AGENCIA PARA LA REINCORPORACIÓN Y LA NORMALIZACIÓN

AGENCIA PARA LA REINCORPORACIÓN Y LA NORMALIZACIÓN (ARN)

MANUAL DE GESTIÓN DEL RIESGO

BOGOTÁ D.C. MAYO 2023

TABLA DE CONTENIDO

1. OBJETIVO 3
1.1 OBJETIVO GENERAL 3
1.2 OBJETIVOS ESPECÍFICOS 3
2. ALCANCE 3
3. DEFINICIONES 4
4. CONSIDERACIONES GENERALES 8
5. POLÍTICA INSTITUCIONAL DE ADMINISTRACIÓN DE RIESGOS 9
5.1 OBJETIVOS DE LA POLÍTICA INSTITUCIONAL DE ADMINISTRACIÓN DE RIESGOS 10
5.2 RESPONSABILIDAD COMPARTIDA 10
5.3 PLAN ANUAL DE AUDITORÍAS BASADO EN RIESGOS 10
5.4 INTOLERANCIA TOTAL FRENTE A RIESGOS DE CORRUPCIÓN 11
5.5 ALINEAMIENTO ESTRATÉGICO 11
5.6 ARMONIZACIÓN CON OTRAS POLÍTICAS, PLANES Y PROYECTOS INSTITUCIONALES 12
6. DIRECTRICES GENERALES FRENTE A LA ADMINISTRACIÓN DEL RIESGO EN LA ARN (ROLES Y RESPONSABILIDADES) 12
7. CONTENIDO Y DESARROLLO 14
7.1 IDENTIFICACIÓN DE RIESGOS 14
7.2 VALORACIÓN DEL RIESGO 17
7.3 TRATAMIENTO DEL RIESGO 28
7.4 MONITOREO Y REVISIÓN 30
7.5 EVALUACIÓN DE LA EFICACIA DE LAS ACCIONES 32
7.6 ACCIONES ANTE RIESGOS MATERIALIZADOS 33

1. OBJETIVO

1.1 OBJETIVO GENERAL

Establecer lineamientos y criterios que se deben aplicar en la Agencia para la Reincorporación y la Normalización - ARN para la identificación, análisis, valoración, seguimiento y monitoreo de los riesgos de gestión, corrupción, seguridad digital, y demás requeridos por la normatividad que pueden afectar el logro de los objetivos institucionales, de procesos, proyectos y planes.

1.2 OBJETIVOS ESPECÍFICOS

- Definir la metodología que facilite a los procesos la adecuada gestión del riesgo.

- Hacer corresponsables a los empleados públicos y contratistas de la ARN en la búsqueda de las acciones encaminadas a prevenir la materialización del riesgo.

- Desarrollar capacidades en cada dependencia de la ARN de manera que les permita gestionar los riesgos de gestión, corrupción, seguridad digital y demás requeridos por la normatividad, inherentes a los procesos en los que participa y el establecimiento de las medidas de prevención y mitigación a través de la formulación y ejecución de acciones de tratamiento.

- Establecer una base confiable para la toma de decisiones y la planificación.

- Asegurar de manera efectiva la aplicación de la normatividad vigente.

- Definir los criterios para el seguimiento y evaluación de las acciones de tratamiento y los controles asociados a los riesgos.

2. ALCANCE

Este documento establece la política institucional de administración de riesgos, define responsabilidades, metodología de gestión y herramientas de evaluación, en concordancia con el Modelo Integrado de Planeación y Gestión-MIPG y los sistemas adoptados por la Entidad. Los lineamientos y criterios establecidos en este documento aplican para los procesos, dependencias, oficinas y grupos territoriales de la ARN.

3. DEFINICIONES

ACTIVO DE INFORMACIÓN: Es cualquier información o sistema relacionado con el tratamiento de esta, que tenga valor para la entidad. 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: Conjunto de elementos de control que, al interrelacionarse, permiten a la entidad pública, evaluar la ocurrencia de eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos, que permitan identificar oportunidades para un mejor cumplimiento de su función.

AMENAZAS: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

ANÁLISIS DE RIESGO: Elemento de control, que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública, para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar la frecuencia que pueden ocurrir eventos especificados y la magnitud de sus consecuencias.

APETITO DE RIESGO: Es el nivel de riesgo que la entidad puede asumir, 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.

AUTOEVALUACIÓN DEL CONTROL: Se basa en una revisión periódica y sistemática de los procesos de la entidad para asegurar que los controles establecidos son aún efectivos y apropiados.

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

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

CIBERSEGURIDAD: Conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio de ataques maliciosos.

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.

COMPARTIR EL RIESGO: Se asocia con la forma de protección para disminuir las pérdidas que ocurran luego de la materialización de un riesgo, es posible realizarlo mediante contratos, seguros, cláusulas contractuales u otros medios que puedan aplicarse.

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.

CONTROL CORRECTIVO: Conjunto de medidas tomadas para mitigar impactos no deseados.

CONTROL PREDICTIVO: Conjunto de medidas tomadas para identificar en el momento en el que se presentan.

CONTROL PREVENTIVO: Conjunto de medidas tomadas para prevenir eventos no deseados.

CRITICIDAD: Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información.

DATO: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la ARN, así como cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para la organización.

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

ESTIMACIÓN DEL NIVEL DEL RIESGO INICIAL O INHERENTE: Se realiza a través de la determinación de la probabilidad y el impacto que puede causar la materialización del riesgo.

EVALUACIÓN DEL RIESGO: Proceso utilizado para determinar las prioridades de la Administración del Riesgo comparando el nivel de un determinado riesgo con respecto a un estándar determinado.

EVENTO: Incidente o situación, que ocurre en un lugar determinado durante un periodo de tiempo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.

FACTORES DE RIESGO: Son las fuentes generadoras de riesgos.

FRECUENCIA: Medida del coeficiente de ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

GESTIÓN DEL RIESGO: 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.

GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL: Conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible.

IDENTIFICACIÓN DEL RIESGO: Etapa que permite identificar los riesgos que estén o no bajo el control de la entidad, para su identificación se debe tener en cuenta el contexto estratégico, el objetivo y alcance de cada proceso.

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

IMPACTO CREDIBILIDAD O IMAGEN: Se refiere a la pérdida de la misma frente a diferentes actores sociales o dentro de la entidad.

IMPACTO DE CONFIDENCIALIDAD DE LA INFORMACIÓN: Se refiere a la pérdida o revelación de esta. Cuando se habla de información reservada institucional se hace alusión a aquella que por la razón de ser de la entidad sólo

puede ser conocida y difundida al interior de esta; así mismo, la sensibilidad de la información depende de la importancia que ésta tenga para el desarrollo de la misión de la entidad.
IMPACTO LEGAL: Se relaciona con las consecuencias legales para una entidad, determinadas por los riesgos relacionados con el incumplimiento en su función administrativa, ejecución presupuestal y normatividad aplicable.

IMPACTO OPERATIVO: Aplica en la mayoría de las entidades para los procesos clasificados como estratégicos o de apoyo, ya que sus riesgos pueden afectar el normal desarrollo de otros procesos dentro de la misma.

INTEGRIDAD: Propiedad de exactitud y completitud.

MATERIALIZACION DEL RIESGO: Ocurrencia del riesgo previamente identificado.

MAPA DE RIESGOS: Documento con la información resultante sobre el análisis y la valoración de los riesgos institucionales.

MONITOREAR: Comprobar, supervisar, observar, o registrar la forma en que se lleva a cabo una actividad con el fin de identificar posibles cambios.

NIVELES DE ACEPTACIÓN DEL RIESGO O TOLERANCIA AL RIESGO: Establece “los niveles aceptables de desviación relativa a la consecución de los objetivos” (NTC GTC 137 Numeral 3.7.16). Están asociados a la estrategia de la entidad y se consideran para cada uno de los procesos. Para los riesgos de corrupción son inaceptables.

PÉRDIDA: Consecuencia negativa que trae consigo un evento.

PROBABILIDAD: Se entiende la posibilidad de ocurrencia del riesgo. Esta asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

REDUCCIÓN DEL RIESGO: Aplicación de controles para reducir las probabilidades de ocurrencia de un evento y/o su ocurrencia.

