Política Administración del Riesgo

Marzo de 2022

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

PRESENTACIÓN.

La E.S.E Hospital San Juan de Dios de Pamplona en el marco de la implementación del Modelo Integrado de Planeación y Gestión – MIPG, tomando como herramienta para la consecución de los objetivos institucionales la Administración del Riesgo, presenta su Política de Administración del Riesgo de Gestión, Corrupción y Seguridad de la información, la cual se establece acorde a las directrices impartidas por el Departamento Administrativo de la Función Pública - DAFP.

OBJETIVO.

Establecer los lineamientos para el control y la gestión de los riesgos de gestión, de corrupción y de seguridad de la información a los que se encuentra expuesta la E.S.E Hospital San Juan de Dios - Pamplona, con el fin de minimizar su incidencia sobre la consecución de los objetivos estratégicos y de los procesos, en pro de garantizar una eficiente y efectiva prestación del servicio de salud.

ALCANCE.

La política de riesgos es aplicable a todos los procesos y proyectos de la Entidad y a todas las acciones ejecutadas por el personal durante el ejercicio de sus funciones y/o cumplimiento de sus actividades, bajo la responsabilidad de los líderes de proceso y línea de defensa.

Esta política involucra el contexto, la identificación, valoración, tratamiento, monitoreo, revisión, comunicación, consulta y el análisis de los riesgos.

POLÍTICA GENERAL.

La política de Administración de Riesgo de la E.S.E Hospital San Juan de Dios de Pamplona, tiene un carácter estratégico y busca que la entidad se comprometa a administrar sus riesgos de gestión, corrupción y/o seguridad de la información, inherentes a cada uno de sus procesos y/o proyectos, estableciendo y ejecutando actividades de control, que le permitan contrarrestar aquellos eventos que puedan afectar el logro de sus objetivos.

METODOLOGÍA

Para la aplicación de la Administración del Riesgo en la entidad, se tendrán en cuenta los lineamientos del Modelo Integrado de Planeación y Gestión - MIPG, la Guía para la Administración de Riesgo y el diseño de Controles en entidades públicas, emitida por el Departamento Administrativo de la Función Pública – Versión 5 y el procedimiento y formatos que a partir de la misma se establezcan en la entidad.

Para la identificación de los riesgos, se deberá tener en cuenta aspectos relacionados con:

Análisis del contexto interno de la entidad:

Procesos: Capacidad, diseño, entradas, proveedores, salidas, clientes, actividades.
Financieros: Presupuesto funcionamiento, presupuesto inversión.
Personal: Formación, competencias, disponibilidad, seguridad y salud en el trabajo, sentido de pertenencia, cultura organizacional.
Tecnológicos: Disponibilidad de sistemas de información, mantenimiento de sistemas de información
Comunicación: Flujo de información, canales de comunicación utilizados.
Direccionamiento: Liderazgo, trabajo en equipo, direccionamiento estratégico, planeación institucional.
Estratégicos: Misión, Visión, Objetivos.

Análisis de factores del contexto externo de la entidad:

Sectoriales: Competencia, regulaciones.
Políticos: Políticas públicas, cambios de gobierno.
Sociales: Orden público, demografía, responsabilidad social, crisis humanitaria.
Tecnológicos: Avances en tecnología, acceso a sistemas de información externos, gobierno digital.
Económicos: Disponibilidad de recursos, situación económica,
Legal: Normatividad y regulación externa aplicable a la entidad.

Resultados de evaluaciones llevadas a cabo por los organismos de control.

Presiones internas o externas que puedan derivar actos de corrupción.

Identificación de activos de seguridad de información

TIPOS Y DESCRIPCION DE RIESGOS

De acuerdo a su tipo los riesgos pueden ser:

Riesgos de gestión:

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

Descripción del riesgo de gestión:

Para evitar la subjetividad en la redacción del riesgo y permitir entender la forma como se puede manifestar el mismo, así como sus causas inmediatas y causas principales o raíz, el riesgo se debe describir siguiendo la siguiente estructura, iniciando siempre con "Posibilidad de":

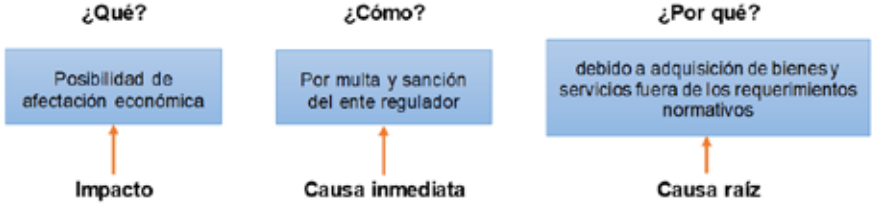
Donde:

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

Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo puede existir más de una causa o subcausas que pueden ser analizadas.

