POLÍTICA PARA
LA GESTIÓN
INTEGRAL DEL RIESGO

UNIDAD DE PLANEACIÓN
MINERO ENERGÉTICA
UPME

JUNIO 2020

TABLA DE CONTENIDO

POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO UPME

Dando cumplimiento a las disposiciones legales establecidas con ocasión al Modelo Integrado de Planeación y Gestión, en su dimensión 7 – Control Interno, de acuerdo con el Decreto 1499 de 2017, así como las demás establecidas a través de:

- ✓ Ley 87 de 1993. Normas para el ejercicio del control interno en las entidades
- ✓ Ley 1474 de 2011 Estatuto Anticorrupción
- ✓ Decreto 338 de 2019 – Creación red anticorrupción

La UPME presenta en este documento, los lineamientos a seguir para la gestión integral del riesgo en al entidad.

1. Declaración

La Alta Dirección de la UPME y todo el equipo humano de la entidad está comprometido para llevar a cabo una gestión integral de riesgos que contribuyan al cumplimiento de sus funciones y el logro de los objetivos estratégicos de manera responsable, ética y segura, que brinden confianza a sus grupos de valor y ciudadanía en general.

2. Objetivo

Establecer los lineamientos metodológicos para identificar, clasificar, valorar, establecer controles, responsables y formular los planes de tratamiento de los riesgos de gestión, corrupción y seguridad digital de la UPME, asociados a todos los procesos, planes, programas, o proyectos, que puedan afectar el cumplimiento de los objetivos estratégicos y misionales de la entidad.

3. Alcance

La Política para la Gestión Integral de Riesgos es extensible y aplicable a todos los procesos del Sistema de Gestión de la entidad, así como a todas las dependencias y niveles. Respecto a los riesgos de seguridad digital, estos deben gestionar de acuerdo con el Plan de Seguridad y Privacidad de la Información de la UPME.

Frente a los riesgos asociados a Seguridad y Salud en el Trabajo, como los asociados a los riesgos Ambientales, serán tratados de acuerdo con la normatividad vigente, liderados por la Secretaría General.

4. Términos y definiciones:

Activo de Seguridad de la Información: En el contexto de seguridad digital, son activos elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO.

Administración de Riesgo: Es el proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar un aseguramiento razonable con respecto al logro de los objetivos. Incluye el conjunto de elementos de control y sus interrelaciones, para que la UPME maneje los eventos, tanto internos como externos, que puedan afectar de manera positiva o negativa el logro de sus objetivos institucionales. La Administración del riesgo contribuye a generar la cultura de autocontrol y autoevaluación al interior de la Unidad.

Análisis de Riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

DAFP: Departamento Administrativo de la Función Pública.

Evaluación del Riesgo: Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Presencia o cambio de un conjunto particular de circunstancias.

Fuente de Riesgos: Elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo.

Gestión del Riesgo: Conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo.

Identificación del Riesgo: Proceso para encontrar, reconocer y describir el riesgo.

Infraestructura crítica cibernética: Es aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado.

Impacto: Resultado de un evento, que afecta los objetivos estratégicos de la entidad.

Mapa de calor de riesgo: consiste en una matriz con dos ejes, donde el eje "y" representa la probabilidad de frecuencia del **riesgo** y el eje "x" representa el impacto **que** puede tener el mismo.

Monitoreo: Verificación, supervisión, observación crítica o determinación continúa del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

Nivel o Zona del Riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en terminaos de la combinación de las consecuencias y su probabilidad.

Nivel de aceptación del riesgo: Decisión informada de tomar un riesgo particular (NTC GTC137, numeral 3.7.1.6). Para riesgo de corrupción es inaceptable.

Plan para la Gestión del Riesgo: Conjunto de acciones preventivas que se encuentran dentro del marco de referencia para gestionar los riesgos, en esta se definen componentes como los responsables, los recursos y las métodos que se van a utilizar para mitigar, eliminar o asumir los riesgos.

Primera línea de defensa: Se refiere a los líderes de los procesos, quienes tiene la responsabilidad de identificar los riesgos , realizar el proceso de valoración y evaluación de riesgos, mantenimiento y actualización de la matriz de riesgos.

Política de Operación: Aquella directriz general que reconoce el marco legal que rige y aplica a la UPME y la cual es desarrollada a través de la definición de los procesos, los procedimientos y las guías internas, que involucran las líneas de acción, los objetivos, actividades, tareas y controles que permiten el logro del objeto misional de la entidad y el cumplimiento de las responsabilidades con el estado.

Política de administración del riesgo: Declaración de la entidad e intenciones generales de la organización con respecto a la gestión del Riesgo[1].

Probabilidad: Oportunidad de que suceda algo.

Revisión: Acción que se emprende para determinar la idoneidad, conveniencia y eficacia de la materia en cuestión para lograr los objetivos establecidos.

Riesgo: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso.

[1] Nota: Tomado de NTC ISO 31000 Numeral 2.4. Algunos de estos fueron ajustados al contexto de la organización.

Riesgo Aceptable: Riesgo que ha sido reducido a un nivel que la organización puede tolerar con respecto a sus obligaciones legales.

Riesgo de Corrupción: Transparencia Internacional define la corrupción como el mal uso del poder encomendado para obtener beneficios privados. Entre tanto el riesgo obedece a la probabilidad de ocurrencia. Esta definición incluye tres elementos:

1. El mal uso del poder
2. Un poder encomendado, es decir, puede estar en el sector público o privado
3. Un beneficio privado, que no necesariamente se limita a beneficios personales para quien hace mal uso del poder, sino que puede incluir a miembros de su familia o amigos.

De manera similar, para Transparencia por Colombia la corrupción se define como el "abuso de posiciones de poder o de confianza, para beneficio particular en detrimento del interés colectivo, realizado a través de ofrecer o solicitar, entregar o recibir, bienes en dinero o en especie, en servicios o beneficios, a cambio de acciones, decisiones u omisiones".

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.

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 incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgo Inherente: Es aquel al que se enfrenta una entidad en ausencia en acciones de la dirección para modificar su probabilidad e impacto.

Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

Riesgo Residual: Riesgo remanente después del tratamiento del riesgo. Es el riesgo que permanece después de que la dirección haya realizado sus acciones para reducir el impacto y la probabilidad de un acontecimiento adverso, incluyendo las actividades de control en respuesta a un riesgo.

