POLÍTICA DE ADMINISTRACIÓN DE RIESGOS
UNIDAD DEL SPE

Bogotá, marzo de 2024

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. OBJETIVO

Establecer las directrices de la Administración de Riesgos de la Unidad Administrativa Especial del Servicio Público de Empleo referenciadas a través de la Guía de Administración de Riesgos y Diseño de Controles Versión 6 emitida por el Departamento Administrativo de la Función Pública, a través de la identificación y el adecuado tratamiento de los riesgos asociados a los procesos institucionales, los riesgos de corrupción y los riesgos de seguridad de la información, entre otros, para garantizar el cumplimiento de su misión y objetivos estratégicos, fortaleciendo la gestión institucional frente a situaciones que puedan impedir el cumplimiento de sus funciones.

2. ALCANCE

La Política de Administración de Riesgos de la Unidad Administrativa Especial del Servicio Público de Empleo tiene como propósito el manejo de los riesgos asociados a los procesos estratégicos, misionales, de apoyo y de evaluación, definidos por la organización en el marco del Sistema Integrado de Gestión. Atendiendo a lo señalado por la Ley 1474 de 2011 en su artículo 73, la identificación, calificación, clasificación y valoración de los riesgos de corrupción se realizará siempre en el marco de los procesos, por lo cual, la presente política es aplicable también para este tipo de riesgos, así como, los riesgos que se identifiquen para la seguridad de la información.

3. RESPONSABLES

- El responsable de la definición de las Políticas de Administración de Riesgos es el Comité Institucional de Coordinación de Control Interno.
- El Asesor de la Dirección, con funciones de Planeación como representante de la Dirección General realiza la coordinación de la implementación del Modelo Integrado de Planeación y Gestión, partiendo de allí se realizará la definición y orientación metodológica de la identificación, análisis y valoración de los riesgos.
- Los Directivos de la Unidad, entendidos como el Secretario (a) General y los Subdirectores, son los responsables de la administración del riesgo, en lo que corresponde a la identificación, valoración y tratamiento del riesgo, para tomar acciones para evitar, reducir, asumir, transferir o compartir el riesgo, al igual que mantener actualizados los mapas de riesgos por procesos, implementar los controles y las acciones preventivas, realizar seguimiento para verificar su efectividad, proponer cambios, velar por su adecuada documentación, por su socialización y aplicación.
- El Subdirector de Desarrollo y Tecnología en coordinación con la Secretaría General, será el encargado de liderar toda la formulación de los riesgos de seguridad de la información, considerando los parámetros establecidos en la *Guía para la administración del riesgo y el diseño de controles en entidades públicas* del Departamento Administrativo de la Función Pública, los lineamientos que en materia expida el Ministerio de las Tecnologías de la Información y las Comunicaciones en el marco de la Política de Gobierno Digital y las mejores prácticas.
- El Asesor de la Dirección, con funciones de Control Interno, como parte del proceso auditor, efectuará de manera aleatoria monitoreo a las acciones definidas en los Mapas de Riesgo y evaluará la efectividad de los controles.

4. ESQUEMA DE LINEAS DE DEFENSA DE LA UNIDAD DEL SPE

Según la nueva estructura del Modelo Estándar de Control Interno MECI, adoptada en el marco de la actualización del Modelo Integrado de Planeación y Gestión MIPG bajo el Decreto 1499 de 2017, se establecieron las siguientes líneas de defensa como ejes articuladores del Control Interno:

4.1 Línea de Defensa Estratégica

Conformada por la Alta Dirección y el Comité de Coordinación de Control Interno, este nivel analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos (objetivos, metas, indicadores). En consecuencia, tendrá la responsabilidad de definir el marco general para la gestión del riesgo (política de administración del riesgo) y garantizar el cumplimiento de los planes de la entidad.

1° Línea de Defensa: compuesta por los Gerentes Públicos o gerentes operativos o los líderes de los procesos, quienes gestionan los riesgos y son responsables de implementar acciones correctivas, igualmente detecta las deficiencias de control. La gestión operacional se encarga del mantenimiento efectivo de controles internos y de ejecutar procedimientos de riesgo y control en el día a día. La gestión operacional identifica, evalúa, controla y mitiga los riesgos.

2° Línea de Defensa: compuesta por aquellos servidores con responsabilidades directas frente al monitoreo y evaluación del estado de los controles y la gestión del riesgo. Entre ellos pueden citarse: jefes de planeación o quienes hagan sus veces, coordinadores de equipos de trabajo, supervisores e interventores de contratos o proyectos, comités de riesgos (donde existan), comité de contratación, áreas financieras, de TIC, entre otros que generen información para el Aseguramiento de la operación.

Esta línea adelanta tareas en relación con el control y la gestión de riesgos, las funciones de cumplimiento, seguridad, calidad y otras similares supervisan la implementación de prácticas de gestión de riesgo eficaces por parte de la gerencia operativa, y ayudan a los responsables de riesgos a distribuir la información adecuada sobre riesgos hacia arriba y hacia abajo en la entidad.

3° Línea de Defensa: esta línea da cuenta de la función de auditoría interna, a través de un enfoque basado en el riesgo, que proporciona aseguramiento sobre la eficacia de la gestión de riesgos y el control interno, incluidas las maneras en que funciona la primera y segunda línea de defensa.