De manera práctica tenemos:



Lo que debemos evitar en la adecuada descripción del riesgo:

No describir como riesgos omisiones ni desviaciones del control.
Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.

No describir causas como riesgos
Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

No describir riesgos como la negación de un control.
Ejemplo: retrasos en la prestación del servicio por no contar con digiturno para la atención.

No existen riesgos transversales, lo que pueden existir son causas transversales.
Ejemplo: pérdida de expedientes.

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.

Descripción del riesgo de corrupción:

Con el propósito de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, el riesgo de corrupción se debe describir teniendo en cuenta los siguientes componentes e iniciando siempre con "Posibilidad de":

De manera práctica tenemos:
Posibilidad de recibir o solicitar cualquier dadiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.

Riesgos 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.

Para identificar los riesgos de seguridad de la información, es necesario identificar los activos de información, que corresponde a cualquier elemento que tenga valor para la entidad, sin embargo, en el contexto de seguridad digital, son activos elementos tales
Como: Aplicaciones, servicios web, redes, información física y digital, tecnologías de información, tecnologías de operación.

Para identificar los activos se deben tener en cuenta los siguientes pasos:

Se podrán identificar tres (3) riesgos inherentes de seguridad de la información, que corresponden a:

Pérdida de la confidencialidad
Pérdida de la integridad
Pérdida de la disponibilidad

CLASIFICACION DE RIESGOS

Los riesgos identificados se pueden clasificar en las siguientes categorías:

Ejecución y administración de procesos: Pérdidas derivadas de errores en la ejecución y administración de procesos.

Fraude externo: Perdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).

Fraude interno: Perdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos, abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos un participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para si mismo o para terceros.

Fallas tecnológicas: Errores en hardware, telecomunicaciones, interrupción de servicios básicos.

Relaciones laborales: Perdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.

Usuarios, productos y prácticas: Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a estos.

Daños a activos fijos/eventos externos: Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

CRITERIOS PARA CALIFICAR PROBABILIDAD

Los siguientes corresponden a los criterios que se tendrán en cuenta para determinar la probabilidad en riesgos de gestión, de corrupción y/o seguridad digital.

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 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 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

CRITERIOS PARA CALIFICAR IMPACTO

Criterios para calificar el impacto en riesgos de gestión y de seguridad de la información

Los siguientes corresponden a los criterios que se tendrán en cuenta para determinar el impacto en riesgos de gestión.

	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 provedores
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 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

CRITERIOS PARA CALIFICAR EL IMPACTO EN RIESGOS DE CORRUPCIÓN

Los siguientes corresponden a los criterios que se tendrán en cuenta para determinar el impacto en riesgos de corrupción

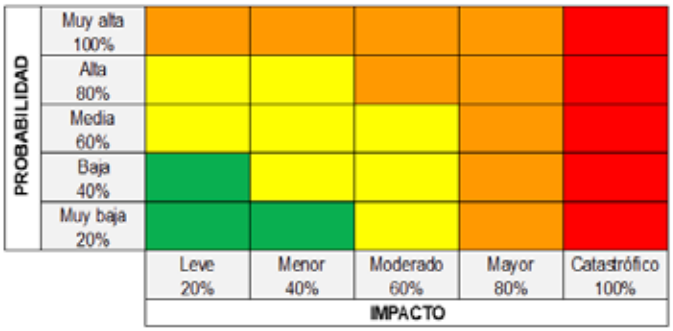
N°	Pregunta Si el riesgo de corrupción se materializa podría...	Respuesta SI	 NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la Entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?		
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?		
9	¿Generar pérdida de información de la Entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
	TOTAL	0	0

- Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto Moderado.
- Responder afirmativamente de SEIS a ONCE preguntas genera un impacto Mayor.
- Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto Catastrófico.