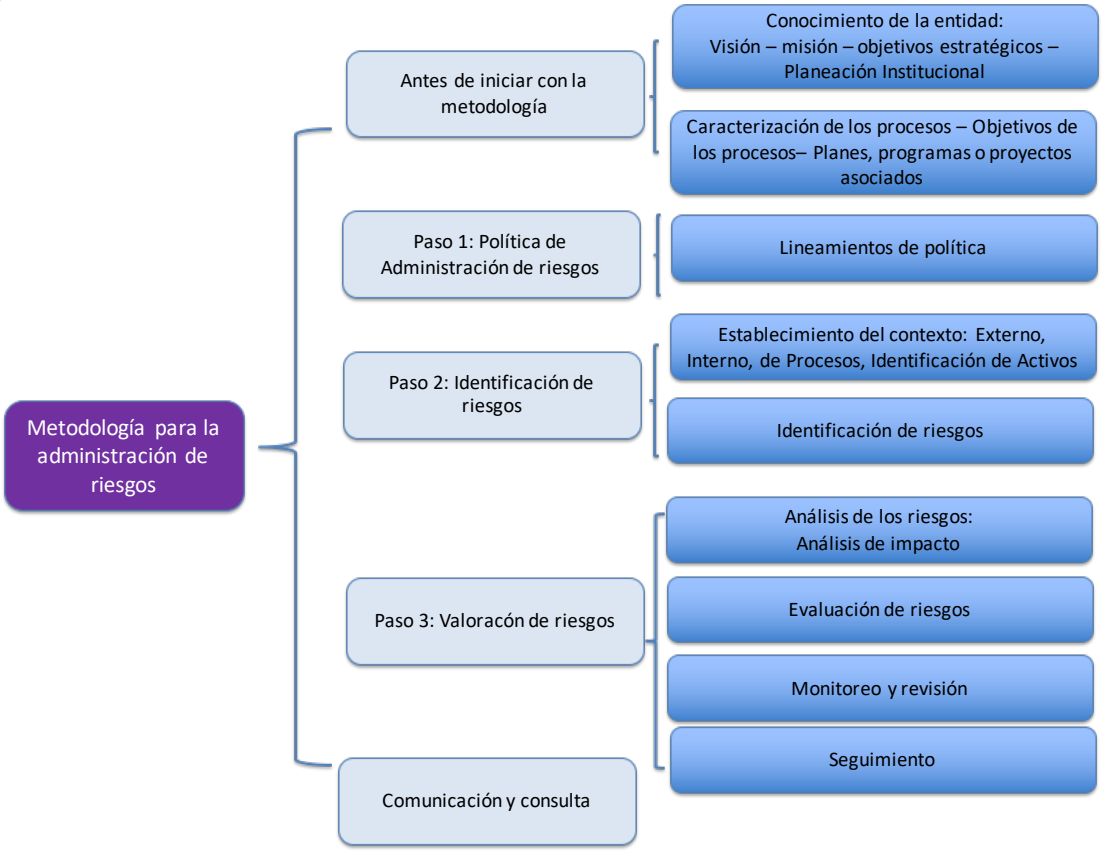
Riesgos de Seguridad Digital: Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

5. Lineamientos metodológicos

A continuación, se presentan los lineamientos metodológicos para la administración de los riesgos de la entidad. Estos lineamientos se basan en la **Guía para la administración del riesgo y el diseño de controles en entidades públicas V_4 Octubre de 2018 del DAFP.**

El desarrollo de la metodología para la administración de riesgos se representa gráficamente de la siguiente manera:



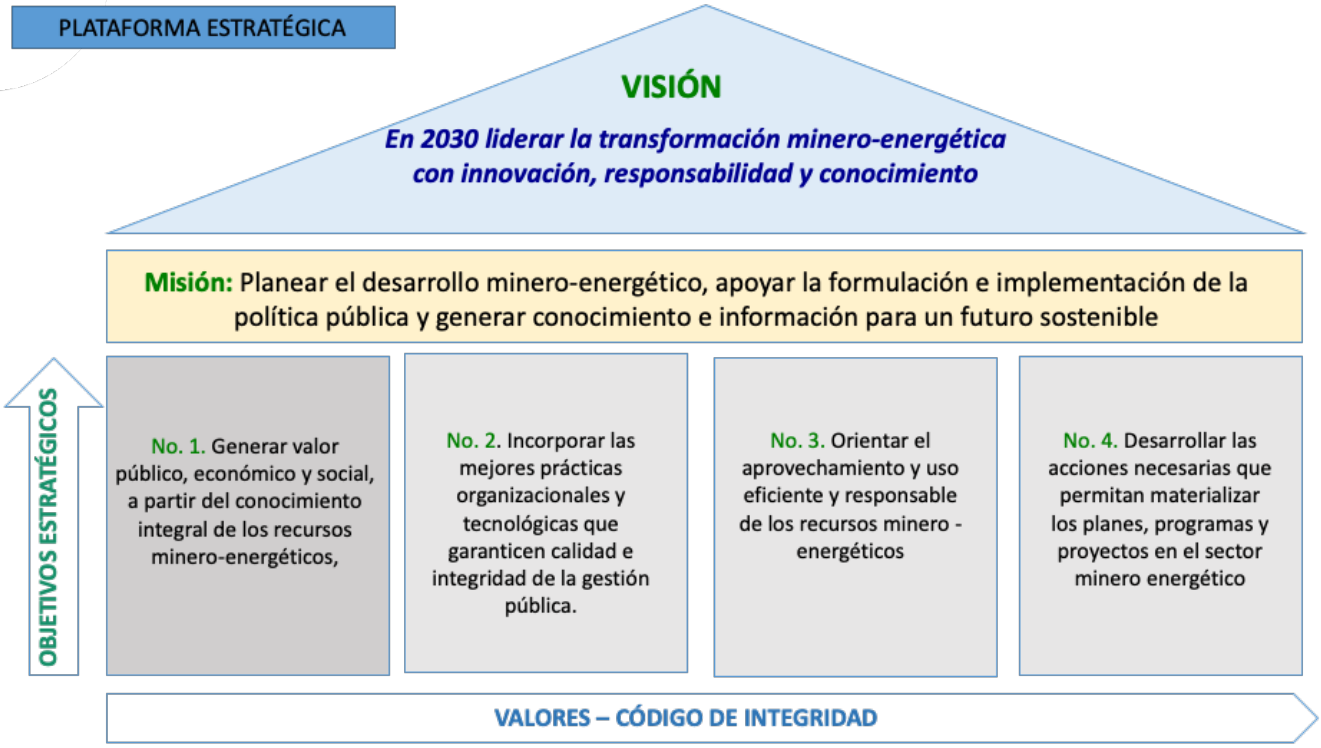
Como se muestra gráficamente, antes de iniciar con los pasos establecidos se debe tener un conocimiento del marco estratégico de la entidad, se deben conocer la misión, visión, objetivos estratégicos de la entidad y todo lo relacionado con la Planeación Institucional.

