TABLA DE CONTENIDO

Contenido

1. OBJETIVO GENERAL 5
2. ALCANCE 5
3. ASPECTOS POSITIVOS DE LA GESTIÓN DE RIESGOS 5
4. CONCEPTOS BÁSICOS 6
4.1. Conceptos Transversales 6
4.2. Conceptos sobre riesgos de corrupción 8
4.3. Conceptos sobre riesgos de soborno 8
4.4. Conceptos sobre riesgos de Seguridad de la Información 9
4.5. Conceptos sobre del Sistema de Gestión Ambiental 10
4.6. Conceptos sobre riesgos del Sistema de Gestión de Seguridad y Salud en el Trabajo 11
5. ADMINISTRACIÓN DEL RIESGO 11
6. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO 12
7. CONTENIDO DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO DEL MINISTERIO DE EDUCACIÓN NACIONAL 13
7.1. Objetivo General 13
7.2. Objetivos Específicos 13
7.3. Alcance 13
7.4. Directrices de la Política 13
7.5. Niveles de aceptación del riesgo 14
7.6. Niveles de calificación del impacto 14
7.7. Tratamiento del riesgo 14
7.8. Periodicidad para el seguimiento de acuerdo con el riesgo residual 14
8. ROLES Y RESPONSABILIDADES 14
8.1. Línea Estratégica 15
8.2. Primera línea de defensa 16

8.3. Segunda línea de defensa 17
8.4. Tercera línea de defensa 18
9. LINEAMIENTOS PARA LA ADMINISTRACIÓN DE RIESGOS 19
9.1. Lineamientos operativos para mapas de riesgos institucionales, corrupción, soborno, fraude y seguridad de la información 22
10. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO 24
10.1. Definición del contexto estratégico 24
10.2. Identificación del Riesgo de Gestión 25
10.3. Valoración de riesgos a nivel transversal 31
11. LINEAMIENTOS SOBRE RIESGOS DE CORRUPCIÓN 44
11.1. Directrices de redacción para riesgos de corrupción 46
11.2. Identificación Riesgos de Soborno 47
11.3. Riesgos de Corrupción y Soborno relacionados con los trámites 47
11.4. Valoración de riesgos de corrupción y/o Soborno 53
12. MONITOREO (SDO) Y SEGUIMIENTO (OCI) 58
13. ACTUALIZACIÓN DEL MAPA DE RIESGOS 58
14. COMUNICACIÓN Y CONSULTA 59
15. GESTIÓN DEL RIESGO AMBIENTAL 59
15.1. Identificación de riesgos en el Sistema de Gestión Ambiental 59
15.2. Identificación de riesgos para el ambiente 60
15.3. Identificación de riesgos para la entidad debido a temas relacionados con el ambiente 61
15.4. Análisis de riesgos ambientales 62
15.5. Tratamiento del riesgo ambientales 62
16. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 63
16.1. Identificación de Riesgos de Seguridad de la Información 63
16.2. Identificación de activos de seguridad de la información 63
16.3. Identificación del riesgo de seguridad de la información 64
16.4. Controles asociados a la seguridad de la información 67

16.5. Tratamiento para los Riesgos de Seguridad de la Información 69
17. RIESGOS DE SEGURIDAD Y SALUD EN EL TRABAJO - SGSST 69
17.1. Identificación de peligros, SGSST. 69

INTRODUCCIÓN

En cumplimiento de lo establecido en el artículo 2.2.21.1.6 del Decreto 648 de 2017 en lo que respecta a la aprobación de la política de administración del riesgo y el "artículo 2.2.21.5.4 Administración de riesgos" del Decreto 1083 de 2015, y siguiendo las directrices de: la norma ISO 37001:2016, la guía para la administración del riesgo y diseño de controles en entidades públicas versión 5 del Departamento Administrativo de la Función Pública y el Decreto 1499 de 2017, que establece el Modelo Integrado de Planeación y Gestión (MIPG), el Ministerio de Educación Nacional adopta la presente guía para la administración del riesgo, la cual aplica de manera transversal a las 7 dimensiones y las 19 políticas de MIPG.

Esta metodología fortalece el Sistema Integrado de Gestión (SIG) con la administración y prevención de la ocurrencia de riesgos que puedan generar efectos negativos al interior de la entidad y al mismo tiempo permite potenciar las oportunidades identificadas. Una adecuada administración de los riesgos facilita tratar la incertidumbre de una manera eficaz y generar más valor en la gestión institucional.

La presente guía contiene los lineamientos establecidos por la Alta Dirección del Ministerio para identificar, valorar, tratar, comunicar, monitorear y hacer seguimiento a los riesgos de gestión, de corrupción y demás riesgos institucionales asociados a los modelos referenciales de: seguridad de la información, del sistema de salud y seguridad en el trabajo y ambientales, con el fin de optimizar y orientar los esfuerzos, para el logro de los objetivos y metas institucionales.

1. OBJETIVO GENERAL

Fortalecer la implementación y desarrollo de la política de administración del riesgo a través de una guía metodológica que brinde lineamientos para un adecuado tratamiento de los riesgos de gestión, de corrupción, de soborno, de seguridad y privacidad en la información, ambientales y de seguridad y salud en el trabajo, identificados en cada uno de los procesos que hacen parte del Sistema Integrado de Gestión, a fin de garantizar el cumplimiento de la misión y objetivos estratégicos de la entidad.

2. ALCANCE

La presente guía será aplicada por todos los procesos del Sistema Integrado de Gestión del Ministerio de Educación Nacional e incluye los principios básicos y metodológicos para la gestión de riesgos y oportunidades de tipo estratégico, operacional y de cumplimiento, en alineación y cumplimiento de la política de administración de riesgos establecida por la alta dirección de la entidad.

3. ASPECTOS POSITIVOS DE LA GESTIÓN DE RIESGOS

La gestión de los riesgos institucionales trae consigo los siguientes beneficios:

- ✓ **Alinea el riesgo y la estrategia:** Cuando en la prospectiva institucional, la dirección considera los riesgos, puede orientar mejor los esfuerzos y los recursos para el logro de los objetivos, desarrollando mecanismos para gestionar las oportunidades o amenazas asociadas.
- ✓ **Mejora las decisiones de respuesta a los riesgos:** Proporciona rigor para identificar las posibles oportunidades o amenazas que hacen parte del quehacer institucional y seleccionar entre las posibles alternativas de respuesta la más viable y efectiva, para alcanzar los resultados esperados.
- ✓ **Reduce las sorpresas y las pérdidas operativas:** Permite mejorar la capacidad de la entidad para identificar las amenazas o vulnerabilidades que pueden afectar su gestión y establecer respuestas, reduciendo la incertidumbre frente a eventos potenciales.
- ✓ **Identifica y gestiona la diversidad de riesgos para toda la entidad:** Desde un enfoque sistémico facilita respuestas eficaces e integradas a los impactos interrelacionados de dichos riesgos, optimiza los recursos disponibles y garantiza la coherencia en las respuestas institucionales, en el momento de

abordar las posibles vulnerabilidades o amenazas, así como las oportunidades identificadas.

- ✓ **Permite aprovechar las oportunidades:** Mediante la consideración de una amplia gama de potenciales eventos, la dirección está en posición de identificar y aprovechar las oportunidades de modo proactivo, a fin de potencializar los efectos deseables.