MAPA DE CALOR

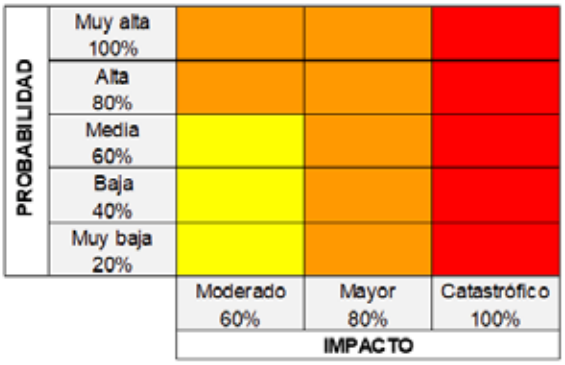
A continuación, se muestra el mapa de calor que se tendrá en cuenta para determinar la intersección entre la probabilidad y el impacto y con ello determinar el nivel de severidad del riesgo.

Riesgos institucionales



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

Riesgos de corrupción



M Zona de riesgo moderada
A Zona de riesgo alta
E Zona de riesgo extrema

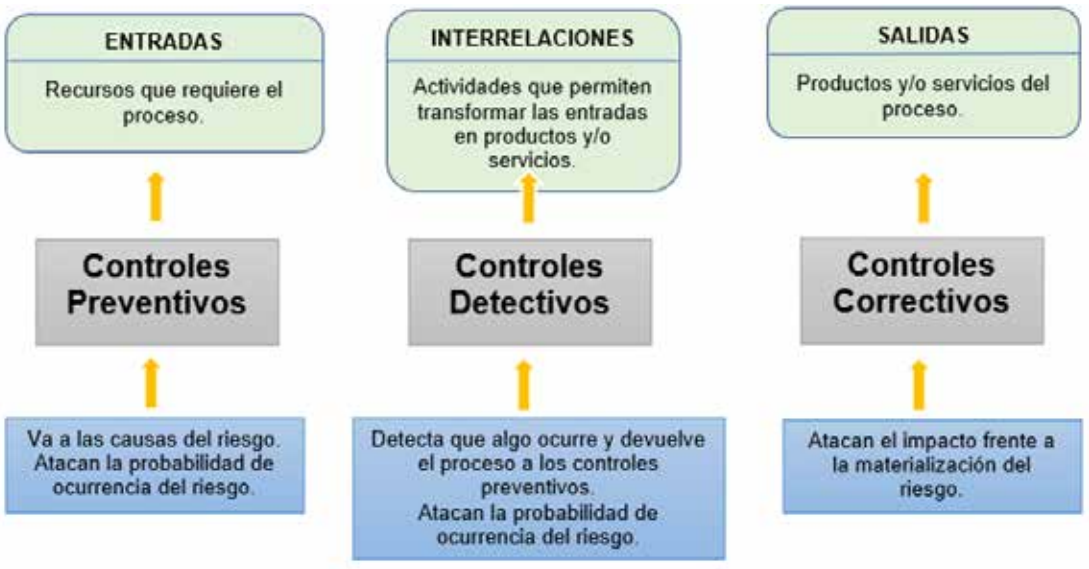
DISEÑO DE CONTROLES

Los controles o actividades de control son medidas que permiten reducir o mitigar las causas que hacen que el riesgo se materialice.

La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.

Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

A través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión, para comprender lo anterior a continuación se muestra de manera gráfica:



Acorde con lo anterior, tenemos las siguientes tipologías de controles:

Control preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

Control manual: controles que son ejecutados por personas.

Control automático: son ejecutados por un sistema.

ESTRUCTURA PARA LA ADECUADA DESCRIPCIÓN DEL CONTROL

Responsable: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.

Periodicidad: indica cada cuanto tiempo se ejecuta el control.

Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.

Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

Documentación: el control está documentado en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.

Frecuencia: el control se aplica siempre que se realiza la actividad que conlleva el riesgo.

Evidencia: el control deja un registro permite evidencia la ejecución del control.