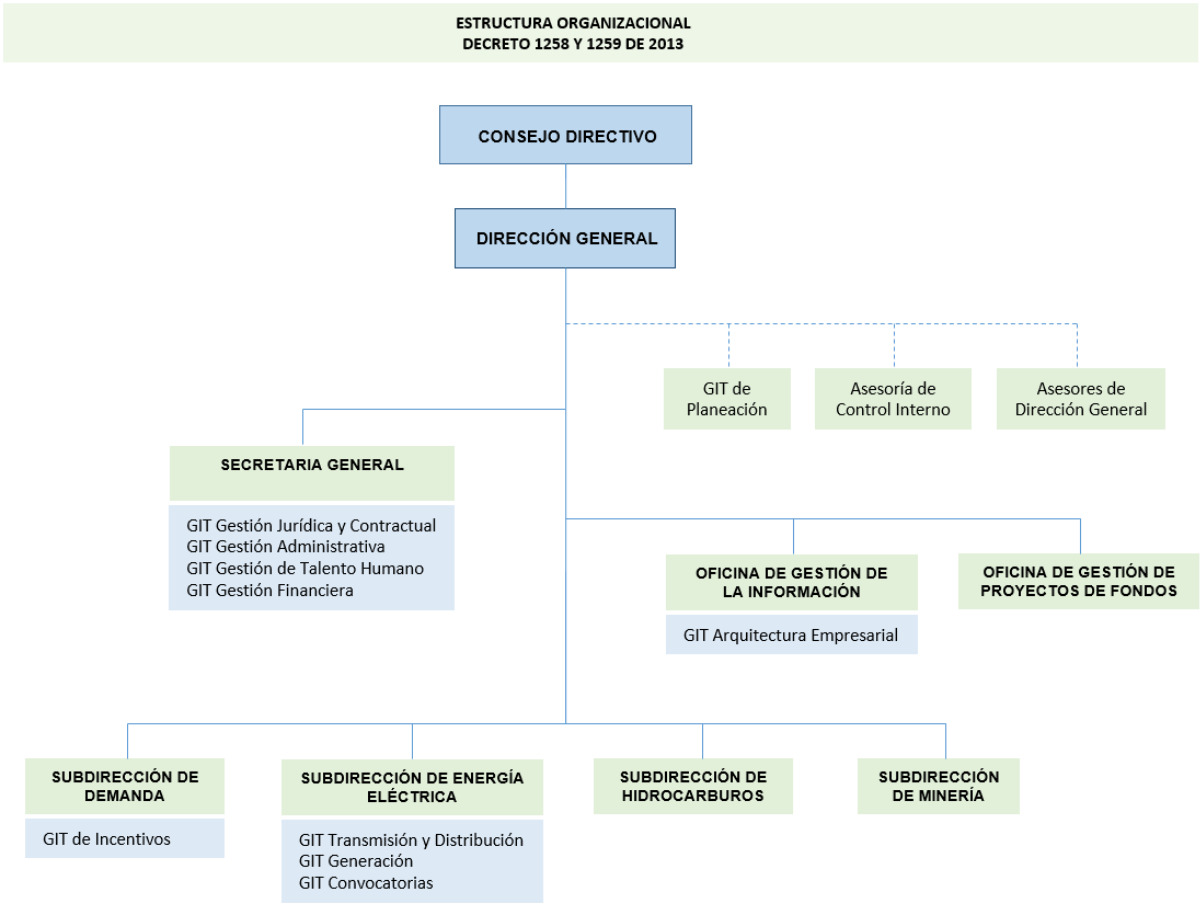
Es importante destacar que la Gestión Integral de Riesgos, la establece la Alta Dirección de la entidad, con el liderazgo del Representante Legal y la participación del Comité Institucional de Coordinación de Control Interno.

La presente política de administración se adopta en forma de guía y establece los lineamientos para la identificación, valoración y tratamiento de los riesgos de la entidad.

Conocimiento de la entidad:

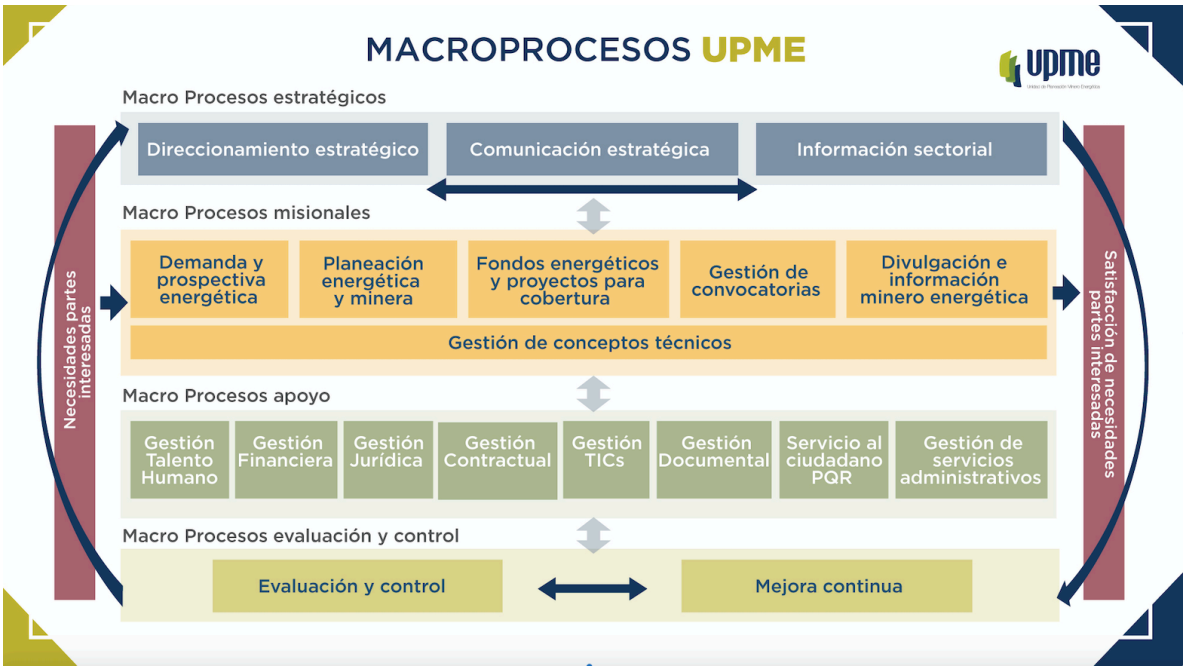
PLATAFORMA ESTRATÉGICA





La UPME cuenta con una planta organizacional de 126 distribuidos así: 8 se en el nivel directivo, 8 en el nivel asesor, 97 en el nivel profesional, 4 en el nivel técnico y 9 en el nivel asistencial. De esta manera, el 87,3% de los empleos de la planta de personal son de carrera administrativa (nivel profesional, técnico y asistencial), mientras que el 12,7% son de libre nombramiento y remoción (nivel directivo y asesor).

