Superintendencia de Sociedades

ADMINISTRACION DE RIESGOS INSTITUCIONALES

1 Objetivo, Definiciones y Marco General

1.1 Objetivo

Definición de una metodología de trabajo para el Sistema de Gestión de Riesgos en la Superintendencia de Sociedades con el uso de herramientas automatizadas.

1.2 Responsables

La aplicación de esta guía está dirigida para todos los líderes de los Procesos de la entidad.

1.3 Alcance

La aplicación de esta guía involucra todos los procesos de la entidad y aquellos enfoques que involucren la identificación, medición, valoración, tratamiento y seguimiento de riesgos independientemente si es para un proceso, proyecto, plan, o actividad. Este documento se ha basado en las recomendaciones emitidas por estándares como ISO 31000, AS/NZS 4360, ISO 27005, entre otros.

1.4 Glosario de Términos

A continuación se describen los términos utilizados en ésta guía.

- **Aceptación del riesgo**

Es la decisión informada de aceptar las consecuencias y la probabilidad de un riesgo particular.

- **Administración del riesgo**

La cultura, los procesos y las estructuras que están dirigidas hacia una efectiva administración de potenciales oportunidades y efectos adversos.

- **Análisis del riesgo**

Proceso sistemático para entender la naturaleza del riesgo y deducir su nivel de riesgo.

- **Amenaza o causa**

Fuente de daño potencial o situación potencial para causar daño.

- **Consecuencia**

El resultado de un evento expresado en forma cualitativa o cuantitativa, que genera pérdida, daño, desventaja o ganancia. Estos pueden ser un rango de posibles resultados asociados con el evento. En algunos escenarios también se conoce como Impacto.

- **Control del Riesgo**

Se refiere a la parte de la administración de riesgo, que involucra la implantación de políticas, estándares, procedimientos y cambios físicos para eliminar o minimizar los riesgos adversos.

- **ERA**

Aplicativo utilizado en la entidad para la gestión y auditoría de riesgo. Las siglas en Ingles son “Enterprise Risk Assessor”**.**

Herramienta de Gestión de Riesgos, Auditoria, entre otros, que permite almacenar, mantener, gestionar, consultar y documentar sobre una base de datos toda la información relacionada con los riesgos, los activos de información, las amenazas, las vulnerabilidades, los objetivos, los responsables y generar mediciones y reportes al respecto. También puede ser accesada viá WEB generando mayor movilidad.

- **Evaluación del riesgo**

El conjunto de procesos para identificar el riesgo, analizar el riesgo y valorar el riesgo.

- **Evento**

Un incidente o suceso, el cual ocurre en un determinado lugar durante un determinado intervalo de tiempo.

- **Identificación del riesgo**

Proceso para determinar el QUE, POR QUE, COMO, CUANDO y DONDE puede suceder un evento de riesgo.

- **ISO 31000**

Guía genérica de principios en la Gestión de Riesgos desarrollada por la International Organization for Standardization y publicada el 13 de Noviembre de 2009.

- **Medición del Riesgo**

El proceso por el cual se compara el nivel de riesgo contra los criterios de aceptación del riesgo.

- **Mitigación del Riesgo**

Planeación y ejecución de medidas dirigidas a reducir o disminuir el riesgo.

- **Monitoreo**

Verificar, supervisar, observar o registrar el progreso de una actividad, acción o sistema sobre una base regular, con el fin de identificar cambios.

- **Partes Involucradas**

(Stakeholders - Objetos del riesgo, los que toman el riesgo)

Son las personas y las organizaciones quienes pueden ser afectadas, son afectadas por, o perciben que ellos mismos pueden ser afectados por una decisión o actividad.

- **Pérdida**

Una consecuencia negativa, financiera o de cualquier otra índole.

- **Probabilidad**

Se usa como una descripción cualitativa de la probabilidad o la frecuencia.

La posibilidad que un evento específico o resultado, medido por la rata (probabilidad) de eventos específicos o resultados dentro de un número total de posibles eventos o resultados. La Probabilidad es expresada como un número entre 0 y 1, en donde cero indica que es imposible que el hecho ocurra y 1

indica que el evento es cierto.

- **Proceso de Administración del Riesgo**

La aplicación sistemática de políticas gerenciales, procedimientos y prácticas, en las actividades para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos.

