PLAN DE TRATAMIENTO DE RIESGOS DE LA INFORMACIÓN
EGAT

Bogotá D.C., enero de 2024

Tabla de contenido

1. INTRODUCCION 3
2. OBJETIVOS 4
3. ALCANCE 4
4. AMBITO DE APLICACIÓN 4
5. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACION DELRIESGO 8
6. POLITICA DE ADMINISTRACION DEL RIESGO DE LA INFORMACIÓN 9
7. ETAPAS PARA LA ADMINISTRACION DEL RIESGO 10
8. IDENTIFICACIÓN Y EVALUACIÓN DE CONTROLES 30

1. INTRODUCCION

La administración de riesgos constituye un método lógico y sistemático destinado a establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso. Su propósito primordial radica en dotar a la entidad de los medios necesarios para minimizar pérdidas y maximizar oportunidades.

En el ejercicio de sus funciones, todos los funcionarios se encuentran expuestos a riesgos que podrían comprometer el éxito de la gestión. Por ende, resulta imperativo adoptar medidas para identificar las causas y consecuencias de la materialización de dichos riesgos. En este sentido, la presente guía tiene como objetivo principal orientar y facilitar la implementación y desarrollo de una gestión del riesgo eficaz, eficiente y efectiva, desde su identificación hasta su monitoreo.

Asimismo, se hace hincapié en la importancia de comprender los fundamentos teóricos de la administración del riesgo, así como en brindar una orientación clara y sencilla para facilitar su identificación, el reconocimiento de las causas y efectos, la definición de controles y el establecimiento de lineamientos adecuados para su gestión integral.

2. OBJETIVOS

• Promover una cultura organizacional orientada a la gestión proactiva de riesgos, fomentando la participación y el compromiso de todos los niveles de la organización.
• Identificar y evaluar los riesgos específicos asociados a cada área de la organización, con el fin de implementar medidas de control y mitigación adaptadas a sus necesidades particulares.
• Fomentar la comunicación efectiva y la colaboración entre los diferentes departamentos y equipos de trabajo, facilitando el intercambio de información relevante para la gestión de riesgos.
• Implementar un sistema de monitoreo continuo que permita evaluar la efectividad de las medidas de control implementadas y realizar ajustes o mejoras según sea necesario.
• Promover la mejora continua en los procesos de gestión de riesgos, mediante la retroalimentación y la revisión periódica de las políticas, procedimientos y prácticas establecidas.
• Fortalecer la capacidad de respuesta de la organización frente a situaciones de crisis o eventos adversos, mediante la preparación y el entrenamiento del personal en la gestión de emergencias y la continuidad del negocio.

3. ALCANCE

Por medio de la presente guía, se proporciona la metodología establecida por la Entidad para la administración y gestión de los riesgos a nivel de procesos. Esta guía orienta sobre las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis, valoración y la definición de las opciones de manejo. Asimismo, se destaca la importancia de formular acciones adicionales que puedan ser necesarias para garantizar una adecuada gestión del riesgo.

4. AMBITO DE APLICACIÓN

Los lineamientos definidos en esta guía, aplica para la gestión de los riesgos.

DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- Acciones asociadas: son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.
- Administración de riesgos: conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
- Amenaza: situación externa que no controla la entidad y que puede afectar su operación
- Análisis del riesgo: etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
- Asumir el riesgo: opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
- Causa: medios, circunstancias y/o agentes que generan riesgos.
- Calificación del riesgo: estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- Compartir o transferir el riesgo: opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.
- Consecuencia: efectos que se pueden presentar cuando un riesgo se materializa.
- Contexto estratégico: son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una entidad.
- Control: acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
- Control preventivo: acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- Control correctivo: acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.
- Debilidad: situación interna que la entidad puede controlar y que puede afectar su operación.
- Evaluación del riesgo: resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.

- Evitar el riesgo: opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.
- Frecuencia: ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- Identificación del riesgo: etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos
- Impacto: medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.
- Mapa de riesgos: documento que de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
- Materialización del riesgo: ocurrencia del riesgo identificado
- Opciones de manejo: posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
- Plan de contingencia: conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio
- Probabilidad: medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.
- Procedimiento: conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
- Proceso: conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.
- Riesgo: eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.
- Riesgo de corrupción: posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

- Riesgo inherente: es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

- Riesgo institucional: Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:

Durante el proceso de identificación de riesgos, aquellos que hayan sido clasificados como estratégicos deben ser marcados como de clase estratégica, lo cual implica que están directamente relacionados con el cumplimiento de los objetivos institucionales, la misión y visión de la organización.

Por otro lado, los riesgos que se ubiquen en la zona alta o extrema después de su valoración indican que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado. Es importante tener en cuenta que estos riesgos pueden requerir una atención prioritaria.