A continuación se muestra el mapa de procesos de la Unidad, sobre los cuales se desarrollará la Política de gestión integral de riesgos:



A continuación, se establecen los aspectos a desarrollar para la Gestión Integral de Riesgos:

5.1 Análisis de Contexto

Se debe hacer un análisis del contexto interno, externo de la entidad en general y de todos los macro procesos y procesos de la organización, identificando las Debilidades, Oportunidades, Fortalezas y Amenazas en el marco estratégico como el misional, involucrando los procedimientos, planes, programas, proyectos, que permita identificar los factores externos e internos que puedan generar riesgos de gestión, corrupción y seguridad digital, impactando de manera negativa la consecución de resultados, la calidad u oportunidad de entrega de los productos y servicios de la entidad.

5.1.1 Establecimiento del contexto externo:

De acuerdo con la guía del DAFP, para realizar un análisis de contexto externo se determina características o aspectos esenciales del entorno en el cual opera la entidad. Se consideran factores tales como:

- Políticos Sociales y Culturales
- Legales y reglamentarios
- Tecnológicos

- Financieros
- Económicos

5.1.2 Establecimiento contexto interno:

Para el análisis del contexto interno, se determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos. Se pueden considerar factores como:

- Estructura Organizacional
- Funciones y Responsabilidades
- Políticas, Objetivos y Estrategias implementadas
- Recursos y Conocimientos con que se cuenta (personas, procesos, sistemas, tecnología)
- Relaciones con las partes involucradas
- Cultura Organizacional

5.1.3 Establecimiento contexto del proceso:

Se debe establecer el contexto del proceso, determinando las características o aspectos esenciales del macroproceso y sus interrelaciones. Se consideran factores tales como:

- Objetivo del macroproceso
- Alcance del macroproceso
- Interrelación con otros macroprocesos
- Procedimientos asociados
- Responsables de los macroprocesos

5.1.4 Identificación de activos de seguridad de la información:

La primera línea de defensa, en este caso los subdirectores, Jefes de Oficina, y Secretario General, así como los coordinadores de los Grupos Internos de Trabajo – GIT, deben identificar los activos en cada proceso, de e esta manera se puede determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, unos archivos, servidores web o aplicaciones claves para que la entidad pueda prestar sus servicios). Así la entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando su confianza en el uso del entorno digital.

Para ello se debe:

1. Listar los activos por cada proceso.
2. Identificar los dueños de los activos
3. Clasificar los activos
4. Clasificar la información
5. Determinar la criticidad del activo
6. Identificar si tiene infraestructura crítica cibernética

Para realizar un correcto proceso de identificación de activos, se recomienda consultar los *Lineamientos para la gestión del riesgo de seguridad digital entidades públicas,* desarrollado por el Ministerio de Tecnologías de la Información y las Comunicaciones, el cual se encuentra en el siguiente link:

https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316352?_com_liferay_document_library_web_portlet_DLPortlet_INSTANCE_bGsp2IjUBdeu_redirect=https%3A%2F%2Fwww.funcionpublica.gov.co%2Fweb%2Feva%2Fbiblioteca-virtual%2F-%2Fdocument_library%2FbGsp2IjUBdeu%2Fview%2F34316316

En la actualidad, la Unidad cuenta con un Plan de Tratamiento de Riesgos de Seguridad de la Información, en el cual se precisan todos los aspectos a tener en cuenta para la gestión de los riesgos asociados a Seguridad Digital, el cual puede ser consultado en:

https://www1.upme.gov.co/Planes/Plan_Tratamiento_Riesgos_Seguridad_Info_2020.pdf

5.2 Identificación del Riesgo

El líder del proceso, junto al equipo de trabajo apoyado en el análisis de contexto, debe identificar los riesgos asociados a los macroprocesos, en los que además deben estar los de corrupción y de seguridad digital y que puedan afectar el cumplimiento de los objetivos estratégicos y misionales de la entidad, determinando las causas que lo originan.

Una vez levantadas las causas e identificado el riesgo que puede afectar el cumplimiento de los objetivos, se debe hacer una descripción del riesgo en el que se haga referencia a las características o las formas en que se observa o manifiesta.

Preguntas clave para la identificación del riesgo:

¿QUÉ PUEDE SUCEDER?
¿CÓMO PUEDE SUCEDER?
¿CUÁNDO PUEDE SUCEDER?
¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN?

Existen algunas técnicas para la identificación del riesgo y redacción, que la Función Pública sugiere a través de la guía mencionada al inicio de este capítulo, y que la UPME adopta; estas son:

- ✓ El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.
- ✓ Evitar iniciar con palabras negativas o con palabras que denoten un factor de riesgos: “ausencia de”, deficiente, debilidades en , entre otros.
- ✓ Generar en lector o escucha la imagen del evento como si ya estuviera sucediendo.
- ✓ Preguntarse si el riesgo de gestión identificado está relacionado directamente con las características del objetivo del proceso, si la respuesta es no, esta puede ser la causa o consecuencia y no el riesgo.
- ✓ Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la **matriz de definición de riesgo de corrupción**, que incorpora cada uno de los componentes de su definición.