- **Reducción del riesgo**

La aplicación selectiva de técnicas apropiadas y principios gerenciales para reducir la probabilidad de ocurrencia de un evento o sus consecuencias o ambos.

- **Riesgo**

Es la incertidumbre de que un evento suceda.

La posibilidad que algo suceda y que podría tener un impacto sobre los objetivos. Está medido en términos de consecuencias y probabilidad de ocurrencia.

> Nota: El riesgo con frecuencia se especifica en términos de un evento o circunstancia y las consecuencias que pueden derivarse de este. Es medido en términos de la combinación de las consecuencias de un evento y la probabilidad de ocurrencia del mismo, el riesgo puede ser positivo o negativo.

- **Riesgo absoluto (inherente)**

El máximo riesgo sin los efectos mitigantes de los controles (riesgos sin controles).

- **Riesgo residual**

Se refiere al margen o residuo de riesgo que puede darse a pesar de las medidas de tratamiento o mejoramiento tomadas para la administración del riesgo.

- **Transferir el riesgo**

Transferir total o parcialmente la responsabilidad de la provisión para pérdidas a un tercero a través de la ley, contratos, seguros u otro medio. Transferir el riesgo puede también hacer referencia a mover físicamente el riesgo o parte del mismo a otro sitio.

- **Tratamiento del riesgo (Administración del riesgo)**

Seleccionar e implementar las opciones apropiadas para reducir el riesgo.

- **Vulnerabilidad**

Una debilidad de un sujeto o sistema expuesto a una amenaza, correspondiente a su predisposición intrínseca a ser afectado o ser susceptible de sufrir pérdida.
En un sistema puede ser aprovechada para violar el comportamiento deseado del mismo relativo a la protección, seguridad, confiabilidad, confidencialidad, disponibilidad e integridad de la información.

Muestra la fragilidad de un sistema (físico, técnico, organizacional, cultural, etc) que puede ser afectado adversariamente causando daño o perjuicio.

2 Proceso de Gestión de Riesgos

Fases definidas para Superintendencia de Sociedades para la Implementación del Sistema de Gestión de Riesgos de acuerdo a la Guía ISO 31000.

