabilidad más comunes e importantes en una organización. Lo anterior no es camisa de fuerza y se pude adaptar o generar nuevas gradaciones y tablas con base al estudio propio de la organización donde se realiza el proceso de gestión del riesgo.

Para la calificación de la frecuencia se establecido una escala numérica que aumenta de manera lineal y cualitativa en años partiendo de cuantos casos se presentan en los lapsos de tiempo determinados y con ello determinando un número y una palabra correspondiente al mismo, así:

Calificación de frecuencias - Análisis de vulnerabilidad		
Valor	**Nivel**	**Casos por año**
1	Improbable	Menos de un caso cada 50 años
2	Remoto	Un caso entre 21 y 50 años
3	Ocasional	Un caso entre 6 y 20 años
4	Moderado	Un caso entre 1 y cinco años
5	Frecuente	Entre 1 y 10 casos al año
6	Constante	Más de 10 casos al año

Tabla 10.
Fuente: propia

Para el caso de la calificación de las consecuencias o impacto, a partir de los factores de vulnerabilidad tenidos en cuenta y que para la presente cartilla se presentan los propuestos por Cesar Duque, como son, el factor humano, ambiental, operacional, económico, de imagen, de mercado y de información. Al igual que el anterior se clasifica es una escala de gradación de menor a mayor, tanto cuantitativa como cualitativa, teniendo en cuenta que la escala numérica es incremental, con el fin de darle mayor importancia y peso a las consecuencias o impacto en el momento de realizar la calificación del riesgo.

Calificación de consecuencias humanas		
Valor	Nivel	Casos por año
1	Insignificante	Sin lesiones
2	Marginal	Lesiones leves sin incapacidad
5	Grave	Lesiones leves incapacitantes
10	Crítico	Víctima grave hospitalizada
20	Desastroso	Varias víctimas graves, un muerto
50	Catastrófico	Varios muertos

Calificación de consecuencias ambientales		
Valor	Nivel	Casos por año
1	Insignificante	Sin contaminación
2	Marginal	Contaminación leve recuperable
5	Grave	Contaminación leve no recuperable
10	Crítico	Contaminación grave recuperable a mediano plazo
20	Desastroso	Contaminación graves recuperable a largo plazo
50	Catastrófico	Contaminación grave no recuperable

Calificación de consecuencias operacionales		
Valor	Nivel	Casos por año
1	Insignificante	Suspensión menor a 8 horas
2	Marginal	Suspensión entre 8 horas y 1 día
5	Grave	Suspensión entre 2 y 5 días
10	Crítico	Suspensión entre 6 y 15 días
20	Desastroso	Suspensión entre 16 y 30 días
50	Catastrófico	Suspensión mayor a 30 días

Calificación de consecuencias económicas		
Valor	Nivel	Casos por año
1	Insignificante	Menor a USD 10.000
2	Marginal	Entre USD 10.000 y USD 100.000
5	Grave	Entre USD 100.000 y USD 500.000
10	Crítico	Entre USD 500.000 y USD 2.000.000
20	Desastroso	Entre USD 2.000.000 y USD 5.000.000
50	Catastrófico	Más de USD 5.000.000

Calificación de consecuencias de imagen		
Valor	Nivel	Casos por año
1	Insignificante	Sólo es de conocimiento dentro de departamento o sección
2	Marginal	Sólo es de conocimiento dentro de la organización
5	Grave	De conocimiento externo a nivel local
10	Crítico	De conocimiento externo a nivel regional
20	Desastroso	De conocimiento externo a nivel nacional
50	Catastrófico	De conocimiento externo a nivel internacional

Calificación de consecuencias de mercado		
Valor	Nivel	Casos por año
1	Insignificante	Pérdida no mayor al 0.1% del mercado
2	Marginal	Pérdida entre el 0.1% y 0.5% del mercado
5	Grave	Pérdida entre el 0.5% y 2% del mercado
10	Crítico	Pérdida entre el 2% y 5% del mercado
20	Desastroso	Pérdida entre el 5% y 10% del mercado
50	Catastrófico	Pérdida mayor al 10% del mercado

Calificación de consecuencias en la información		
Valor	Nivel	Casos por año
1	Insignificante	Pérdida hasta el 10% de información no crítica
2	Marginal	Pérdida entre el 10% y 30% de información no crítica
5	Grave	Pérdida de más del 30% de información no crítica
10	Crítico	Pérdida hasta el 10% de información crítica
20	Desastroso	Pérdida entre el 10% y 30% de información crítica
50	Catastrófico	Pérdida de más del 30% de información crítica

Tabla 11.
Fuente: Mejía, (2006)

La etapa de calificación del riesgo se realiza cuando se tiene en cuenta la tabla de frecuencia o probabilidad y esta se contrasta con cualquiera de las tablas que se considere para el trabajo de los factores de vulnerabilidad, los cuales están debidamente gradados en una tabla de calificación de consecuencias.

Evaluación de riesgo (método)

Método Matriz de análisis de vulnerabilidad – Evaluación de Riesgos

En esta sección de la cartilla y continuando con el desarrollo del método matriz de análisis de vulnerabilidad, se trabajará en las matrices de riesgo, de vulnerabilidad, de criterios y nivel de aceptabilidad del riesgo y de la matriz de aceptabilidad, con esta última de realiza la evaluación de los riesgos calificados anteriormente.

La matriz de riesgo se construye a partir de la gradación trabajada en el capítulo anterior donde se cruzan las variables frecuencia o probabilidad y consecuencias o impacto, su ubicación en la matriz empleando la estructura de un plano cartesiano, van de menor a mayor desde el punto cero en el vértice donde se cruzan el eje de las abscisas (las X o la horizontal) y el eje de las ordenadas (las Y o la vertical).