RIESGO: Efecto que se causa sobre los objetivos de la entidad, debido a eventos potenciales.

RIESGO DE CORRUPCIÓN: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio propio o de un tercero.

RIESGO DE GESTIÓN: Posibilidad de que suceda algún evento que tiene impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

RIESGO DE SEGURIDAD DIGITAL O 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 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.

TRATAMIENTO DE DATOS PERSONALES: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. En el caso de las imágenes de personas determinadas o determinables, operaciones como la captación, grabación, transmisión, almacenamiento, conservación, o reproducción en tiempo real o posterior, entre otras, son consideradas como tratamiento de datos personales y, en consecuencia, se encuentran sujetas al régimen general de protección de datos personales.

TRATAMIENTO DE RIESGOS: Proceso para modificar el riesgo (NTC GTC137, Numeral 3.8.1).

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.

Para los casos de riesgos de corrupción no puede existir tolerancia al riesgo.

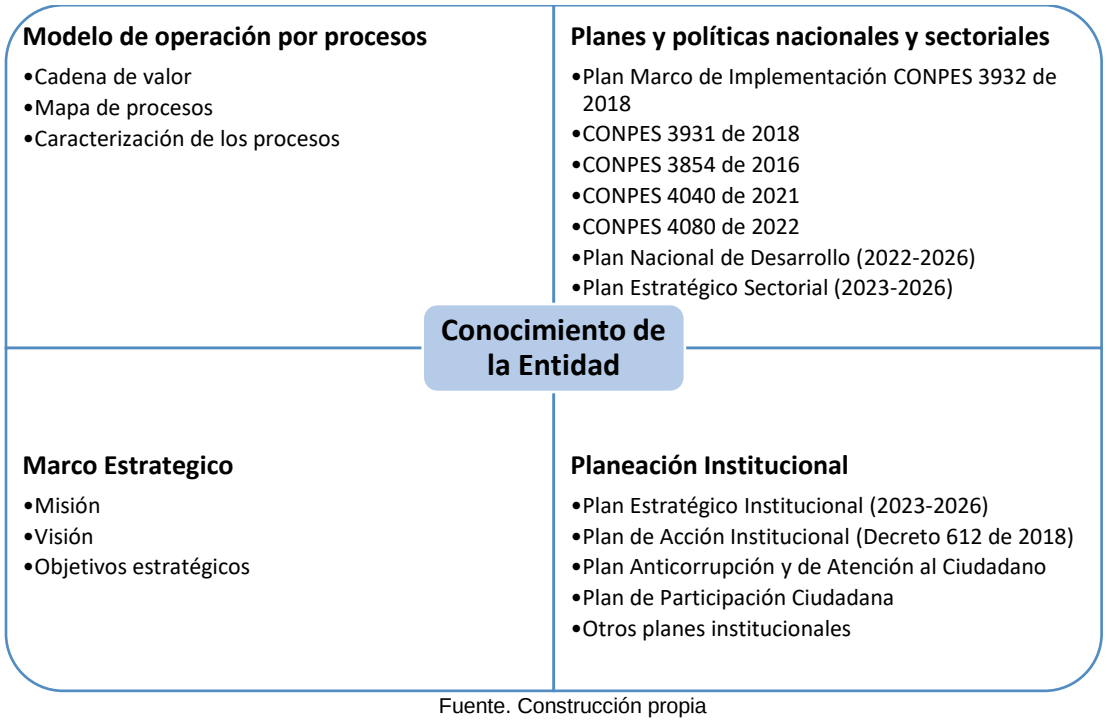
VULNERABILIDAD: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

4. CONSIDERACIONES GENERALES

La ARN determina los lineamientos para la identificación, administración, tratamiento, control y seguimiento de riesgos que puedan afectar la consecución de los objetivos de los procesos y los propósitos institucionales.

El enfoque de la ARN para la gestión de riesgos es proactivo, preventivo e integral; armónico con los lineamientos trazados por el Departamento Administrativo de la Función Pública-DAFP; de acuerdo con el Marco Estratégico institucional establecido.

Para el desarrollo de la metodología de construcción del mapa de riesgos se debe seguir el esquema que se presenta a continuación:



Fuente. Construcción propia

5. POLÍTICA INSTITUCIONAL DE ADMINISTRACIÓN DE RIESGOS

La ARN adopta una política institucional de administración de riesgos integral que establece funciones y responsabilidades para la gestión del riesgo, con estructuración de metodología y herramientas que dispone de una evaluación sistemática de los riesgos por parte de los líderes de proceso y sus equipos de trabajo, así como la evaluación del Grupo de Control Interno de Gestión.

Acorde con el Modelo Integrado de Planeación y Gestión-MIPG, los lineamientos del Departamento Administrativo de la Función Pública-DAFP y los sistemas de gestión adoptados por la Entidad; la política institucional de administración de riesgos de la ARN está basada en una línea estratégica y tres líneas de defensa, responsabilidad compartida, plan anual de auditorías basado en riesgos, monitoreo de riesgos, intolerancia total frente a los riesgos de corrupción,

alineamiento estratégico y establecimiento de zonas de riesgo, y armonización con otras políticas y planes institucionales.

5.1 OBJETIVOS DE LA POLÍTICA INSTITUCIONAL DE ADMINISTRACIÓN DE RIESGOS

El objetivo general de la política institucional de administración de riesgos es proteger la gestión de la entidad ante la posible ocurrencia de eventos que afecten el logro de sus objetivos estratégicos u operacionales, contribuir a la formulación e implementación de sus estrategias y facilitar el desarrollo de sus acciones mediante la mitigación de la probabilidad y el impacto de los riesgos.

Los objetivos específicos de la política institucional de administración de riesgos son:

- Trazar lineamientos para que todos los procesos de la entidad desarrollen los mecanismos de identificación, valoración, control y acciones de mitigación de los riesgos, verificados por sólidos mecanismos de seguimiento y gestión, con un enfoque preventivo, detectivo y correctivo, en el marco del Modelo Integrado de Planeación y Gestión-MIPG y los sistemas de gestión adoptados por la Entidad.

- Establecer mecanismos, definiendo roles, responsabilidades, herramientas y procedimientos para el control de los riesgos institucionales.

- Involucrar a todas las dependencias, empleados públicos y contratistas de la Entidad en la corresponsabilidad de control de los riesgos institucionales, desarrollando diversos mecanismos de sensibilización y comunicación al respecto.

5.2 RESPONSABILIDAD COMPARTIDA

La ARN involucra como sujetos corresponsables de su política institucional de administración de riesgos a todos los empleados públicos, contratistas de la entidad, pasantes, voluntarios y visitantes.

El Comité Institucional de Coordinación de Control Interno se asegura de su incorporación en todos los niveles de la entidad.

5.3 PLAN ANUAL DE AUDITORÍAS BASADO EN RIESGOS

En concordancia con las normas legales, el Grupo de Control Interno de Gestión en su plan anual de auditorías establece las actividades a cumplir para realizar el seguimiento y evaluación a los controles que ayudan a mitigar los riesgos de la

entidad. Este plan de auditoria se formula teniendo en cuenta la priorización del universo basado en riesgos y otros criterios definidos en la Matriz de Calificación y Programación de Auditorías, establecida en el EM-M-01 Manual de Auditoría Interna.

5.4 INTOLERANCIA TOTAL FRENTE A RIESGOS DE CORRUPCIÓN

La ARN no tolera ningún nivel de riesgos de corrupción. Por ello, todos los riesgos son identificados en el mapa de riesgos y definidas las medidas de tratamiento orientadas a evitar, reducir o compartir el riesgo y en ningún caso el tratamiento para este tipo de riesgos es aceptar el riesgo.

La evaluación de la gestión de la ARN frente a los riesgos de corrupción se incluye en el plan anual de auditorías basado en riesgos, en todas las vigencias.

5.5 ALINEAMIENTO ESTRATÉGICO

La administración de riesgos institucionales debe estar alineada con los objetivos estratégicos y con los procesos institucionales, de manera que se prevenga y/o minimice cualquier evento que pueda afectar negativamente el logro de los objetivos institucionales o de los procesos.