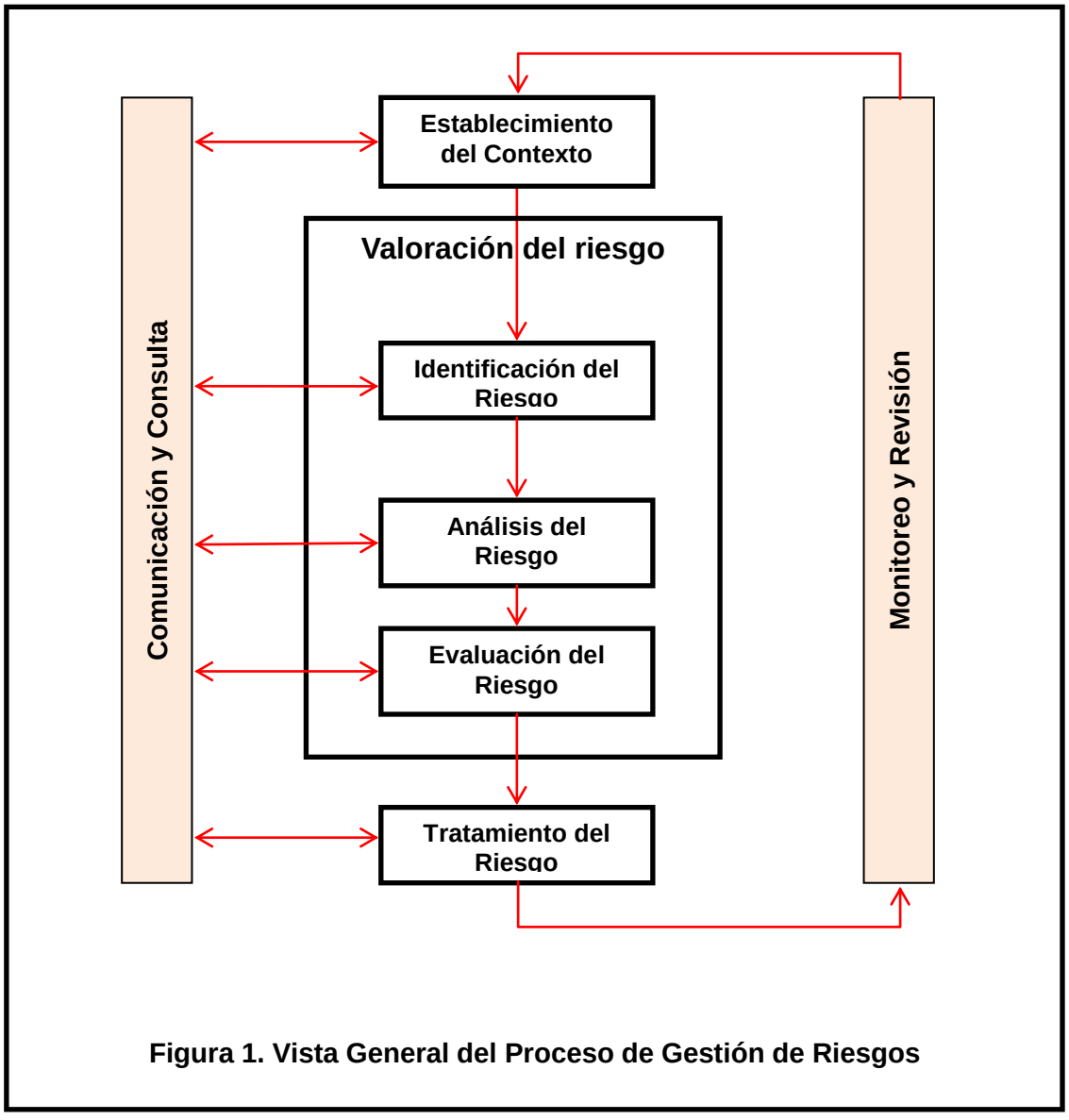


Figura 1. Vista General del Proceso de Gestión de Riesgos

2.1 Comunicación y Consulta

Es necesario que las personas y partes involucradas tanto internas como externas, se mantengan informadas en cada fase del proceso de la gestión de riesgos y que se establezcan los mecanismos de consulta y comunicación con el fin de mantener informados y al día este proceso.

Para tal efecto se publicaran la Intranet de la Entidad.

2.2 Establecer el Contexto

En esta fase se establece el contexto y se define claramente el alcance del trabajo a desarrollar. Este alcance especifica el proceso / área / proyecto / servicio de TI / o del negocio que se contemplará para implementar la gestión de riesgos.

El contexto externo es determinar el alcance organizacional y de administración de riesgos en el cual tendrá lugar el resto del proceso.

2.2.1 Conocimiento de la Organización y/o Proceso / Área / Servicio / Producto / Proyecto a Evaluar

Dependiendo del contexto definido, el responsable deberá conocer los aspectos más relevantes de la Entidad, el proceso / área / proyecto / servicio de TI / o del negocio a la cual se le desarrollará el proceso de Gestión de Riesgos. Entre otros podrían contener lo siguiente:

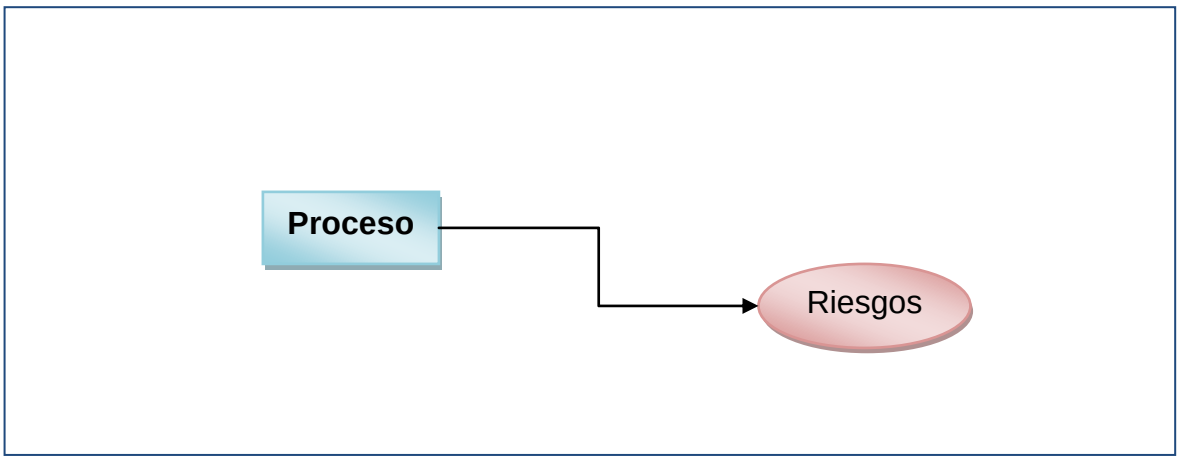
- Misión, visión y objetivos de la organización.
- Objetivos del proceso / área / producto / servicio / proyecto.
- Caracterización del proceso / área / servicio / producto / proyecto y responsable(s)
- Normatividad vigente.