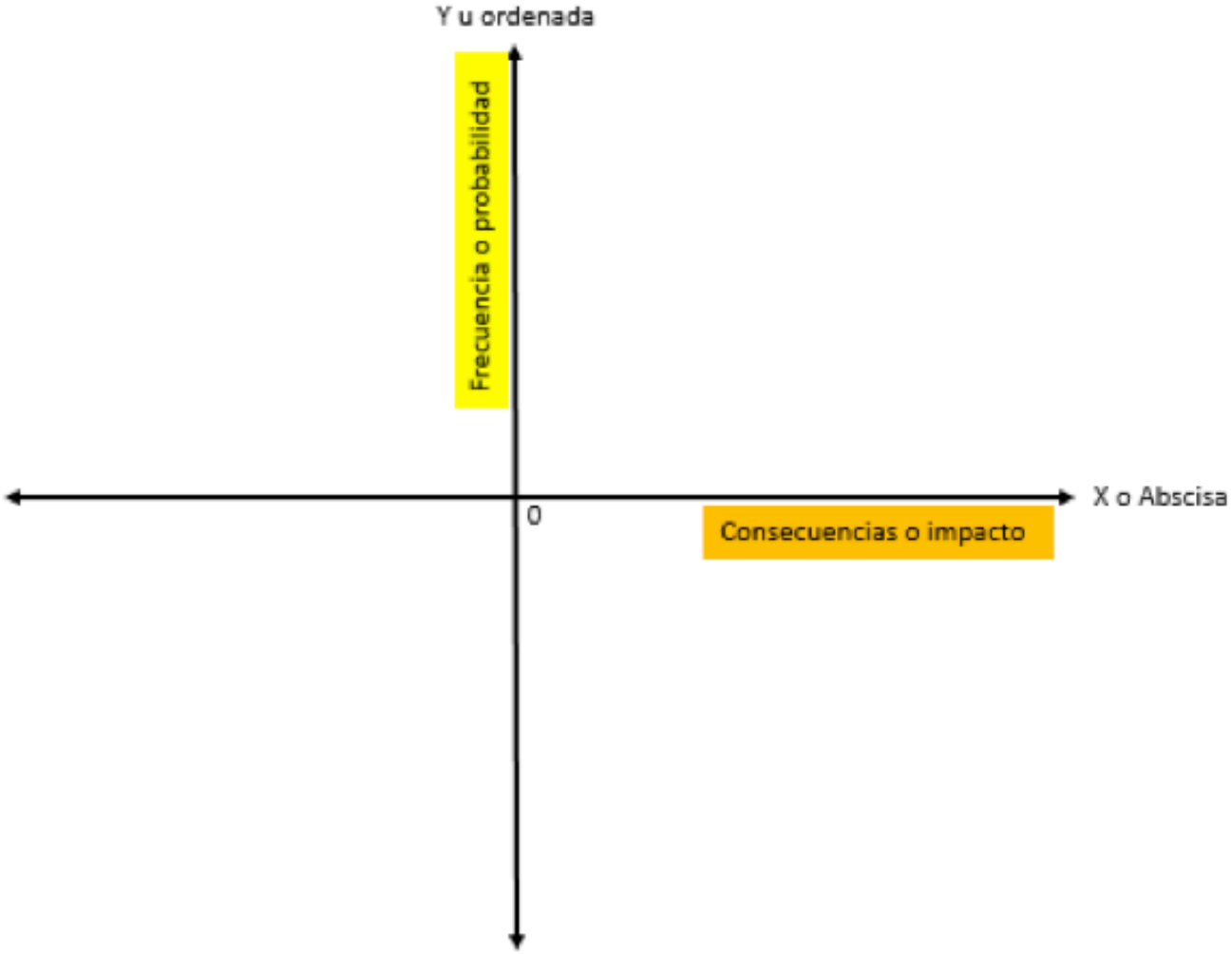


Figura 3.
Fuente: Castañeda, (2016)

Una vez se han colocado en la columna la frecuencia y en la fila las consecuencias, tanto de manera cuantitativa como cualitativa, de menor a mayor los valores de las celdas restantes se determinan multiplicando el valor de la frecuencia por el valor de la consecuencia, como se grafica a continuación en el cuadro matriz de riesgos, este modelo es susceptible de modificar, el autor César Duque fijó unos valores, los cuales pueden ser modificados, para este caso el máximo valor es de 300 en la matriz, en la frecuencia es de 6 y en la consecuencia es de 50.

Frecuencia	Constante	6	12	30	60	120	300
	Frecuente	5	10	25	50	100	250
	Moderado	4	8	20	40	80	200
	Ocasional	3	6	15	30	60	150
	Remoto	2	4	10	20	40	100
	Improbable	1	2	5	10	20	50
Matriz de riesgo		Insignificante	Marginal	Grave	Crítico	Desastroso	Catastrófico
		Consecuencia					

Tabla 12.
Fuente: Castañeda, (2016)

La matriz de vulnerabilidad se construye a partir de los valores obtenidos en la matriz de riesgo, esta se expresa en términos porcentuales, los cuales se obtienen mediante una regla de tres simple, es decir que, si el máximo valor que es de 300 corresponde al 100 del máximo valor en la matriz de riesgos, el resultado de las demás casillas será el de multiplicar el número de la casilla por 100 y dividirlo por 300, un ejemplo para la casilla con el número 1 es:

$$1*100/300 = 0{,}3\%$$

Ese valor en términos relativos permite tener la matriz con porcentajes con base a la gradación del riesgo de acuerdo a su consideración, su resultado permite medir la vulnerabilidad para la empresa, siendo mayor a medida que aumenta el porcentaje.

Frecuencia	Constante	2,0%	4,0%	10,0%	20,0%	40,0%	100,0%
	Frecuente	1,7%	3,3%	8,3%	16,7%	33,3%	83,3%
	Moderado	1,3%	2,7%	6,7%	13,3%	26,7%	66,7%
	Ocasional	1,0%	2,0%	5,0%	10,0%	20,0%	50,0%
	Remoto	0,7%	1,3%	3,3%	6,7%	13,3%	33,3%
	Improbable	0,3%	0,7%	1,7%	3,3%	6,7%	16,7%
Matriz de vulnerabilidad		Insignificante	Marginal	Grave	Crítico	Desastroso	Catastrófico
		Consecuencia					

Tabla 13.
Fuente: Castañeda, (2016)

En el desarrollo de la evaluación del riesgo es muy importante definir los niveles de aceptación del riesgo que tiene la empresa, los cuales determinan con base a sus fortalezas y capacidades para soportarlos, el siguiente cuadro da un referente, sin embargo, cada organización lo puede adaptar a su situación particular.

En el ejemplo se establecieron cuatro zonas de aceptabilidad con un umbral de vulnerabilidad que las define, estas son:

- Zona aceptable: los riesgos ubicados en esta por su frecuencia e impacto no requieren ser intervenidos, ni tratados.

- Zona tolerable: son riesgos que requieren intervención y tratamiento, pero en una escala secundaria, adoptando medidas que se pueden proyectar a mediano plazo.

- Zona inaceptable: en este nivel la intervención y tratamiento demanda una escala primaria con medidas para su manejo a corto plazo.

- Zona inadmisible: en esta zona el riesgo reviste una alta importancia y por ello debe ser intervenido y tratado de manera urgente y prioritaria, ya que por su evaluación reviste un peligro inminente.