4. CONCEPTOS BÁSICOS

4.1. Conceptos Transversales

- **Administración de riesgos:** Proceso efectuado por la Alta Dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino con la apropiación de la evaluación de los riesgos como una parte natural del proceso de planeación institucional.
- **Análisis de riesgo:** Uso sistemático de la información disponible para valorar los riesgos en función de las causas, las consecuencias, su severidad y la posibilidad de ocurrencia de este, con el fin de estimar la zona de riesgo inicial (riesgo inherente).
- **Apetito al Riesgo**: Es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. Este puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **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.
- **Causa:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituye la causa principal o base para que se presente el riesgo.
- **Causa raíz:** Causa principal o básica, corresponde a las razones por las cuales se puede presentar el riesgo.
- **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**.**

- **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.
- **Evaluación del riesgo:** Determinación de las prioridades de gestión del riesgo, mediante la comparación del nivel de riesgo hallado (riesgo inherente) y la evaluación de las medidas de control existentes. Es una etapa que busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (riesgo residual).
- **Factores de riesgo:** Son las fuentes generadoras de riesgo.
- **Impacto:** Son las consecuencias o efectos que puede ocasionar a la organización la materialización del riesgo.
- **Probabilidad**: Se entiende como la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se está analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **Mapas de riesgo:** Documento con la información resultante de la identificación, valoración y tratamiento del riesgo.
- **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 de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo puede ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una Matriz de Probabilidad – Impacto.
- **Plan de tratamiento de riesgos:** Se define como las decisiones de tratamiento de los riesgos y las actividades de control para su mitigación, a través de la aplicación selectiva de técnicas apropiadas y principios de administración para reducir las probabilidades de ocurrencia de los riesgos, sus consecuencias o ambas.
- **Política de Administración del Riesgo:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Riesgo 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.

4.2. Conceptos sobre riesgos de corrupción

- **Riesgos de Corrupción**: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Fraude:** Acción de engaño intencional, que un servidor público o particular con funciones públicas, realiza con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero.
- **Riesgo de fraude:** Efecto que se causa sobre los objetivos de las entidades, debido a una acción de engaño intencional, que un servidor público o particular con funciones públicas, realiza con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero.
- **Plan Anticorrupción y de Atención al Ciudadano**: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

4.3. Conceptos sobre riesgos de soborno

- **Soborno:** Oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (que puede ser de naturaleza financiera y no financiera), directa o indirectamente, e independiente de su ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o deje de actuar en relación con el desempeño de las obligaciones de esa persona (ISO 37001)
- **Controles Financieros:** Los controles financieros se refieren a los sistemas de gestión y procesos que implementa la organización para gestionar sus transacciones financieras correctamente y para registrar estas transacciones con precisión de forma completa y de manera oportuna. Dependiendo del tamaño y de las transacciones de la entidad podrían reducir el riesgo de soborno.

- **Controles no financieros:** Los controles no financieros se refieren a los sistemas de gestión y a los procesos que implementa la entidad para ayudar a asegurar que los aspectos de estructuración, contratación, seguimiento a los proyectos, operaciones y otros aspectos no financieros, relacionadas con las actividades propias del negocio se gestionen de forma apropiada. Dependiendo del tamaño de la entidad, todos los controles que se implementen en cada una de estas áreas ayudarán a reducir el riesgo de soborno.
- **Posibles Hechos del riesgo:** Los posibles hechos son las causas que pueden generar que se presente el riesgo.
- **Función de cumplimiento antisoborno:** La función de cumplimiento antisoborno la desarrolla un funcionario, un comité o un tercero que tenga las competencias, status, autoridad e independencia adecuados. Que tenga acceso directo a la alta dirección y al órgano de gobierno (junta directiva), con el fin de comunicar la información relevante.
- **Debida diligencia:** Es hacer lo correcto, antes, durante y después del desarrollo de todos los proyectos. Implica identificar las debilidades para corregirlas y los riesgos para mitigarlos, mediante acciones concretas. En otras palabras, es la capacidad de la entidad para hacerse responsable de los impactos negativos ocasionados por sus actividades. La debida diligencia encamina a la entidad a que adopte buenas prácticas, que le permita conocer, prevenir y mitigar los riesgos.

4.4. Conceptos sobre riesgos de Seguridad de la Información

- **Activos de información:** En el contexto de la seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Amenaza:** Causa potencial de un incidente no deseado, el cual puedo ocasionar daño a un sistema o a una organización
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- **Evento de seguridad de la información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de

la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

- **Gestión de activos:** Consiste en obtener el máximo rendimiento de los bienes o recursos, es decir de todo aquello que tenga valor para una organización.
- **Infraestructuras criticas cibernéticas- ICC-:** Instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar de los ciudadanos.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Riesgo cibernético:** Posibilidad de que se materialice una falla en la seguridad de los componentes tecnológicos o sistemas de información, sistemas de control, sistemas electrónicos y las telecomunicaciones que por ataques o intrusiones podrían impactar la movilidad de personas, alimentos, mercancías peligrosas y elementos esenciales y de carácter vital.
- **Riesgo de seguridad digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial el orden institucional y los intereses nacionales, incluye aspectos relacionados con el aspecto físico, digital y las personas.
- **Seguridad digital:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.
- **Clasificación de Activos de información:** Orden y agrupación de los activos de información en función de los requisitos legales, valor, criticidad y susceptibilidad a la divulgación o a la modificación no autorizada de los recursos tecnológicos con los que cuenta una organización para agilizar su gestión.
- **Vulnerabilidad:** Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

4.5. Conceptos sobre del Sistema de Gestión Ambiental

- **Riesgo Ambiental:** Se relaciona con los efectos potenciales adversos (amenazas) en el ambiente, generados por el desarrollo de los procesos de la entidad (ISO 14001).

- **Impacto Ambiental:** Cambio en el medio ambiente, ya sea adverso o beneficioso, como resultado total o parcial de los aspectos ambientales de una organización (ISO 14001).

Los riesgos ambientales se pueden agrupar en dos categorías:

- **Riesgo para el ambiente:** Actividades de una entidad en condiciones normales y/o de emergencias que puedan causar cambios o impactos ambientales (Estos se identifican, analizan y evalúan de acuerdo con el procedimiento PM-PR-05 - Identificación y valoración de aspectos e impactos, y el formato PM-FT-02 - Identificación y valoración de aspectos e impactos ambientales.
- **Riesgo para la entidad debido a temas relacionados con el ambiente:** Situaciones relacionadas con la gestión ambiental, que si llegasen a presentarse pueden ocasionar incumplimiento legal, pérdidas de recursos, multas, crisis de reputación, costos por no asegurar y mantener los permisos y licencias para el desarrollo de las actividades operativas (Estos se identifican por medio de la Matriz de Riesgos descrita en la metodología de la presente guía).