2.2.2 Estructura del Proceso / Área / Servicio / Producto / Proyecto

Para iniciar el trabajo de implementación del proceso de Gestión de riesgos es de gran importancia la estructura de áreas / procesos / servicios / productos / proyectos que se defina. Al especificar la misma, tenga en consideración los siguientes aspectos:

- Definir la estructura a niveles superiores. No es conveniente llegar a un nivel de detalle de muy bajo nivel.
- Los niveles más bajos se usan como referencia para identificar las posibles causas de los riesgos.

Un ejemplo de esta estructura se muestra a continuación en el caso de procesos del negocio:



En este esquema, la identificación de riesgos se haría a nivel de los procesos y los resultados de las evaluaciones de riesgo, tratamientos y planes de acción se harían a este nivel, sirviendo como punto de referencia para la organización de la estructura dentro de la herramienta .

2.2.3 Mapas de Riesgo (Perfiles de Riesgo)

Es posible obtener perfiles de riesgo o mapas de calor que podrán ser visualizados, dependiendo de la información que sea contenida, facilitando a la Entidad actuar de manera proactiva frente a esta información, entre otros:

- Perfil de Riesgos por Procesos del Negocio.
- Perfil de Riesgos por Activos de Información.
- Perfil de Riesgos por Amenazas.
- Perfil de Riesgos por Vulnerabilidades.
- Perfil de Riesgos por Objetivos de Control de ISO2700.
- Perfil de Riesgos por Objetivos Instituciones

Se deben generar las relaciones correspondientes.

2.2.4 Criterios de Aceptación de Riesgos

La Entidad ha considerado los siguientes niveles de aceptación del riesgo que se visualizan a través de un mapa cartesiano donde en el interior se observan variación en la asignación del calor, como se describe en los siguientes apartados acorde a las recomendaciones y mejores prácticas de Gestión de Riesgos reconocidas a nivel internacional.

2.2.4.1 Tabla de Configuración de la Severidad

La severidad del riesgo se da como una resultante de la consecuencia (Impacto) por la probabilidad (evento/causa) del riesgo y al ubicar en el plano cartesiano se visualiza una tabla de colores a la que se le ha dado el nombre de tabla de Severidad, configurada con los siguiente colores que denotan el grado de alerta que la Entidad debe adoptar frente a este resultado.

A continuación se describe la severidad, que va de bajo a extremo y los colores utilizados en el interior del plano cartesiano:

E	**Extremo**	
A	**Alto**	
M	**Medio**	
B	**Bajo**	

Los descriptores definidos se especifican a continuación:

- **Extremo**: Riesgo extremo, **se requiere acción inmediata**. Planes de Tratamiento o mejoramiento requeridos, implementados y aprobado por el Comité Gerencial de la Entidad.

- **Alto**: Riesgo alto, **requiere atención de la alta gerencia**. Planes de Tratamiento o de mejoramiento requeridos, implementados y aprobados por Comité Gerencial de la Entidad.

- **Medio**: Riesgo moderado, la responsabilidad gerencial debe ser especificada. Es un riesgo aceptable – Administrado con procedimientos normales de control y no requiere una acción específica.

- **Bajo**: Riesgo bajo, se administra con procedimientos rutinarios. Riesgo insignificante No se requiere ninguna acción.

La Matriz de Configuración de la Severidad que refleja la ubicación de cada uno de los riesgos dentro del mapa de riesgos (mapa de calor o perfil de riesgos) definido para la Superintendencia de Sociedades y de acuerdo a las mejores prácticas seria el siguiente:

MATRIZ DE CONFIGURACIÓN DE LA SEVERIDAD

Probabilidad					
Casi Cierta (5)	A	A	E	E	E
Muy Probable (4)	M	A	A	E	E
Posible (3)	B	M	A	E	E
Improbable (2)	B	B	M	A	E
Rara (1)	B	B	M	A	A
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)

Consecuencia

La mayor severidad que se puede dar de un riesgo de acuerdo a los rangos y tablas definidos en esta guía es de **25** (**5** x **5**) y la menor es de **1** (**1** x **1**).