El cuadro grafica de los porcentajes de vulnerabilidad considerados por el autor Cesar Duque;

Criterios o niveles de aceptabilidad del riesgo	
Criterio o Nivel	**Rango**
Aceptable	Vulnerabilidad hasta el 3%
Tolerable	Vulnerabilidad del 3,1% al 5%
Inaceptable	Vulnerabilidad del 5,1% al 30%
Inadmisible	Vulnerabilidad mayor al 30%

Tabla 14.
Fuente: Duque, (1999)

La matriz de aceptabilidad grafica los criterios y niveles de aceptabilidad con base a los porcentajes establecidos en la matriz de criterios o niveles de aceptabilidad del riesgo, para ello se debe tener en cuenta también la matriz de vulnerabilidad, allí se califican los porcentajes para facilitar el trabajo del equipo evaluador, así:

Frecuencia	Constante	Aceptable	Tolerable	Inaceptable	Inaceptable	Inadmisible	Inadmisible
	Frecuente	Aceptable	Tolerable	Inaceptable	Inaceptable	Inadmisible	Inadmisible
	Moderado	Aceptable	Aceptable	Inaceptable	Inaceptable	Inaceptable	Inadmisible
	Ocasional	Aceptable	Aceptable	Tolerable	Inaceptable	Inaceptable	Inadmisible
	Remoto	Aceptable	Aceptable	Tolerable	Inaceptable	Inaceptable	Inadmisible
	Improbable	Aceptable	Aceptable	Aceptable	Tolerable	Inaceptable	Inaceptable
Matriz de aceptabilidad		Insignificante	Marginal	Grave	Crítico	Desastroso	Catastrófico
		Consecuencia					

Tabla 15.
Fuente: Castañeda, (2016)

La matriz de aceptabilidad permite apreciar la ubicación de los riesgos calificados y se define con base al criterio o nivel de aceptabilidad su tratamiento, dependiendo la casilla y zona donde quede ubicado, estableciéndose un perfil de riesgos.

En el siguiente cuadro se sitúan siete escenarios de riesgos con base a su calificación tanto por la frecuencia o probabilidad y también por la consecuencia o impacto, los códigos con los cuales fueron nombrados es A1, A2, A3, B1, B2, C1 y C2, para el caso del escenario de riesgo A1 su ubicación por la calificación es que su manifestación con base a la frecuencia o probabilidad es "Frecuente" y con base a la consecuencia o impacto es "Insignificante", por ello al graficarlo se ubica en la zona de color verde que es la que está determinada como un criterio o nivel de aceptabilidad del riesgo "Aceptable" y que por consiguiente como se mencionó anteriormente "no requieren ser intervenidos, ni tratados", por otra parte el escenario C1 está ubicado en la zona de inaceptable por ello "en este nivel la intervención y tratamiento demanda una escala primaria con medidas para su manejo a corto plazo".

Frecuencia	Constante						
	Frecuente	A1	B2				
	Moderado		A2		B1		
	Ocasional					C1	
	Remoto	A3					
	Improbable		C2				
		Insignificante	Marginal	Grave	Crítico	Desastroso	Catastrófico
		Consecuencia					
Aceptable							
Tolerable							
Inaceptable							
Inadmisible							

Tabla 16.
Fuente: Castañeda, (2016)

Tratamiento del riesgo (medidas)

Existen varias clasificaciones de las medidas para el tratamiento del riesgo, en el presente documento se tendrá en cuenta la taxonomía propuesta en la ISO 31000, donde convergen prácticamente todas las medidas de tratamiento del riesgo, el cual se puede valorar desde dos perspectivas como un control y/o como una actividad de financiamiento de las consecuencias o impacto de la materialización del riesgo, como se mencionó en el eje 2.

Las medidas de tratamiento del riesgo no necesariamente son mutuamente excluyentes y tampoco se ajustan a todos los casos, en el presente documento se tendrán en cuenta las medidas como evitar, aceptar, anticipar, proteger, transferir y retener.

Medidas

En todo caso las medidas que se tomen para tratar el riesgo son producto de la gestión del riesgo donde se tiene identificado los riesgos y con ello se tienen definidas políticas, normatividad, controles, procesos y procedimientos orientados a que el riesgo no se materialice o que de llegar a hacerlo los costos sean mínimos.

Evitar

Para evitar un riesgo se debe garantizar desde la probabilidad de que no ocurra o con frecuencia cero de ocurrencia o que desde la consecuencia o impacto sea nulo el daño.

Para eliminar la probabilidad o frecuencia se debe suprimir la acción o actividad que representa el riesgo o dado el caso ubicar fuera de la órbita de alcance del mismo los recursos amenazados, para anular el daño producto del impacto o consecuencias muchas veces las acciones que se deben tomar son tan amplias y extremas que sus costos las hacen poco inviables.

Para evitar un riesgo se puede manjar desde dos opciones:

Evitar	
No hacer	Dejar de hacer
Es decir no emprender la actividad por ser inviable desde lo económico, lo financiero, lo comercial, etc.	Cuando el ejercicio de la organización es poco rentable o inseguro.

Tabla 17.
Fuente: Castañeda, (2016)

También se puede reubicar el negocio, reconfigurar una estrategia, sustituir un producto o rediseñar un procedimiento, en todas las consideraciones anteriores hay que reconsiderar la actividad inicial con base a la probabilidad y al impacto para generar nuevas ideas que eviten o minimicen a cero o cercano a cero la exposición a la amenaza que configura el riesgo.

Aceptar, tomar o incrementar (riesgo calculado)

Cuando en la evaluación del riesgo su probabilidad de ocurrencia o la intensidad de su impacto se conocen y se sabe que aceptar el riesgo no pondrá a la organización en una eventual desestabilización, se opta previo aval del equipo de gestión del riesgo, siendo un riesgo calculado, es decir, que se tiene bajo control y aun así no es representativo, sin embargo, se debe estar monitoreando constantemente para evitar que se reconfigure ante los constantes cambios del entorno tanto interno como externo.

Los costos de la materialización de un riesgo aceptado, normalmente son asumidos por la empresa con sus recursos propios.

Anticipar o prevenir

Es estar delante de la manifestación de una situación de riesgo manifiesto, se requiere anticiparse con actividades que limiten la ocurrencia del evento de riesgo o su impacto sea de poca consideración y afectación.

Figura 4.
Fuente: Shutterstock/654409159

Normas y políticas de seguridad

Desarrollar normas y políticas tendientes a sensibilizar a la organización frente a la identificación y prevención de riesgos es vital con el fin de reducir la probabilidad o frecuencia de manifestación del mismo. Cuando todos los miembros de la empresa conocen los protocolos y los aplican de manera importante se disminuyen los escenarios de riesgo.