NIVEL DE ACEPTACIÓN Y TRATAMIENTO DE RIESGOS

TIPO DE RIESGO	NIVEL DE SEVERIDAD DEL RIESGO	NIVEL DE ACEPTACIÓN
Riesgo de Gestión y Riesgo de Seguridad Digital	Bajo	- Se acepta el riesgo y los posibles efectos de su materialización. Se gestiona mediante las actividades y/o controles del proceso o proyecto. El riesgo debe ser objeto de seguimiento continuo.
	Moderado	- Se mitiga el riesgo mediante acciones, no necesariamente corresponden a controles adicionales. - Se hace seguimiento trimestral.
	Alto y Extremo	- Se mitiga el riesgo mediante acciones, no necesariamente corresponden a controles adicionales. - O se evita le riesgo, cancelando la actividad o actividades que causan los riesgos. - O se terceriza el proceso o proyecto o se traslada el riesgo. - Se hace seguimiento mensual.
Riesgo de corrupción	Moderado, Alto y Extremo	- Ningún de riesgo de corrupción es aceptado. - Se mitiga el riesgo mediante acciones, no necesariamente corresponden a controles adicionales - O se evita el riesgo, cancelando la actividad o actividades que causan los riesgos. - O se terceriza el proceso o proyecto o se traslada el riesgo. - Se hace seguimiento mensual

ACCIONES A EMPRENDER ANTE LA MATERIALIZACIÓN DE RIESGOS

TIPO DE RIESGO	RESPONSABLE	ACCIONES
Riesgo de corrupción	Oficina de Control Interno	– Convocar al Comité de Coordinación de Control Interno e informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos. – Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo. – Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos y sus controles asociados. – Verificar que se tomaron las acciones y se actualizó el mapa de riesgos.
	Líder del proceso u otro(s) funcionario(s) que participa(n) o interactúa(n) con el proceso	– Informar a la Alta Dirección y a la oficina de control interno sobre el hecho encontrado. – De considerarlo necesario, realizar la denuncia ante el ente de control respectivo – Iniciar con las acciones de contingencia necesarias. – Realizar el análisis de causas y determinar acciones preventivas y de mejora. – Análisis y actualización del mapa de riesgos.
Riesgo de Gestión y de Seguridad Digital (Zona de riesgo Extrema, Alta y Moderada)	Oficina de Control Interno	– Informar al líder del proceso sobre el hecho encontrado. – Orientar al líder del proceso para que realice la revisión, análisis y acciones correspondientes para resolver el hecho. – Verificar que se tomaron las acciones y que se actualizó el mapa de riesgos correspondiente. – Convocar al Comité de Coordinación de Control Interno e informar sobre la actualización realizada.
	Líder del proceso u otro(s) funcionario(s) que participa(n) o interactúa(n) con el proceso	– Tomar las acciones de contingencia necesarias, dependiendo del riesgo materializado. – Iniciar el análisis de causas y determinar acciones preventivas y/o de mejora. – Analizar y actualizar el mapa de riesgos. – Informar a la Alta Dirección sobre el hallazgo y las acciones tomadas.
Riesgo de Gestión y de Seguridad Digital (Zona de riesgo Baja)	Oficina de Control Interno	– Informar la líder del proceso sobre el hecho. – Orientar técnicamente sobre las acciones determinadas en la política de Riesgos institucional.
	Líder del proceso u otro(s) funcionario(s) que participa(n) o interactúa(n) con el proceso	– Iniciar el análisis de causas y determinar acciones preventivas y/o de mejora. – Analizar y actualizar el mapa de riesgos

ACCIONES DE CONTINGENCIA

Para los riesgos ubicados en zonas de riesgo Moderada, Alta y Extrema, los responsables de los procesos y/o proyectos deberán establecer acciones de contingencia, entendidas éstas como las acciones que se implementarán una vez un riesgo se materializa.