De acuerdo con la ubicación del riesgo dentro de la matriz de configuración de la severidad, en la que se está dando mayor peso a la consecuencia o efecto del riesgo, les permite a los responsables del riesgo definir, establecer o tomar decisiones y acciones sobre éstos.

2.2.4.2 Medidas de la Consecuencia

Generalmente la consecuencia se mide en términos financieros pero no todos los riesgos se pueden evaluar utilizando esta medida. Existen otros valores cualitativos que pueden ser utilizados para poder medir la consecuencia en términos de impacto para la organización.

Además de la consecuencia financiera, se pueden considerar otras alternativas como por ejemplo:

- Cumplimiento de los objetivos de la organización y/o proceso/servicio/producto.
- Productividad,
- Salud y seguridad de empleados y clientes.
- Protección de información confidencial o privada.

- Efecto en la imagen y reputación de la organización.
- Comunidad Reputacional

La siguiente tabla será utilizada por la Superintendencia de Sociedades como punto de referencia para la calificación de la consecuencia (efecto o impacto) de los riesgos.

TABLA DE LA CONSECUENCIA

Valor	Descriptor	Impacto en Objetivos Corporativos (Estratégicos y de Calidad).	Impacto Financiero	PRODUCTIVIDAD	Salud y Seguridad	Comunidad / Reputación / Medios	Comunidad / Reputación / Medios a nivel interno	Legales
5	Catastrófico	Impacto sobre la misión y visión de la Entidad	Mayor a 275,000,000	Sobrecarga de trabajo > 80% (Sí inicia de cero y Sí es indispensable la participación de otros). Tiempo tolerable de interrupción menor o igual a 24 horas.	Pérdida de vidas humanas, discapacidad permanente (mayor al 50%) o incapacidad mayor o igual a 91 días.	Efecto publicitario sostenido a nivel país e internacional.	De conocimiento del Comité Gerencial	Acusaciones y multas significativas organismo regulador. Litigios muy serios.
4	Mayor	Impacto crítico sobre por lo menos un objetivo corporativo	Mayor a 100,000,000 y menor a 275,000,000	Sobrecarga de trabajo >= 50% y < 80 % (Sí inicia de cero y posiblemente Sí es indispensable la participación de otros). Tiempo tolerable de Interrupción entre 24 horas y 48 horas.	Discapacidad superior o igual al 26% y menor al 50% de la capacidad laboral o incapacidad mayor o igual a 31 días y menor o igual a 90 días.	Efecto publicitario y sostenido a nivel departamental.	De conocimiento Grupo Primario	Requerimiento formal o investigación organismo regulador. Litigios mayores.
3	Moderado	Afecta por lo menos un objetivo del proceso.	Mayor a 42,000,000 y menor a 100,000,000	Sobrecarga de trabajo >= 30% y < 50 % (Sí inicia de cero y posiblemente, No es indispensable la participación de otros. Tiempo tolerable de Interrupción entre 2 y 4 días.	Discapacidad menor al 25% o incapacidad mayor o igual a 15 y menor o igual 30 días.	Efecto publicitario en la ciudad y en las empresas	De conocimiento Áreas y Jefaturas	Requerimiento del organismo regulador. Litigios menores.
2	Menor	Afecta el cumplimiento de objetivos individuales.	Mayor a 20,000,000 y menor a 42,000,000	Sobrecarga de trabajo >= 10% y < 30 % (posiblemente, No inicia de cero y No es indispensable la participación de otros). Tiempo tolerable de Interrupción entre 5 y 10 días.	Incapacidad mayor o igual a 3 días y menor a 15 días.	Efecto publicitario en las empresas vinculadas.	De conocimiento Equipos de Trabajo	Requerimiento del organismo regulador. Conciliaciones menores.
1	Insignificante	Afecta el cumplimiento de las metas en una actividad específica.	Hasta $ 20,000,000	Sobrecarga de trabajo < 10% (No inicia de cero y No es indispensable la participación de otros) . Tiempo tolerable de Interrupción más de 10 días.	Incapacidad menor a 3 días.	Sin efecto publicitario, incremento en quejas y reclamos	De conocimiento de algunos los Funcionarios del proceso.	Asuntos legales menores.