Capacitación

Muchos accidentes y daños se presentan por falta de capacitación y entrenamiento en los procesos, el desconocimiento es un aspecto proclive a generar actividades inseguras, la inversión que hace la organización en capacitación y entrenamiento es vital para garantizar la integridad de los recursos y el capital humano.

Sistemas de información

Para poder hacer una verdadera gestión del riesgo se requiere de información disponible de calidad y de oportunidad, normalmente las situaciones inseguras se da ante la ausencia de información, por ello la inversión en sistemas de información y procesos de registro y trazabilidad de actividades de manera sistemática, a los sistemas de información se suman entidades dedicadas al suministro de información especializada de temas de interés para las organizaciones, la suma de un sistema de registro amplio y el empleo de datos exógenos permite tomar decisiones con un alto nivel de precisión.

Chequeo, inspección y pruebas de vulnerabilidad

Los listados de chequeo antes, durante y después de un proceso, las revistas de inspección a procesos y áreas de trabajo y el desarrollo de pruebas de vulnerabilidad de documentos, de personal, de instalaciones, de recursos informáticos, etc., permiten disminuir y a la vez desestimular la probabilidad de que se dé una situación de riesgo.

Diversificar el negocio

"No poner todos los huevos en la misma canasta", en un negocio es sano que se hagan inversiones por separado, es decir, que se tenga otros proyectos o inversiones de capital en otras compañías sean propias o no, es buscar la rentabilidad de cada una y no la integración de sus actividades fin de evitar que, si se produce un siniestro, este afecte una parte de la organización y no toda la operación.

Compartimentación

En una organización de acuerdo al cargo, la persona que se desempeña en el mismo debe conocer la información que le corresponde por su rol, no toda la información es pertinente para todo el mundo, la información a nivel gerente es mucho más profunda, completa e importante, mientras a nivel del trabajador se debe circunscribir a su rol como

operario, obrero, etc., Este aspecto garantiza que aquellas cosas que solo debe saber el equipo directivo tenga un nivel de reserva que permita mantener los asuntos propios de la organización, lejos de la competencia o de personas que pueden emplearla para realizar acciones contra la organización para afectar su estabilidad.

Descentralización

La funciones o actividades que por su nivel de decisión de la empresa son claves, se deben distribuir entre varias personas, a fin de evitar una excesiva concentración de poder y de toma de decisiones en una sola persona, aspecto que puede generar corrupción, errores, fraude, demoras, etc.

Otra modalidad de esta medida es tener aislados aquellos departamentos o secciones de trabajo que, por su nivel de peligrosidad en el desarrollo del proceso empresarial, en caso de materializarse un riesgo podría afectar la integridad de toda la organización, por ello se aconseja tenerlas en otras áreas distantes para evitar una reacción en cadena.

Disminución de la exposición

Aquí la medida busca que si se está realizando una actividad que genera riesgo, se disminuya su frecuencia de ejecución a fin de evitar la probabilidad de materialización del mismo. Un ejemplo es el movimiento de grandes sumas de dinero en horas de poca presencia de autoridades, para disminuir la probabilidad de hurto se debe centrar el movimiento solo en horas donde hay garantía de seguridad por parte de las autoridades.

Mantenimiento Preventivo vs. Correctivo

Mantener y desarrollar una política de mantenimiento preventivo tiene varias ventajas, entre ellas la corrección de fallas y el aumento de la vida útil de los equipos y maquinaria, los chequeos programados bajo los estándares de las casas matrices permiten una garantía de línea de servicio de los equipos y con ello el normal desarrollo de la actividad empresarial que se tiene programada en tiempos de almacenamiento, producción y distribución.

Cosa diferentes sucede cuando se trabaja es para el mantenimiento correctivo, el cual se aplica cuando ya hay daños y fallas en los equipos y maquinaria y se quiere restablecerlos a línea de servicio.

Medicina preventiva

La medida básicamente busca prevenir de manera temprana las enfermedades de tipo profesional, así como los accidentes laborales, su aplicación con políticas y procesos claros ayuda a mantener la integridad y actividad empresarial de manera ininterrumpida y productiva.

Los chequeos médicos, la inspección a puestos de trabajo, la educación y las campañas preventivas, etc., son acciones que multiplican la seguridad y con ello la reducción de escenarios de riesgo que afectan el capital humano.

Proteger

La protección es la acción que se ejecuta en el momento que está latente el riesgo, son todas aquellas medidas que buscan disminuir la intensidad de la materialización del riesgo o la dimensión del impacto negativo en el recurso, por su responsabilidad su aplicación son activas o pasivas, en el caso de las primeras estás dependen de la intervención humana para que se puedan aplicar, mientras que las pasivas se manifiestan como una respuesta a la adopción de una norma establecida, entre otros están:

Equipos de protección de personal (EPP)

Son todos aquellos accesorios, vestimenta y equipos que emplean los trabajadores con el fin de proteger su integridad ante accidentes o para hacer frente a enfermedades de carácter profesional, normalmente estos atuendos se empelan con base a la exposición al riesgo específico, siendo diferentes para cada oficio, pero que de todas formas protegen al trabajador en su integridad corporal.

Sistema de protección automáticos y electrónicos

Son todos aquellos dispositivos automáticos y electrónicos cuya función es la monitorear constantemente el desarrollo de procesos mecánicos, automáticos y/o electrónicos, mediante sensores que alertan cuando algo está funcionando mal y su acción es avisar al encargado del seguimiento o parar el proceso hasta que se haga una inspección correctiva del mismo.

Con el desarrollo de la tecnología, cada vez es más común encontrar dispositivos que alertan en tiempo real de errores en procesos mecanizados, o comandos erróneos en equipos sensibles, su implementación se ha masificado por su facilidad de operación, por lo económico en su instalación y sobre todo por el nivel de protección que brinda reduciendo costos en reparaciones o pérdidas humanas.

Planes de contingencia, de emergencia, de evacuación.

Son todas aquellas previsiones que se adelantan al interior de la organización para dar respuesta a eventos inesperados pero considerados que por su nivel de afectación pueden dañar personas y recursos, por ello es importante tener dispuestos estos planes y sobre todo que los integrantes de la organización los conozcan, los apliquen y tengan claro cuál es responsabilidad en el momento que se manifieste el riesgo. Es responsabilidad de la organización realizar las simulaciones de los mismo y más importante que ello los simulacros, pues es el ejercicio más cercano a los hechos reales y es donde se puede identificar las fallas del plan como tal.