La ARN establece el monitoreo y seguimiento para los riesgos y sus acciones de prevención o mitigación de manera trimestral y define los siguientes tratamientos como respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Evitar el riesgo:
Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades. Este tratamiento es simple, menos arriesgado y costoso, pero es un obstáculo porque implica no realizar la actividad que conlleva al riesgo, por lo tanto, hay situaciones donde no es una opción.

Reducir (Compartir el Riesgo):
Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido

con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que no se transfiere la responsabilidad del riesgo.

Reducir (Mitigar el Riesgo):
El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.
Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

5.6 ARMONIZACIÓN CON OTRAS POLÍTICAS, PLANES Y PROYECTOS INSTITUCIONALES

La política institucional de administración de riesgos se armoniza con los planes que hacen parte de las estrategias, productos o acciones del Plan Estratégico Institucional, de los proyectos de inversión de la Entidad o los que surjan con motivo del desarrollo del plan de continuidad del negocio, de políticas públicas del Gobierno Nacional o de normas legales.

6. DIRECTRICES GENERALES FRENTE A LA ADMINISTRACIÓN DEL RIESGO EN LA ARN (ROLES Y RESPONSABILIDADES)

- La Alta Dirección, en cabeza del representante legal, lidera la política institucional de administración de riesgos.

- La Oficina Asesora de Planeación orienta, asesora la implementación de la metodología de gestión del riesgo en la entidad y administra la herramienta dispuesta por la entidad para la operatividad de los mapas de riesgos.

- La Oficina Asesora de Planeación realiza el seguimiento y monitoreo de los riesgos trimestralmente.

- El Grupo de Control Interno de Gestión efectúa la evaluación de la eficacia y efectividad en la gestión del riesgo, de forma semestral para los riesgos de gestión y cuatrimestral para los riesgos de corrupción.

- Cada líder de proceso, con la asesoría y acompañamiento de la Oficina Asesora de Planeación y Grupo de Control Interno de Gestión, tiene la

responsabilidad sobre la identificación, análisis, valoración, evaluación y tratamiento de los riesgos.

- Los líderes de proceso a cargo de los riesgos (primera y segunda línea de defensa) tienen la responsabilidad sobre la implementación de los controles y acciones contenidas en el mapa de riesgos, el seguimiento, la verificación de su eficacia y efectividad, el proponer cambios y proporcionar la evidencia.

  Las acciones definidas para el tratamiento de los riesgos se consignan en la herramienta establecida por la Entidad, con la identificación de responsables de su reporte, y con sus respectivas fechas de inicio y terminación.

- Los líderes de proceso tienen la responsabilidad de la administración de los riesgos específicos en lo que corresponde a sus funciones. Dicha gestión también será responsabilidad de empleados públicos y los contratistas que actúen en representación de la Entidad, en el marco de sus funciones u obligaciones contractuales según aplique.

- Para el seguimiento del tratamiento de los riesgos se debe tener en cuenta lo establecido en el título “Seguimiento basado en reporte de acciones”, del documento Manual de Seguimiento a la Planeación y Gestión Institucional, código DE-M-03.

- Para el tratamiento de los riesgos se tiene en cuenta la valoración determinada en el mapa de riesgos de la siguiente manera:

  - Las acciones por emprender sobre los riesgos y los tiempos de ejecución de estas son definidas por los líderes de proceso y/o jefes de dependencia y los responsables del riesgo. Dichas acciones estarán orientadas a evitar, compartir o reducir el riesgo.

  - Las acciones por ejecutar en el marco de la administración del riesgo deben orientarse a la mejora continua de los procedimientos, fortalecimiento de los controles, implementación y fortalecimiento de las políticas encaminadas a cumplir con los objetivos institucionales.

- Corresponde a la Oficina Asesora de Planeación impulsar a nivel institucional una cultura de prevención y gestión del riesgo congruente con el Sistema Integrado de Gestión, facilitando así el cumplimiento de los propósitos de la Entidad y los requerimientos del Sistema, para ello se deben planificar y desarrollar acciones en el marco del Plan Institucional de Capacitación.

- La Política de Administración del Riesgo y los controles establecidos se revisan al menos una vez al año, en el último trimestre de cada vigencia, y se ajustan si es necesario para adaptarlos a los cambios que se puedan presentar en la Entidad.

- Para la difusión y apropiación de la política institucional de administración de riesgos, en el plan institucional de capacitación y en el plan de comunicaciones se incluyen actividades sobre la apropiación.

7. CONTENIDO Y DESARROLLO

Para implementar la política institucional de riesgos y aplicar las directrices señaladas, en la ARN se sigue la siguiente metodología:

7.1 IDENTIFICACIÓN DE RIESGOS

7.1.1 Contexto Estratégico

Para establecer los riesgos en los procesos de la Entidad se parte de analizar el contexto externo, el contexto interno y el contexto del proceso, que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos, así mismo, determinar las partes interesadas y los requisitos de estas que son relevantes para el Sistema Integrado de Gestión. El contexto estratégico está definido como las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos institucionales.

Con esta identificación la ARN determina los riesgos y oportunidades que es necesario tratar con el fin de prevenir o reducir efectos no deseados y lograr la mejora continua, asimismo incorporar e implementar las acciones en los procesos del Sistema Integrado de Gestión y realizar la evaluación de la eficacia de esas acciones.

Partiendo del contexto estratégico de la Entidad cada proceso es responsable del análisis para la identificación de los factores internos y externos que pueden afectar el cumplimiento del objetivo del proceso; en consecuencia, se constituye en un insumo a partir del cual cada proceso identifica las causas generadoras de riesgos sobre las cuales, de acuerdo con su naturaleza y alcance, debe desarrollar acciones eficaces para su prevención y/o tratamiento.

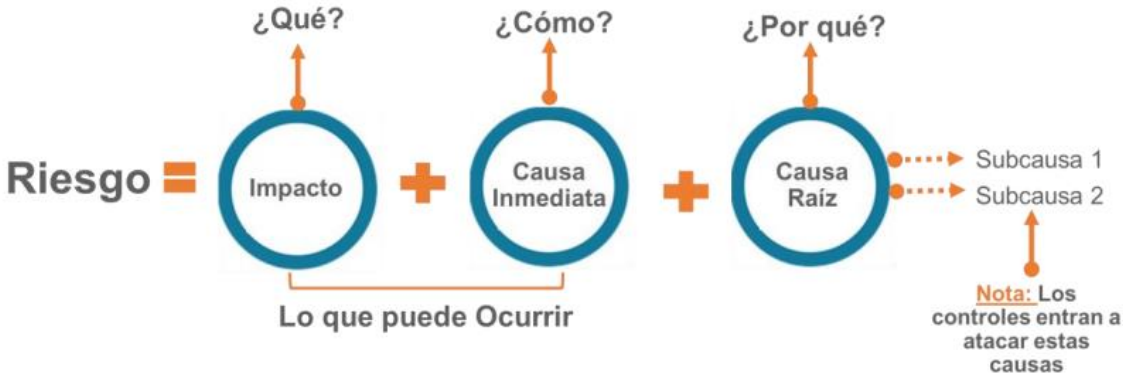
7.1.2 Identificación del Riesgo

En este punto se determinan aquellos eventos o situaciones que pueden o tienen

el potencial de afectar el logro de los objetivos de los procesos y por consiguiente de la entidad.

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso.

Se propone una estructura que facilita la redacción y claridad. que inicia con la frase “posibilidad de” y se analizan los siguientes aspectos:



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, Bogotá, Departamento Administrativo de la Función Pública. Versión 5. 2020

Desglosando la estructura propuesta tenemos:

- Impacto: las consecuencias que puede ocasionar a la entidad la materialización del riesgo. Para los riesgos de gestión, los impactos que aplican son afectación económica (o presupuestal) y reputacional.
- 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 pueden existir más de una causa o subcausas que pueden ser analizadas.

Ejemplo:

- Impacto: Pérdida económica y reputacional

- Causa inmediata: Incumplimiento de la ley de transparencia y acceso a la información pública y las normativas relacionadas
- Causa raíz: Desactualización de información pública disponible en la sede electrónica de la ARN acorde a los diferentes requerimientos.