En este sentido, para la Unidad Administrativa Especial del Servicio Público de Empleo se tendrá que las líneas de defensa en mención están conformadas por:

- **Línea de Defensa Estratégica:** Comité Institucional de Control Interno
- **1° Línea de Defensa:** Directora General, Secretario General, Subdirectores Misionales
- **2° Línea de Defensa:** Asesora de Planeación**,** supervisores y coordinadores de grupos de trabajo.
- **3° Línea de Defensa:** Asesor de Control Interno

5. DEFINICIONES

- **Activo**: Es el hardware, sistemas de software o información que tienen valor para una organización y se identifican en cada proceso de acuerdo con el desarrollo de su actividades y funciones.
- **Análisis de riesgos:** proceso sistemático para entender la naturaleza del riesgo y evaluar la criticidad de reducir el nivel del riesgo.
- **Apetito de riesgo:** es el nivel de riesgo que la entidad puede aceptar en relación 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 la alta dirección considera 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 las 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 la información de estar accesible y utilizable a demanda por una entidad.
- **Evaluación del control:** revisión sistemática de los procesos para garantizar que los controles aún son eficaces y adecuados.
- **Evaluación del riesgo:** proceso de comparar el nivel de riesgo frente a los criterios del riesgo.
- **Evitar el riesgo:** decisión de no involucrarse en o retirarse de una situación de riesgo**.**
- **Factores de riesgo**: son las fuentes generadoras de riesgos.
- **Frecuencia:** medición del número de ocurrencias por unidad de tiempo.
- **Gestión del Riesgo:** un 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.
- **Impacto**: las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** propiedad de la información relativa a su exactitud y completitud.
- **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 puede ser 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.
- **Nivel de Aceptación/ Apetito de Riesgo:** Se considera el apetito del riesgo en la descripción de cada riesgo como su tolerancia aceptada.
- **Mapa de riesgos:** herramienta metodológica que permite hacer un inventario de los riesgos detallando la descripción de cada uno de éstos y las posibles consecuencias.
- **Monitorear:** verificar, supervisar, observar críticamente o medir regularmente el progreso de una actividad, una acción o un sistema para identificar los cambios en el nivel de desempeño requerido o esperado.

- **Política de administración de riesgos:** declaración de la dirección y las intenciones de una organización con respecto a la gestión del riesgo. La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento; manejo y seguimiento a los riesgos. Es establecida por la dirección de la entidad, con la participación del comité institucional
- **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.
- **Plan de manejo o tratamiento del riesgo:** plan de acción propuesto por el grupo de trabajo.
- **Reducción del riesgo:** acciones que se toman para disminuir la posibilidad, las consecuencias negativas, o ambas, asociadas con un riesgo.
- **Responsables:** son las dependencias o áreas encargadas de adelantar las acciones propuestas.
- **Riesgo:** efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: lo 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.
- **Riesgo Contractual:** El riesgo contractual en general es entendido como todas aquellas circunstancias que pueden presentarse durante el desarrollo o ejecución de un contrato y que pueden alterar el equilibrio financiero del mismo.
- **Riesgo fiscal**: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.
- **Riesgo de Gestión:** posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **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 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 Inherente:** nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos 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.
- **Seguimiento:** recolección regular y sistemática sobre la ejecución del plan, qué sirven para actualizar y mejorar la planeación futura.
- **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.
- **Valoración del riesgo:** proceso total de identificación del riesgo, análisis del riesgo y evaluación del riesgo
- **Vulnerabilidad:** representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

6. DISPOSICIONES GENERALES

Es documento permite a los funcionarios y contratistas de la Unidad del Servicio Público de Empleo, seguir la metodología y los lineamientos necesarios para la identificación y el análisis de los riesgos de gestión, de corrupción y de seguridad de la información, adoptando lo contenido en la guía del DAFP para la Administración de Riesgos y Diseño de Controles.

- Estos lineamientos son establecidos por los directivos que hacen parte de la línea estratégica de la Entidad, apoyados en la recomendaciones realizadas en el Comité Institucional de Coordinación de Control Interno.
- La identificación de riesgos y su actualización deben tener en cuenta como insumo la misión, visión, objetivos estratégicos, metas, planes, proyectos y las prioridades de la Entidad, incluyendo las del plan de desarrollo vigente. Adicionalmente, se debe tener en cuenta el contexto organizacional, caracterizaciones de los procesos y será realizada a todos los procesos de la Entidad.
- La matriz de riesgos será actualizada de acuerdo con la necesidades de la Entidad, los lineamientos emitidos por el DAFP, la normatividad técnica vigente y las mejores prácticas.
- Los riesgos de gestión, corrupción, seguridad de la información, entre otros, deben ser elaborados y/o revisados como mínimo una vez al año, dado que es factible que antes del año se realicen revisiones y ajustes conforme lo demanda la operatividad del proceso.
- La identificación o actualización de activos de información se debe realizar teniendo en cuenta los lineamientos establecidos por la Subdirección de Desarrollo y Tecnología, los lineamientos emitidos por el Ministerio TIC y las mejores prácticas.
- Es importante precisar que, la actualización del GS-Ft-21 Formato Inventario de activos de información y el GS-Ft-20 Formato del registro de riesgos de seguridad de la información, deben ser gestionados y actualizados por todos los procesos de la entidad, de acuerdo con lo establecido en GS-Pr-14 Procedimiento Clasificación de Activos y GS-Pr-15 Procedimiento de análisis, valoración y tratamiento de riesgos de SI.

7. GESTIÓN DE RIESGOS

La política de administración de riesgos se rige por las disposiciones legales y en particular por la *Guía para la administración del riesgo y el diseño de controles en entidades públicas* del Departamento Administrativo de la Función Pública (versión 2023) que establece las directrices de obligatorio cumplimiento para las entidades públicas.

Los riesgos en la Unidad del SPE se categorizan por procesos (Modelo de Operación por Procesos). Teniendo en cuenta que el adecuado manejo de los riesgos favorece el desarrollo y sostenibilidad de la gestión de la entidad, es importante que el líder del proceso (Directivos, entiéndase como Secretario general y subdirectores), a través de los formatos dispuestos por la Dirección General, establezca la identificación, análisis, valoración y definición de las alternativas de acciones de mitigación de los riesgos.