Transferir

En la gestión del riesgo una medida de tratamiento es externalizar el riesgo a través de la participación de un tercero quien asume parcialmente la pérdida ocasionada por el impacto del riesgo, dependiendo de la modalidad de transferencia incluso debe responsabilizarse por la aplicación de los controles para minimizar su impacto.

Normalmente se realiza a través de la contratación de un seguro de manera directa o indirecta, con el fin de garantizar que se pueda financiar el daño que reciba la organización al materializarse el riesgo.

Transferencia a través de cláusulas en contratos

Se realiza cuando expresamente en el clausulado de un contrato queda determinado que el contratante transfiere al contratista la responsabilidad ante la materialización de un riesgo, para ello este último debe constituir una póliza o contratación de un seguro para cubrir la eventual materialización del mismo, como sucede en los contratos de transporte, los contratos de prestación de servicios y la responsabilidad civil extracontractual, etc.

Transferencia a través de contrato de seguros

Se evidencia cuando se contrata con una empresa aseguradora el cubrimiento de un riesgo, se realiza cuando se paga la prima por la póliza solicitada, a partir de allí en el momento que se materialice el riesgo los daños producidos por el mismo en términos económicos son responsabilidad de la aseguradora, la cobertura del riesgo no exime a la organización de realizar sus tareas preventivas y protectivas ante el riesgo, de hecho cuando se produce el daño la aseguradora cubre una parte y la otra la debe asumir la organización o empresa contratante del seguro, cuota que se denomina deducible, el cual está calculado con base al monto del valor del daño.

Cuando la materialización el riesgo es alto por su probabilidad de ocurrencia, normalmente la prima es alta y se incrementa en la medida que sea más frecuente, este factor determina que muchas veces no es rentable para las partes por su alto valor a invertir, cuando se toma la decisión de invertir en un seguros esta debe obedecer a un estudio serio ya que se puede incurrir en excesos o déficit de la cobertura contratada, haciendo gastos innecesarios o dejando de cubrir aspectos determinantes que a postre pueden dañar seriamente la organización o la empresa.

Existen varias opciones o tipos de seguros, a continuación, se relacionan en tres grupos los más comunes en el ámbito de seguros:

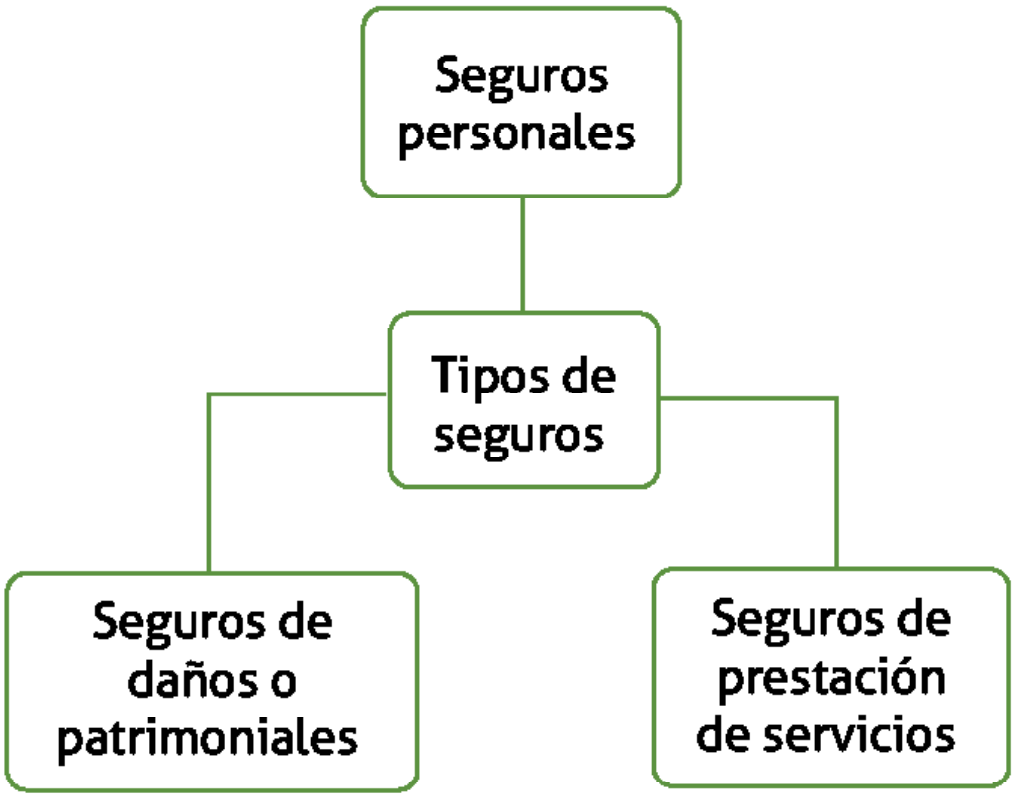


Figura 5.
Fuente: Castañeda, (2016)

Retener

La diferencia entre aceptar y retener el riesgo es que en la primera no se cuenta con medidas para enfrentar las pérdidas producto de los daños por el impacto del riesgo, en la retención del riesgo se afrontan las consecuencias de manera planeada.

Constitución fondo de riesgo

La empresa u organización tiene un fondo constituido para afrontar pérdidas o daños por la materialización de riesgos, se realiza cuando se prevén las pérdidas y su correspondiente amortización.

Presupuesto cobertura riesgos

Se incluye en el presupuesto de la organización o empresa, una suma de recursos monetarios destinados a cubrir pérdidas por efecto de riesgos y su impacto.

Línea de crédito para riesgos

Trámite ante la banca, para poder obtener un cupo crediticio que pueda cubrir eventuales pérdidas en la operación empresarial por riesgos materializados, se cuenta con una opción inmediata para cubrir estos gastos y evitar que se pueda detener la actividad empresarial.

Combinación retención y transferencia de riesgos

En esta medida la organización retiene una parte del riesgo y la otra la transfiere mediante un contrato de seguros, se realiza cuando las tres anteriores no alcanzan para cubrir eventuales daños producto de riesgos materializados.

Empresas de seguros "cautivas"

Son aquellas empresas u organizaciones que debido a su gran tamaño se convierten en sus propias aseguradoras para trabajar el capital que invierte en la compra de seguros, la ventaja es que estás a su vez emplean el seguro o reaseguro donde son las reaseguradoras las que responden por los montos que se aseguren.