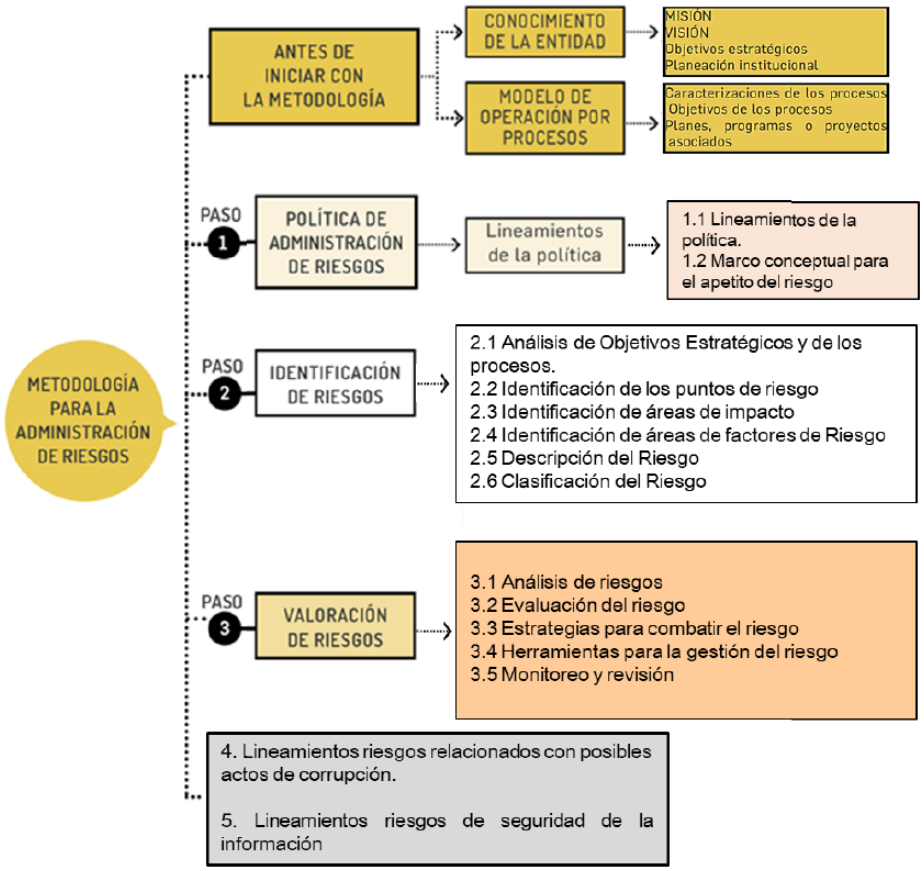
4.6. Conceptos sobre riesgos del Sistema de Gestión de Seguridad y Salud en el Trabajo

- **Amenaza**: Peligro latente de que un evento físico de origen natural, o causado, o inducido por la acción humana de manera accidental, se presente con una severidad suficiente para causar pérdida de vidas, lesiones u otros impactos en la salud, así como también daños y pérdidas en los bienes, la infraestructura, los medíos de sustento, la prestación de servicios y los recursos ambientales.
- **Peligro**: Fuente, situación o acto con potencial de causar daño en la salud de los trabajadores, en los equipos o en las instalaciones.

5. ADMINISTRACIÓN DEL RIESGO

En la figura 1 se ilustran los principales componentes de la administración del riesgo que se desarrollarán en detalle a lo largo del presente documento:

Figura 1. Componentes de la gestión del riesgo



Fuente: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - V5", 2020

6. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO[1]

En el Ministerio de Educación Nacional declaramos nuestro compromiso con la adecuada administración de los riesgos asociados a los objetivos estratégicos y a los procesos y proyectos de la entidad, determinando los factores que pueden causar desviaciones en los resultados planificados, para poner en marcha controles

[1] Resolución vigente de Políticas de Gestión y Desempeño Institucional

preventivos, detectivos y correctivos que minimicen los efectos negativos y maximicen el uso de las oportunidades y la mejora del desempeño institucional.

7. CONTENIDO DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO DEL MINISTERIO DE EDUCACIÓN NACIONAL

7.1. Objetivo General

Establecer los lineamientos y criterios para orientar en el Ministerio de Educación Nacional la correcta identificación, valoración, tratamiento, monitoreo y seguimiento de los riesgos a los que se enfrenta y que puedan impactar el cumplimiento de los objetivos institucionales en el marco de los procesos, planes y proyectos de la entidad.

7.2. Objetivos Específicos

1. Fomentar la cultura de la prevención del riesgo en todos los niveles de la organización.
2. Contribuir al cumplimiento de los objetivos del MEN a través de la Gestión del Riesgo.
3. Mantener los controles que permitan el adecuado aprovechamiento de los recursos destinados a planes, programas, y proyectos, siempre bajo las mejores condiciones de eficacia, eficiencia, y efectividad.

7.3. Alcance

Esta política aplica a todos los procesos establecidos en el marco del Sistema Integrado de Gestión – SIG de la entidad, bajo los lineamientos metodológicos definidos por el Ministerio de Educación Nacional.

7.4. Directrices de la Política

De conformidad con lo establecido en el Modelo Integrado de Planeación y Gestión MIPG y como parte de las directrices que se deben establecer desde el del equipo directivo, tanto en la Guía de Administración del Riesgo como en el Procedimiento de Administración del Riesgo, se emiten los lineamientos para el tratamiento, manejo y seguimiento a los riesgos que puedan afectar el logro de los objetivos institucionales. Los documentos mencionados corresponden a documentos

complementarios de la Política de Administración del Riesgo del Ministerio de Educación Nacional.

7.5. Niveles de aceptación del riesgo

La entidad, como resultado de la identificación y valoración de los riesgos de gestión asociados a todos los procesos, ha definido tolerar los riesgos que tengan baja probabilidad de ocurrencia y bajo potencial de impacto. Para el caso de los riesgos residuales (después de controles) cuya calificación se ubique en zona de riesgo **ALTO o EXTREMO** se debe implementar plan de manejo para los mismos.

Esta directriz excluye los riesgos asociados a soborno, corrupción o fraude, en cuyo caso la tolerancia es inaceptable y la entidad siempre debe formular acciones orientadas a eliminar el riesgo.

7.6. Niveles de calificación del impacto

Los niveles de calificación del impacto se determinan de conformidad con los criterios establecidos en la Guía de Administración del Riesgo V5 del DAFP:
Criterios para definir el nivel de impacto. Estos se presentan en el numeral 10.2.1. de la presente guía – Análisis del riesgo.

7.7. Tratamiento del riesgo

Las opciones para el tratamiento se definen en el numeral 10.3. de la presente guía - Estrategias para combatir el riesgo (opciones de manejo transversales).

7.8. Periodicidad para el seguimiento de acuerdo con el riesgo residual

La periodicidad de seguimiento se establece en el numeral 12. de la presente guía MONITOREO (SDO) Y SEGUIMIENTO (OCI)-

8. ROLES Y RESPONSABILIDADES

Teniendo en cuenta lo establecido en Decreto 1499 de 2017 sobre la Dimensión de Control Interno del Modelo Integrado de Planeación y Gestión, las responsabilidades de las líneas de defensa del Modelo Estándar de Control Interno, para la administración y evaluación de los riesgos de la entidad son las siguientes:

Línea Estratégica

Le corresponde a la **Línea Estratégica**, definir el marco general para la gestión del riesgo y el control y supervisar su cumplimiento. Está a cargo de la Alta Dirección (Comité Institucional de Coordinación de Control Interno), de conformidad con las funciones definidas en su creación, la verificación del cumplimiento de los objetivos a través de una adecuada gestión de riesgos, en relación con:

- ✓ Definir la Política de Administración del Riesgo asociada a la estrategia, procesos, seguridad de la información y medidas anticorrupción; es determinada y aprobada por el Comité Institucional de Coordinación de Control Interno, previa socialización ante el Comité de Desempeño Institucional.
- ✓ Revisar los cambios en el "Direccionamiento estratégico" y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados.
- ✓ Revisar la adecuada alineación de los objetivos institucionales con los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos.
- ✓ Hacer seguimiento en el Comité Institucional de Coordinación de Control Interno 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, de sus indicadores e identificar en caso de que no se estén alcanzando las metas, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
- ✓ Hacer seguimiento y pronunciarse por lo menos una vez al trimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo con las políticas de tolerancia establecidas y aprobadas.
- ✓ Revisar los informes trimestrales elaborados por la Subdirección de Desarrollo Organizacional 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.

