promueve+

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

Contenido

1. INTRODUCCIÓN 2
2. OBJETIVO 2
3. ALCANCE 3
4. CONDICIONES GENERALES 3
5. GLOSARIO 3
6. DESCRIPCIÓN 5
   6.1 Organigrama 6
7. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO 6
   Metodología por utilizar 6
   Herramientas para la Gestión del Riesgo 6
   Análisis del riesgo 7
      Determinar la probabilidad 7
      Análisis de la probabilidad (Riesgo de corrupción) 7
   Determinar la probabilidad riesgos de seguridad digital 8
   Calificación del Impacto 8
   Medidas de Tratamiento de Riesgo 8
   Periodicidad para el monitoreo, revisión y seguimiento de los riesgos 11
   Líneas de Responsabilidad frente a la gestión del riesgo 12
   Comunicación 13
8. Bibliografía 13

1. INTRODUCCIÓN

La administración del riesgo contextualiza diferentes variables como elementos de control y sus interrelaciones, para que las empresas evalúen e intervengan aquellos eventos, tanto internos como externos, que puedan perturbar de manera positiva o negativa el logro de los objetivos empresariales; favorece a que la empresa consolide su sistema de control interno y forje una cultura de autocontrol y autoevaluación al interior de esta. Teniendo en cuenta que la administración de riesgos es estratégica para el logro de los objetivos empresariales y de procesos, en este manual se enuncia la política general de acción que permitirá tomar decisiones relativas a la administración del riesgo; así mismo, este manual está alineado con el Modelo Integrado de Planeación y Gestión MIPG, la Guía para la Gestión del Riesgo establecida por el Departamento Administrativo de la Función Pública; el Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación y la Norma Técnica sobre Gestión del Riesgo, ISO 31001.

En la actualidad, la tendencia más común es la valoración del riesgo como una amenaza; en este sentido, los esfuerzos institucionales se dirigen a reducir, mitigar o eliminar su ocurrencia. Sin embargo, el riesgo como oportunidad, implica que su gestión está dirigida a optimizar los resultados que este genera. En este sentido, PROMUEVE MÁS S.A.S., no es inmune al riesgo, teniendo en cuenta que estos son dinámicos en su naturaleza y las consecuencias potenciales que se enfrentan son cada vez más complejas.

Asimismo, los constantes cambios, la dinámica de la economía mundial, las expectativas más exigentes de la comunidad, los requerimientos del Estado colombiano, el impacto de una posible falla en los controles, los rápidos cambios en las tecnologías y un sinnúmero de otros factores pueden afectar la empresa, de tal manera que es necesario generar resiliencia y tener una organización preparada ante cualquier afectación.

2. OBJETIVO

Establecer los lineamientos generales e instrumentos requeridos para la administración y el control de los riesgos que puedan afectar el logro de los objetivos institucionales y de proceso, con el propósito de minimizar potenciales desviaciones y efectos negativos para la empresa.

3. ALCANCE

La política de administración de riesgos es aplicable a todos los procesos de la empresa y a las acciones realizadas por los servidores y/o contratistas durante el ejercicio de sus funciones. Circunscribe los principios básicos y metodológicos para la administración y gestión de riesgos y oportunidades de tipo estratégico, operacional y de cumplimiento.

4. CONDICIONES GENERALES

Una vez realizada la fase de valoración del riesgo después de definidos los controles se debe aplicar la opción de tratamiento. Esto se define a partir de datos cuantitativos del nivel de riesgo residual, de la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la empresa, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento.

5. GLOSARIO

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Administración de riesgos: Proceso efectuado por la Alta Dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino con la apropiación de la evaluación de los riesgos como una parte natural del proceso de planeación institucional (INTOSAI, 2000).

Análisis de riesgo: Uso sistemático de la información disponible para valorar los riesgos en función de las causas o agentes que los generan, las consecuencias generadas por un incidente y/o evento, su severidad y la posibilidad de ocurrencia de este, con el fin de estimar la zona de riesgo inicial (riesgo inherente).

Apetito de Riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir

del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Consecuencia: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Medida que permite reducir o mitigar un riesgo.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Factores de riesgo: Son las fuentes generadoras de riesgos.

Integridad: Propiedad de exactitud y completitud.