Matriz de respuesta ante la materialización de riesgos

Para enfocar el empleo de las medidas para el tratamiento del riesgo se sugiere como orientación la siguiente matriz:

Frecuencia o probabilidad	**Constante**	Aceptable (2,0%) (AC)	Tolerable (4,0%) (AN, RE)	Inaceptable (10,0%) (AN, PR, TR)	Inaceptable (20,0%) (AN, PR, TR)	Inadmisible (40%) (AN, PR, TR)	Inadmisible (100,0%) (EV, AN, PR)
	Frecuente	Aceptable (1,7%) (AC)	Tolerable (3,3%) (AN, RE)	Inaceptable (8,3%) (AN, PR, TR)	Inaceptable (16,7%) (AN, PR, TR)	Inadmisible (33,3%) (AN, PR, TR)	Inadmisible (83,3%) (EV, AN, PR)
	Moderado	Aceptable (1,3%) (AC)	Aceptable (2,7%) (AC)	Inaceptable (6,7%) (AN, PR, TR)	Inaceptable (13,3%) (AN, PR, TR)	Inaceptable (26,7%) (AN, PR, TR)	Inadmisible (66,7%) (EV, AN, PR)
	Ocasional	Aceptable (1,0%) (AC)	Aceptable (2,0%) (AC)	Tolerable (5,0%) (AN, PR, RE)	Inaceptable (10,0%) (AN, PR, TR)	Inaceptable (20,0%) (PR, TR)	Inadmisible (50,0%) (AN, PR, TR)
	Remoto	Aceptable (0,7%) (AC)	Aceptable(1,3%) (AC)	Tolerable (3,3%) (AN, PR, RE)	Inaceptable (6,7%) (AN, PR, TR)	Inaceptable (13,3%) (PR, TR)	Inadmisible (33,3%) (AN, PR, TR)
	Improbable	Aceptable (0,3%) (AC)	Aceptable 0,7%) (AC)	Aceptable (1,7%) (AC)	Tolerable (3,3%) (PR, TR)	Inaceptable (6,7%) (PR, TR)	Inaceptable (16,7%) (PR, TR)
Matriz de aceptabilidad		**Insignificante**	**Marginal**	**Grave**	**Crítico**	**Desastroso**	**Catastrófico**
		Consecuencia o impacto					

Tabla 18.
Fuente: Castañeda, (2016)

En ella se establece de acuerdo a los niveles o criterios de aceptabilidad del riesgo, las posibles aplicaciones de las medidas para tratamiento del riesgo, para ello se debe tener en cuenta las siguientes siglas, vista en la unidad 2 en el cuadro "Medidas de control de riesgos".

Instrucción

Apreciado estudiante, con el fin de llevar lo teórico a lo práctico, lo invito a desarrollar la actividad de aprendizaje denominada "Se encoge la fortuna del magnate dueño de Zara de Amancio Ortega", donde se podrán identificar algunos riesgos, valorarlos y proponer un tratamiento. Esta actividad se encuentra disponible en la página principal de este eje.

Evitar	EV	Anticipar o prevenir	AN	Transferir	TR
Aceptar, tomar o incrementar	AC	Proteger	PR	Retener	RE

Tabla 19.
Fuente: Castañeda, (2016)

Una vez se ha realizado el proceso de valoración del riesgo y se decide aplicar el tratamiento al mismo, las decisiones que se tomen van vinculadas a diferentes variables que vas desde lo que oferta el mercado de las aseguradoras en términos de riesgos asegurables hasta los recursos con que se cuenta en la organización para invertir en el pago de primas, todo dentro de los conceptos de la política de aceptación del riesgo y disposición a invertir en su tratamiento.

Lectura recomendada

Apreciado estudiante, en el marco del desarrollo de la prevención y gestión del riesgo, lo invito a realizar la lectura de los estándares de gerencia de riesgos, documento que compila el desarrollo de la gestión del riesgo con un modelo que es coherente con la ISO 31000.

Estándares de gerencia

Ferma (Federation of European Risk Management Associations)

Implementación de políticas y medidas para el tratamiento del riesgo

Para implementar medidas de tratamiento de riesgos, se deben diseñar políticas de gestión del riesgo, aspecto que se logra al cumplir una secuencia que va de lo general a lo particular o método deductivo, el cual inicia desde la alta gerencia, así:

Figura 6.
Fuente: Castañeda, (2016)

Diseño de políticas de gestión del riesgo

Uno de los pivotes de toda organización son las políticas que se estructuran para orientar su derrotero, estos lineamientos generales son determinantes para garantizar que a la hora de la toma de decisiones no se desborden los encargados sobrepasando límites que guardan la integridad de la empresa, las políticas abarcan diferentes campos y aspectos de interés, en este caso es importante que estas políticas orienten de manera clara la gestión del riesgo, con guías generales a todas las áreas de la empresa para que en el desarrollo de estas se estructuren niveles más abajo el detalle de la gestión del riesgo correspondiente de manera específica, las políticas tienen dos momentos, el general enfocado a la gestión del riesgo de manera estratégica y el específico para gestionar los riesgos de manera particular a cada área de la empresa.

Su diseño e implementación corresponde desde la alta dirección a todos los rincones de la organización, pues su efectividad depende de que sean conocidas y acatadas de manera acertada y oportuna, siendo importante la posibilidad de estar actualizándolas cada vez que se requiera pues es claro que el entorno tanto interno como externo es cambiante y con ello la percepción y la presencia de nuevos riesgos o cambios en los escenarios presentes.

Políticas generales de gestión del riesgo

Las políticas generales en la organización deben consideran entre otras las siguientes posturas:

- Debe estructurarse desde la alta dirección una política general clara frente a la gestión del riesgo.
- La política general debe permitir que en cada departamento, sección o área se puedan desarrollar políticas específicas para la valoración y tratamiento del riesgo.
- Se debe establecer las instancias responsables en la gestión del riesgo.
- Deben estar las directrices para documentar el proceso.
- También se debe determinar claramente el ámbito de aplicación.
- Se hará mención a la valoración y tratamiento del riesgo definiendo los parámetros y escalas para su calificación, así como la valoración de la probabilidad e impacto.
- Se definirá las medidas para el tratamiento del riesgo, así como la prioridad de aplicación.
- Un aspecto definitivo que debe estar definido es la prioridad que la organización tendrá para la protección de los recursos y el capital humano.
- Para complementar lo anterior se citan las políticas definidas en la norma ISO 31000 (2009), así:
  - La justificación de la organización para gestionar el riesgo.
  - Los vínculos entre los objetivos y las políticas de la organización y la política para la gestión del riesgo.
  - Las obligaciones y responsabilidades para gestionar el riesgo.
  - La forma de tratar los conflictos de intereses.
  - El compromiso para poner a disposición los recursos necesarios con el fin de ayudar a los responsables de la gestión del riesgo y de rendir cuentas con respecto a ésta.
  - La forma en la cual se va a medir y a reportar el desempeño de la gestión del riesgo.
  - El compromiso para revisar y mejorar periódicamente la política y el marco de la gestión del riesgo y en respuesta a un evento o un cambio en las circunstancia. La política para la gestión del riesgo se debería comunicar de manera adecuada.