Además, los riesgos que tengan incidencia directa en el usuario o destinatario final externo deben ser identificados y gestionados con especial atención, considerando su impacto directo en dichos usuarios.

Cabe destacar que todos los riesgos que hagan referencia a situaciones de corrupción serán considerados como riesgos de tipo institucional, reflejando la importancia de abordar este tipo de riesgos de manera integral.

El riesgo residual se refiere al nivel de riesgo que permanece luego de determinar y aplicar controles para su administración. Es fundamental evaluar adecuadamente este riesgo residual para tomar decisiones informadas sobre las acciones de manejo a seguir.

En resumen, la valoración del riesgo implica la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. Esta etapa determina el riesgo residual, la opción de manejo a seguir y la necesidad de acciones adicionales.

5. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACION DEL RIESGO

El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

- Alta Dirección: aprueban las directrices para la administración del riesgo en la Entidad. La Alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.

- Proceso Administración del Sistema Integrado de Gestión: Genera la metodología para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.

- Responsables de los procesos: Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos e institucionales) al menos una vez al año. Si bien los Líderes SIG apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso. No se debe olvidar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.

- Servidores públicos y contratistas: ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

- Quien haga las veces de Control Interno: debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos

6. POLITICA DE ADMINISTRACION DEL RIESGO DE LA INFORMACIÓN

EGAT adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, y para ello todos los servidores de la entidad se comprometen a:

- Conocer y cumplir las normas internas y externas relacionadas con la administración de los riesgos.
- Fortalecer la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.
- Someter los procesos y procedimientos permanentemente al análisis de riesgos con base en la aplicación de las metodologías adoptadas para el efecto.
- Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.
- Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.
- Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.
- Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad para así aumentar nuestra eficacia y efectividad.

Para lograr lo anteriormente enunciado la Alta Dirección asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

De igual manera, la presente guía forma parte de la política de administración del riesgo, por cuanto detalla las directrices que deben tenerse en cuenta para la gestión del riesgo en la entidad y que tienen como propósito evitar la materialización del riesgo

- Someter los procesos y procedimientos permanentemente al análisis de riesgos con base en la aplicación de las metodologías adoptadas para el efecto.
- Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.
- Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.
- Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.
- Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad para así aumentar nuestra eficacia y efectividad.

Para lograr lo anteriormente enunciado la Alta Dirección asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

De igual manera, la presente guía forma parte de la política de administración del riesgo, por cuanto detalla las directrices que deben tenerse en cuenta para la gestión del riesgo en la entidad y que tienen como propósito evitar la materialización del riesgo

7. ETAPAS PARA LA ADMINISTRACION DEL RIESGO

A continuación, se presenta cada una de las etapas a desarrollar durante la administración del riesgo; en la descripción de cada etapa se desplegarán los aspectos conceptuales y operativos que se deben tener en cuenta.

- Contexto estratégico: determinar los factores externos e internos del riesgo.
- Identificación: identificación de causas, riesgo, consecuencias y clasificación del riesgo.
- Análisis: Calificación y evaluación del riesgo inherente.
- Valoración: identificación y evaluación de controles; incluye la determinación del riesgo residual.
- Manejo: determinar, si es necesario, acciones para el fortalecimiento de los controles.

- Seguimiento: evaluación integral de los riesgos.

Análisis contexto estratégico

Definir el contexto estratégico contribuye al control de la entidad frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos, impidiendo con ello que la entidad actúe en dirección contraria a sus propósitos institucionales.

Para la definición del contexto estratégico, es fundamental tener claridad de la misión institucional, sus objetivos y tener una visión sistémica de la gestión, de manera que se perciba la administración del riesgo como una herramienta gerencial y no como algo aislado del accionar administrativo. Por lo tanto, el diseño de esta primera etapa, se fundamenta en la identificación de los factores internos (debilidades) y externos (amenazas) que puedan generar riesgos que afecten el cumplimiento de los objetivos institucionales.

Esta etapa es orientadora, se centra en determinar las amenazas y debilidades de la entidad; es la base para la identificación del riesgo, dado que de su análisis suministrará la información sobre las CAUSAS del riesgo.

Desarrollo práctico - Contexto Estratégico

Tomando como referente lo anterior, se debe atender y seguir las siguientes orientaciones:

- Cada responsable de proceso del Sistema Integrado de Gestión, deberá identificar a los funcionarios que por su competencia pueden ser considerados claves dentro de cada una de las dependencias que participan en el proceso, serán factores de selección de estos, el conocimiento y nivel de toma de decisiones sobre el proceso.
- Los funcionarios seleccionados deberán ser convocados a una reunión inicial, en donde se presentará el propósito de esta actividad
- Se establecerán los factores internos y externos que afectan el proceso, para esto, se debe diligenciar el formato Matriz DOFA para identificación de riesgos:

MATRIZ DOFA PARA IDENTIFICACIÓN DE RIESGOS
PROCESO:
OBJETIVO:
FECHA:

DEBILIDADES
FUENTE
AMENAZAS

Para diligenciar la matriz anterior, y como parte introductoria se deberá informar a los asistentes: la dependencia a la cual corresponde el proceso y el objetivo (se debe presentar indicando que se hace, cual es el mediante y la finalidad). Con esta información, se identificarán las posibles debilidades como:

- La administración, la estructura organizacional, las funciones y las responsabilidades.
- Las políticas, los objetivos y las estrategias que existen para su realización.
- Las capacidades, entendidas en términos de recursos y de conocimiento (humanos, de capital, tiempo, personas, infraestructura, procesos, sistemas y tecnologías).
- Los sistemas de información y comunicación, flujos de información formales e informales y toma de decisiones.
- Las normas, directrices y modelos adoptados por la organización.
- La forma y el alcance de las relaciones contractuales.

Las debilidades deberán ser expresadas con términos similares a estos

- Ausencia de….
- ... obsoletos
- Falta….
- ….insuficientes
- Disminución de…
- Fallas de….

Este tipo de palabras no necesariamente deben aparecer al inicio de la idea, ejemplo: número equipos de cómputo de obsoletos.

Nota: Se recomienda que las ideas, en lo posible, se soporten de experiencias, registros y demás, por eso en el cuadro relacionado se establece una columna denominada “Fuente”, en caso de que la idea cuente con una fuente se colocará tal y como aparece a continuación,en caso contrario se dejará no aplica (N/A).

Debilidad Fuente

Falta de respeto entre funcionarios Evaluar Clima Laboral

Posteriormente, se articularán las ideas afines de la siguiente manera:

Es importante destacar que no todas las ideas tendrán afinidad y se conservarán como fueron establecidas en la lluvia de ideas; después de articular y organizar las ideas, se debe identificar a que factor corresponde cada idea, como se muestra en el siguiente ejemplo:

Ideas Factores internos
Número de equipos insuficiente Tecnología y sistemas de información
Desconocimiento de la normatividad aplicada Talento Humano
Proceso manual Modelo de Operación
Desmotivación Talento Humano
Fallas en el seguimiento a los procedimientos del proceso Modelo de Operación
Equipos obsoletos Talento Humano
Resistencia al cambio Talento Humano
Bajo presupuesto de inversión Financiero

Se consideran factores internos:

- Dirección
- Estructura organizacional
- Comunicación Interna
- Normativo
- Tecnología y sistemas de Información
- Talento humano
- Ético
- Clima Organizacional
- Infraestructura
- Financiero
- Operativo
- Insumos e información
- Modelo de operación
- Mecanismos de Control

Una vez se tengan identificados los factores internos, se debe diligenciar el formato Contexto Estratégico:

CONTEXTO ESTRATEGICO
PROCESO:
OBJETIVO:
FECHA:
FACTORES INTERNOS CAUSAS
FACTORES EXTERNO CAUSAS

En la primera parte, se diligenciarán los factores internos a los cuales se les vincularán las causas, estas corresponderán a las ideas que salieron del análisis y agrupación por afinidad de las debilidades y que dieron origen a los factores. A continuación, presentamos un ejemplo:

CONTEXTO ESTRATÉGICO
PROCESO:
OBJETIVO:
FECHA:
FACTORES INTERNOS
CAUSAS FACTORES EXTERNO
CAUSAS

Tecnología • Equipos insuficientes
• Equipos obsoletos
Procesos • Ausencia de políticas de operación
• Proceso manual
• Fallas en el seguimiento a los procedimientos del proceso
Talento Humano • Desconocimiento de la normatividad aplicada
• Desmotivación
• Resistencia al cambio
Sistemas de información • Información desactualizada
Medición • Los indicadores no miden nada
Financiero • Najo presupuesto de inversión

Definidos los factores internos, se procede a identificar los factores externos, para ello deben ser identificadas las amenazas. Mediante lluvia de ideas se identifican los aspectos del entorno, para este caso puntual, no existe una regla específica de redacción, sin embargo, tendrán el mismo tratamiento de las debilidades, es decir afinidad por agrupación, generando como resultado un listado como:

- Nueva tecnología disponible
- Nuevas leyes
- Demoras en la respuesta de comunicaciones enviadas por otras entidades
- Incremento en el número de solicitudes por alta demanda de usuarios
- Cambio de Gobierno
- Poco conocimiento por parte de la ciudadanía
- Adaptación a normatividad internacional

Con el listado de estas ideas, se debe identificar el factor externo al cual perteneces cada idea:

Idea Factores Externos
Nueva tecnología disponible Tecnológico
Nuevas leyes Legal
Demoras en la respuesta de comunicaciones enviadas por otras entidades Interinstitucional
Incremento en el número de solicitudes por alta demanda de usuarios Social
Cambio de Gobierno Político
Poco conocimiento por parte de la ciudadanía Social
Adaptación a normatividad internacional Legal