Impacto: Las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo es Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

Probabilidad: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la

infraestructura o por la ocurrencia de acontecimientos externos.

Riesgos de corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

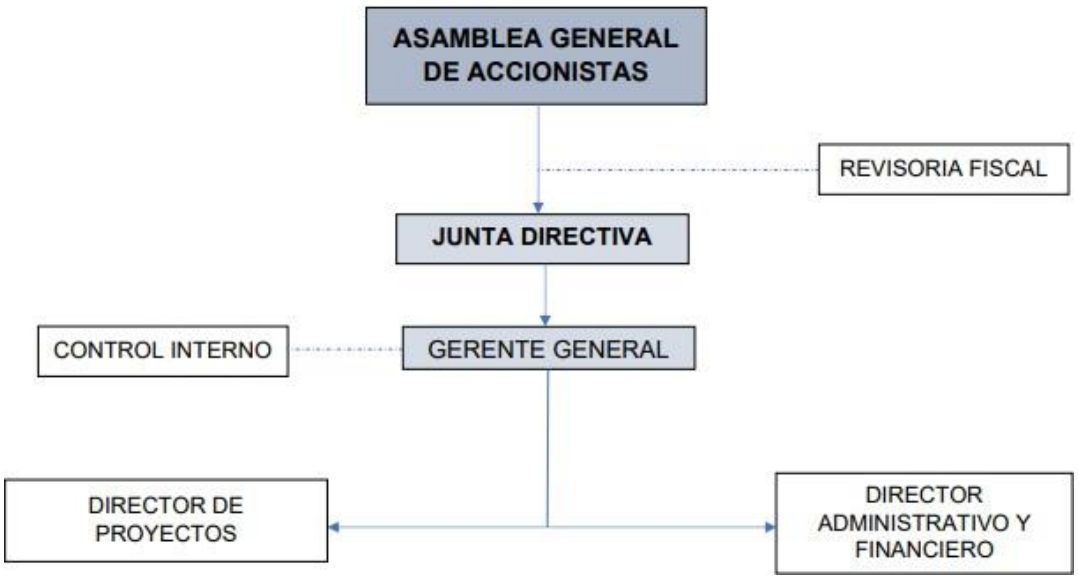
Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

6. DESCRIPCIÓN

PROMUEVE MÁS S.A.S. se compromete con la asignación de recursos, condiciones, lineamientos, responsabilidades e instrumentos necesarios para la adecuada administración de los riesgos, asegurando de este modo y de manera razonable, el logro de sus objetivos e iniciativas, implementando las acciones necesarias para una efectiva administración del riesgo, que permitan su identificación, valoración, monitoreo, tratamiento y comunicación en coherencia con los roles que desempeña cada una de las líneas de defensa.

Organigrama



7. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO

Metodología por utilizar

Se utilizará para riesgos de Gestión la metodología moderna publicada por el Departamento Administrativo de la Función Pública DAFP para la administración del riesgo y el diseño de controles en entidades públicas y/o la que modifique o sustituya. En cuanto a los riesgos de corrupción la metodología adoptada es la instituida por la Secretaría de Transparencia de la Presidencia de la República. Además, se utilizará la metodología vigente por Colombia Compra Eficiente, para la administración de riesgos para el proceso de contratación dirigido a los partícipes del sistema de compras y contratación pública.

Herramientas para la Gestión del Riesgo

PROMUEVE MÁS S.A.S. cuenta con el formato *"Matriz Mapa de Riesgos",* como herramienta asociada al Manual *"Metodología para la Administración de Riesgos de Gestión, Corrupción y Seguridad de la Información".* En este se gestionan los riesgos, desde la identificación de los factores de riesgos hasta el respectivo seguimiento de acuerdo con la periodicidad establecida.

Análisis del riesgo

En el análisis de riesgos se establece la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

Determinar la probabilidad

Por probabilidad se entiende la posibilidad de ocurrencia del riesgo, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año. Con base en lo anterior, la exposición al riesgo estará asociada a la frecuencia de ejecución de la actividad generadora del riesgo que se esté analizando, es decir, al número de veces que se ejecuta la actividad, y por ende que se pasa por el punto de riesgo en el periodo de 1 año, en la tabla 1 se establecen los criterios para definir el nivel de probabilidad.