8.2. Primera línea de defensa

Desarrolla e implementa procesos de control y gestión de riesgos, a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. Está conformada por los gerentes públicos y líderes de procesos, programas y proyectos, quienes deben monitorear y revisar el cumplimiento de los objetivos institucionales y sus procesos a través de una adecuada gestión de riesgos, incluyendo los 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.
- ✓ Revisar el adecuado diseño y ejecución de los controles establecidos para mitigar los riesgos de sus procesos.
- ✓ 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, y en caso de que no se estén alcanzando las metas identificar los posibles riesgos que se estén materializando.
- ✓ Identificar y controlar los riesgos relacionados con posibles actos de corrupción en el ejercicio de sus funciones y en el cumplimiento de sus objetivos, así como, en la prestación del servicio.
- ✓ Revisar y reportar en los medios que disponga la Subdirección de Desarrollo Organizacional (SDO), 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.
- ✓ Monitorear la ejecución de los controles y reportar la eficacia de estos en la mitigación de los riesgos, conforme a la periodicidad establecida en la circular de reportes de cada vigencia.
- ✓ 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 de 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.

- ✓ Mantener actualizados los mapas de riesgos por procesos y mapas de riesgo de corrupción, de conformidad con las políticas institucionales aprobadas y las normas nacionales vigentes; así como, velar por el cumplimiento de los lineamientos señalados por la metodología de administración del riesgo aprobada, en lo concerniente al análisis del contexto estratégico, la identificación del riesgo, su análisis, valoración, medidas de tratamiento, monitoreo y seguimiento.

8.3. Segunda 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 el apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos; 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 (Subdirección de Desarrollo Organizacional, Oficial de Transparencia, Equipo de Transparencia, supervisores e interventores de contratos o proyectos, líderes de los modelos referenciales que conforman el Sistema Integrado de gestión, etc.), ellos deben monitorear y revisar el cumplimiento de los objetivos institucionales y sus procesos a través de una adecuada gestión de riesgos, incluyendo los 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 los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos.
- ✓ 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 realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.
- ✓ La Subdirección de Desarrollo Organizacional debe capacitar a los servidores de la entidad y asesorar a los líderes de procesos en la metodología de la administración del riesgo y su implementación.
- ✓ Los líderes de los modelos referenciales que conforman el Sistema Integrado de Gestión y los líderes de las Políticas de Gestión y Desempeño deben impulsar a nivel institucional una cultura de gestión del riesgo, coherente con el Modelo Integrado de Planeación y Gestión, el Modelo Estándar de Control Interno – MECI, el Modelo de Seguridad y Privacidad de la Información y las

Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano.

- ✓ Los líderes de los modelos referenciales deben informar sobre la incidencia de los riesgos en el logro de objetivos, evaluar si la valoración del riesgo es la apropiada y asegurar que las evaluaciones de los riesgos y los controles incluyan los riesgos de fraude.
- ✓ La Subdirección de Desarrollo Organizacional debe ayudar a la primera línea de defensa con evaluaciones del impacto de los cambios en el Sistema de Control Interno (SCI).
- ✓ Los líderes de los modelos referenciales deben reportar la gestión realizada frente a los mapas de riesgos.
- ✓ La Subdirección de Desarrollo Organizacional, elaborará trimestralmente un informe consolidado de monitoreo a los mapas de riesgos de conformidad con la periodicidad establecida en la circular de reportes de cada vigencia. Lo anterior, no exime a los líderes de los procesos de su responsabilidad de realizar monitoreo a los riesgos de sus procesos, de conformidad con los lineamientos institucionales establecidos para el efecto.
- ✓ La Subdirección de Desarrollo Organizacional debe elaborar informes consolidados de la gestión de riesgos para las diversas partes interesadas con el apoyo de los líderes de proceso.
- ✓ Los supervisores de contratos deben realizar seguimiento a los riesgos de estos e informar las alertas respectivas.
- ✓ La Subdirección de Desarrollo Organizacional debe realizar la gestión necesaria para la publicación de la versión vigente de los mapas de riesgos en las páginas web de la entidad, en el marco de la política de transparencia y acceso a la información pública.
- ✓ La Subdirección de Desarrollo Organizacional, debe realizar la difusión de lineamientos, metodologías, roles y responsabilidades para el monitoreo y seguimiento de los mapas de riesgo.
- ✓ El oficial de transparencia y el equipo de transparencia apoyarán con la identificación de los riesgos de soborno y harán monitoreo periódico de los mismos, sin menoscabo de la responsabilidad que tienen los líderes de proceso en la identificación, valoración y tratamiento de los riesgos de corrupción.

8.4. Tercera línea de defensa

Provee aseguramiento, evaluación independiente y objetiva 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 (OCI), la cual revisa de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, a través del seguimiento a la adecuada gestión de riesgos a con las siguientes responsabilidades:

- ✓ Evaluar la ejecución de los controles para la mitigación de los riesgos que se han identificado por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos.
- ✓ Asesorar en la metodología para la identificación y administración de los riesgos y oportunidades, en coordinación con la segunda línea de defensa.
- ✓ Identificar y evaluar cambios que podrían tener un impacto significativo en el SCI, durante los seguimientos trimestrales de riesgos y en el curso del trabajo de auditoría interna.
- ✓ Comunicar al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo y oportunidades, detectados en las auditorías.
- ✓ Alertar a la alta dirección sobre la probabilidad de riesgo de corrupción, fraude o soborno en las áreas auditadas.
- ✓ Realizar el seguimiento a los riesgos de corrupción y hacer la gestión que se requiera de conformidad con las directrices establecidas en la normatividad vigente relacionada con la materia.
- ✓ En sus procesos de auditoría, esta oficina debe analizar el diseño e idoneidad de los controles, determinando si son o no adecuados para prevenir o mitigar los riesgos de los procesos, haciendo uso de las técnicas relacionadas con pruebas de auditoría que permitan determinar la efectividad de los controles implementados para abordar las amenazas o vulnerabilidades.

Bajo los principios de autocontrol y autogestión, todos los servidores públicos del Ministerio, en el marco de sus funciones y obligaciones son responsables de aplicar mecanismos de control adecuados que busquen mitigar los riesgos a los que están expuestas las labores que le sean designadas, incluso aquellos riesgos que estén enmarcados en sus responsabilidades, pero que no se encuentren especificados en el mapa de riesgos institucional.