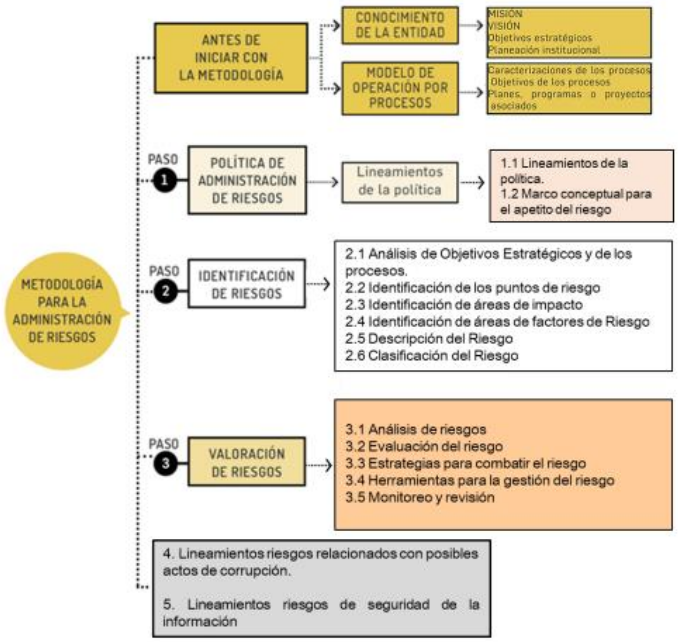
7.1 Riesgos que se van a controlar

La administración de riesgos en la Unidad Administrativa Especial del Servicio Público de Empleo tendrá un carácter prioritario y estratégico, en el marco del modelo de operación por procesos, teniendo en cuenta los establecidos en el Mapa de Procesos, en sus cuatro tipos (Estratégicos, Misionales, de Apoyo y de Evaluación); para cada uno de los procesos se establecerán las etapas descritas en esta política.

7.1.1 Contexto estratégico

El contexto estratégico es la base para la identificación de los riesgos en los procesos y actividades. El análisis se realiza a partir del conocimiento de situaciones del entorno de la organización, tanto de carácter social, económico, cultural, ambiental, de orden público, político, legal y/o cambios tecnológicos, entre otros; se alimenta también con el análisis de la situación actual de la organización, basado en los resultados de los Componentes de Ambiente de Control, Estructura Organizacional, Modelo de Operación, cumplimiento de los Planes y Programas, informes de auditoría y evaluaciones previas, sistemas de información, procesos y procedimientos y los recursos económicos, entre otros.

Figura 1. Metodología General para la Gestión de Riesgos



Fuente: Guía de Administración de Riesgos y Diseño de Controles DAFP 2023, V6.

7.1.2 Revisión previa a la aplicación de la metodología

- Revisión de la misión y la visión.
- Revisión de objetivos estratégicos.
- Los objetivos estratégicos deben estar alineados a la misión, visión y propósito superior.
- Los objetivos deben incluir el qué, cómo, para qué, cuándo, cuánto.

- Los objetivos definidos deben contemplar al menos las siguientes características: específico, medible, alcanzable, relevante y proyectado en el tiempo.
- Revisión de objetivos estratégico y del proceso: Le corresponde a la segunda línea de defensa la revisión de los objetivos de la Entidad tanto del orden estratégico como de procesos. Es decir, en la medida que se construyen los procesos, La Asesora de Planeación entre sus funciones de calidad realiza las recomendaciones y/o sugerencias pertinentes con el fin de que los objetivos institucionales y de procesos se encuentren bien definidos.
- Análisis de objetivos de los procesos: Al menos se deben analizar qué cumplan con las características mencionadas anteriormente y asegurar que contribuyan a los objetivos estratégicos.

8. IDENTIFICACIÓN DE RIESGOS

El proceso de la identificación del riesgo debe ser permanente e interactivo basado en el resultado del análisis del contexto estratégico, en el proceso de planeación y los objetivos estratégicos de la organización. Esta parte, implica hacer un inventario de los riesgos, definiendo en primera instancia sus causas con base en los factores de riesgo internos y externos (contexto estratégico), presentando una descripción de cada uno de estos y finalmente definiendo los posibles efectos (impacto). Tener en cuenta el concepto de apetito del riesgo.

- **Tipo de Riesgo:** Cada riesgo identificado se clasificará de acuerdo con la siguiente tipología:

    - **Riesgos de Cumplimiento:** se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
    - **Riesgos de Seguridad de la Información:** combinación de amenazas y vulnerabilidades de los activos de información de la entidad, que pueden afectar su disponibilidad, integridad y confidencialidad.
    - **Riesgo Estratégico**: se asocia con la forma en que se administra la entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
    - **Riesgos Financieros:** se relacionan con el manejo de los recursos de la entidad, que incluye la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada entidad. De la eficiencia y transparencia en el manejo de los recursos, así como de su interacción con las demás áreas, dependerá en gran parte el éxito o fracaso de toda entidad.
    - **Riesgos Operativos:** comprende los riesgos relacionados tanto con la parte operativa como con la técnica de la entidad, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la entidad, la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.
    - **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
    - **Riesgos de Integridad y Conflictos de Interés:** conjunto de riesgos asociados a la no interiorización o incumplimiento del código de integridad del servicio público por parte de los servidores y contratistas de la entidad, así como en relación con la posible mala gestión de conflictos de interés.

Previo a la identificación de los riesgos, el grupo de Planeación debe revisar los objetivos estratégicos y los objetivos de los procesos; debe validar que los objetivos en su descripción o redacción den respuesta a las siguientes preguntas: ¿qué se quiere lograr?, ¿para qué quiere lograrlo?, ¿cómo quiere lograrlo?, ¿cuándo piensa lograrlo? y ¿cuánto avance debo cumplir en cada vigencia?