5.2.1 Riesgos de Corrupción:

De acuerdo con la siguiente matriz, si para cada riesgo descrito, se marca con una X cada casilla, quiere decir que se trata de un riesgo de corrupción:

MATRIZ : DEFINICIÓN RIESGO DE CORRUPCIÓN				
DESCRIPCIÓN DEL RIESGO	ACCIÓN U OMISIÓN	USO DEL PODER	DESVIAR LA GESTIÓN DE LO PÚBLICO	BENEFICIO PRIVADO

Fuente: Secretaría de Transparencia de la Presidencia de la República

- ✓ Los riesgos de corrupción se establecen sobre los procesos
- ✓ Se debe elaborar el mapa de riesgos de corrupción anualmente. Estos riesgos los identifica cada responsable de los procesos y su equipo de trabajo.
- ✓ La consolidación del mapa de riesgos está a cargo del GIT Planeación.
- ✓ Se debe socializar de manera interna y externa el mapa de riesgos consolidado, para conocer sus apreciaciones, mejoras, propuestas, para realizar los ajustes a los que haya lugar. Es importante dejar evidencias de este proceso de socialización.

- ✓ El mapa de riesgos se debe publicar antes del 31 de enero de cada año, en la sección de Transparencia y Acceso a la Información Pública de la página de la entidad.
- ✓ Monitoreo: en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.
- ✓ Seguimiento: el jefe de control interno o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

5.3 Tipo de riesgos:

Una vez identificados los riesgos, se determinan a que clase de riesgos pertenecen de acuerdo con la siguiente tipología:

a. **Riesgos de Gestión,** los cuales tendrán la siguiente clasificación:
- Riesgo Estratégico
- Riesgo Operativo
- Riesgo Financiero
- Riesgo de Cumplimiento

b. **Riesgos de Corrupción**

c. **Riesgos de Seguridad Digital** (Seguridad y Privacidad de la Información)

La definición de cada uno de estos riesgos se encuentra en el numeral 4 de este documento. Para mayor ilustración y orientación para identificar los riesgos se puede consultar la guía de la función pública versión 4 octubre de 2018, disponible en el siguiente link: https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499

Como propuesta metodológica, se utilizará la siguiente matriz para plasmar los puntos 5.2 y 5.3, como apoyo para el desarrollo de los siguientes numerales.

Para riesgos de Gestión y de Corrupción:

IDENTIFICACIÓN DEL RIESGO

RIESGO IDENTIFICADO	DESCRIPCIÓN DEL RIESGO	TIPO DE RIESGO	CAUSAS QUE LO ORIGINAN	CONSECUENCIAS

Para riesgos de Seguridad Digital:

Como se indicó anteriormente, los riesgos de Seguridad Digital se gestionarán de acuerdo al Plan de Tratamiento de Riesgos de Seguridad de la Información 2020, el cual se encuentra en el siguiente link:

https://www1.upme.gov.co/Planes/Plan_Tratamiento_Riesgos_Seguridad_Info_2020.pdf

5.4 Valoración del riesgo

Para valorar los riesgos identificados, se debe establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riegos inicial, **llamado Riesgo Inherente,** posteriormente implementar controles y evaluar nuevamente los riesgos una vez establecidos dichos controles, y así determinar el riesgo final, **llamado Riesgo Residual.**

5.4.1 Valoración del Riesgo Inherente:

5.4.1.1 Análisis de Causas:

Para el análisis de las causas que originan los riesgos, existen diferentes metodologías, sin embargo, para unificar criterios en la entidad, se establece que la técnica a utilizar sea la de los ***5 Por Qué***.

Esta técnica consiste en identificar la causa raíz de un problema, para este caso se debe analizar las causas que generan el riesgo identificado, repitiendo la pregunta "¿**Por** qué?" para cada respuesta; se sugiere realizar este ejercicio de manera sistemática, teniendo en cuenta la siguiente estructura:

ESTRUCTURA DE LA TÉCNICA DE LOS 5 POR QUÉ?

POR QUÉ	RESPUESTA 1.
POR QUÉ DE LA RESPUESTA 1.	RESPUESTA 2.
POR QUÉ DE LA RESPUESTA 2.	RESPUESTA 3.
POR QUÉ DE LA RESPUESTA 3.	RESPUESTA 4.
POR QUÉ DE LA RESPUESTA 4.	RESPUESTA 5.

5.4.1.2 Determinación de la probabilidad:

Otra variable necesaria para valorar el riesgo, es la probabilidad de que se materialice el riesgo identificado, el cual se expresa en términos de frecuencia.

Lo anterior significa que la probabilidad se determina según el número de eventos que se hayan presentado, durante un periodo establecido, de acuerdo con la siguiente tabla:

CRITERIOS PARA CALIFICAR LA PROBABILIDAD

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años
1	Rara Vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años

Fuente: Departamento Administrativo de la Función Pública - DAFP

5.4.1.3 Determinación de impacto o consecuencias:

Por impacto se entienden las consecuencias que se pueden generar a la entidad, en caso de llegar a la materialización de los riesgos. Para ello se deben tener en cuenta los criterios establecidos en la guía de la Función Pública:

CRITERIOS PARA EVALUAR EL IMPACTO EN LOS RIESGOS DE GESTIÓN

NIVEL	IMPACTO	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
5	Catastrófico	- Impacto que afecte la ejecución presupuestal en un valor ≥50%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
4	Mayor	-Impacto que afecte la ejecución presupuestal en un valor ≥20%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
3	Moderado	- Impacto que afecte la ejecución presupuestal en un valor ≥5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden na- cional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
2	Menor	- Impacto que afecte la ejecución presupuestal en un valor ≥1%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el pre- supuesto total de la entidad en un valor ≥1%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por algunas horas. - Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
1	Insignificante	- Impacto que afecte la ejecución presupuestal en un valor ≥0,5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad.	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

Fuente: Guía del DAFP - Adaptado de Instituto de Auditores Internos. COSO ERM. Agosto 2004.

CRITERIOS PARA CALIFICAR EL IMPACTO EN LOS RIESGOS DE CORRUPCIÓN

No. PREGUNTA: SI EL RIESGO DE CORRUPCION SE MATERIALIZA PODRIA...	RESPUESTA	
	SI	NO
1 ¿Afectar al grupo de funcionarios del proceso?		
2 ¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3 ¿Afectar el cumplimiento de misión de la entidad?		
4 ¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5 ¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6 ¿Generar pérdida de recursos económicos?		
7 ¿Afectar la generación de los productos o la prestación de servicios?		
8. ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9 ¿Generar pérdida de información de la entidad?		
10 ¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11 ¿Dar lugar a procesos sancionatorios?		
12 ¿Dar lugar a procesos disciplinarios?		
13 ¿Dar lugar a procesos fiscales?		
14 ¿Dar lugar a procesos penales?		
15 ¿Generar pérdida de credibilidad		
16 ¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17 ¿Afectar la imagen regional?		
18 ¿Afectar la imagen nacional?		
19 ¿Generar daño ambiental?		
TOTAL		
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico		
MODERADO: Genera medianas consecuencias sobre la entidad. MAYOR: Genera altas consecuencias sobre la entidad. CATASTRÓFICO: Genera consecuencias desastrosas para la entidad.		