De acuerdo con la estructura, este riesgo de gestión se describiría como: "Posibilidad de pérdida económica y reputacional por incumplimiento de la ley de transparencia y acceso a la información pública y las normativas relacionadas debido a fallas en la actualización de información pública disponible en la sede electrónica de la ARN acorde a los diferentes requerimientos.

En el mismo orden de ideas para los riesgos de corrupción es necesario que se aplique la siguiente estructura gramatical: Acción u omisión + Uso del poder + Desviación de la gestión de lo público + El beneficio privado.

Para el caso de los riesgos de seguridad digital, se parte de la identificación de los activos de información de cada proceso, permitiendo determinar cuáles son los activos de información más relevantes para la Entidad y sus procesos.

La ARN prioriza la gestión de los riesgos de seguridad digital para aquellos activos de información identificados y valorados en la matriz de activos de información con un nivel de criticidad *alta*, y clasificación tipo *información*.

En seguridad digital, se pueden identificar los siguientes riesgos inherentes a los cuales están expuestos los activos de información:

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

Un activo de información puede estar expuesto a uno de los riesgos inherentes o a una combinación de ellos, lo cual debe ser evidenciado en la descripción del riesgo, como se muestra en el siguiente ejemplo:

> Posibilidad de uso indebido de la información, por manipulación o accesos no autorizados de software y fallas en los controles para la seguridad de los datos que afecta la confidencialidad e integridad de la información.

- **Clasificación del Riesgo**

Permite agrupar los riesgos de gestión en las siguientes categorías:

CLASIFICACIÓN	DESCRIPCIÓN
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida 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 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas 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 éstos.
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.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, Bogotá, Departamento Administrativo de la Función Pública. Versión 5. 2020. Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

7.2 VALORACIÓN DEL RIESGO

Consiste en primer lugar, en realizar un análisis del riesgo frente a su probabilidad de ocurrencia y sus consecuencias para estimar la zona de riesgo inicial (riesgo inherente), seguido por una evaluación del riesgo que busca confrontar el análisis de riesgo inicial con el resultado del riesgo final (riesgo residual), después de confrontar el análisis con los controles establecidos.
A continuación, se describen cada uno de los elementos que conforman esta valoración.

7.2.1 Análisis del Riesgo

El análisis del riesgo busca establecer la probabilidad de ocurrencia de este y sus consecuencias (impacto), con el fin de obtener información para establecer el nivel de riesgo inicial (riesgo inherente) y las acciones que se van a implementar.

Para realizar un adecuado análisis de riesgos se debe tener en cuenta:
Calificación de la probabilidad: Es la posibilidad de ocurrencia del riesgo.
La probabilidad de ocurrencia está asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente es el número de veces que se pasa por el punto de riesgo en el periodo de 1 año. Este método de calificación aplica para riesgos de gestión, corrupción y seguridad digital.

La calificación de probabilidad se realiza de conformidad con la siguiente tabla:

	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 para la administración del riesgo y el diseño de controles en entidades públicas, Bogotá, Departamento Administrativo de la Función Pública. Versión 5. 2020*

Calificación del impacto: Es el cálculo de la magnitud de las consecuencias de la materialización del riesgo y se calcula a partir de 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.

La calificación del impacto del riesgo objeto de análisis, se realiza mediante la aplicación de los siguientes criterios:

a) Para los riesgos de gestión y seguridad digital:

Se puede valorar el impacto en los cinco niveles descritos de la siguiente tabla:

	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 dircetiva 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

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, Bogotá, Departamento Administrativo de la Función Pública. Versión 5. 2020*

b) Para los riesgos de corrupción

Contestar la siguiente serie de preguntas por cada riesgo de corrupción identificado, registrando con una X si la respuesta es SÍ o NO para su posterior conteo.

CUESTIONARIO DE PREGUNTAS

No.	Si el riesgo de corrupción se materializa podría…	Respuesta	
		SÍ	NO
1	¿Afectar al grupo de servidores 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 del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza en la entidad, afectando su reputación?		
6	¿Generación pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de los servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicio o de recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la fiscalía u otro ente?		

No.	Si el riesgo de corrupción se materializa podría…	Respuesta	
		SÍ	NO
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?		

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, Bogotá, Departamento Administrativo de la Función Pública. Versión 5. 2020*

Una vez finalizado el registro del cuestionario se hace el conteo para saber la cantidad de respuestas para SÍ y para NO.

La siguiente tabla muestra en nivel en que quedaría el impacto para los riesgos de corrupción:

Valoración de impacto para los riesgos de corrupción
Respuesta afirmativa de UNO a CINCO preguntas genera impacto Moderado
Respuesta afirmativa de SEIS a ONCE preguntas genera impacto Mayor
Respuesta afirmativa de DOCE a DIECINUEVE preguntas genera impacto Catastrófico

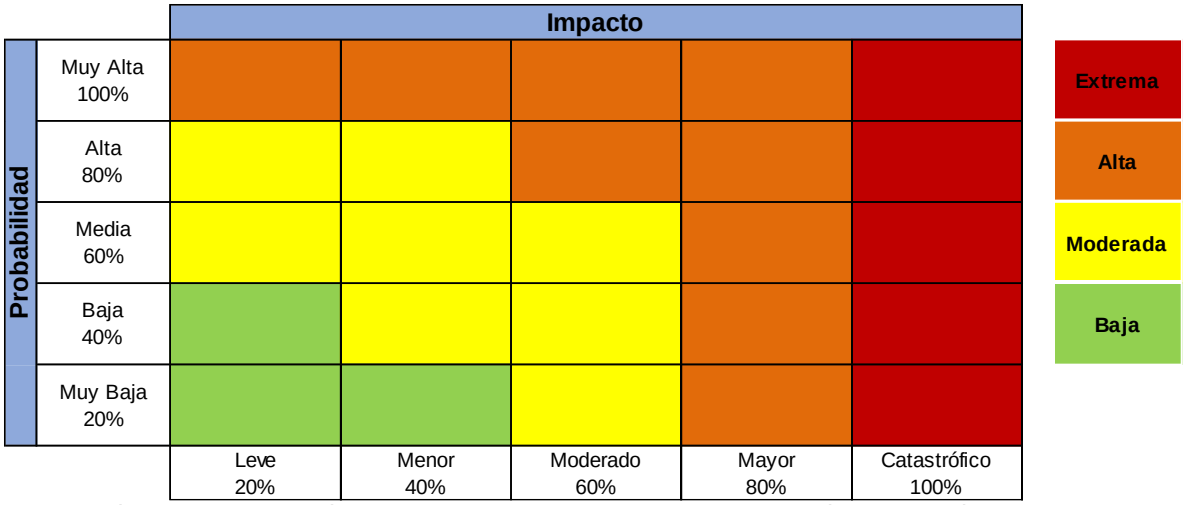
Nota: La política de riesgos de la ARN establece intolerancia total frente a los riesgos de corrupción, por ello en ningún caso la opción de tratamiento sería aceptar.

7.2.2 Evaluación del riesgo

Una vez calificada la probabilidad y el impacto del riesgo objeto de análisis, se determina la zona de riesgo inicial (riesgo inherente), para ello se realiza el cruce de acuerdo con la Matriz de calor, la cual permite determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto definiendo cuatro zonas de severidad.

El resultado de la evaluación del riesgo se hace de manera automática una vez calificadas la probabilidad y el impacto y quedan consignadas en el software para la Administración de la Planeación y la Gestión.

Matriz de calor (niveles de severidad del riesgo)



Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, Bogotá, Departamento Administrativo de la Función Pública. Versión 5. 2020*

7.2.3 Valoración y diseño de los controles

Un control se define como la medida que permite reducir o mitigar el riesgo. Una vez establecida la evaluación del riesgo se identifican, diseñan y valoran los controles, para lo cual es necesario seguir las siguientes pautas:

- **Redacción del Control**: En el diseño del control su redacción debe tener la siguiente estructura:

Responsable de ejecutar el control	Acción	Complemento
Si el control es manual, se describe el cargo de la persona que ejecuta el control. Si el control es automático, se describe el sistema que realiza la actividad	Se determina mediante verbos que indican la acción que deben realizar como parte del control.	Contiene los detalles que permiten identificar claramente el objeto del control, describiendo como mínimo: la periodicidad, detalles de cómo se realiza la actividad y la evidencia de la ejecución del control.