8.1 Establecimiento del contexto

Se debe identificar los riesgos que estén o no bajo el control de la Unidad del SPE, teniendo en cuenta el contexto estratégico en el que opera la Entidad, la caracterización de procesos contemplando su objetivo y alcance. Los líderes de procesos deben establecer el contexto interno y externo de la Entidad, el contexto de los procesos y los activos de seguridad de la información. Los factores para cada categoría son:

Tabla 1. Factores de Riesgo

FACTORES	
CONTEXTO EXTERNO	POLÍTICOS: cambios de gobierno, legislación, políticas públicas, regulación.
	ECONÓMICOS Y FINANCIEROS: disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	SOCIALES Y CULTURALES: demografía, responsabilidad social, orden público.
	TECNOLÓGICOS: avances en tecnología, acceso a sistemas de información externos, Gobierno Digital.
	AMBIENTALES: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	LEGALES Y REGLAMENTARIOS: Normatividad externa (leyes, decretos, ordenanzas y acuerdos).
CONTEXTO INTERNO	FINANCIEROS: presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
	PERSONAL: competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
	PROCESOS: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	TECNOLOGÍA: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
	ESTRATÉGICOS: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
	COMUNICACIÓN INTERNA: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
CONTEXTO DEL PROCESO	DISEÑO DEL PROCESO: claridad en la descripción del alcance y objetivo del proceso.
	INTERACCIONES CON OTROS PROCESOS: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	TRANSVERSALIDAD: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.

	PROCEDIMIENTOS ASOCIADOS: pertinencia en los procedimientos que desarrollan los procesos.
	RESPONSABLES DEL PROCESO: grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	COMUNICACIÓN ENTRE LOS PROCESOS: efectividad en los flujos de información determinados en la interacción de los procesos.
	ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO: información que se debe proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

Fuente: Unidad del SPE.

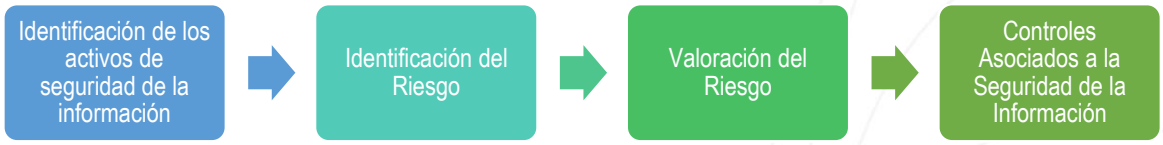
Luego de establecer el contexto (incluyendo causas e impactos) se deben identificar los riesgos, que son aquellos eventos o situaciones que pueden llegar a entorpecer el normal desarrollo de los objetivos de los procesos o generar afectación de los activos de información. Para ello, es necesario responder las siguientes preguntas para la identificación: ¿qué puede suceder?, ¿Cómo puede suceder?, ¿Cuándo puede suceder? y ¿Qué consecuencias tendría su materialización?, y con las respuestas construir la descripción del riesgo.

Luego se deben identificar las causas del riesgo que pueden afectar el logro de los objetivos y los impactos o efectos resultantes de la materialización de un riesgo que afecte los objetivos del proceso, la entidad o partes interesadas. Se debe tener conocimiento general del proceso y tener acceso o conocimiento de datos y hechos históricos de la Entidad para realizar una completa identificación.

8.2 Riesgos de Seguridad de la Información

La definición de los riesgos de seguridad de la información se realiza considerando los siguientes pasos:

Figura 2. Pasos para la identificación de riesgos de seguridad de la información



Fuente: Unidad del SPE

En el caso de los riesgos de seguridad de la información, es importante en primera instancia identificar los activos de información de cada proceso con el fin de determinar la información que la Entidad debe proteger para asegurar su funcionamiento interno, como de cara al ciudadano.

Para cada riesgo de seguridad de la información, se deben vincular los activos relacionados y se deben evaluar amenazas y vulnerabilidades que pueden causar la materialización del riesgo. Se pueden identificar tres tipos de riesgos de seguridad de la información:

- Pérdida de confidencialidad.
- Pérdida de integridad.
- Pérdida de disponibilidad.

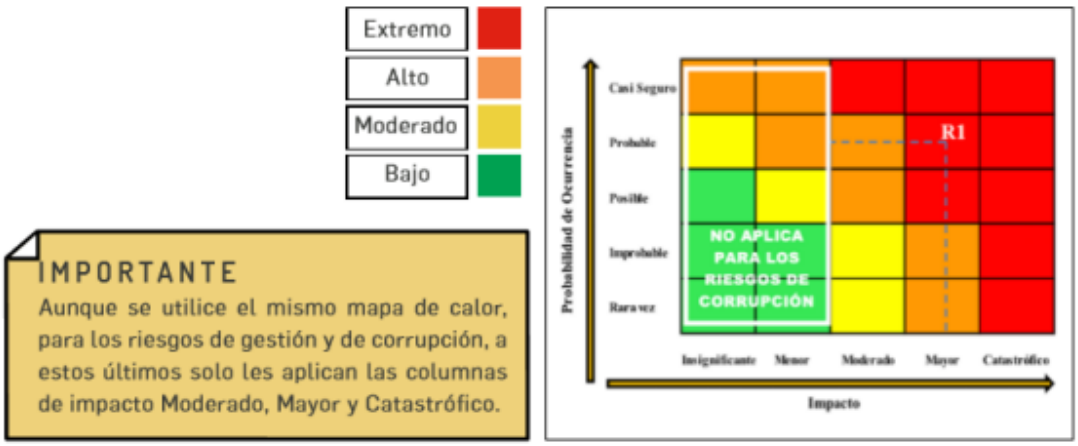
Adicionalmente, se realiza la valoración del riesgo y se definen los controles asociados a seguridad de la información. Es importante precisar que, la actualización del GS-Ft-21 Formato Inventario de activos de información y el GS-Ft-20 Formato del registro de riesgos de seguridad de la información, deben ser gestionados y actualizados por todos los procesos de la entidad, de acuerdo con lo establecido en GS-Pr-14 Procedimiento Clasificación de Activos y GS-Pr-15 Procedimiento de análisis, valoración y tratamiento de riesgos de SI.