Se consideran factores externos:

- Interinstitucional
- Político
- Económico
- Ambiental
- Social

- Tecnológico
- Cultural
- Legal
- Imagen
- Entre otros

Con esta información, se procede a complementar el formato Contexto Estratégico, en lo correspondiente a factores externos:

CONTEXTO ESTRATÉGICO
PROCESO:
OBJETIVO:
FECHA:

FACTORES INTERNOS CAUSAS FACTORES EXTERNO CAUSAS
Tecnología y sistemas de información • Equipos insuficientes
• Equipos obsoletos Tecnológico • Nuevo tecnología disponible.
Modelo de operación • Ausencia de políticas de operación
• Proceso manual
• Fallas en el seguimiento a los procedimientos del proceso Legal • Nuevas leyes
• Adaptación a normatividad internacional
Talento Humano • Desconocimiento de la normatividad aplicada
• Desmotivación
• Resistencia al cambio Interinstitucional Demoras en la respuesta de comunicaciones enviadas por otras entidades
Tecnología y sistemas de información • Información desactualizada Social
Incremento en el número de solicitudes para alta demanda de usuarios
Mecanismos de control • Los indicadores no miden nada Político
Cambio de gobierno

En conclusión, los resultados de esta etapa son:

- Identificar los factores internos que pueden ocasionar la presencia de riesgos.
- Identificar los factores externos que pueden ocasionar la presencia de riesgos, con base en el análisis de la información externa y los planes y programas de la entidad.
- Aportar información que facilite y enriquezca las demás etapas de la Administración del Riesgo.

Conocidos los factores generadores de riesgo y dado por entendido que la Administración del Riesgo es un trabajo en equipo liderado y motivado constantemente por la Alta Dirección, se continúa con la identificación del riesgo.

Identificación de riesgos

Es la etapa que permite conocer los eventos potenciales, estén o no bajo el control de la entidad pública, que ponen en riesgo el logro de su misión, estableciendo las causas y los efectos de su ocurrencia". Adicionalmente, en esta etapa también se realiza la clasificación del riesgo.

Causas
Son los medios o circunstancias
Riesgos
Evento que tendrá un impacto
Consecuencia
Efecto que se puede presentar
Clasificación
De acuerdo a las características
Identificación del Riesgo
Descripción a adecuada de los Riesgos Resultado esperado

En este paso se identifican los riesgos institucionales y por procesos que la organización debe gestionar. Esta identificación se realiza con base en el Contexto Estratégico, definido en el paso anterior.

Componentes de la identificación del riesgo

a) Causas del riesgo

Son las causas, uno de los aspectos a eliminar o mitigar para que el riesgo no se materialice; esto se logra mediante la definición de controles efectivos. Para realizar el análisis de las causas existen varias técnicas que serán analizadas a continuación.

• Lluvia de ideas: usualmente se utiliza la técnica de lluvia de ideas para identificar todo aquello que puede ser considerado dentro del análisis de riesgos y para que esta sea eficaz, se debe considerar que:

1. Debe haber un moderador que tome nota y que organice las exposiciones de todos los participantes, indicando el tiempo que cada cual tiene para presentar sus ideas.
2. Es más importante la cantidad de ideas que la calidad de las mismas. Todas las ideas son valiosas para el proceso de recopilación de información.
3. No se deben calificar las ideas como buenas o malas, son simplemente puntos de vista que capitalizados pueden brindar alternativas no consideradas.
4. Es importante soportarse en las ideas de los otros. Es decir, agregar valor a las apreciaciones de otros o considerar situaciones a partir de las mismas.
5. El análisis de las ideas se debe realizar al final, por el moderador, quien las organizará y las expondrá a manera de resultado.
6. Todos deben participar de manera equitativa, es importante no fijar la atención en pocos participantes, ni mantenerse en la palabra sin dar la oportunidad a otro de expresar sus ideas.

• Diagrama Causa-efecto (Espina de pescado): es un método que permite visualizar de manera estructurada todas las causas posibles del riesgo mediante el análisis desde los factores generadores de riesgo.

b) Consecuencias

Son los efectos que se generan o pueden generarse con la materialización del riesgo sobre los objetivos de los procesos y de la entidad; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como daños físicos y fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

Se deben determinar las consecuencias del riesgo en escala ascendente; definiendo cual podría ser el efecto menor que puede causar la materialización del riesgo hasta llegar al efecto mayor generado.

c) Clasificación de los riesgos

Durante la etapa de identificación, se realiza una clasificación del riesgo, según sus características, con el fin de orientar la formulación de un tratamiento adecuado que posibilite la mitigación del riego mediante la definición de controles y planes de manejo:

Clases de riesgo	Definición
Estratégico	Son los riesgos relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
Operativo	Relacionados con el funcionamiento y operatividad de los sistemas de información de la entidad: definición de procesos, estructura de la entidad, articulación entre dependencias.
Financieros	Relacionados con el manejo de los recursos de la entidad: ejecución presupuestal, elaboración estados financieros, pagos, manejos de excedentes de tesorería y manejo de los bienes.
Cumplimiento	Capacidad de cumplir requisitos legales, contractuales, ética pública y compromiso con la comunidad.
Tecnología	Capacidad para que la tecnología disponible satisfaga las necesidades actuales y futuras y el cumplimiento de la misión.
Imagen	Tienen que ver con la credibilidad, confianza y percepción de los usuarios de la entidad.