Las políticas para gestión del riesgo deben estar asistidas por el grupo de apoyo en la gestión del riesgo, quedando debidamente documentadas para su difusión, deben ser claras, sencillas de entender, así como estar al alcance de todos en la empresa.

Figura 7.
Fuente: Shutterstock/561776362

Políticas específicas de gestión del riesgo

Son todas aquellas normas que adopta la organización para tratar aquellos riesgos que por su probabilidad e impacto pueden considerarse los más peligrosos, puede ser de carácter anticipado o protectivo, buscando de manera continua influir sobre los agentes que generan el riesgo, las causas y el impacto reconocido previamente.

Controles

Son todas aquellas medidas tomadas o diseñadas para detectar y/o reducir un riesgo, de allí que el control tenga tres significados en sí mismo, en primera instancia el control como una medida tomada, tales como una valla de seguridad que tiene un desempeño pasivo o un vigilante armado con un rol activo en el proceso, la segunda consideración es la necesidad de instaurar controles que permitan evidenciar la ocurrencia del riesgo para el cual fue diseñado y por último que estos controles permitan anticipar o proteger como una medida de tratamiento que influye sobre la frecuencia y el impacto de la materialización del riesgo.

Los controles tienen su génesis en el análisis de los riesgos, al establecerlos se logra fortalecer la seguridad de una actividad, como la lista de chequeo que realiza un piloto antes de despegar su aeronave. Los controles contribuyen a detectar desviaciones en los estándares de operación y desempeño, así como de lo planeado contra lo que se está ejecutando.

Características de los controles

Las características que deben tener los controles para que sean efectivos en para detectar y/o reducir los riesgos, deben tener ciertas características en su diseño, a continuación, se relacionan las más representativas.

- Suficiencia necesaria: es decir que la cantidad de controles que se hayan estructurado sean los necesarios, teniendo en cuenta que no se conviertan en un problema pero que tampoco sean tan escasos que no cumplan con su función.

- Alta simplicidad: los controles deben ser claros, simples, flexibles, fácilmente comprensibles, sencillos de implementar, para ello debe haber una capacitación que aporte información a su desarrollo y sus objetivos.

- Económicos: un control en su diseño debe ser estructurado teniendo en cuenta que su costo sea menor que su beneficio, por ello solo de deben implementar para riesgos que realmente sean significativos para la organización.

- Efectivos: es decir que en su diseño se tenga en cuenta que sean eficientes en términos del empleo acertado de recursos y eficaces, o sea que sean capaces de detectar y disminuir los riesgos. Los controles se implementar por un objetivo y si hay varios se debe revisar cuales son efectivos y cuales no cumplen el fin para el cual fueron implantados.

- Oportunos: este aspecto es muy importante, ya que se refiere a la implementación de controles que actúen cuando sea realmente necesario, ni antes ni después, ello permite tomar acciones a tiempo para corregir desviaciones y encausar nuevamente la normalidad de los procesos.

- Embebido en el proceso: es decir que el desarrollo del proceso per se lleve incluido el control, hay controles antes, durante y después, pero lo recomendable es que sean antes y durante, ya que después es una condición pasada que por su condición extemporánea ya no permite un proceso preventivo sino correctivo.

Tipos de controles

Existen varios tipos de clasificación, tal vez la clasificación más reconocida es la auditoria de sistemas que abarca cuatro controles que se dan el antes, el durante y el después del proceso

- Control anticipado (AN): se constituye en el primer anillo de seguridad, su función es disminuir el riesgo actuando sobre la causa y los agentes que lo generan, reduciendo la frecuencia con que pueden ocurrir. Un ejemplo es un letrero preventivo "Piso húmedo", que avisa la presencia de un riesgo.

- Control detectivo (DE): es el segundo anillo de seguridad, se activa cuando se produce una situación fuera de lo normal o que no había sido prevista, normalmente se genera en la supervisión y trazabilidad de un proceso. Un ejemplo son los registros en las ordenes e ingresos en la intranet de una organización, que permiten seguir la trazabilidad de quienes han ingresado, modificado o borrado datos.

- Control protectivo (PR): es el tercer anillo, su función es actuar de manera inmediata para que una vez se ha detectado el riesgo se pueda proceder a neutralizar o disminuir el impacto del mismo en su materialización, todo con el ánimo de proteger los recursos de la organización. Un ejemplo siguiendo con el caso anterior es bloqueo inmediato del acceso a la intranet de una persona mediante el cambio de usuario y claves para evitar que se siga afectando los datos del sistema sea por modificación, ingreso o borrado de los mismos.

- Control correctivo (CO): es el último anillo de seguridad y se constituye en las acciones que la organización adopte para corregir los escenarios de riesgo que se presentaron en la deviación del proceso y con ello se pueda prevenir futuros eventos similares. En esta fase se deben mejorar los controles ya que se requiere un estudio de la situación y un reproceso que consecuentemente genera costos adicionales. Un ejemplo es la corrección en la intranet de los permisos que tienen los usuarios y su accesibilidad a manipular datos que son claves en la organización.

Algunos controles por su diseño pueden abarcar varios tipos, como por ejemplo el servicio de vigilancia humana sobre un recurso:

Control	Tipos de control que puede y deben ejecutar
	Anticipado o preventivo: por su presencia y vigilancia es un factor disuasivo reduciendo con ello la probabilidad de que ocurra un robo.
	Detectivo: ya que debido a su función de vigilancia puede detectar la materialización del riesgo.
	Protección: este control se pone en ejecución cuando el vigilante detecta el robo y actúa para neutralizar o disminuir el impacto del mismo.

Tabla 20.
Fuente: Castañeda, (2016)

En el siguiente cuadro se grafican varios tipos de controles con base a su clasificación.