8.3 Riesgos de Corrupción

Para el caso de los riesgos del Mapa de Riesgo de corrupción, componente del Programa de Transparencia y Gestión Pública, se tendrá como base lo estipulado por la Guía para la Gestión de Riesgo de Corrupción del Departamento Administrativo de la Función Pública, en cuanto a la valoración de los riesgos el impacto se calificará en las escalas de: Moderado, Mayor y Catastrófico, cada año la entidad deberá publicar en su página Web a más tardar el 31 de Enero de cada vigencia el Mapa de Riesgos de Corrupción, con respecto a los demás riesgos, éstos tienen nivel de tolerancia de cero, por el tratamiento y la importancia que tiene en la gestión institucional.

En la descripción de riesgos de corrupción, es preciso atender al cumplimiento de los siguientes componentes: Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado. La descripción del riesgo debe ser clara y precisa, además para clasificarse como riesgo de corrupción debe cumplir con las cuatro condiciones.

***Tabla* 2.Tabla de Impacto riesgos de corrupción**



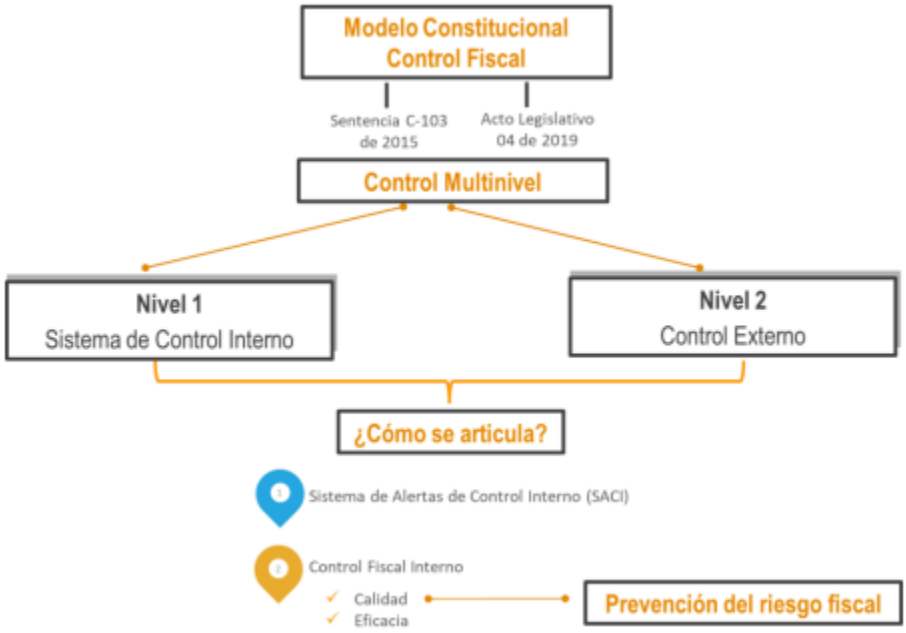
Fuente: Secretaría de Transparencia

8.4 Riesgos Fiscales

El riesgo fiscal hace alusión al daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado (Decreto 403, 2020, art.6).

El control fiscal además de posterior y selectivo a través de las auditorías (control micro), es preventivo y concomitante, buscando con ello el control permanente al recurso público, para lo cual, una de las herramientas previstas es la articulación con el sistema de control interno.

Figura 3. Estructura de los Riesgos Ficales



Fuente: Guía de Administración de Riesgos y Diseño de Controles - Función Pública

Paso a paso para la definición del riesgo fiscal:

- **Descripción del riesgo:** teniendo en cuenta que el riesgo fiscal se define como *"Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial"*, para su estructuración se debe tener en cuenta lo siguiente:

  a. **Efecto:** es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.
  - **Evento Potencial:** Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. En esta guía, el evento potencial es equivalente a la causa raíz.

Entonces la fórmula para su descripción es la siguiente:

Riesgo Fiscal = Evento Potencial (Potencial Conducta) + Efecto dañoso

9. VALORACIÓN DE RIESGOS (Análisis y Evaluación)

En esta fase se define la probabilidad de ocurrencia del riesgo (eventos positivos y/o negativos) y su consecuencia o impacto para estimar la zona de riesgo inicial (riesgo inherente antes del diseño de controles), y luego comparar los resultados frente a los controles diseñados y evaluados, para determinar la zona de riesgo final (riesgo residual) y estipular de acuerdo con las capacidades de la Entidad su aceptación y tratamiento.

La valoración del riesgo es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados, esto se hace con el objetivo de establecer prioridades para su manejo y para la fijación de políticas. Para adelantar esta etapa se hace necesario tener claridad sobre los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones.

Los controles deben tener relación directa con las causas generadoras del riesgo identificado, para ello es importante revisar que las actividades de control subsanen y/o prevengan los agentes generadores del riesgo identificado. Así mismo, es importante considerar las acciones de manera correctiva que se puedan adelantar para mitigar los efectos de un riesgo cuando se ha materializado.