2.2.4.3 Medidas de la Probabilidad

Se utiliza como una descripción general de Probabilidad, Frecuencia o posibilidad de que un evento ocurra.

Las definiciones utilizadas para cada una de ellas son:

- **Probabilidad**: Probabilidad Matemática, cuantitativa, es la posibilidad de un evento específico o resultado, medido por la rata (frecuencia) de eventos específicos o resultados sobre el número total de posibles eventos o resultados. (Rango de 0 – 1 / %).

- **Frecuencia**: Es una medida del coeficiente de ocurrencia de un evento expresado como la cantidad de ocurrencias de un evento en un tiempo dado.

- **Posibilidad**: Expresión cualitativa de la Probabilidad.

La siguiente Tabla de la Probabilidad será utilizada por la Superintendencia de Sociedades como punto de referencia para la calificación o valoración de las medidas de probabilidad riesgo.

TABLA DE LA PROBABILIDAD

Valor	Descriptor	Posibilidad, nunca se ha materializado el evento, no hay historia en el sector	Frecuencia, para actividades diarias	Frecuencia Operaciones, eventos operativos donde hay estadística.	Frecuencia, para procesos esporádicos.	Frecuencia, Eventos naturales	Probabilidad Matemática
5	Casi Cierta	Ocurre en la mayoría de veces	El evento ocurre diariamente	Error mayor al 10% de las operaciones	Más de 5 veces al año	Una vez al año o hasta tres años	Mayor al 0.5
4	Muy Probable	Posiblemente ocurra en todas las veces	El evento ocurre mensualmente	Error mayor al 5% y menor o igual al 10% de las operaciones	4 veces al año	Una vez cada tres años	Entre el 0.3 y el 0.5
3	Posible	Alguna posibilidad en que el evento ocurra	El evento ocurre una vez cada seis meses	Error mayor al 3% y menor o igual al 5% de las operaciones	3 veces al año	Una vez cada diez años	Entre el 0.1 y el 0.3
2	Improbable	Insignificante posibilidad de que el evento ocurra	El evento ocurre una vez al año	Error mayor al 1% y menor al 3% de las operaciones	2 veces al año	Una vez cada treinta años	Entre el 0.01 y el 0.1
1	Rara	Puede ocurrir en circunstancias excepcionales	El evento ocurre una vez cada 5 años o más	Error menor o igual al 1% de las operaciones	1 vez al año	Una vez cada cien años	Menor del 0.01

3 Valoración del Riesgo

3.1 Identificar el Riesgo

Identificar ***Qué*** puede suceder (Impacto, consecuencia, efecto) del riesgo, y adicionalmente se identifica el ***Por qué*** podría suceder y ***Como, Cuando*** y ***Donde*** podría suceder el riesgo (probabilidad). Esta fase pretende establecer todos los riesgos a administrar, estén o no estén bajo el control de la organización.

Para esta fase se utilizará la metodología de fuentes de riesgo y áreas de impacto donde cada responsable del proceso analiza la fuente de riesgo y la cruza contra el área de impacto, si éste considera que podría haber un riesgo, procede ha realizar la descripción del riesgo.

Dentro de la descripción del riesgo se tiene en cuenta los siguientes elementos:

Que puede ocurrir: Este elemento descriptivo, se asocia a las áreas de impacto identificadas.

Porque puede ocurrir: Esta parte del riesgo se asocia a las fuentes de riesgo identificadas y específicamente, tratando de identificar la causa raíz o evento que pudiera generar la consecuencia o impacto del riesgo.

Como puede ocurrir: Se asocia igualmente a las fuentes de riesgo identificadas pero en este caso se identifica la causa mediata que posiblemente pueden en una mayor o menor medida, incidir en la consecuencia o impacto del riesgo.

Cuando y Donde puede ocurrir: Específicamente cuando (en qué momento) puede ocurrir el riesgo y Donde (en qué lugar/área) puede este ocurrir.

Contemplando aquellos recursos económicos, físicos, humanos, logísticos, de activos de información que son críticos para el desarrollo del propósito del proceso.

3.2 Analizar Riesgos

3.2.1 Identificación de Controles

Los controles son las políticas, procesos, dispositivos, prácticas u otras acciones que actúan para eliminar, mitigar, tratar o minimizar los riesgos adversos o mejorar oportunidades positivas. ***Proveen una seguridad***

razonable relativa al logro del propósito del proceso, los objetivos de la Entidad, y por ende su misión y visión.