Fuente: Secretaría de Transparencia de la Presidencia de la República.

Nota importante: Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico. Por cada riesgo de corrupción identificado, se debe diligenciar una tabla de estas.

5.4.1.4 Análisis de impacto

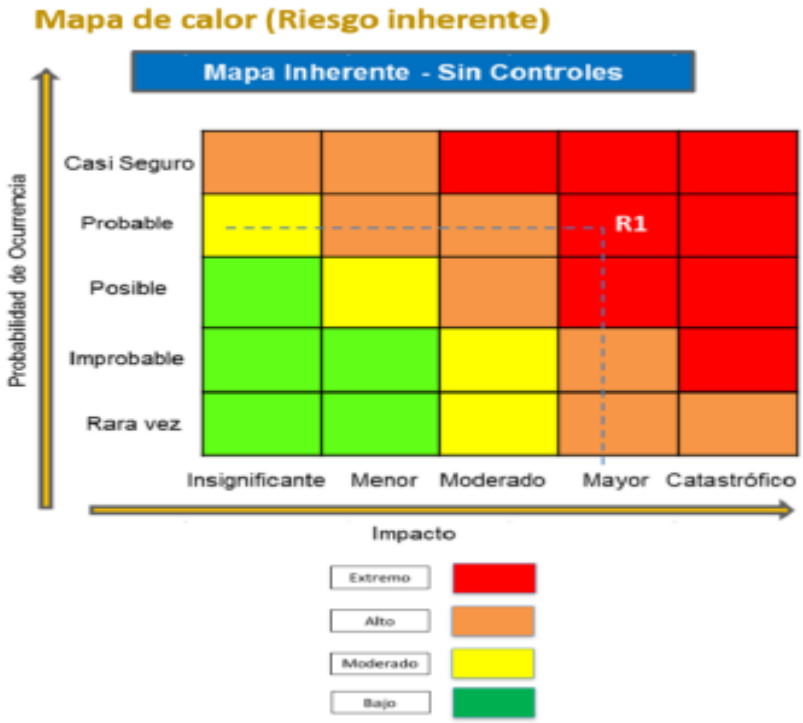
El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo; para ello se debe construir el mapa de calor.

Mapa de calor de riesgos:

Con el fin de visualizar los riesgos en un espacio bidimensional, y poder tomar decisiones de gestión de acuerdo a su ubicación, se debe construir el mapa de calor de riesgos de la siguiente manera:

Se toma la calificación de probabilidad resultante de la tabla del numeral 5.4.1.2 *Criterios para calificar la probabilidad*, y la calificación de impacto, de acuerdo con la tabla del numeral 5.4.1.3 *Criterios para evaluar el impacto en los riesgos de gestión,* utilizando el plano cartesiano, ubica la calificación de probabilidad en el eje Y, y la calificación de impacto en el eje X, se establece la intersección de las dos calificaciones, y ese punto de cruce corresponde al nivel del riesgo, el cual se identificará como (R1), y se repite esta acción para todos los riesgos inherentes.

El mapa de calor tendrá unos colores que determinan la zona de riesgo, que permiten determinar los riesgos que requieren implementación de controles.



Según ubicación del riesgo Inherente en el mapa de calor:

- Zona de riesgo baja: no requiere implementar controles
- Zona de riesgo moderada: proponer e implementar controles
- Zona de riesgo alta: proponer e implementar controles
- Zona de riesgo extrema: proponer e implementar controles

Dependiendo de la zona de riesgo en donde se haya ubicado el riesgo inherente, se formulan los controles, solo en caso de estar en zona de riesgo baja, no se formularán controles, pero si se debe garantizar que en caso de que los procedimientos asociados a dicho proceso sufren alguna modificación, se debe volver a evaluar a identificar los riesgos, valorarlos y corroborar que el riesgo se mantiene controlado.

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

Como se ha mencionado en capítulos anteriores, los riesgos de seguridad Digital se valoran de acuerdo al Plan de Tratamiento de Riesgos de Seguridad de la Información 2020, el cual se encuentra en el link:

https://www1.upme.gov.co/Planes/Plan_Tratamiento_Riesgos_Seguridad_Info_2020.pdf

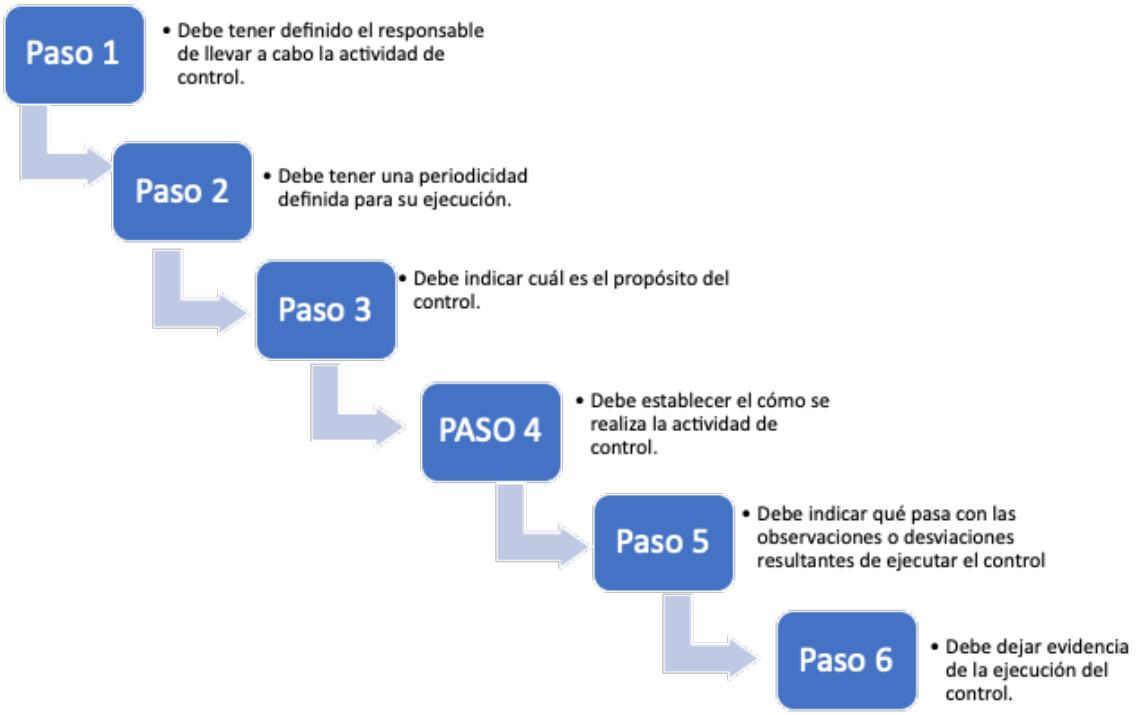
5.4.2 Diseño de controles – Valoración de controles

5.4.2.1 Diseño de controles:

Una vez se tienen los riesgos inherentes susceptibles de implementar controles, de acuerdo a lo definido en el numeral 5.4.1.4, se relacionan las causas identificadas en el análisis de causas expuesto en el numeral 5.4.1.1 y se identifica el control para cada una de las causas.