Estructura adecuada de la identificación del riesgo

La identificación del riesgo no se puede realizar de manera fragmentada; debe existir una relación total entre las causas identificadas, el riesgo y las consecuencias que podrían presentarse producto de la materialización; para evitar confusiones y definir articuladamente todos los componentes de la identificación del riesgo se establece un método apropiado que consiste en el uso del metalenguaje del riesgo para una identificación estructurada en tres partes:

Debido a	Podría ocurrir	Lo que podría generar
Una o más causa	Riesgo	Uno o más consecuencia

Figura 4. Metalenguaje del riesgo

El metalenguaje pretende asegurar que se identifiquen correctamente causas, riesgos y consecuencias, sin confundir unas con otras; de no ser así, los pasos posteriores quedan viciados de error.

Ejemplo:

Debido a Podría ocurrir Lo que podría generar
Manejar con excesiva velocidad Un accidente Lesiones personales.

Desarrollo práctico - Identificación

De acuerdo con la etapa de Contexto Estratégico, se retomarán las ideas establecidas para cada uno de los factores internos y externos, las cuales se utilizarán para determinar las causas del riesgo identificado; posteriormente, se debe describir el riesgo y las posibles consecuencias de su materialización.

Esta información, se debe registrar en el formato Metalenguaje del riesgo (Cuando se estén construyendo los componentes de identificación) y posteriormente, diligenciar el formato de identificación de riesgos (Cuando se tenga toda la información depurada).

METALENGUAJE DEL RIESGO
PROCESO:
OBJETIVO:
FECHA:
DEBIDO A
(una o más causas) PUEDE OCURRIR QUE
(riesgo) DESCRIPCIÓN LO QUE PODRÍA GENERAR
(uno o más efectos)

A continuación se presenta un ejemplo de diligenciamiento del formato del riesgo

METALENGUAJE DEL RIESGO

PROCESO:
OBJETIVO:
FECHA:
DEBIDO A
(una o más causas) PUEDE OCURRIR QUE
(riesgo) DESCRIPCIÓN LO QUE PODRÍA GENERAR
(uno o más efectos)

- Equipos insuficientes
- Equipos obsoletos
- Desconocimiento de la normatividad aplicable Incumplimiento en la generación de respuesta a los usuarios No se generan las respuestas dentro de los términos legales • Sanciones
- Demandas
- Desmotivación
- Resistencia al cambio
- Información desactualizada Generación de respuestas inadecuadas o errores a los usuarios Respuestas sin la competencia técnica o no acorde a lo requerido • Pérdida de imagen
- Alto nivel de quejas por parte de los usuarios

Notas:

- Debido a (una o más causas): Documente las causas asociadas al riesgo identificado
- Puede ocurrir que (riesgo): Indique el nombre del riesgo
- Descripción: Utilice este espacio para describir en que consiste el riesgo identificado
- Lo que podría generar (uno o más efectos): Documente las consecuencias asociadas al riesgo

De acuerdo con la información anterior, se diligencia el formato Identificación del riesgo:

IDENTIFICACIÓN DEL RIESGO
PROCESO:
OBJETIVO:
FECHA:
CAUSAS RIESGO DESCRIPCIÓN CONSECUENCIAS POTENCIALES

A continuación, se presenta un ejemplo de diligenciamiento del formato Identificación del riesgo

IDENTIFICACIÓN DEL RIESGO
PROCESO:
OBJETIVO:
FECHA:
CAUSAS RIESGO DESCRIPCIÓN CONSECUENCIAS POTENCIASLES
- Equipos insuficientes
- Equipos obsoletos
- Desconocimiento de la normatividad aplicable Incumplimiento en la generación de respuesta a los usuarios No se generan las respuestas dentro de los términos legales • Sanciones
- Demandas
- Desmotivación
- Resistencia al cambio
- Información desactualizada Generación de respuestas inadecuadas o errores a los usuarios Respuestas sin la competencia técnica o no acorde a lo requerido •
Pérdida de imagen
- Alto nivel de quejas por parte de los usuarios

Análisis de Riesgos

El análisis del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo.