Tabla 1. Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 52 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 52 veces al año y máximo 300 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 300 veces por año	100%

Fuente: Modificado de DAFP, 2020. Guía para la Administración del Riesgo y diseño de controles en entidades públicas.

Análisis de la probabilidad (Riesgo de corrupción)

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde la frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda.

Determinar la probabilidad riesgos de seguridad digital

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas para los riesgos de gestión.

Calificación del Impacto

Riesgos de Gestión y de Seguridad de la Información

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales, cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto. En la tabla 3 se establecen los criterios para definir el nivel de impacto.

Tabla 3. Criterios para definir el nivel de impacto

Tabla Criterios para definir el nivel de impacto

	Afectación Económica (o presupuestal)	Pérdida Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de alguna área de la organización
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país

Fuente: Adaptado de DAFP, 2020. Guía para la Administración del Riesgo y diseño de controles en entidades públicas, V05.

Medidas de Tratamiento de Riesgo

El objetivo de esta etapa es identificar las opciones para tratar los riesgos de acuerdo con el nivel de riesgo residual obtenido, esto para procesos en funcionamiento, pero cuando se trate de procesos nuevos se procede a partir del riesgo inherente. En PROMUEVE MÁS S.A.S. se ha definido que los

riesgos que se **tratan** de forma adicional al uso de controles (criterio de aceptabilidad del riesgo), son aquellos que estén en las siguientes situaciones:

- ✓ Si el riesgo residual es extremo, alto o moderado.
- ✓ Si hay causas sin controles asociados.
- ✓ Si hay controles sin evidencias.

Dentro de las actividades a desarrollar en esta etapa se encuentra la de identificar y formalizar las opciones de tratamiento adecuadas, dentro de las cuales se encuentran:

a) Evitar: Después de realizar un análisis y considerar que el nivel del riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

b) Aceptar: Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización. Para esta opción se debe tener en cuenta las siguientes consideraciones:

- ✓ En este caso no se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.
- ✓ La aceptación del riesgo puede ocurrir sin tratamiento, lo que implica que los riesgos aceptados están sujetos a monitoreo.
- ✓ Los **riesgos de corrupción** están excluidos de esta medida de manejo o control. Es decir, ningún riesgo de corrupción podrá ser aceptado.
- ✓ Para el caso de riesgos residuales que sean aceptados por el líder del proceso o dueño del riesgo y que tengan calificación extrema, alta o moderada, deberá **reportarse** a la Oficina Asesora de Planeación formalmente a través de un memorando que justifique el porqué de la situación y posteriormente al Comité Institucional de Coordinación de Control Interno.

c) Reducir: Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante mitigar o compartir el riesgo.

- ✓ **Compartir:** Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, transfiriendo o compartiendo una parte del riesgo. Para el caso que se decida tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas, la responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional. De igual forma, los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.
- ✓ **Mitigar:** Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. Por lo tanto, se adoptan medidas para reducir la probabilidad o el impacto del riesgo. No necesariamente es un control adicional.

Nota: frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para

la gestión y control de tareas o proyectos. Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un **plan de acción** que especifique: I) responsable, II) fecha de implementación, y III) fecha de seguimiento. Con el propósito de ilustrar las estrategias para combatir los riesgos de gestión y seguridad de la información, en la siguiente tabla se indican las opciones de tratamiento aplicables de acuerdo con la zona de riesgo:

Tabla 5. Opciones de tratamiento Riesgo de Gestión y Seguridad de la Información

Zona de riesgo	Semáforo	Evitar	Reducir		Aceptar
			Compartir	Mitigar	
Extremo	Rojo	X	X	X	X
Alto	Naranja	X	X	X	X
Moderado	Amarillo	X	X	X	X
Bajo	Verde				X

De la misma forma, se ilustran las estrategias para combatir el riesgo de corrupción de acuerdo con la zona de riesgo:

Tabla 6. Opciones de tratamiento Riesgo de Corrupción

Zona de riesgo	Semáforo	Evitar	Reducir		Aceptar
			Compartir	Mitigar	
Extremo	Rojo	X	X	X	Ningún riesgo de corrupción podrá ser aceptado.
Alto	Naranja	X	X	X	
Moderado	Amarillo	X	X	X	
Bajo	Verde				

Nota 1: Para los riesgos de corrupción, la respuesta será evitar, compartir o mitigar el riesgo.