Los controles para mitigar/tratar los riesgos de Seguridad Digital, son los definidos en el Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas” y han sido incorporados en el módulo de riesgos del Software para la Administración de la Planeación y la Gestión (SAPYG) para selección, cuando se esté valorando este tipo de riesgos.

Ejemplo:

Retomando el riesgo identificado en el numeral 7.1.2, a continuación, se presenta como se redactan los controles.

Riesgo identificado: Posibilidad de pérdida económica y reputacional por incumplimiento de la ley de transparencia y acceso a la información pública y las normativas relacionadas debido a fallas en la actualización de información pública disponible en la sede electrónica de la ARN acorde a los diferentes requerimientos.
Probabilidad inherente: Muy alta (100%), La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.
Impacto inherente: Moderado (60%) El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Zona de riesgo: Alta. Resulta del cruce en el mapa de calor de la calificación de la probabilidad e impacto.

Ejemplo de la redacción del control:

El profesional designado por parte del proceso Direccionamiento Estratégico, cada vez que se requiera (PERIOCIDAD), debe revisar el cumplimiento de la ley de transparencia y acceso a la información pública y las normativas relacionadas en la sede electrónica de la ARN, realizando la revisión y actualización de la información publicada y el espacio de transparencia, en las que revisa e identifican el cumplimiento de los ítems asignados (CÓMO SE REALIZA). En caso de detección de un incumplimiento por parte del proceso (QUÉ PASA CON LAS OBSERVACIONES O DESVIACIONES), se debe realizar la aplicación a lo establecido para tales efectos en el Manual de Gestión del Riesgo de la ARN. La evidencia del control (CÓMO SE EVIDENCIA SU EJECUCIÓN) corresponde al acta de seguimiento por parte del líder de proceso que soporta el registro del Índice de Transparencia y Acceso a la Información Pública (ITA) de la Procuraduría General de la Nación.

Para la valoración del control asociado al riesgo, se toman en consideración los atributos del diseño de controles tales como la eficiencia (tipo de control preventivo, detectivo o correctivo) y la implementación (control manual o automático.

- **Tipología de controles**: Los controles pueden ser, preventivos, detectivos o correctivos, dependiendo de cuando se activan en el ciclo de los procesos (Entradas, interrelaciones, salidas), como se describe a continuación:

Tipo (Atributo Eficiencia)	Propósito	Ciclo del proceso

Preventivos	Intenta evitar la ocurrencia de los riesgos, por lo que está dirigido a las causas del riesgo y atacan su probabilidad de ocurrencia.	Se acciona en la entrada del proceso y antes de que se realice la actividad originadora del riesgo.
Detectivos	Detectan el riesgo y generan un reproceso devolviendo el proceso a los controles preventivos atacando la probabilidad de ocurrencia.	Se acciona durante la ejecución del proceso.
Correctivos	Atacan el impacto frente a la materialización del riesgo. Generan un costo en su implementación.	Se acciona en las salidas del proceso y después que se materializa el riesgo.

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, Bogotá, Departamento Administrativo de la Función Pública. Versión 5. 2020*

- **Tipología de controles de acuerdo como se ejecutan:** Los controles pueden ser manuales o automáticos de acuerdo con la forma de cómo se ejecutan:

Tipo (Atributo Eficiencia)	Descripción
Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.
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. Ejemplo: controles ejecutados por los sistemas con que cuenta la ARN.

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, Bogotá, Departamento Administrativo de la Función Pública. Versión 5. 2020*

- **Tipología de controles de acuerdo con atributos informativos:** 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.

Tipo (Atributo Informativo)	Característica	Descripción

Documentado	Documentación	Controles que están documentados en el proceso, 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.
Continua	Frecuencia	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.
Aleatoria		El control se aplica aleatoriamente a la actividad que conlleva el riesgo.
Con registro	Evidencia	El control deja un registro permite evidencia la ejecución del control.
Sin registro		El control no deja registro de la ejecución del control.

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, Bogotá, Departamento Administrativo de la Función Pública. Versión 5. 2020*

7.2.4 Análisis y Evaluación de los Controles

Las acciones de control asociadas a los riesgos actúan sobre la probabilidad de ocurrencia de este o sobre el impacto que generan al materializarse. Por lo tanto, para la evaluación de los controles existentes se debe valorar cada control asociado al riesgo teniendo en cuenta los atributos o características del control y su peso asignado, así:

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 de Formalización**	**Documentación**	**Documentado**	Controles que están documentados en el proceso, 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	-
	Frecuencia	**Continua**	Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo.	-
		Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo	-
	Evidencia	**Con Registro**	El control deja un registro que permite evidenciar la ejecución del control	-
		Sin Registro	El control no deja registro de la ejecución del control	-

Nota: Los atributos de formalización se recogerán de manera informativa, con el fin de conocer el entorno del control y complementar el análisis con elementos cualitativos; éstos no tienen una incidencia directa en su efectividad.

Una vez redactado el control de acuerdo con las disposiciones descritas, se debe hacer una valoración del diseño teniendo en cuenta el peso asignado a cada característica o atributo del control definida en la tabla anterior, dicho valor se debe sumar para establecer la calificación del control.

***Los controles de tipo preventivo**:* evitan que un evento suceda, disminuye la probabilidad. Ejemplo: *usuario* y *contraseña* en un sistema de información previene (teóricamente) que personas no autorizadas puedan ingresar al mismo.

Los controles de tipo correctivo: No prevé que un evento suceda, pero permiten enfrentar la situación una vez se ha presentado, disminuye el impacto. Ej. Pólizas de seguro y otros mecanismos de recuperación de negocio o respaldo.

Los controles de tipo detectivo: Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Disminuyen la probabilidad de ocurrencia del riesgo. Ej.: conciliaciones contables.

Determinación del riesgo residual (nivel de riesgo): es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Teniendo en cuenta que el control puede afectar probabilidad o impacto, una vez aplicada la valoración de controles, el riesgo residual disminuye en probabilidad o impacto según el control aplicado.

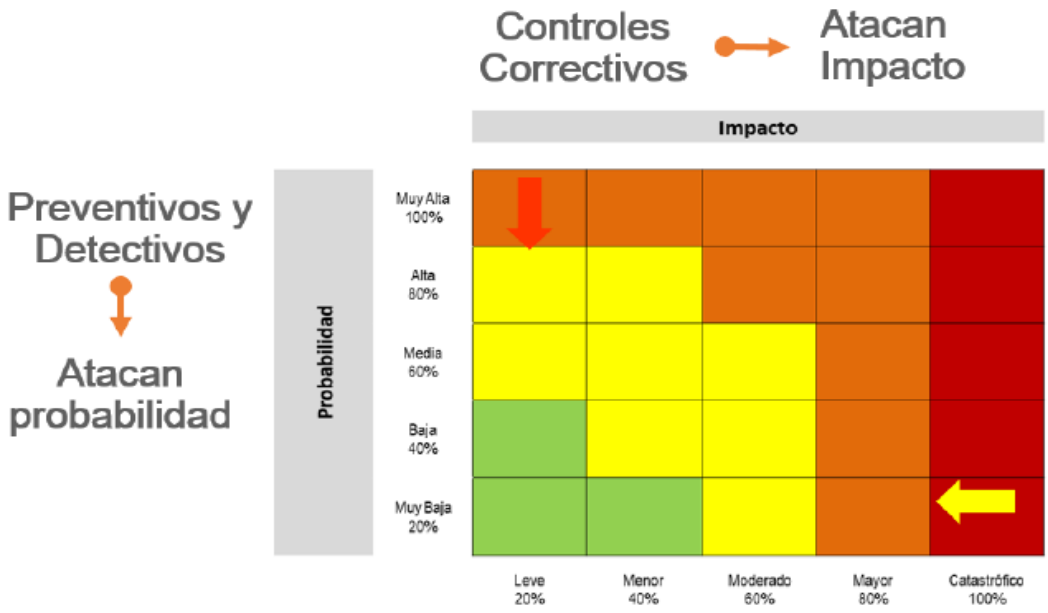
Para determinar la probabilidad o impacto residual, se debe multiplicar el valor de probabilidad o impacto inherente por el valor de la calificación del control, el resultado de esta multiplicación se resta del valor de la probabilidad o impacto inherente y es el valor de la probabilidad o impacto residual. Dicha operación se representa en la siguiente imagen:

Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = 36%

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, Bogotá, Departamento Administrativo de la Función Pública. Versión 5. 2020*

Un riesgo puede tener asociados más de un control, en este caso se debe tener en cuenta que los controles mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Según el tipo de control aplicado al riesgo, se da el movimiento de ubicación en el mapa de calor en el eje de probabilidad o en el eje de impacto, tal como se muestra en la siguiente imagen.



Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, Bogotá, Departamento Administrativo de la Función Pública. Versión 5. 2020*

Siguiendo con el ejemplo del riesgo “Posibilidad de pérdida económica y reputacional por incumplimiento de la ley de transparencia y acceso a la información pública…”

Probabilidad inherente: Muy alta (100%)

Al valorar el control definido, tenemos:
Tipo: Preventivo (25%) afecta la probabilidad.
Implementación: Manual (15%)
Valoración control: 40% (sumatoria del tipo de control + implementación)

Probabilidad residual:

100% * 40% = 40% (Probabilidad inherente * valoración control)
100% - 40% = **60%** probabilidad residual.

Después de valorado este control, el riesgo cuya probabilidad inherente era Muy Alta, ha quedado con probabilidad residual Media, pasando de zona de riesgo inherente Alta, a zona de riesgo residual Moderada.

7.3 TRATAMIENTO DEL RIESGO

Los elementos de control son los que permiten estructurar los criterios orientadores en la toma de decisiones respecto al tratamiento de los riesgos y sus efectos.

De conformidad con los resultados obtenidos en la evaluación del riesgo después de haber evaluado los controles existentes, se define la opción de manejo del riesgo de acuerdo con la zona donde éste se encuentre ubicado.

ZONA DE RIESGO	OPCIÓN DE MANEJO
B: Zona de riesgo Baja	Asumir el riesgo
M: Zona de riesgo Moderada	Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo Alta	Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo Extrema	Reducir el riesgo, Evitar, Compartir o Transferir

Las políticas identifican las acciones para tratar y manejar los riesgos, permitiendo tomar las decisiones adecuadas acerca de si se acepta, se evita, se comparte o se transfiere legalmente el impacto en cada uno de los riesgos identificados que al materializarse puede obstaculizar el cumplimiento de los objetivos institucionales y de los objetivos de los procesos.

7.3.1 Características de manejo de riesgos

- **Evitar el riesgo**: Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades.

- **Reducir el riesgo**: El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda

reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.

- **Compartir o Transferir el riesgo:** Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

- **Asumir el riesgo**: Si el nivel de riesgo cumple con los criterios de aceptación de riesgo no es necesario establecer controles y acciones, y este puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo. En ningún caso aplica para riesgos de corrupción.

En la herramienta establecida por la entidad se debe seleccionar la opción de manejo del riesgo.

7.3.2 Acciones

De acuerdo con la opción de manejo del riesgo definida a partir de la calificación de este, cada proceso debe establecer de manera concreta que acciones o actividades debe desarrollar para el manejo de los riesgos, orientadas a evitar, reducir, compartir o asumir el riesgo.

Las acciones definidas deben ser realizables y efectivas en el tratamiento del riesgo, para ello, se debe considerar la viabilidad jurídica, técnica, institucional, financiera y económica (balance costo-beneficio). Algunas de las acciones podrían ser: la implementación de las políticas, definición de estándares, optimización de procesos y procedimientos, cambios físicos, entre otros.

Las acciones definidas deben estar relacionadas con los controles descritos de manera que al evaluarlas se pueda determinar si estos están siendo adecuados para mitigar el riesgo, por su eficacia y efectividad.

El reporte de las acciones definidas se debe registrar en la herramienta establecida por la entidad y las evidencias de los resultados finales se deben guardar de acuerdo con lo definido en el Manual de Seguimiento de la Planeación y Gestión Institucional (DE-M-03).

7.4 MONITOREO Y REVISIÓN

Línea Estratégica
Define el marco general para gestión del riesgo y el control y supervisa su cumplimiento.

Primera Línea de Defensa
Desarrolla e implementa proceso de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

Segunda Línea de Defensa
Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y función como se pretende.

Tercera Línea de Defensa

Proporciona información sobre la efectividad del Sistema de Control Interno, a través de un enfoque basado en riesgos, incluida la generación de la primera y segunda línea de defensa.

LÍNEAS	RESPONSABLE	MECANISMO	PRINCIPALES RESPONSABILIDADES DE CONTROL	EVIDENCIA DE CONTROL
LÍNEA ESTRATÉGICA	**Director General** **Comité Institucional de Coordinación de Control Interno**	**EVALUACIÓN**	➢ Someter a aprobación la Política de Administración del Riesgo de la Agencia y efectuar seguimiento. ➢ Evaluar el estado del Sistema de Control Interno y aprobar sus modificaciones, actualizaciones y acciones de fortalecimiento. ➢ Aprobar y realizar seguimiento al Plan Anual de Auditoría. ➢ Revisar los estados financieros y hacer las recomendaciones a que haya lugar. ➢ Definir el marco general para la gestión del riesgo y el control junto con la supervisión de su cumplimiento.	✓ Documento de Política del Riesgo. ✓ Informe de seguimiento de los Riesgos ✓ Documento de evaluación del Sistema de Control Interno (SCI) de la Agencia. ✓ Plan Anual de Auditoria aprobado ✓ Informe de Control Interno Contable ✓ Reporte de seguimiento del Plan Anual de Auditorías (PAA). ✓ Actas de reunión.
PRIMERA LÍNEA DE DEFENSA	**Líderes de Procesos (Directores; Subdirectores; Jefes de Oficina; Asesores; y, Coordinadores** **Todos los Empleados Públicos y Contratistas adscritos a la Agencia**	**AUTOCONTROL**	➢ Identificar, hacer seguimiento y evaluar el riesgo que puede afectar la gestión u obligación desarrollada. ➢ Identificar y aplicar los controles asociado al riesgo que puede afectar la gestión u obligación desarrollada. ➢ Ejecutar las acciones preventivas, correctivas y de mejora a que haya lugar producto del riesgo y control que puede afectar o afectó la gestión u obligación desarrollada.	✓ Registro en los aplicativos autorizados (Sistema de Información para la Reintegraicón y Reincorporaciói n (SIIR); software para la Administración de la Planeación y la Gestión; Sistema de Correspondencia de la Entidad; Sistema Integrado de Información Financiera (SIIF); y, Sistema Nacional de Evaluación de Gestión y Resultados (SINERGIA), entre otros).

LÍNEAS	RESPONSABLE	MECANISMO	PRINCIPALES RESPONSABILIDADES DE CONTROL	EVIDENCIA DE CONTROL
SEGUNDA LÍNEA DE DEFENSA	Líderes de Proceso; Directores; Asesores con funciones institucionales; Coordinadores de Grupos; y, Supervisores de contratos con obligaciones institucionales o transversales COMITÉS: institucional de Gestión y Desempeño, De presupuesto y Contratación	**AUTOEVALUACIÓN**	➢ Consolidar, analizar y reportar información Institucional o transversal de la Agencia de acuerdo con la temática de gestión designada. ➢ Hacer seguimiento y monitoreo a los riesgos de los procesos para la toma de decisión de la línea estratégica y aplicación de la Primera Línea de Defensa. ➢ Realizar seguimiento y verificar la eficacia de los planes de mejoramiento.	✓ Documento de Información Institucional o transversal (Ejemplo: Informes de Gestión: Financiera, Planeación Institucional; Reintegración y Reincorporación; ETCR's; Convenios; e Informe Ejecutivo de Control Interno, entre otros). ✓ Informe de seguimiento y monitoreo a los riesgos. ✓ Registro software para la Administración de la Planeación y la Gestión ✓ Actas de reunión.
TERCERA LÍNEA DE DEFENSA	Grupo de Control Interno de Gestión quipo de Auditores Internos	**EVALUACIÓN INDEPENDIENTE**	➢ Evaluar y presentar la gestión de los Riesgos de la Agencia para la toma de decisiones de la Línea Estratégica y la Segunda Línea de defensa. ➢ Elaborar, presentar y ejecutar el Plan Anual de Auditorías. ➢ Evaluar el Sistema de Control Interno de la Agencia para la toma de decisiones de la Línea Estratégica y la Segunda Línea de defensa. ➢ Elaborar, consolidar y presentar los informes de ley y de gestión. ➢ Evaluar la eficacia de los planes de mejoramiento.	✓ Informe de Riesgos. ✓Plan Anual de Auditorias aprobado. ✓Informes de auditoria. ✓Reporte Formulario Único Reporte de Avances de la Gestión e informe de percepción del SCI. ✓Informes de ley y de gestión (Informe SIGEP; Informe PQRS-D, entre otros).. ✓Informe de planes de mejoramiento.