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados, probabilidad e impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado, o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por Impacto se entiende las

consecuencias que puede ocasionar a la Entidad la materialización del riesgo. La etapa de análisis de los riesgos se divide en:

Calificación del riesgo

Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse, y la segunda se refiere a la magnitud de sus efectos. Para la determinación de la calificación del riesgo, con base en la probabilidad y el impacto se debe tener en cuenta las siguientes tablas:

Escala para calificar la probabilidad del riesgo
Nivel Concepto Frecuencia
Raro El evento puede ocurrir solo en circunstancias excepcionales. No se ha presentado en los últimos 5 años.
Improbable El evento puede ocurrir en algún momento. Al menos de 1 vez en los últimos 5 años.
Moderado El evento podría ocurrir en algún momento. Al menos de 1 vez en los últimos 2 años.
Probable El evento probablemente ocurrirá en la mayoría de las circunstancias. Al menos de 1 vez en el último año.
Casi certeza Se espera que el evento ocurra en la mayoría de las circunstancias. Más de 1 vez al año.

Escala para calificar el impacto del riesgo
Tipos de efecto o impacto a) Estratégico b) Operativo c) Financieros d) Cumplimiento e) Tecnología f) Imagen

PROBABILIDAD IMPACTO
Insignificante, Menor, Moderado, Mayor, Catastrófico

Insignificante: Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos o bajos sobre la entidad. Puede afectar el cumplimiento de algunas actividades, generar ajustes en una actividad concreta, pero no afecta la operación normal de la entidad.
Menor: Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.

Puede afectar el cumplimiento de las metas del proceso, generar ajustes en los procedimientos y requerir investigaciones disciplinarias, fiscales o penales. También puede afectar el proceso o a los servidores del proceso.
Moderado: Si el hecho llegara a presentarse, tendría consecuencias medianas sobre la entidad. Puede afectar el cumplimiento de las metas de un grupo de procesos, generar ajustes o cambios en los procesos y afectar considerablemente la prestación del servicio. También puede generar interrupciones en la prestación del bien o servicio y afectar varios procesos de la entidad, así como a todos los servidores de la entidad.
Mayor: Si el hecho llegara a presentarse, tendría altas consecuencias sobre la entidad. Puede afectar el cumplimiento de las metas de la entidad, generar intermitencia en el servicio y afectar considerablemente el presupuesto de la entidad, así como generar sanciones. También puede afectar a toda la entidad y al sector en general.
Catastrófico: Si el hecho llegara a presentarse, tendría desastrosas consecuencias sobre la entidad. Puede afectar el cumplimiento de las metas del sector y del gobierno, generar paro total de la entidad, afectar el presupuesto de otras entidades o del departamento e incluso generar el cierre definitivo de la entidad. También puede afectar al departamento, al gobierno y a todos los usuarios de la entidad.
Es importante tener en cuenta la clasificación del riesgo (estratégico, operativo, financiero, cumplimiento, tecnología, imagen) para determinar el nivel en el que se encuentra el riesgo, así como la magnitud del impacto que puede tener sobre la entidad.

Evaluación del riesgo

Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente (antes de la definición de controles). La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas.

Raro	B	B	B	M	M
Improbable	B	M	M	A	A
Moderado	B	M	A	A	E
Probable	M	A	A	E	E
Casi certeza	M	A	E	E	E

Color	Zona de riesgo
B	Zona de riesgo baja
M	Zona de riesgo moderada
A	Zona de riesgo alta
E	Zona de riesgo extrema

Con la evaluación del riesgo, previa a la formulación de controles se obtiene la ubicación del riesgo en la matriz de evaluación; esto se denomina evaluación del riesgo inherente.

Desarrollo práctico - Análisis

Formato de Análisis de riesgos, el cual hace parte del proceso Administración del Sistema Integrado de Gestión, donde se debe relacionar la siguiente información:

- Riesgo: Relacionar el riesgo redactado en el formato Identificación de riesgos
- Calificación de probabilidad: de acuerdo con la información cuantitativa y cualitativa
- Calificación de impacto: de acuerdo con la información cuantitativa y cualitativa que
- Clasificación del riesgo: Ver componentes de la identificación del riesgo, en el apartado de clasificación de los riesgos.
- Evaluación: surge del cruce de los resultados cuantitativos de la calificación para probabilidad e impacto;

ANÁLISIS DEL RIESGO
PROCESO:
OBJETIVO:
FECHA:

Riesgo	Calificación Probabilidad	Clasificación del riesgo Impacto	Evaluación

A continuación, se presenta un ejemplo de diligenciamiento del formato Análisis del riesgo

ANÁLISIS DEL RIESGO
PROCESO:
OBJETIVO:
FECHA:

Riesgo	Calificación	Clasificación del riesgo	Evaluación
	Probabilidad	Impacto	
Incumplimiento en la generación de respuesta a los usuarios	3	5	
	Cumplimiento	Zona de riesgo extrema	
Generación de respuestas inadecuadas o errores a los usuarios	Operativo	Zona de riesgo extrema	

Valoración de los riesgos
Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo. Lo anterior de acuerdo con los formatos Identificación y evaluación de controles y Valoración del riesgo.