ROLES Y RESPONSABILIDADES

En la E.S.E. Hospital San Juan de Dios son responsables de la Administración del riesgo las siguientes instancias:

Línea de defensa	Responsables	Responsabilidades frente al riesgo
Estratégica	Alta dirección Comité de Control Interno	– Establece y aprueba la Política de Administración del Riesgo. – Analiza los cambios en el entorno tanto interno como externo, que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles. – Hace seguimiento a cada una de las etapas de la gestión del riesgo. – Realiza seguimiento y análisis periódico a los riesgos institucionales – Identifica posibles riesgos que se estén materializado. – Revisa periódicamente informes de riesgos que se han materializado. – Realimenta al Comité de Gestión y Desempeño sobre los ajustes que se deban hacer frente a la gestión del riesgo
Primera Línea	Servidores públicos en todos los niveles de la entidad.	– Identifican y valoran los riesgos que pueden afectar el logro de los objetivos institucionales. – Definen y diseñan los controles a los riesgos. – A partir de la política de administración del riesgo, establecen sistemas de gestión de riesgos y las responsabilidades para controlar riesgos específicos bajo la supervisión de la alta dirección. Con base en esto, establecen los mapas de riesgos. – Identifican y controlan los riesgos relacionados con posibles actos de corrupción en el ejercicio de sus funciones y el cumplimiento de sus objetivos, así como en la prestación del servicio y/o relacionados con el logro de los objetivos.

		– Implementan procesos para identificar, disuadir y detectar fraudes; y revisan la exposición de la entidad al fraude con el auditor interno de la entidad
Segunda Línea	Subdirecciones	– Informan sobre la incidencia de los riesgos en el logro de objetivos y evalúan si la valoración del riesgo es la apropiada. – Aseguran que las evaluaciones de riesgo y control incluyan riesgos de fraude. – Monitorean cambios en el riesgo legal, regulatorio y de cumplimiento. – Consolidan los seguimientos a los mapas de riesgo. – Elaboran informes consolidados para las diversas partes interesadas. – Siguen los resultados de las acciones emprendidas para mitigar los riesgos, cuando haya lugar. – Los supervisores y/o interventores de contratos realizan seguimiento a los riesgos de estos e informan las alertas respectivas.
Tercera Línea	Oficina de Control Interno	– Asesorar en la metodología para la identificación y administración de los riesgos, en coordinación con la segunda línea de defensa. – Identificar y evaluar cambios que podrían tener un impacto significativo en el SCI, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna. – Comunicar al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías. – Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad. – Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas.

ACCIONES PARA LA APROPIACIÓN DE LA GESTIÓN DEL RIESGO

Para contribuir a una adecuada gestión del riesgo al interior de la entidad, se llevarán a cabo las siguientes acciones:

- Capacitaciones para el fortalecimiento conceptual y operativo de la gestión del riesgo, que garanticen la competencia necesaria del personal de la Entidad.
- Sensibilización y comunicación, que promuevan el pensamiento basado en riesgos.

- Asesoría y acompañamiento para el desarrollo del enfoque de administración de riesgos en las actividades diarias.
- Seguimiento a los riesgos identificados en los procesos y que hacen parte del mapa de riesgos institucional.
- Divulgación de los resultados de la gestión de riesgos en la Entidad.

REVISIÓN Y ACTUALIZACIÓN

Los mapas de riesgos por proceso y/o proyecto y el mapa de riesgos institucional, serán objeto de revisión y actualización mínimo una vez al año, o cuando las circunstancias de los procesos, proyectos y/o eventualidades institucionales así lo ameriten, a partir de cualquier hecho de carácter interno o externo que los afecte. Para tal resultado se tendrá en cuenta la metodología dispuesta por el Departamento Administrativo de la Función Pública y el procedimiento documentado al interior de la entidad.

MONITOREO Y REVISIÓN POR LINEAS DE DEFENSA

El monitoreo y revisión de la gestión del riesgo al interior de la entidad por líneas de defensa esta asignada de la siguiente manera:

Línea de defensa	Responsables	Responsabilidades frente al riesgo
Estratégica	Alta dirección Comité de Control Interno	– Definir el marco general para la gestión del riesgo y el control y supervisar su cumplimiento.
Primera Línea	Servidores públicos en todos los niveles de la entidad	– Diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad. – Orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprenden las acciones de mejoramiento para su logro.
Segunda Línea	Subdirecciones	– Monitorear la gestión del riesgo y control, ejecutada por la primera línea de defensa complementando su trabajo.