Dentro del análisis de los riesgos identificados el responsable identifica los controles asociados al riesgo. Esta lista contendrá el nombre corto del control, la descripción, el responsable y la periodicidad.

Como apoyo a esta fase, se podrá contar con la caracterización de los procesos donde se debería encontrar detallados todos los controles asociados. Igualmente, el responsable del riesgo debe tener en cuenta que existen controles que no necesariamente están bajo su responsabilidad.

3.2.2 Valoración Riesgo Absoluto (Inherente)

A medida que se identifican los riesgos y los mismos son validados y depurados, se inicia la valoración del riesgo absoluto.

De acuerdo a los estándares reconocidos a nivel mundial en gestión de riesgos, el **riesgo absoluto** es la evaluación de la ***consecuencia*** y la ***probabilidad*** que Ignora los **controles** que están **vigentes** asociados al riesgo, excepto los controles Inherentes del entorno. En otras palabras, el riesgo absoluto podemos definirlo como el peor escenario posible o la máxima pérdida posible.

La técnica a ser utilizado para la valoración del riesgo absoluto ***es la de Juicio de expertos o experiencia del responsable del proceso***, en donde se analiza el riesgo para cada componente de manera individual tomando como referencia las Tablas de Consecuencia y Probabilidad. El responsable dejará sustentación escrita de cada una de las valoraciones.

El riesgo absoluto resulta de multiplicar el valor de la consecuencia por la probabilidad de ocurrencia obteniéndose el nivel de riesgo absoluto.

3.2.3 Valoración Riesgo Controlado

La valoración de los riesgos controlados consiste en el analizar los riesgos en términos de consecuencias y probabilidades en el contexto de los controles reales identificados. El análisis debe considerar el rango de consecuencias potenciales y cuan probable es que ocurran para determinar un nivel estimado del riesgo controlado.

Para los controles identificados para reducir, mitigar o minimizar la ocurrencia de riesgo, se realizará la evaluación de la efectividad de cada control, que consistirá en asignarle una calificación a cada factor ó atributo del control y la

suma de los resultados dará un valor máximo de 100. A continuación se describen los factores ó atributos y escalas de calificación:

FACTOR DE EVALUACIÓN	Máximo Puntaje	CARACTERÍSTICA	CALIFICACIÓN
Modo de Implementación del Control	30	Automático	30
		Combinado	20
		Manual	10
Documentado	20	Está documentado	20
		Está Parcialmente Documentado	12
		No está documentado	8
El porcentaje de veces que se ejecuta el control	20	Entre el 81 y 100% de las veces	20
		Entre el 61 y 80% de las veces	15
		Entre el 31 y 60% de las veces	10
		Entre el 01 y 30% de las veces	5
Grado de Complejidad del Control	20	Simple	20
		Medianamente Complejo	12
		Complejo	8
Deja evidencia de ejecución	10	De todas las actividades del proceso (Sustancial)	10
		Deja Evidencia en algunas actividades del Proceso (Material)	6
		No deja evidencia (Informal)	4
TOTAL CALIFICACIÓN	**100**		

Una vez asociado el control a cada riesgo en la lista de controles se evaluará la cobertura de cada uno, asignando una calificación de 10 a 100, donde 10 es el nivel de cubrimiento ó reducción que tiene el control sobre el riesgo y el valor de 100 indica que el nivel de reducción o cobertura que tiene el control sobre el riesgo.

Para determinar el resultado de la eficacia de cada control, los resultados de la efectividad y cobertura se multiplicaran por el peso descrito a continuación:

VARIABLE	PESO
Efectividad	70%
Cobertura	30%

Al presentarse varios controles asociados a los riesgos, los valores resultados de todos, se promediarán para encontrar el porcentaje promedio total (%) que se aplica a los valores de probabilidad y consecuencia del riesgo absoluto (inherente), encontrando el nivel de riesgo controlado ó riesgo residual.

También es importante establecer el tipo de control, es decir, si es Preventivo, Detectivo ó Correctivo

4 Evaluar Riesgos

La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis de riesgo contra los criterios preestablecidos, permitiendo darle una prioridad a los riesgos y establecer el nivel del riesgo tanto absoluto (inherente) como el nivel de riesgo controlado, el cual puede ser aceptable, cuando el nivel de riesgo es bajo o medio, o requerir un tratamiento si el nivel del riesgo es alto o extremo. Este resultado puede ser visualizado en la matriz de configuración de la severidad.