Nota 2: Cuando un riesgo de corrupción se encuentre en zona de riesgo (**Moderado:** 3, **Rara Vez:** 1), no aplicarán las opciones de tratamiento compartir o reducir el riesgo, ya que en este caso el

riesgo se encontrará en su máxima disminución posible dentro del mapa de calor.

Periodicidad para el monitoreo, revisión y seguimiento de los riesgos

El monitoreo y revisión de los riesgos corresponde a la Primera Línea de Defensa como un seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos. Por otra parte, el monitoreo y revisión realizado por la Oficina Asesora de Planeación – OAP se lleva a cabo en los siguientes cortes:

- Primer monitoreo: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los cinco (05) primeros días del mes de mayo.
- Segundo monitoreo: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los cinco (05) primeros días del mes de septiembre.
- Tercer monitoreo: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los cinco (05) primeros días del mes de enero.

El Jefe de Control Interno o quien haga sus veces, debe proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del Sistema de Control Interno. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles. Por consiguiente, de acuerdo con la normatividad, se deberá realizar tres seguimientos a los riesgos corrupción, de acuerdo con lo siguiente:

- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Hay que asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

Líneas de Responsabilidad frente a la gestión del riesgo.

Las responsabilidades se definen mediante la línea estratégica y las tres líneas de defensa las cuales se encuentran definidas en la siguiente tabla:

Líneas de Defensa	Responsables	Operatividad
Línea estratégica	Alta Dirección y Comité Institucional de Coordinación de Control Interno.	Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento. Analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos
1ª. Línea de Defensa	Líderes de proceso, programas y proyectos y sus equipos (En general servidores públicos de todos los niveles de la organización).	Desarrollar e implementar procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora, reportando a la segunda línea sus avances o dificultades. Diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad. Asimismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad, emprender las acciones de mejoramiento para su logro.
2ª. Línea de Defensa	A cargo de los servidores que tienen responsabilidades directas de monitoreo y revisión de los controles de la gestión del riesgo: jefes de planeación, supervisores o interventores de proyectos, coordinadores de otros sistemas de gestión de la entidad, coordinadores de equipos de trabajo, comités de riesgos (donde existan), comité de contratación, áreas financieras, Oficina de Información Pública del Interior - OIP, entre otros que generen información para el Aseguramiento de la operación.	Monitorear la gestión de riesgos y control ejecutada por la primera línea de defensa complementando su trabajo. Hay que asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas eficaces, de gestión de riesgo. Consolidan y analizan información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos. Asesorar a la 1ª línea de defensa en temas clave para el Sistema de Control Interno: I) riesgos y controles; II) planes de mejoramiento; III) indicadores de gestión; IV) procesos y procedimientos.
3ª. Línea de Defensa	A cargo de la Oficina de Control Interno, Auditoría Interna o quién haga sus veces.	Proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del Sistema de Control Interno. El alcance de este aseguramiento, a través de la auditoría interna, cubre todos los componentes del Sistema de Control Interno. Genera a través de su rol de asesoría un orientación técnica y recomendaciones frente

Líneas de Defensa	Responsables	Operatividad
		a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces. Monitorear la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. Brinda un nivel de asesoría proactiva y estratégica, frente a la Alta Dirección y los líderes de proceso.

Comunicación

Esta estrategia de comunicación busca socializar e interiorizar en todos los sectores de la empresa que presten sus servicios a PROMUEVE MÁS S.A.S., de los distintos niveles de responsabilidad, sobre la importancia de la gestión del riesgo así:

- **Nivel de procesos**: Teniendo en cuenta las responsabilidades sobre una base del día a día estará a cargo de los líderes de proceso y consiste en realizar la divulgación de los mapas de riesgos por proceso al interior de sus respectivos equipos de trabajo.

8. Bibliografía

DAFP. (2020). Guía para la administración del riesgo y el diseño de controles en entidades públicas Bogotá: Departamento Administrativo de la Función Pública.

NTC-ISO 31000. (2018). Gestión del riesgo. Principios y directrices. Icontec Internacional.

Decreto 2641 de 2012. Por el cual se reglamentan los artículos 73 y 76 de la Ley 1474 de 2011.