9.1 Análisis de Riesgos

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar. En el análisis del riesgo se deberán considerar los aspectos de análisis y evaluación del riesgo; además dependerá de la información obtenida, de la identificación de riesgos y de la disponibilidad de datos históricos y aportes de los servidores de la organización.

Se deben contemplar dos aspectos en el análisis de los riesgos identificados: Probabilidad e Impacto. Por probabilidad 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 puedan propiciar el riesgo, aunque este no se haya materializado. Por impacto se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo. Para adelantar el análisis del riesgo se deben considerar los siguientes aspectos:

- **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.
- **Bajo el criterio de probabilidad:** el riesgo se debe medir a partir de las siguientes especificaciones:

Tabla 3.Tabla 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 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%

Fuente: Guía de Administración de Riesgos y Diseño de Controles - Función Pública

- Bajo el criterio de impacto, el riesgo se debe medir a partir de las siguientes especificaciones:

Tabla 4.Tabla de Impacto

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún 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 publicitario sostenido a nivel país

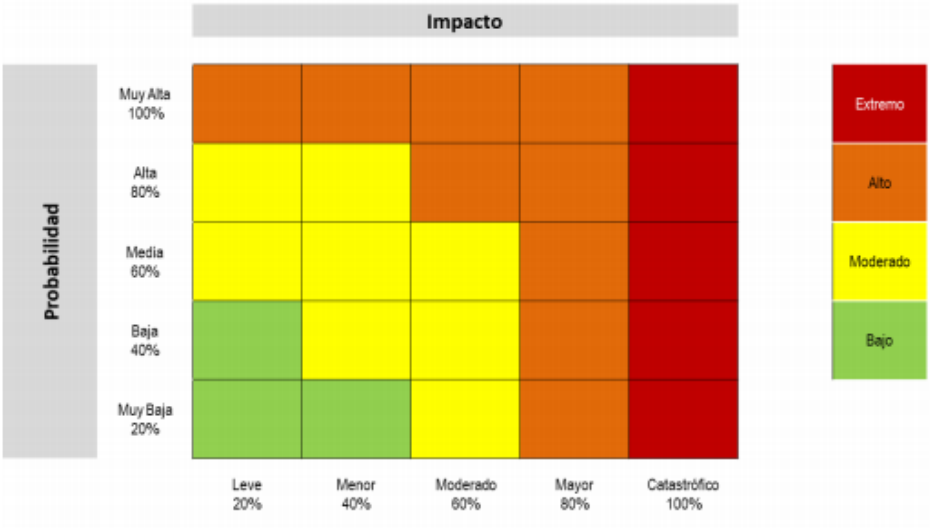
La afectación económica se calcula en 500SMLMV, el impacto del riesgo es **mayor**.

Probabilidad inherente= media 60%, **Impacto inherente:** mayor 80%

Fuente: Guía de Administración de Riesgos y Diseño de Controles - Función Pública

Con el resultado de la calificación del riesgo, se ubica el impacto y probabilidad en el mapa de calor, para determinar el nivel de riesgo, y como resultado se obtiene el ***riesgo inherente***:

Tabla 5.Tabla de Probabilidad / Impacto



Extremo	Reducir el riesgo, Evitar, Compartir o Transferir.
Alto	Reducir el riesgo, Evitar, Compartir o Transferir.
Moderado	Asumir el Riesgo, Reducir el Riesgo.
Bajo	Asumir el Riesgo.

Fuente: Guía de Administración de Riesgos y Diseño de Controles - Función Pública

Nota: para los riesgos de corrupción solo aplican las columnas de Impacto Moderado, Mayor y Catastrófico.

10. EVALUACIÓN DE RIESGOS

Para esto es necesario diseñar los controles para mitigar de manera adecuada el riesgo. La descripción del control debe contener las variables como responsable, periodicidad, propósito, cómo se realiza, qué pasa con las observaciones o desviaciones, y evidencia. Para cada causa debe existir un control. Luego del diseño de los controles, se debe valorar si está bien diseñado para mitigar el riesgo y si se ejecuta como fue diseñado y es consistente.

Nota: Ningún riesgo con medida de tratamiento se evita o elimina.

Finalmente, de acuerdo con los resultados de la evaluación realizada frente a la valoración de los controles, se debe determinar el desplazamiento del riesgo en el mapa de calor, si disminuyen la probabilidad o el impacto.

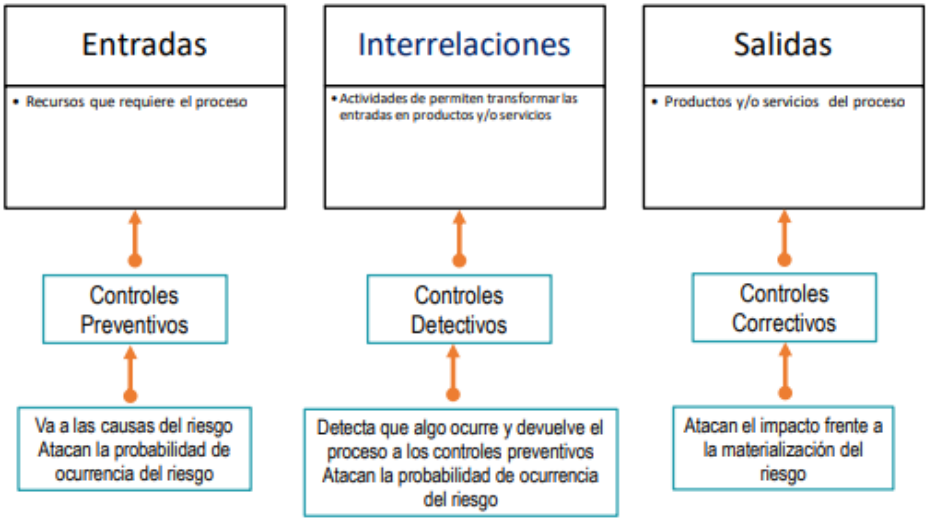
La valoración del riesgo es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados, esto se hace con el objetivo de establecer prioridades para su manejo y para la fijación de políticas. Para adelantar esta etapa se hace necesario tener claridad sobre los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones.