Las actividades de control las diseña la primera línea de defensa, es importante asegurar que los controles estén bien diseñados, es decir, que efectivamente estos mitiguen las causas que hacen que el riesgo se materialice. Para este caso se debe hacer un análisis riguroso acerca del control que se está proponiendo y si efectivamente está atacando las causas que generan el riesgo identificado.

Pasos para diseñar un control



Las actividades de control se diseñan buscando:

- ✓ Disminuir la probabilidad: acciones encaminadas a gestionar las causas del riesgo.
- ✓ Disminuir el impacto: acciones encaminadas a disminuir las consecuencias del riesgo.

Es importante tener en cuenta:

- ✓ Al definir responsables de los controles, no se relacionan nombres de funcionarios, se deben asignar a un cargo específico.
- ✓ El control debe tener una periodicidad especifica para su realización (diario, mensual, trimestral, anual, etc.) y su ejecución debe ser consistente y oportuna para la mitigación del riesgo. Por lo que en la periodicidad se debe evaluar si este previene o se detecta de manera oportuna el riesgo. El responsable del control, debe establecer la periodicidad de su ejecución.
- ✓ El control debe tener un propósito que indique para qué se realiza, y que ese propósito conlleve a prevenir las causas que generan el riesgo

(verificar, validar, conciliar, comparar, revisar, cotejar) o detectar la materialización del riesgo, con el objetivo de llevar acabo los ajustes y correctivos en el diseño del control o en su ejecución. El solo hecho de establecer un procedimiento o contar con una política por sí sola, no va a prevenir o detectar la materialización del riesgo o una de sus causas. Siguiendo las variables a considerar en la evaluación del diseño de control revisadas, veamos algunos ejemplos de cómo se deben redactar los controles, incluyendo el propósito del control, es decir, lo que este busca.

- ✓ El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control, es confiable para la mitigación del riesgo.

- ✓ El control debe indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control. Al momento de evaluar si un control está bien diseñado para mitigar el riesgo, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones.

- ✓ El control debe dejar evidencia de su ejecución. Esta evidencia ayuda a que se pueda revisar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control y se pueda evaluar que el control realmente fue ejecutado de acuerdo con los pasos establecidos para su diseño.

Si se requiere ampliar información sobre el correcto diseño de los controles, se recomienda consultar la **Guía para la administración del riesgo y el diseño de controles en entidades públicas V_4 Octubre de 2018 del DAFP.**

5.4.2.2 Valoración de controles:

El Grupo Interno de Trabajo de Planeación, debe analizar y evaluar los controles para la mitigación del riesgo propuestos por la primera línea de defensa, de acuerdo con las siguientes variables:

Análisis y evaluación de los controles

CRITERIO DE EVALUACIÓN	ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA / CALIFICACIÓN			
1. Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	15	No Asignado	0
	¿El responsable tiene la autoridad y adecua- da segregación de funciones en la ejecución del control?	Adecuado	15	Inadecuado	0
2. Periodicidad	La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	15	Inoportuna	0
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	Prevenir ó detectar	15 ó 10	No es un control	0
4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	15	No Confiable	0
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	15	No se investigan, ni resuelven oportunamente	0
6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa	15	Incompleta ó no existe	5 ó 0
				TOTAL	

RANGO DE CALIFICACIÓN	RESULTADO - PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 96%, se debe establecer un plan de acción que permita tener un control o controles bien diseñados.

5.4.3 Valoración del riesgo Residual:

Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, nuevamente se hace valoración de riesgos y se elabora el mapa de calor de riesgo residual (después de implementar el control).

Una vez se tenga el nuevo mapa de calor de riesgo residual, las decisiones de tratamiento de riesgos se tomarán de acuerdo con la zona donde hayan quedado después de la implementación de los controles:

Zona de riesgo baja: asumir el riesgo
Zona de riesgo moderada: asumir el riesgo, reducir el riesgo
Zona de riesgo alta: reducir el riesgo, evitar, compartir o transferir
Zona de riesgo extrema: reducir el riesgo, evitar, compartir o transferir

5.5 Tratamiento de los riesgos:

El tratamiento de los riesgos se enmarca dentro de las siguientes categorías:

Teniendo en cuenta el mapa de calor de riesgo residual, se definen niveles de aceptación, y se determinan las medidas que se debe adoptar según la zona de riesgo en la que se ubique y las categorías anteriormente mencionadas, de acuerdo a la siguiente tabla:

Niveles de Aceptación del Riesgo		
Tipo de riesgo	**Zona de riesgo**	**Nivel de aceptación**
	Baja	Se acepta el riesgo, es decir se asume. Sin embargo se debe hacer monitoreo

Gestión (Incluye los riesgos tipicados en numeral 5.3)		anualmente
	Moderada	Se establecen controles que permitan reducir el riesgo. Se realiza seguimiento a los controles trimestralmente.
	Alto y Extremo	Se establecen nuevos controles o fortalecen los existentes que permitan reducir el riesgo. Se debe analizar si es posible compartirlo o evitarlo. Se hace seguimiento a los controles mensualmente.
Corrupción	Moderada	Son inaceptables. Se establecen controles que permitan reducir el riesgo. Se realiza seguimiento a los controles trimestralmente.
	Alto y Extremo	Son inaceptables, se establecen nuevos controles o fortalecen los controles que reduzcan el riesgo. Se debe analizar si es posible compartirlo o evitarlo Se hace seguimiento a los controles mensualmente.
Seguridad digital	Baja	Se acepta el riesgo, es decir se asume. Se realiza seguimiento a los controles anualmente.
	Moderada	Se establecen controles que permitan reducir el riesgo. Se realiza seguimiento a los controles trimestralmente.
	Alto, extremo	Se establecen nuevos controles o fortalecen los existentes que permitan reducir el riesgo. Se debe analizar si es posible compartirlo o evitarlo. Se hace seguimiento a los controles mensualmente.