Identificación de controles

Los controles son las acciones orientadas a minimizar la probabilidad de ocurrencia o el impacto del riesgo; estos, deben estar directamente relacionados con las causas o las consecuencias identificadas para el riesgo y eliminarlas o mitigarlas. La administración del riesgo contribuirá a la gestión de la entidad, en la medida en que los controles se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos.

A continuación, se presentan las características mínimas que se deben tener en cuenta para la definición de los controles:

Característica	Descripción

Objetivos	No dependen del criterio de quien lo define y/o ejecute, sino de los resultados que se esperan obtener
Pertinentes	Están directamente orientados a atacar las causas o consecuencias del riesgo
Realizables	Se deben definir controles que la entidad o el proceso esté en capacidad de llevar a cabo
Medibles	Permiten el establecimiento de indicadores para verificar el cumplimiento de su aplicación y/o efectividad
Periódicos	Tienen frecuencia de aplicación en el tiempo
Efectivos	Eliminan o mitigan las causas o consecuencias y evitan la materialización del riesgo
Asignables	tienen responsables definidos para su ejecución

En el siguiente ejemplo se presenta una forma de redacción de un control.

Causa	Riesgo	Efecto/Consecuencia	Control
Uso de un calendario tributario obsoleto	Declaración de impuestos extemporánea	sanciones pecuniarias para la entidad o disciplinaria para un(os) funcionario(s)	El contador y/o el subdirector Administrativo y Financiero debe realizar la actualización u divulgación, en enero de cada año, de los calendarios tributarios nacionales y departamentales, en la página web, intranet, físicos, etc.

En esta etapa se deben describir todos los controles, existentes y por definir, deben estar orientados a atacar las causas y/o consecuencias (mitigar y/o eliminar) del riesgo. Una vez se hayan identificado y descrito los controles se debe determinar la clase del control; un control puede ser de tipo preventivo o correctivo como se presenta a continuación:

Clases de controles

PREVENTIVO	CORRECTIVO
Acción o Conjunto de acciones que elimina o mitiga las causas del riesgo	Acción o conjunto de acciones que eliminan o mitigan las consecuencias

Orientación a disminuir la probabilidad de ocurrencia del riesgo Orienta a disminuir el nivel de impacto del riesgo

Evaluación de los controles

Permite determinar en qué medida los controles identificados están aportando para disminuir los niveles de probabilidad e impacto del riesgo. Se evalúan verificando su documentación, aplicación y efectividad de la siguiente manera:

¿El control está documentado, incluye el responsable y la frecuencia de aplicación? ¿El control se está aplicando? ¿El control es efectivo (¿sirve o cumple su función?

- Si la pregunta relacionada con documentación se está cumpliendo, se deben asignar 25 puntos; en caso contrario marque 0.
- Si la pregunta relacionada con aplicación se está cumpliendo, se deben asignar 25 puntos; en caso contrario marque 0.
- Si la pregunta relacionada con efectividad se está cumpliendo, se deben asignar 50 puntos; en caso contrario marque 0.

La evaluación se debe aplicar a cada control definido para el riesgo, determinando si se cumple o no el factor, según corresponda.

Riesgo residual y definición de opciones de manejo

Previo a la definición del riesgo residual se debe determinar qué escala (probabilidad, impacto o ambas) se afecta positivamente con la aplicación del control teniendo en cuenta las siguientes indicaciones:

Escala de afectación

PROBABILIDAD IMPACTO AMBAS

Cuando el control está orientado a eliminar o mitigar las causas de los riesgos Cuando el control está orientado a eliminar o mitigar las consecuencias Cuando el control elimina o mitiga causas y consecuencias del riesgo
Figura 6. Afectación de escalas según la probabilidad y/o el impacto

La evaluación de los controles (documentación, aplicación y efectividad) definirá la ubicación del riesgo en la matriz de evaluación; este paso se denomina “evaluación del riesgo residual”; los riesgos se pueden desplazar de la siguiente manera según la calificación de los controles y la definición de la escala que afecta cada riesgo.

Cuando se ha determinado el riesgo residual se debe asociar la opción de manejo mediante la cual se dará tratamiento al riesgo residual. Las opciones de manejo se determinan teniendo en cuenta la ubicación del riesgo según las zonas definidas así:

Color	Zona de riesgo	Opciones de manejo
B	Zona de riesgo baja	Asumir el riesgo
M	Zona de riesgo moderada	Asumir el riesgo Reducir el riesgo
A	Zona de riesgo alta	Reducir el riesgo Evitar el riesgo Compartir o transferir el riesgo
E	Zona de riesgo extrema	Reducir el riesgo Evitar el riesgo Compartir o transferir el riesgo

- Asumir el riesgo: aceptar la pérdida residual probable y elaborar los planes de contingencia para su manejo.
- Reducir el riesgo: implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). Ej.: optimización de procesos, definición de nuevos controles, entre otros.
- Evitar el riesgo: tomar las medidas encaminadas a prevenir su materialización. Ej.: cambios a la infraestructura, cambios en software.
- Compartir o transferir el riesgo: reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o mediante otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Ej.: seguros, sitios alternos, contratos de riesgos compartidos, etc.