9. LINEAMIENTOS PARA LA ADMINISTRACIÓN DE RIESGOS

El aspecto central para el desarrollo y la consolidación de la política de administración de riesgos es la identificación y análisis del mapa de riesgos institucional y la formulación y actualización de la matriz de riesgos (matriz de calor y zonas de riesgo) con base en los siguientes criterios:

a. Los mapas de riesgos de gestión y corrupción serán de conocimiento de la Alta Dirección, y su riesgo residual será el soporte para aprobación y/o modificación de la Política de Administración del Riesgo.

b. Los mapas de riesgos deben estar alineados con el Sistema Integrado de Gestión y con la planeación estratégica de la entidad.

c. Se deben focalizar los riesgos estratégicos y operacionales residuales que queden ubicados en zona de riesgos extremos y altos con propósito de toma de decisiones en cuanto a su tratamiento.

d. Los riesgos residuales ubicados en zona de riesgo alto o extremo, podrán tener diferentes opciones de manejo “reducir (mitigar, transferir) o evitar” según lo establece la metodología, esto considerando los eventos registrados para dichos riesgos en periodos anteriores, y a partir de este análisis deberán tener una propuesta o acción de tratamiento coherente que busquen gestionar el riesgo; sin embargo, todos los procesos con riesgos residuales ubicados en estas categorías deberán establecer planes de manejo adicionales para los mismos.

e. Los riesgos residuales que queden ubicados en zona de riesgo Moderado o Bajo podrán llevar cualquiera de las opciones de manejo indicadas por la presente guía “aceptar, evitar, reducir”. Si se elige como tratamiento para el riesgo la opción de “aceptar el riesgo”, significará que para la vigencia no se generarán nuevos planes de acción para mitigar el riesgo. Sin embargo, el que se incluya esta opción no excluye al líder de proceso de la obligación de continuar aplicando los controles establecidos y hacer el respectivo seguimiento tanto a los controles ya implementados como a la posible materialización del riesgo. Para riesgos de corrupción y/o soborno no se puede aceptar o asumir el riesgo.

f. La Subdirección de Desarrollo Organizacional y/o el Comité de Desempeño Institucional, podrá incluir en los diferentes mapas de riesgos, aquellos riesgos potenciales que considere pertinente y que no hayan sido incluidos en los mapas de riesgos del proceso.

g. Se deberán asignar recursos que permitan evaluar el desempeño de los controles, asignar indicadores claves de riesgos y metas, que permitan

identificar o alertar estados de criticidad o posibles materializaciones de estos.

h. Las acciones de mitigación del riesgo, así como las acciones para desarrollar las oportunidades deben ser incluidas en el plan de acción de la entidad con el fin de llevar un solo control.

i. De igual forma, los ajustes o nuevos lineamientos de política para la administración de riesgos y medidas de transparencia que deba tomar la Alta Dirección, podrán ser formalizados a través de actas aclaratorias, ayudas de memoria o memorandos, para las cuales se sugiere tener en cuenta lo siguiente:

- Definir los objetivos que se esperan obtener como parte del análisis de contexto.
- Priorizar los riesgos que pueden generar mayor impacto en la entidad y que afecte a los productos y servicios generados para el cumplimiento de la misión y objetivos institucionales.
- Tener en cuenta el plan estratégico, plan sectorial y planes de acción.
- Tener en cuenta los procedimientos aprobados dentro del Sistema Integrado de Gestión.
- Pensar en los componentes que conforman la cadena productiva del proceso y no solo las áreas.
- Determinar políticas y/o estrategias a largo, mediano y corto plazo.
- Determinar una línea base de recursos disponibles.
- Si se sugieren estrategias a largo y mediano plazo, dejar definidas políticas, recursos necesarios y líder responsable.
- Plantear responsables para la implementación, seguimiento de las políticas y otros responsables diferentes para actividades de evaluación de efectividad y auditoría.

j. La Política de Transparencia del Ministerio será determinada, modificada y aprobada por la Alta Dirección en cabeza del Ministro(a) de Educación, bajo los lineamientos normativos indicados por la Presidencia de la República o sus entidades delegadas.

k. A partir de la Política y los Objetivos de Transparencia, la Subdirección de Desarrollo Organizacional, apoyará al Equipo de Transparencia, al menos una vez por año en identificar oportunidades de mejora que sean diferentes

de las acciones para abordar los Riesgos de corrupción/soborno priorizados.

l. A partir de la identificación de las oportunidades de mejora enunciadas en el punto anterior, se hace una selección de las oportunidades de mejora que muestren viabilidad según el criterio de la Subdirección de Desarrollo Organizacional y con base en estas se establecen procedimientos documentados o Planes de Mejoramiento Institucional, sujetos a aplicación y posterior seguimiento y auditoría.

m. Los planes, deben establecer indicadores de eficacia para evaluar el logro de los objetivos de acciones para abordar las oportunidades.

n. De acuerdo con lo que establece la guía de riesgos del Departamento Administrativo de la Función Pública (DAFP), la identificación de riesgos de la entidad deberá contemplar como mínimo los siguientes aspectos en los procesos que correspondan: Riesgos que afecten la capacidad de cumplir con la estrategia de la entidad, riesgos operativos, riesgos de cumplimiento, riesgos de contratación, riesgos para la defensa jurídica, riesgos de seguridad digital.

9.1. Lineamientos operativos para mapas de riesgos institucionales, corrupción, soborno, fraude y seguridad de la información

a. Los mapas de riesgos deberán ser aprobados por los líderes de los correspondientes procesos; sin embargo, la Subdirección de Desarrollo Organizacional y/o el Comité Institucional de Gestión y Desempeño, podrán solicitar que se incluyan en el Mapa de Riesgos, aquellos riesgos potenciales que no hayan sido incluidos por estos.

b. El mapa de riesgos de corrupción se hará para los procesos misionales, estratégicos y de apoyo, enfocando las áreas identificadas en el Ministerio como posiblemente vulnerables, en razón a sus actividades y procedimientos.

c. Para los riesgos de soborno se generará un mapa de calor por proceso en el cual se evidenciarán los procesos de mayor riesgo.

d. Es normal y frecuente que, al analizar un proceso con respecto a los riesgos de soborno, los planes de acción no sean ejecutables por el área o áreas que participan en el proceso, puesto que las prácticas de soborno se previenen normalmente a partir de acciones de alcance institucional y no en todos los casos de acciones puntuales. Por lo tanto, en el análisis de un

proceso se puede identificar la necesidad de emprender acciones que deben liderar otras áreas de la entidad, para lo cual se requerirá el apoyo de la Subdirección de Desarrollo Organizacional con el fin de articular estas.

e. Los mapas de riesgos deberán ser consolidados, publicados y socializados a toda la entidad propendiendo por el desarrollo de la cultura organizacional de gestión de riesgos.

f. Los mapas de riesgo deben como mínimo cubrir los riesgos asociados a las políticas del MIPG: Gestión presupuestal y eficiencia del gasto público, talento humano, integridad, fortalecimiento organizacional y simplificación de procesos, servicio al ciudadano, participación ciudadana en la gestión pública, racionalización de trámites, gestión documental, gobierno digital.

g. La actualización de los mapas institucionales de riesgos de gestión, así como los de corrupción, soborno, seguridad digital y demás modelos referenciales se realizarán de forma anual según los lineamientos normativos, salvo que por necesidades del servicio se requiera su actualización con otra periodicidad.

h. La eliminación de cualquier riesgo deberá ser justificada y aprobada por el líder del proceso y deberá registrarse en la matriz de cambios de la entidad. Sin embargo, de presentarse justificaciones poco argumentadas, la Subdirección de Desarrollo Organizacional deberá pedir ampliación de la justificación, hasta tener evidencia de que dicha eliminación no acarreará perjuicios para el Ministerio, para lo cual se podrá solicitar concepto de otros líderes de procesos que puedan dirimir la decisión.

i. Teniendo en cuenta la norma ISO 27001 de Seguridad de la Información y el Decreto 612 de 2018, el área de Tecnología y Sistemas de Información deberá apoyar en la actualización de los riesgos de seguridad de la información a los que se puedan ver expuestos los diferentes procesos de la entidad, teniendo en cuenta los principios de gestión para estos riesgos que se exponen en la presente guía.

j. Los riesgos de seguridad digital por su naturaleza e impacto se clasificarán como reservados; por lo tanto, los riesgos identificados para el Ministerio no deben ser públicos ya que esto expondría a la entidad y daría la oportunidad de acceso a información reservada a terceros, situación que puede ser usada en su contra a través de posibles ataques cibernéticos, esto generaría una vulneración de la plataforma informática y de los activos de información, en especial los denominados reservados y confidenciales.