Fuente: Elaboración propia

Una vez diseñado y validado el mapa de riesgos es necesario monitorearlo, teniendo en cuenta que éstos nunca dejan de representar amenazas para el cumplimiento de los objetivos estratégicos o de los procesos.

La acción de monitorear los riesgos es permanente y permite establecer si los planes de acción implementados fueron efectivos, si los niveles de riesgos permanecen o se han modificado, cuántos riesgos permanecen, si aparecen nuevos riesgos, si se requieren nuevos o ajuste en los controles definidos y si se han materializado o no para determinar la eficacia de estos.

De acuerdo con lo anterior, los líderes de los procesos deben asegurar que las acciones establecidas en los mapas de riesgos se están llevando a cabo y evaluar la eficacia y efectividad en su implementación, adelantando monitoreo periódico para evidenciar todas aquellas situaciones o factores que pueden influir en la aplicación de las acciones para el manejo de los riesgos.

Todos los riesgos identificados tienen seguimiento a través de sus acciones de tratamiento, de manera trimestral y se deben adjuntar las evidencias del seguimiento en la carpeta compartida definida para cada riesgo y trimestre de la vigencia.

El registro del seguimiento se realiza a través del módulo de riesgos del software para la Administración de la Planeación y la Gestión (SAPYG), el cual trimestralmente lanza una tarea por cada riesgo identificado y se registra el avance de la gestión. Para el reporte trimestral de las acciones para el tratamiento del riesgo, el responsable debe iniciar identificando el trimestre del reporte, adicionalmente describir de manera detallada las actividades (fechas de realización, número de participantes, número de capacitaciones, sesiones, charlas, entrenamientos, reuniones etc.) que realiza en el periodo de reporte, cumpliendo con la acción asignada.

Para el monitoreo y seguimiento se debe tener en cuenta los siguientes aspectos:

- Aplicación de los controles definidos para el riesgo.
- Eficacia de las acciones implementadas.
- Evaluación de plan de mejoramiento cuando se requiera.
- Determinar si se materializó o no el riesgo

El líder del proceso realiza análisis trimestral del comportamiento del riesgo en el periodo, el aporte de las acciones al cumplimiento de los controles definidos identifica si el riesgo se materializa, en este caso debe indicar cuál fue la acción y el control que no se cumplió para esta situación, y las acciones de mejora a tomar.

En caso de materialización de un riesgo, el sistema envía de manera automática una solicitud de plan de mejoramiento al líder del proceso donde se materializa el riesgo. El líder del proceso debe formular y registrar en el Software para la Administración de la Planeación y la Gestión (SAPYG) dicho plan de mejoramiento en un plazo no mayor a 15 días.

El análisis del riesgo al final de la vigencia debe contar con un resumen del año de manera concreta y clara de las acciones realizadas para el manejo del riesgo; si el riesgo se materializa se debe indicar cuál fue la acción y el control que no se cumplió para esta situación y las acciones de mejora que se tomaron o se tomarán en caso de que la materialización haya sido en el cuarto trimestre.

7.5 EVALUACIÓN DE LA EFICACIA DE LAS ACCIONES

El Grupo de Control Interno de Gestión, evalúa la gestión del riesgo de la Entidad de forma integral con la generación de observaciones y recomendaciones para la mejora, de acuerdo con lo siguiente:

- **Plan Anual de Auditorias:** De conformidad con lo establecido en el Plan Anual de Auditorias el Grupo de Control Interno de Gestión se ejecutan

auditorias basadas en riesgos, en las cuales se provee una evaluación independiente, objetiva, e imparcial de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de la Entidad; lo anterior permite informar sobre la exposición al riesgo de la Agencia acorde con los lineamentos y la política institucional.

- **Seguimiento Mapa de Riesgos:** Se realiza de forma semestral una evaluación de los riesgos y controles diseñados por la Agencia en cumplimiento de lo establecido en el artículo 17 del decreto 648 de 2017 frente a la evaluación de la gestión del riesgo, así como con el análisis y seguimiento a cargo de las Oficinas de Control Interno de Gestión descrito en el MIPG, en su Séptima Dimensión (Control Interno). La evaluación de cumplimiento se realiza a partir de la información reportada en el software para la Administración de la Planeación y la Gestión y de las evidencias aportadas para tal fin.

- **Seguimiento Mapa Riesgos de Corrupción:** Se realiza de forma cuatrimestral una evaluación a los riesgos y controles diseñados por los procesos de la Agencia para hacer frente a posibles casos de corrupción. La evaluación de cumplimiento se realiza a partir de la información reportada en el software para la Administración de la Planeación y la Gestión y de las evidencias aportadas para tal fin.

La línea estratégica (Comité Institucional de Coordinación de Control Interno) analiza para la toma de decisiones los resultados del seguimiento a la gestión del riesgo en la entidad y las recomendaciones de mejoramiento aportadas por la tercera línea de defensa con una periodicidad mínima de dos veces al año.

7.6 ACCIONES ANTE RIESGOS MATERIALIZADOS

En caso de la materialización de un riesgo, dependiendo del tipo de riesgo y los responsables se debe actuar de la siguiente manera:

A continuación, se presenta la propuesta sobre los responsables y actividades:

TIPO DE RIESGO	RESPONSABLE	ACTIVIDAD
Riesgo de corrupción	Empleado público y/o contratista Dependencia o Proceso	Una vez detectado el evento de corrupción este debe ser informado por correo electrónico al respectivo líder de proceso o jefe de dependencia, coordinador de grupo o responsable competente.

TIPO DE RIESGO	RESPONSABLE	ACTIVIDAD
	Líder de proceso o jefe de dependencia o coordinador de grupo	Cuando se haya confirmado el evento de corrupción, es decir la materialización del riesgo, informar mediante correo electrónico a la Dirección General, a la Oficina Asesora Jurídica, al Grupo de Control Interno de Gestión y la Oficina Asesora de Planeación.
	Grupo de Control Interno de Gestión	Realizar la denuncia ante la instancia de control correspondiente, de acuerdo con los mecanismos establecidos por la instancia de control, una vez establecido el alcance del evento materializado a partir de la normatividad asociada al hecho.
	Grupo de Control Interno de Gestión	En cumplimiento del rol de evaluación y seguimiento, a través de las auditorías y el seguimiento que se les hacen a los riesgos, informará a los responsables de los procesos y/o dependencias la materialización del riesgo, así como a los órganos de control del estado competentes. En caso de que la Dependencia o Proceso no Informe a la Oficina Asesora Jurídica y a la Oficina Asesora de Planeación, el Grupo de Control Interno de Gestión reportará mediante correo electrónico a dichas dependencias el hecho ocurrido.
	Líder de proceso o jefe de dependencia o coordinador de Grupo de Control Interno de Gestión	Identificar las acciones correctivas necesarias y formular el plan de mejoramiento en el módulo correspondiente del *Software* para la Administración de la Planeación y Gestión Institucional (Ver Procedimiento de Acciones Correctivas y de Mejora, Código: EM-P-01).
	Grupo de Control interno de Gestión	Informar a la Oficina Asesora de Planeación, por correo electrónico con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos.
	Líder de Proceso	Efectuar el análisis de causas; redefinir el control; y determinar acciones de tratamiento del riesgo con aprobación del líder del proceso.
	Dependencia o Proceso	Identificar las acciones correctivas necesarias y formular el plan de mejora correspondiente; este debe ser registrado, en un tiempo no mayor a 15 días después de haber ocurrido el hecho, en el módulo correspondiente del Software para la Administración de la Planeación y la Gestión Institucional.
	Dependencia o Proceso	Solicitar a la Oficina Asesora de Planeación la actualización del mapa de riesgos, por correo electrónico.
Riesgos de Seguridad Digital	Empleado público y/o contratista	Informar la materialización del riesgo mediante correo electrónico al respectivo líder de proceso por parte del empleado público o contratista de la Entidad al que se le ha asignado la responsabilidad sobre un activo de información; lo anterior, en