El resultado de una evaluación de riesgos es un listado de los riesgos con sus respectivas prioridades para una acción posterior.

5 Tratar el Riesgo

El tratamiento de los riesgos permite identificar y documentar las diferentes opciones para tratar los riesgos, evaluar estos posibles tratamientos y preparar planes para implementarlos, los cuales deben ser aprobado por el Comité Gerencial.

Entre los posibles tratamientos se tiene evitar el riesgo no procediendo con la actividad, reducir la probabilidad de ocurrencia, reducir las consecuencias, transferir los riesgos y retener los riesgos.

a. Evitar el riesgo, decidiendo no proceder con la actividad que probablemente genera el riesgo. (Cuando esto es practicable).

   Puede ocurrir que ignorar el riesgo se efectúe de una manera inapropiada porque exista una actitud de aversión al riesgo. Evitar de manera inadecuada un riesgo puede incrementar la significancia de otros riesgos.

   Decisiones de ignorar riesgos a pesar de la información disponible y los costos incurridos en el tratamiento de dicho riesgo, fallar en el tratamiento del riesgo, trasladar decisiones críticas a terceras partes, aplazar decisiones las cuales la organización no puede evitar, o seleccionar una opción porque ésta representa un potencial menor de riesgo, sin considerar los beneficios.

b. Reducir la probabilidad de la ocurrencia.

c. Reducir las consecuencias.

d. Transferir el riesgo parcial o totalmente.

e. Retener y auto financiar la consecuencia del riesgo.

Si después de determinado el nivel de riesgo controlado, el residuo de los riesgos resulto en un nivel de severidad ***Alto o Mayor***, se debe aplicar el plan de tratamiento aprobado siguiendo el procedimiento GC-PR-002 de acciones preventivas y correctivas y de gestión de incidentes, que se encuentra en INTRANET/ SITEMA DE GESTION INTEGRADO / PROCESO DE GESTION INTEGRAL.

De manera gradual y en paralelo, se van incorporando esta información a través del aplicativo ERA.

6 Monitorear y Revisar

Consiste en realizar un seguimiento y revisar el desempeño del Sistema de administración del riesgo y los cambios que puedan afectarlo.

Es necesario monitorear los riesgos, la efectividad del plan de tratamiento de los riesgos y la efectividad de las medidas de control, para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos, ***por cuanto pocos riesgos permanecen estáticos***.

Los Riesgos bajos o aceptables, aunque no requieren acción, deben ser monitoreados y periódicamente revisados, para asegurar que ellos se mantienen en niveles aceptables.

Adicionalmente, se requiere que se reporte y registre la información de los eventos que se estén presentando en cada proceso para ir construyendo una base de datos de conocimientos para la siguiente evaluación. Se debe realizar a la cuenta de correo electrónico sgi@supersociedades.gov.co o por los responsables de los procesos sobre el aplicativo ERA dependiendo de la disponibilidad de recursos.

7 Metodología para la actualización del Mapa de Riesgos

Como mínimo una vez al año se revisa y actualiza el mapa de riesgos de la entidad; a menos que por el estado del proceso o por su nivel de importancia sea necesario hacerlo con mayor frecuencia.

Esta actualización es responsabilidad del líder de proceso quien con el apoyo de los líderes del Sistema de Gestión de Calidad y del Sistema de Gestión de

Seguridad de la información o quien haga sus veces, revisara y actualizara el mapa de riesgos de su proceso facilitando esta labor. Cuando corresponda se deberá incorporar las Intendencias Regionales.

Para esta revisión el líder de proceso puede reunirse con los involucrados o a través de mecanismos virtuales solicitarles una revisión al mapa actual para determinar que riesgos deben incluirse, excluirse o mantenerse en la herramienta.

8 CONTROL DE CAMBIOS

Versión	Vigencia Desde	Vigencia Hasta	Identificación de los cambios	Responsable
001	31-05-2010	16-05-2011	Creación del documento	Líder de Gestión Integral
002	16-05-2011	12-10-2011	Aclaración la gestión del tratamiento de riesgo antes de controles y residual	Coordinadora Grupo de Planeación.
003	13-10-2011		Ajustes al Sistema de Gestión Integrado	Líder de Gestión Integral