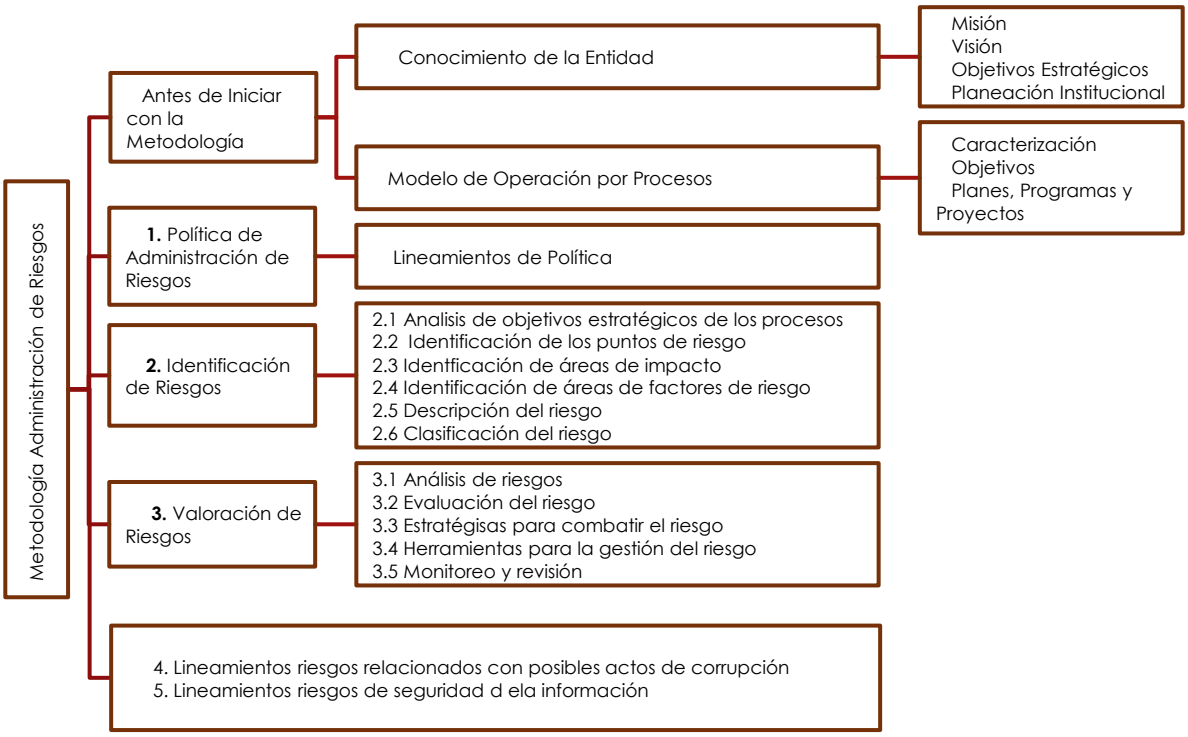
k. Las opciones de tratamiento de los riesgos deberán estar dentro de la Política de Gestión Integral de Riesgos del Ministerio de Educación.

l. Se formarán a través de talleres, a los enlaces responsables de la generación de reportes de desempeño institucional, designados por cada proceso.

10. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

En la Figura 2 se pueden observar las etapas definidas para la administración del riesgo en el MEN.

Figura 2. Administración del riesgo en el Ministerio de Educación Nacional



Fuente: SDO (2022) basados en la Guía para la administración del riesgo V5 - DAFP.

10.1. Definición del contexto estratégico

Con el fin de identificar los factores externos e internos que inciden en el desempeño de los procesos y en el logro de las metas y objetivos establecidos en la planeación estratégica, se debe identificar el contexto externo, interno y del proceso. En la tabla 1 se puede apreciar los tipos de contexto.

Tabla 1. Características por tipo contexto

FACTORES INTERNOS Y EXTERNOS DE RIESGO		
CONTEXTO EXTERNO		**CONTEXTO INTERNO**
Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad, retoma los siguientes factores:		Se determinan las características del ambiente en el cual la organización busca alcanzar sus objetivos, se analizan aspectos como:
Económicos: Disponibilidad de recursos financieros, liquidez, mercados financieros, desempleo, competencia.		**Financieros:** Presupuesto funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
Político: cambios de gobierno, legislación, políticas públicas, regulación		**Personal:** Competencia y disponibilidad de personal, seguridad y salud laboral.
Medioambientales: Condiciones ambientales residuos, energía, agua, catástrofes naturales, desarrollo sostenible		**Procesos:** Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento, interacción, transversalidad, responsables, lineamientos internos definidos, registros.
Seguridad y Salud en el Trabajo: Condiciones de Seguridad y salud en el trabajo externas, emergencias, eventos catastróficos, residuos peligrosos.		**Seguridad y Salud en el Trabajo:** Condiciones de Salud, condiciones de trabajo, presupuesto, recursos, infraestructura, comunicación, responsabilidades.
Sociales y Culturales: Demografía, responsabilidad social, orden público.		**Estructura organizacional:** Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
Tecnológicos: Avances en tecnología, acceso a sistemas de información externos, interrupciones, tecnología emergente, gobierno en línea.		**Tecnología:** integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información
Comunicación Externa: Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que los mismos se comunique con la entidad		**Comunicación Interna:** Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.

CONTEXTO DEL PROCESO
Diseño del proceso: Claridad en la descripción del alcance y objeto del proceso
Interrelación con otros procesos: Claridad en la descripción del alcance y objetivo del proceso
Transversalidad: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad
Procedimientos asociados: pertinencia en los procedimientos que desarrolla el proceso
Responsables del proceso: Grado de autoridad y responsabilidad de los funcionarios frente al proceso
Comunicación entre los procesos: efectividad en los flujos de información determinados en la interacción de los procesos
Activos de seguridad digital del proceso: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, de cara al ciudadano.

Fuente: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – V4", 2018

10.2. Identificación del Riesgo de Gestión

La identificación del riesgo se realiza determinando, el impacto, la causa inmediata y la causa raíz con base en las actividades establecidas en la caracterización de cada proceso, las cuales deben tener una alineación con los objetivos estratégicos de la entidad, de tal forma que una vez se identifiquen los riesgos, se pueda determinar si estos pueden o no afectar el logro de los objetivos. Las causas externas se tendrán en cuenta dentro del análisis, especialmente para el tratamiento de los riesgos, sin embargo; solo se tendrán en cuenta para la identificación de riesgos, las causas internas, de tal forma que los mismos sean de total control de la entidad.