Para mitigar/tratar los riesgos de seguridad digital se deben emplear como mínimo los controles del anexo A de la ISO/IEC 27001:2013, estos también se encuentran en el anexo 4. “Lineamientos para la gestión del riesgo de seguridad digital de la Función Pública”.

5.6. Monitoreo, Revisión y Seguimiento

Teniendo en cuenta que la entidad debe asegurar el logro de sus objetivos anticipándose a los eventos negativos relacionados con la gestión de la entidad. El modelo integrado de

plantación y gestión (MIPG) en la dimensión 7 “Control interno”, que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles con las líneas de defensa, define las actividades de monitoreo y revisión que se deben llevar a cabo por la Línea Estratégica y cada una de las Líneas de Defensa:

LINEA ESTRATÉGICA Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la alta dirección y el comité institucional de coordinación de control interno.
La alta dirección y el equipo directivo, a través de sus comités deben monitorear y revisar el cumplimiento a los objetivos a través de una adecuada gestión de riesgos con relación a lo siguiente: ■ Revisar los cambios en el “Direccionamiento estratégico” y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados. ■ Revisión del adecuado desdoblamiento de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos. ■ HacerseguimientoenelComitéInstitucionalydeControlInterno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna. ■ Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. ■ Hacer seguimiento y pronunciarse por lo menos cada trimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo a las políticas de tolerancia establecidas y aprobadas. ■ Revisar los informes presentados por lo menos cada trimestre de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos. ■ Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.

1ª LÍNEA DE DEFENSA
Desarrolla e implementa procesos de control y gestión de riesgos a través de su identifica- ción, análisis, valoración, monitoreo y acciones de mejora. Está conformada por los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad.
Los gerentes públicos y los líderes de proceso deben monitorear y re visar el cumplimiento de los objetivos institucionales y de sus procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente: ■ Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso. ■ Revisión como parte de sus procedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos. ■ Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos. ■ Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. ■ Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos. ■ Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos. ■ Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.

2ª LÍNEA DE DEFENSA
Soporta y guía la línea estrategia y la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y sus procesos, incluyendo los riesgos de corrupción a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y lleva a cabo un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos. Está conformada por los responsables de monitoreo y evaluación de controles y gestión del riesgo (jefes de planeación, supervisores e interventores de contratos o proyectos, responsables de sistemas de gestión, etc.).
Los gerentes públicos y los líderes de proceso deben monitorear y revisar el cumplimiento de los objetivos institucionales y de sus procesos a través de una adecuada gestión de riesgos, además de incluir los riesgos de corrupción con relación a lo siguiente: ■ Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos. ■ Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar. ■ Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de los mismos. ■ Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad. ■ Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos. ■ Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.

3ª LÍNEA DE DEFENSA
Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. La tercera línea de defensa está conformada por la oficina de control interno o auditoría Interna.
La oficina de control interno o auditoría interna monitorea y revisa de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, a través de la adecuada gestión de riesgos, además de incluir los riesgos de corrupción con relación a lo siguiente: ■ Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables. ■ Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar. ■ Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción. ■ Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos. ■ Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas. ■ para mitigar los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.

Reporte de la gestión del riesgo

La primera línea de defensa reporta a la segunda línea de defensa el estado de avance del tratamiento del riesgo en la operación, y la consolidación de los riesgos en todos los niveles será reportada por la segunda línea de defensa (encargado de la gestión del riesgo) hacia la alta dirección. Este reporte se hará trimestralmente en comité de Coordinación de Control Interno.

5.6.1 Monitoreo y Seguimiento de riesgos de corrupción

Los gerentes públicos y los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa). Le corresponde, igualmente, a la oficina de planeación adelantar el monitoreo (segunda línea de defensa). Dicho monitoreo se hará de acuerdo con la periodicidad definida en el tratamiento de los riesgos.

El Seguimiento de riesgos de corrupción, está a cargo del Asesor de Control Interno, y las fechas establecidas corresponden a:como se indica a continuación:

- **Primer seguimiento:** Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.

- **Segundo seguimiento:** Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- **Tercer seguimiento:** Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

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

En especial deberá adelantar las siguientes actividades:

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

Acciones a seguir en caso de materialización de riesgos de corrupción

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

1) Informar a las autoridades de la ocurrencia del hecho de corrupción.

2) Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.

3) Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.

4) Llevar a cabo un monitoreo permanente.

La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva. Las acciones adelantadas se refieren a:

- Determinar la efectividad de los controles.
- Mejorar la valoración de los riesgos.
- Mejorar los controles.
- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo.

5.7. Comunicación y consulta

Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo. De igual manera se debe garantizar la comunicación y consulta de los usuarios o ciudadanos, de modo tal que los riesgos identificados permitarn encontrar puntos críticos para la mejora en la prestación de los servicios.

5.7.1 Información, Comunicación y Reporte

Responsabilidades por línea de defensa para la Información, comunicación y reporte.

Línea estratégica:

Corresponde al Comité de coordinación de control interno establecer la Política de Gestión de Riesgos y asegurarse de su permeabilización en todos los niveles de la organización pública, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo.

Primera línea de defensa:

Corresponde a los jefes de área y/o grupo (primera línea de defensa) asegurarse de implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades.

Segunda línea de defensa:

Corresponde al área encargada de la gestión del riesgo (segunda línea de defensa) la difusión y asesoría de la presente metodología, así como de los planes de tratamiento de riesgo identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación.

Tercera línea de defensa

Le corresponde a las unidades de control interno, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la entidad, catalogándola como una unidad auditable más dentro de su universo de auditoría y, por lo tanto, debe dar a conocer a toda la entidad el Plan Anual de Auditorias basado en riesgos y los resultados de la evaluación de la gestión del riesgo.

Todos los formatos que se deriven de los lineamientos metodológicos aquí establecidos, así como procedimientos que se consideren necesarios, se deben

documentar e integrar en el sistema de gestión de calidad, antes de iniciar su desarrollo y socialización con los funcionarios de la entidad.

CONTROL DE CAMBIOS

Fecha	Versión	Motivo de cambio
19 de junio de 2020	1	Creación del documento e inclusión en el Sistema de Gestión de Calidad

Elaboró	Revisó	Aprobó
Yudy Andrea Linares Asesora Planeación	Comité Coordinación Control Interno	Comité de Coordinación de Control Interno 19 de junio 2020