Desarrollo práctico – Valoración

En el formato Identificación y evaluación de controles, se deben identificar y documentar los controles asociados al riesgo y calificar de acuerdo con las preguntas descritas en el formato; finalmente, se debe hacer la sumatoria de los resultados de calificación por control.

8. IDENTIFICACIÓN Y EVALUACIÓN DE CONTROLES

PROCESO:
OBJETIVO:
FECHA:
RIESGO:

Controles	Tipo de control		Evaluación del control			Total
	Probabilidad	Impacto	¿El control está documentado, incluye el responsable y la frecuencia de aplicación?	¿El control se está aplicando?	¿El control es efectivo (sirve o cumple su función)?	

Posterior a la identificación y evaluación de los controles, se debe diligenciar el formato Valoración del riesgo; en este formato se debe registrar la valoración final del riesgo de acuerdo con la calificación de cada control.

VALORACIÓN DE RIESGOS
PROCESO:
OBJETIVO:
FECHA:

RIESGO	CALIFICACIÓN		CONTROLES VALORACIÓN			NUEVA VALORACIÓN	
	Probabilidad	Impacto	Tipo de control o impacto	Puntaje final probabilidad	Puntaje final impacto	Puntaje final	Probabilidad	Impacto

Manejo de riesgos

Una vez determinada la zona donde está ubicado el riesgo, y dependiendo de las opciones de manejo, se deben formular las acciones orientadas al mejoramiento y fortalecimiento de los controles identificados. Las acciones que se definan para el manejo del riesgo deben contemplar:

- Corregir las fallas identificadas en los controles según la evaluación realizada a cada uno.
- Reforzar o fortalecer los controles existentes.

Acción Por Desarrollar

\+ Definición de responsables
\+ Definición de Plazo
= Definición Adecuada de Acciones
Resolución adecuada de los Riesgos Resultado esperado
Figura 8. Definición adecuada de las acciones

Si la evaluación del riesgo residual, lo ubica en la zona baja no se deben formular acciones de manejo, el manejo estará únicamente enfocado en garantizar que los controles previamente establecidos operan de manera adecuada. Los riesgos ubicados en las zonas moderada, alta o extrema exigen realizar acciones que fortalezcan los puntos débiles identificados en la evaluación de los controles.

Seguimiento de riesgos

Cada cuatro meses Control Interno realizará seguimiento a todo el componente de administración de riesgos y verificará aspectos como:

- Cumplimiento de las políticas y directrices para la administración del riesgo: metodología de Administración del Riesgo (diseño y funcionamiento).
- Administración de los riesgos por proceso e institucionales: calificación y evaluación, efectividad de los controles y cumplimiento de las acciones.

Los resultados de la evaluación y las observaciones de la persona que haga las veces de Control Interno deben ser presentados a la Alta Dirección, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración del Riesgo en la organización.

Además del seguimiento realizado por Control Interno cada cuatro meses, es fundamental que se establezcan mecanismos para asegurar la efectividad continua del componente de administración de riesgos. Algunas sugerencias adicionales para complementar este proceso podrían incluir:

Implementar un sistema de reporte regular, que permita a todas las áreas de la organización informar sobre incidentes o cambios en el entorno que puedan afectar los riesgos identificados.

Realizar revisiones periódicas de las políticas y directrices para la administración del riesgo, con el fin de asegurar su vigencia y relevancia en el contexto actual de la organización.

Promover una cultura de mejora continua, incentivando a los colaboradores a identificar oportunidades de mejora en la gestión de riesgos y proponer soluciones innovadoras.

Realizar sesiones de capacitación y sensibilización sobre la importancia de la administración de riesgos, dirigidas a todos los niveles de la organización, con el fin de fortalecer la conciencia y el compromiso de los colaboradores.

Establecer un sistema de seguimiento de acciones correctivas y preventivas derivadas de las evaluaciones de riesgos, para asegurar su implementación oportuna y efectiva.

Fomentar la participación activa de la Alta Dirección en el proceso de administración de riesgos, garantizando su apoyo y compromiso con la toma de decisiones para garantizar la sostenibilidad de la Administración del Riesgo en la organización.

La combinación de estas medidas adicionales con el seguimiento realizado por Control Interno fortalecerá el proceso de administración de riesgos y contribuirá a la mejora continua de la gestión de riesgos en la organización.

Elaborado por: Kevin Andres Solaque Arango