11. DISEÑO DE CONTROLES

Los controles deben tener relación directa con las causas generadoras del riesgo identificado, para ello es importante revisar que las actividades de control subsanen y/o prevengan los agentes generadores del riesgo identificado. Así mismo, es importante considerar las acciones de manera correctiva que se puedan adelantar para mitigar los efectos de un riesgo cuando se ha materializado.

Tipología de controles y los procesos: 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 esta estructura conceptual, se consideran 3 fases globales del ciclo de un proceso así:

Figura 4. Ciclo del proceso y las tipologías comunes



Fuente: Guía de Administración de Riesgos y Diseño de Controles - Función Pública

Es importante revisar que los controles documentados son actividades recurrentes o periódicas. Existen tres tipos de controles, en cuanto al efecto sobre el riesgo:

- **Preventivos:** son aquellas acciones encaminadas a eliminar las causas generadoras de un riesgo, de tal manera que eviten o disminuyan su ocurrencia o materialización
- **Detectivos:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos
- **Correctivos:** son aquellas acciones que permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable. A través de estos controles se puede cambiar o modificar las acciones que propiciaron su ocurrencia y corregir los productos o servicios generados de la actividad crítica antes de ser suministrados al cliente.

El procedimiento para la valoración del riesgo parte de la evaluación de los controles existentes, lo cual, implica:

- Describirlos (estableciendo si son preventivos o correctivos)
- Revisarlos para determinar si los controles están documentados, si se están aplicando en la actualidad y si han sido efectivos para minimizar el riesgo
- Es importante que la valoración de los controles incluya un análisis de tipo cuantitativo, que permita saber con exactitud cuántas posiciones dentro de la matriz de calificación, evaluación y respuesta al riesgo

¿Cómo se valoran los controles?: con las siguientes herramientas se podrán ponderar de manera objetiva los controles y poder determinar el desplazamiento dentro de la Matriz de Calificación, Evaluación y Respuesta a los riesgos

Diseño del control, análisis y evaluación de los controles – atributos: a continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la siguiente tabla se puede observar la descripción y peso asociados a cada uno así:

Tabla 6. Atributos para el Diseño de Controles

Características			Descripción	Peso
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos Informativos	Documentación	Documentado	Controles que están documentados en el proceso,	N/A

Características			Descripción	Peso
			ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso .	N/A
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	N/A
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	N/A
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	N/A
		Sin registro	El control no deja registro de la ejecución del control.	N/A

Fuente: Guía de Administración de Riesgos y Diseño de Controles - Función Pública

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles. Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Tabla 7. Tipos de Controles

Controles de Gestión	Políticas claras aplicadas
	Seguimiento al plan estratégico y operativo
	Indicadores de gestión
	Tableros de control
	Seguimiento al cronograma
	Evaluación del desempeño
	Informes de gestión
	Monitoreo de riesgos
Controles Operativos	Conciliaciones

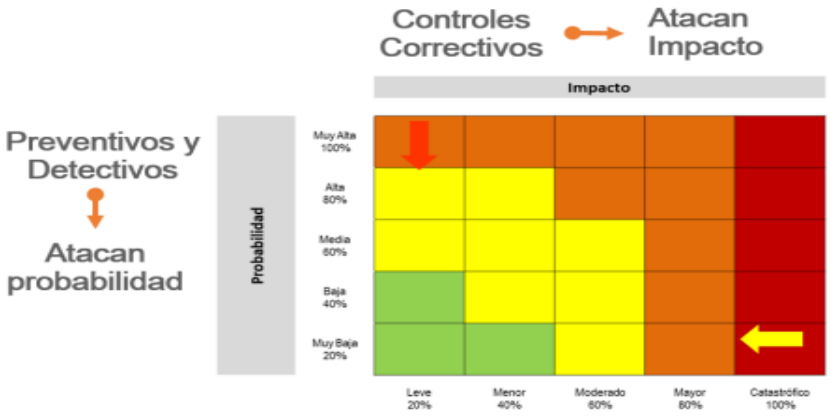
	Consecutivos
	Verificación de firmas
	Listas de chequeo
	Registro controlado
	Segregación de funciones
	Niveles de autorización
	Custodia apropiada
	Procedimientos formales aplicados
	Pólizas
	Seguridad física
	Contingencias y respaldo
	Personal capacitado
	Aseguramiento y calidad
Controles Legales	Normas claras
	Control de términos

Fuente: Guía de Administración de Riesgos y Diseño de Controles - Función Pública

El procedimiento para la valoración del riesgo parte de la evaluación de los controles existentes, lo cual implica:

a) Describirlos (estableciendo si son preventivos o correctivos).
b) Revisarlos para determinar si los controles están documentados, si se están aplicando en la actualidad y si han sido efectivos para minimizar el riesgo.
c) Es importante que la valoración de los controles incluya un análisis de tipo cuantitativo, que permita saber con exactitud cuántas posiciones dentro de la matriz de calificación, evaluación y respuesta al riesgo.