No.	Control	Tipo de controles			
		AN	DE	PR	CO
1	Acceso limitado	X			
2	Auditoría integral		X		
4	Plan de siniestro			X	
5	Renovación de protocolos				X
6	Servicio de vigilancia humana	X	X	X	

Tabla 21.
Fuente: Castañeda, (2016)

Existen otros tipos de controles que se emplean y que van de acuerdo con la actividad y los recursos con que cuenta la organización tales como:

- Control manual y/o automático.
- Control discrecional y/o no discrecional.
- Control obligatorio o voluntario.
- Control de aplicación.
- Control general.

Análisis de la efectividad de un control

Todo control debe ser analizado desde la efectividad del mismo, teniendo en cuenta la eficiencia y la eficacia que existe en su implementación para la gestión del riesgo, la eficacia se mide en términos de la reducción del riesgo y la eficiencia que se circunscribe a los recursos invertidos para su implementación, y su comparación con los costos de los beneficios obtenidos por su funcionamiento.

Un ejemplo de la efectividad de un control se obtiene calculando a partir de su implementación, que efecto tiene en la disminución de la calificación del riesgo. En una empresa de que vende láminas de tablex, existe el riesgo de error y generar grandes cantidades de desperdicio de material al cortarlo, el error de corte se ha calificado con una frecuencia de 5 es decir que es Frecuente y con un impacto de 5, es decir Grave, pero debido a que en muchas veces el cliente es quien sugiere el corte, por ello no impacta a la empresa, la calificación que resulta de multiplicar la Frecuencia 5 por el Impacto 5, da como resultado 25, en la matriz de aceptabilidad en los criterios o niveles establecidos se determina que es un riesgo Inaceptable, por ello se debe tratar y para controlarlo tanto por su frecuencia como por su impacto, se consulta la matriz de actividades o respuestas ante un riesgo, la cual recomienda que se puede implementar un control Anticipativo o Preventivo y/o un control Protectivo o un control de transferencia del riesgo, en el caso se puede implementar uno o dos o hasta los tres o dado el caso y el estudio del mismo inclusive se pude optar por implementar otro tipo de control.

Para el caso de referencia se optó por diseñar un control Anticipativo o Preventivo que disminuya la frecuencia y el impacto permitiendo llevar el riesgo al área de aceptable, se propone desarrollar o adquirir un software que permita mediante el suministro de las medidas de corte y la dirección de la veta de la madera, para el mismo genere de manera automatizada una propuesta donde sea mínimo el desperdicio, favoreciendo a los cliente y a la vez evitando problemas con los mismo por los errores en el corte en el sentido de generar mucho desperdicio. Al implementar el corte se disminuirá ostensiblemente la frecuencia del error y también el impacto en el cliente, siendo la calificación de la frecuencia después del control, de 2, es decir Remoto y del impacto de 2 o Marginal, con ello

al multiplicar la Frecuencia por el Impacto el nuevo valor de la calificación del riesgo es de 4, al consultar la matriz de aceptabilidad, de manera cualitativa este riesgo se ubica en la Zona de "Aceptable", por ello no requiere tratamiento ni intervención.

La conclusión es que la implementación del control es muy efectiva porque reduce tanto la frecuencia como el impacto.

En la efectividad de un control se estiman los beneficios calculando los efectos que podría tener la materialización del riesgo, tales como:

- Pérdidas humanas.
- Pérdidas económicas.
- Pérdidas de información.
- Pérdidas de bienes de capital.
- Daños medioambientales.
- Daño a la imagen corporativa.
- Pérdida de mercado.
- Interrupción de la producción y/o distribución.
- Etc.

A partir de la evaluación se puede estimar hasta donde la organización está dispuesta a aceptar el riesgo o a tratarlo para minimizar su daño en la misma.

En la evaluación de la efectividad de los controles se puede emplear la siguiente matriz que permite tener una perspectiva de la misma, así:

En el manejo de la matriz se pueden dar varios escenarios que permiten evaluar el control.

Eficacia	Alta	Media	Alta	Muy alta
	Media	Baja	Media	Alta
	Baja	Muy baja	Baja	Media
Matriz de efectividad de controles		Baja	Media	Alta
		Eficiencia		

Tabla 22.
Fuente: Duque, (1999)

Por ejemplo, si la eficacia es baja y la eficiencia también es muy baja, la efectividad del control es muy baja, en sentido inverso si la eficacia y la eficiencia son altas la efectividad del control es muy alta.

Para los escenarios donde el control en su evaluación es muy bajo o bajo, se debe replantear el control buscándose uno de mayor efectividad, cuando la efectividad sea calificada como media, se debe realizar un estudio más profundo del control en términos de costo o eficiencia para revisar si es factible que se aplique o se siga aplicando, finalmente para los escenarios de alto o muy alto, se considera que el control cumple con su diseño y objetivo para contribuir de manera efectiva a la gestión del riesgo.

En esta etapa finaliza el presente referente de pensamiento, donde se abordó el concepto de la valoración del riesgo, como un recurso estratégico en la gestión del riesgo que un gerente actual deberá tener en cuenta si quiere mantenerse vigente y competitivo en el escenario comercial.

Como se ha observado a lo largo del módulo, no se puede pensar en acciones aisladas frente a la administración y gestión del riesgo, todo está concatenado, la actuación de la alta gerencia y todos los miembros de la organización deben estar cohesionados en un concepto sinérgico a fin de poder implantar las medidas para el tratamiento de los riesgos y con ello minimizar su impacto y materialización frente a los objetivos que tiene la empresa.

Instrucción

Con el fin de cerrar el presente referente le invitamos a realizar la actividad evaluativa de carácter individual. Disponible en la sección de tareas de la plataforma.

BIBLIOGRAFÍA

Asociación Española de Gerencia de Riesgos y Seguros (Agers). (2011). Trabajo ISO 31000. España.

Business Alliance for Secure Commerce. (s.f.). Lista de chequeo pólizas de seguros. Recuperado de http://www.bascbogota.com/es/material_curso/CHEQUEO%20POLIZA%20DE%20SEGUROS.xls

Centra Hidroeléctrica de Lorena. (2010). Normas de seguridad operacionales. Recuperado en http://www.asep.gob.pa/electric/PADE_LORENA/Anexo%20C%20-%20NORMAS%20DE%20SEGURIDAD%20OPERACIONALES.pdf

Duque, C., et ál. (1999). Seminario taller gestión integral de riesgos organizacionales. Bogotá, Colombia.

Icontec. (2009). NTC – ISO 31000. Bogotá. Colombia: Instituto Colombiano de Normas Técnicas y Certificación.

Mapfre. (1998). Libro gerencia de riesgos y seguros en la empresa. España: Mapfre.

Mejía, C. (2006). Administración de riesgos. Un enfoque empresarial. Colombia: Fondo Editorial Universidad Eafit.