Para facilitar el proceso de identificación de los riesgos se recomienda tener en cuenta el conocimiento previo de aquellas situaciones que puedan obstaculizar el cumplimiento de los objetivos, la obtención de un resultado, la generación de procesos transparentes, el cumplimiento de requisitos legales o la satisfacción de un usuario, por ello es importante tener en cuenta:

- ✓ Resultados de las auditorías internas y externas.
- ✓ Resultados de las actividades de rendición de cuentas.
- ✓ Medición del desempeño institucional en periodos anteriores.
- ✓ Medición de la satisfacción de grupos de valor en periodos anteriores.
- ✓ Medición de indicadores de los procesos.
- ✓ Medición de los servicios y tratamiento no conforme.
- ✓ Resultados de la evaluación de las obligaciones de cumplimiento legal y otros.
- ✓ Situaciones latentes que puedan generar emergencias.

Para la identificación del riesgo es necesario seguir los siguientes parámetros:

10.2.1. Analizar los objetivos estratégicos y de los procesos

Se debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso. Los objetivos estratégicos deben estar alineados con la Misión, la Visión institucional; de igual forma, cada uno debe tener una adecuada formulación (que sea especifico, medible alcanzable, relevante y proyectado en el tiempo - SMART). Para los objetivos de proceso se debe realizar el mismo análisis y que estos contribuyan a los objetivos estratégicos.

10.2.2. Identificar los puntos de riesgo

Las actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios que pueden ocurrir eventos de riesgo operativo y que deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

10.2.3. Identificar áreas de Impacto

La consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional

10.2.4. Identificar áreas de factores de riesgo

Las fuentes generadoras de riesgos. (Estos se pueden ver en la tabla 2).

Tabla 2. Factores de riesgo

Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización.
			Errores en cálculos para pagos internos y externos.
			Falta de capacitación, temas relacionados con el personal
Talento Humano	Incluye Seguridad y Salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Hurto activos
			Posibles comportamientos no éticos de los empleados.
			Fraude interno (corrupción, soborno).
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos

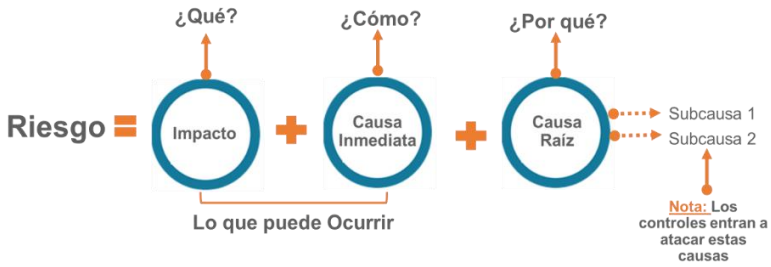
Factor	Definición		Descripción
			Caída de aplicaciones.
			Caída de redes.
			Errores en programas.
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos.
Evento Externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

Fuente: Adaptado de Curso Riesgo Operativo Universidad del Rosario por Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

10.2.5. Descripción del riesgo

La descripción del riesgo debe contener todos los detalles que sean necesarios para que sea de fácil entendimiento para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad, su redacción inicia con POSIBILIDAD DE y se debe observar la estructura establecida en la figura 3.

Figura 3. Definición de riesgo



Fuente: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - V5", 2020

- ✓ **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- ✓ **Causa Inmediata:** Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- ✓ **Causa raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo puede existir más de una causa o subcausas que pueden ser analizadas.

Nota: Para la identificación de la causa inmediata y causa raíz, se sugiere el uso de la metodología de árbol de problemas, especialmente porque nos permite identificar el problema, efecto y causas secundarias que deben ser controladas.

Recomendaciones para una Adecuada Redacción del Riesgo:

☹ **No describir como riesgos omisiones ni desviaciones del control.**

Ejemplo: Errores en la liquidación de la nómina por fallas en los procedimientos existentes.

☹ **NO describir causas como riesgos**

Ejemplo: Inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

☹ **NO describir riesgos como la negación de un control.**

Ejemplo: Retrasos en la prestación del servicio por no contar con digiturno para la atención.

☹ **NO existen riesgos transversales, lo que pueden existir son causas transversales.**

Ejemplo: Pérdida de expedientes.

10.2.6. Clasificación del riesgo

Los riesgos identificados se pueden agrupar en las siguientes categorías:

Tabla 3. Clasificación del riesgo

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 - V5", 2020

Teniendo en cuenta que en apartes anteriores se definieron una serie de factores, como generadores de los posibles riesgos, para la clasificación, atendiendo la tabla 3, su interrelación es la siguiente:

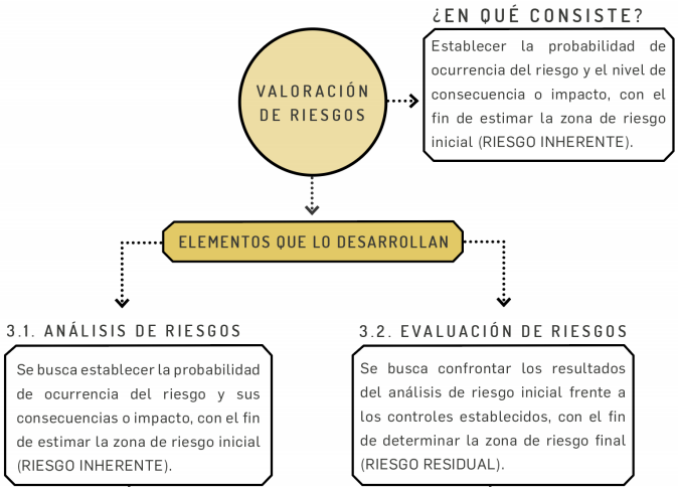
Figura 4. Relación entre factores de riesgo y clasificación del riesgo

Fuente: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - V5", 2020

10.3. Valoración de riesgos a nivel transversal

La valoración del riesgo comprende dos fases: el análisis de riesgos y la evaluación de los riesgos

Figura 5. Estructura para la valoración del riesgo



Fuente: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - V5", 2020

10.3.1. Análisis del riesgo

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

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

En la tabla 4 se establecen los criterios para definir el nivel de probabilidad que serán aplicados en el Ministerio.

Tabla 4. Criterios para definir la probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - V5", 2020

IMPACTO: La valoración del impacto está asociada a los criterios definidos en la tabla 4. En ella se clasifican los impactos en económicos y reputacionales, como variables principales. En la versión anterior de la Guía del DAFP se contemplaban afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal, así como, afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, estos temas se agrupan en impacto económico y reputacional.
Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, los cuales tienen diferentes niveles, se debe tomar el más alto, así,

por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará en este caso el reputacional en nivel moderado.
Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede dar en este tipo de análisis.

Tabla 5. Criterios para definir el nivel de impacto

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

Fuente: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - V5", 2020

IMPORTANTE: Frente al análisis de probabilidad e impacto **no se utiliza criterio experto**, quiere decir esto que el líder del proceso como conocedor de su quehacer define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, igual situación se dará para el impacto, no se trata de un análisis subjetivo.

Se debe señalar que el criterio experto, es decir el conocimiento y experticia del líder del proceso se utiliza para definir aspectos como: número de veces que se ejecuta la actividad, cadena de valor del proceso, factores generadores y para la definición de los controles.

10.3.2. Evaluación de los riesgos

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se determina la zona de riesgo inicial (RIESGO INHERENTE) donde estará ubicado el riesgo en la matriz de calor.