Figura 5. Efectividad del Control



Fuente: Departamento Administrativo de la Función Pública

12. TRATAMIENTO DEL RIESGO

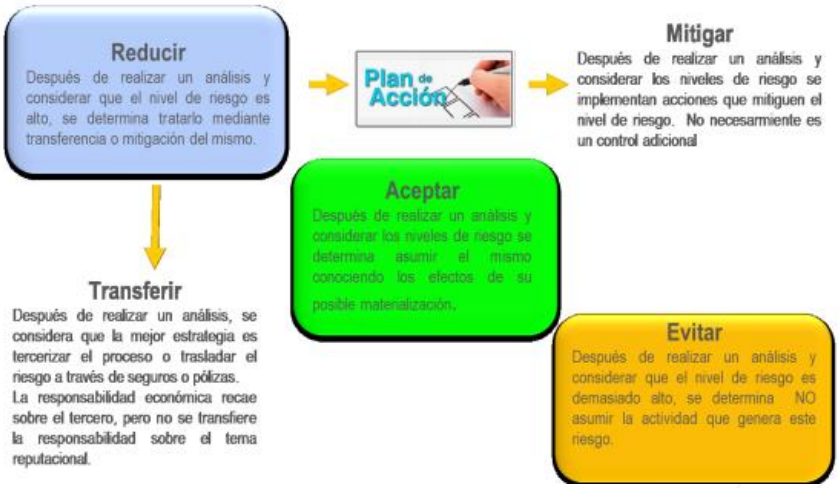
La primera línea de defensa es la responsable de definir las acciones de tratamiento para mitigar los riesgos identificados (Plan de Tratamiento de Riesgos). Para los riesgos de corrupción las opciones de tratamiento después de la valoración de controles solo deben ser: evitar, compartir o reducir el riesgo. Todos los riesgos deberán contar con acciones para el tratamiento de los riesgos. Las opciones de tratamiento y los lineamientos para cada uno son:

- **Aceptar el riesgo:** no se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. Cuando el riesgo residual es bajo se aceptan las consecuencias o impactos de la posible materialización de ese riesgo, pero aún asi se deben implementar controles . Para esta opción de tratamiento se debe realizar seguimiento continuo al riesgo *(Ningún riesgo de corrupción debe ser aceptado)*.
- **Reducir el riesgo:** se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.
- **Evitar el riesgo:** se abandonan las actividades que dan lugar al riesgo, es decir, no dar inicio o no continuar con la actividad que lo provoca.
- **Compartir el riesgo:** se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir pero no transferir su responsabilidad. Las opciones más utilizadas para esta situación es que la Entidad adquiera seguros y/o realice la tercerización que aumenta la probabilidad del riesgo, y en caso de decidir esta opción de tratamiento, debe estar formalizada a través de un acuerdo contractual

Para tratar o mitigar los riesgos de seguridad digital, se deben tomar como referencia los controles establecidos en el Anexo A de la Norma ISO 27001:2013. Una vez se implementen estos controles, debe actualizarse el documento que contiene la declaración de aplicabilidad de la Entidad, con el fin de incluir en cada control los soportes de su implementación. Esta tarea está a cargo del responsable de riesgos en seguridad de la información de la Entidad. Es preciso definir actividades de control para prevenir que el riesgo se materialice, y si llega a pasar, debe ser detectado de manera oportuna.

Después de definidos los mapas de riesgos de todos los procesos, desde Planeación se debe consolidar y generar el mapa de riesgos Institucional, el cual debe contener los riesgos de gestión, corrupción y seguridad digital. El mapa debe ser aprobado en Comité Institucional de Control Interno, para su posterior socialización y publicación.

Figura 6. Estrategias para combatir el riesgo



Fuente: Guía de Administración de Riesgos y Diseño de Controles - Función Pública

Una vez se establezca el tratamiento que se le hará a los riesgos de acuerdo con su zona, se deberán establecer las acciones que se desarrollarán con sus debidos responsables y las fechas de realización de las acciones, éstas deberán contemplar la disponibilidad de recursos económicos de cada uno de los procesos, así como los demás recursos que se deberán utilizar como físicos, tecnológicos, entre otros.

13. MONITOREO Y REVISIÓN

- El Mapa de riesgos de proceso, debe contener aquellas acciones de control definidas para el manejo del riesgo, buscando prevenir o reducir el riesgo detectado, teniendo en cuenta su viabilidad técnica y financiera. El monitoreo de las acciones de tratamiento debe realizarlo el responsable del proceso.

- El responsable del proceso deben verificar que los controles establecidos en el plan de tratamiento de riesgos operen de manera adecuada para mitigar los riesgos.

- El seguimiento de los riesgos identificados (incluyendo el plan de tratamiento) se debe realizar de manera trimestral por cada uno de los líderes de los procesos, quienes reportarán a Planeación

(Riesgos de Gestión y Corrupción) y la Subdirección de Desarrollo y Tecnología (Riesgos de Seguridad Digital).

- En caso de materialización de un riesgo, el responsable del proceso debe generar una acción correctiva, y debe revisar nuevamente la identificación del riesgo, el diseño y valoración de controles, y el plan de tratamiento para mitigar el riesgo.

- Anualmente se debe realizar la valoración de los riesgos de gestión, corrupción y seguridad digital con el fin de verificar que los planes de tratamiento fueron efectivos y los niveles de riesgo disminuyeron. El monitoreo por parte de Planeación se realizará trimestralmente.

- De manera periodica los responsables operativos de cada proceso adelantarán un ejercicio de autoevaluación de sus riesgos con el fin de identificar si hubo materializaciones o si se requieren ajustes a los riesgos o controles de su proceso. Así mismo se recomienda hacer una verificación de las recomendaciones y observaciones arrojadas por los informes de auditoría del asesor de control interno con el fin de identificar los controles efectivos para disminuir la probabilidad de materialización de los mismos.

ELABORÓ	REVISÓ	APROBÓ	Versión
Jenny Marcela Mesa Julio Novoa Contratistas Dirección General	Natalia Lozano Sierra Asesora de la Dirección con Funciones de Planeación	Comité Institucional de Coordinación de Control Interno	Número 4 de 2024
Fecha: 26 marzo de 2024			