TIPO DE RIESGO	RESPONSABLE	ACTIVIDAD
		concordancia con lo establecido en el Manual del Sistema de Gestión de Seguridad de la Información (Código: TI-M-01).
	Líder de Dependencia o Proceso	Informar la materialización del riesgo, por correo electrónico <Soporte@reincorporacion.gov.co>, al jefe de la Oficina de Tecnologías y de la Información, al Oficial de Seguridad de la información y al Grupo de Control Interno de Gestión. En caso de que la materialización del riesgo genere un incidente de seguridad informar por correo electrónico al responsable de Seguridad Informática del Grupo de Infraestructura y Soporte. con el fin de que aplique lo dispuesto en la Guía para la gestión de incidentes de seguridad (TI-G-04) y en el procedimiento de gestión de incidentes de seguridad (TI-P-03)
	Oficina de Tecnologías y de la Información	Informar la ocurrencia del evento de seguridad a la Dirección General, al Oficial de Seguridad de la Información y al Grupo de Control Interno de Gestión, a través del correo electrónico de la Jefatura de la Oficina de Tecnologías y de la Información y/o del responsable de seguridad informática del Grupo de Infraestructura y Soporte.
	Grupo de Control Interno de Gestión	En caso de ser detectada la materialización del riesgo en proceso de auditoría interna o verificación de información para un informe se reportará, mediante correo electrónico, el hallazgo a la Dirección General; Oficial de Seguridad de la Información; a la Jefatura de la Oficina de Tecnologías y de la Información y al responsable de seguridad informática del Grupo de Infraestructura y Soporte.
	Oficial Seguridad de la Información	Programar y efectuar Mesa de Seguridad de la Información con la participación del propietario del activo de información; el líder de su proceso o jefe de dependencia, y los integrantes de la mesa de seguridad, para determinar las causas del evento y tomar las acciones necesarias.
	Dependencia o Proceso Oficina Asesora de Planeación Grupo de Control Interno de Gestión	Evaluar y mejorar o crear el(los) control(es), para mitigar, efectivamente, el(los) riesgo(s); determinar las correspondientes acciones de tratamiento conforme a lo establecido en el numeral 7.3 de este manual; y, adicionalmente, formular plan de mejoramiento por parte del líder del proceso en que se presentó el hecho; para realizar esta acción se debe contar con el apoyo del personal adscrito a la Oficina de Tecnologías y de la Información. Dicha mejora en los riesgos debe contar con los siguientes ítems: a) replantear el control; b) redefinir acciones de tratamiento; c) formular plan de mejoramiento; d) someterlo a visto bueno de la Jefatura de la Oficina de Tecnologías y de la Información, para los casos que involucren tecnología de la información; y, e) solicitar a la Oficina Asesora de Planeación

TIPO DE RIESGO	RESPONSABLE	ACTIVIDAD
		la actualización del Mapa de Riesgos, dentro de los tres (3) días hábiles siguientes a la fecha del haber ocurrido la materialización del riesgo.
	Dependencia o Proceso	a) Registrar, en el módulo correspondiente del *Software* para la Administración de la Planeación y la Gestión Institucional, el plan de mejoramiento. Dicho Plan debe contar con la aprobación del Asesor del Grupo de Control Interno de Gestión. b) Solicitar a la Oficina Asesora de Planeación la actualización del mapa de riesgos.
	Grupo de Control Interno de Gestión	Como resultado del seguimiento al Mapa de Riesgos, el Grupo de Control Interno de Gestión verificará que el líder del proceso o jefe de dependencia en que se presentó la materialización del riesgo formuló el correspondiente plan de mejoramiento para registrar en el Software para la Administración de la Planeación y la Gestión Institucional y, también, si solicitó a la Oficina Asesora de Planeación la actualización del mapa de riesgos correspondiente y realizó el cargue de las evidencias en la carpeta compartida correspondiente. En caso de que el Oficial de Seguridad de la Información no haya efectuado una Mesa de Seguridad, el Asesor del Grupo de Control Interno de Gestión solicitará al Oficial de Seguridad de la Información que programe y realice dicha Mesa; posteriormente con el propósito de garantizar la continuidad del servicio o el restablecimiento de este. En caso de que la dependencia o proceso donde se materializó el riesgo no haga un plan de mejoramiento, el Asesor del Grupo de Control Interno de Gestión debe solicitar, mediante correo electrónico, al líder del proceso y/o jefe de dependencia que se defina dicho plan y que cuente con los criterios mencionados.
Riesgos de gestión	Empleado público y/o contratista	Informar la materialización del riesgo mediante correo electrónico al respectivo líder de proceso por parte del empleado público o contratista de la Entidad al que se le ha asignado la responsabilidad del riesgo.
	Líder de Dependencia o Proceso	Para Sede Central: Informar la materialización del riesgo, vía correo electrónico, a la Oficina Asesora de Planeación y Grupo de Control Interno de Gestión. Para Grupos ARN de la Subdirección Territorial: Informar de lo sucedido, a través de correo electrónico del Grupo ARN de la Subdirección Territorial donde se materializó el riesgo, al jefe de la Oficina Asesora de Planeación y al Grupo de Control Interno de Gestión.

TIPO DE RIESGO	RESPONSABLE	ACTIVIDAD
	Grupo de Control Interno de Gestión	En caso de ser detectada la materialización del riesgo en proceso de auditoría interna o verificación de información para un informe se reportará, mediante correo electrónico, el evento hallado a la Oficina Asesora de Planeación.
	Dependencia o Proceso	Evaluar y mejorar o crear el(los) control(es), para mitigar, efectivamente, el(los) riesgo(s); determinar las correspondientes acciones de tratamiento conforme a lo establecido en los numerales 8.2 y 8.3 de este manual; y, adicionalmente, formular plan de mejoramiento por parte del líder del proceso en que se presentó el hecho; para realizar esta acción se debe contar con el apoyo del personal adscrito a la Oficina Asesora de Planeación y al Grupo de Control Interno de Gestión. Dicha mejora en los riesgos debe contar con los siguientes ítems: a) replantear el control; b) redefinir acciones de tratamiento; c) formular plan de mejoramiento; d) someterlo a visto bueno de la Jefatura del Grupo de Control Interno de Gestión; y, e) solicitar a la Oficina Asesora de Planeación la actualización del Mapa de Riesgos, dentro de los tres (3) días hábiles siguientes a la fecha del haber ocurrido la materialización del riesgo.
	Grupo de Control Interno de Gestión	Como resultado del seguimiento al Mapa de Riesgos, el Grupo de Control Interno de Gestión verificará que el líder del proceso o jefe de dependencia en que se presentó la materialización del riesgo formuló el correspondiente plan de mejoramiento para registrar en el Software para la Administración de la Planeación y la Gestión Institucional y, también, si solicitó a la Oficina Asesora de Planeación la actualización del mapa de riesgos correspondiente y realizó el cargue de las evidencias en la carpeta compartida correspondiente. En caso de que un empleado público o contratista encargado de manejar los riesgos de un proceso o dependencia no informe al líder de proceso o jefe de dependencia acerca de la materialización de un riesgo a su cargo, el Asesor del Grupo de Control Interno de Gestión debe informarle, vía correo electrónico, acerca de esta situación. En caso de que el líder del proceso o jefe de la Dependencia no lo haga, informar mediante correo electrónico a la Oficina Asesora de Planeación sobre la materialización del riesgo, con el fin de facilitar el dar inicio de a las acciones correspondientes para la revisión del mapa de riesgos.