Valoración de controles

Un control se define como la medida que permite reducir o mitigar el riesgo. Se debe tener en cuenta:

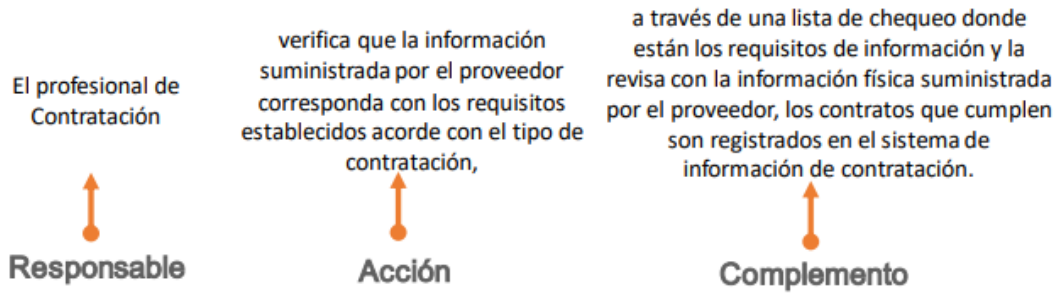
- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Estructura para la descripción del control a nivel transversal:

Para una adecuada redacción del control se establece una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

- **Responsable de ejecutar el control:** Identifica el cargo del servidor que ejecuta el control, en caso se ser controles automáticos se identificará el sistema que realiza la actividad.
- **Acción:** Se determina mediante verbos en los cuales se identifica la acción a realizar como parte del control.
- **Complemento**: Corresponde a los detalles que permiten identificar claramente el objeto del control.

Figura 6. ejemplo aplicado bajo la estructura propuesta para la redacción del control

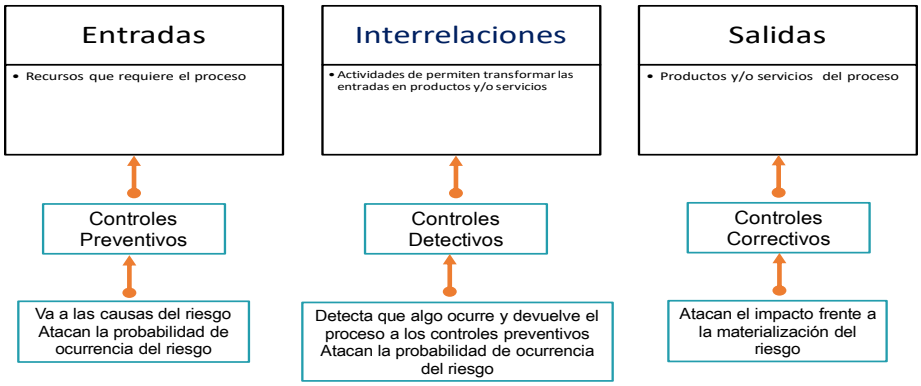


Fuente: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - V5", 2020

Tipología de controles y los procesos:

A través del ciclo de los procesos es posible establecer cuándo se activa un control y por lo tanto establecer su tipología con mayor precisión, para comprender esta estructura conceptual se consideran 3 fases globales del ciclo de un proceso así:

Figura 7. Ciclo del proceso y las tipologías de controles



Fuente: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - V5", 2020

Acorde con lo anterior tenemos las siguientes tipologías de controles:

- **Control preventivo:** Control accionado en la entrada del proceso y antes que se realice la actividad originadora del riesgo, se busca establecer condiciones que aseguren el resultado final esperado.
- **Control detectivo:** Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control correctivo:** Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

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

- **Control manual:** Controles que son ejecutados por personas.
- **Control automático:** Son ejecutados por un sistema.

Análisis y evaluación de los controles – Atributos:

En la tabla 6 se puede observar la descripción y peso asociados a cada uno de los atributos para el diseño de los controles, teniendo en cuenta sus características relacionadas con la eficiencia y la formalización:

Tabla 6. Atributos de para el diseño de controles

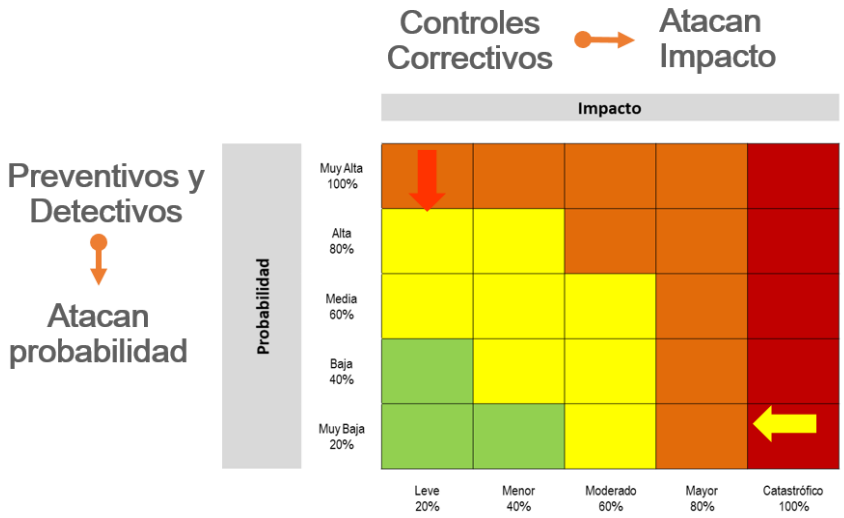
Características			Descripción	Peso
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	15%
***Atributos Informativos**	Documentación	Documentado	Controles que están documentados en el proceso, 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 el proceso	-
	Frecuencia	Continua	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	-
	Evidencia	Con Registro	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 - V5", 2020

***Nota:** 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.**

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde a la figura 8, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles establecidos por la entidad:

Figura 8. Movimiento en la matriz de calor acorde con el tipo de control



Fuente: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - V5", 2020

EJEMPLO

- ✓ **PROCESO:** Contratación.
- ✓ **OBJETIVO DEL PROCESO:** Adquirir los bienes, servicios y obras requeridos por la entidad mediante la aplicación de procedimientos precontractuales, contractuales y poscontractuales, que permitan el cumplimiento de los principios y la normatividad vigentes de la Contratación pública.
- ✓ **RIESGO IDENTIFICADO:** Posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.
- ✓ **PROBABILIDAD INHERENTE**= moderada 60%
- ✓ **IMPACTO INHERENTE:** mayor 80%
- ✓ **ZONA DE RIESGO:** alta

Controles identificados

- ✓ **Control 1**
  El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el

proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.

- ✓ **Control 2**
  El jefe del área de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.

En la tabla 7 se observa la aplicación de atributos para el caso anteriormente descrito, el cual sirve de ejemplo para el análisis y valoración de los dos controles propuestos:

Tabla 7. Aplicación de atributos de controles a ejemplo propuesto

Controles y sus características				Peso
CONTROL 1 El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación	**Tipo**	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual		15%
	Documentación	Documentado	X	-
		Sin documentar		
	Frecuencia	Continua	X	-
		Aleatoria		
	Evidencia	Con registro	X	-
		Sin registro		
TOTAL VALORACIÓN CONTROL 1				**40%**
CONTROL 2 El jefe de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.	**Tipo**	Preventivo		
		Detectivo	X	15%
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	
		Sin documentar		
	Frecuencia	Continua	X	
		Aleatoria		
	Evidencia	Con registro	X	
		Sin registro		
TOTAL VALORACIÓN CONTROL 2				**30%**

Fuente: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - V5", 2020

NIVEL DE RIESGO (riesgo residual): es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Riesgo residual: Riesgo Inherente - Controles

Desplazamiento de la matriz a partir de controles: Para la aplicación de los controles se debe tener en cuenta que estos 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.

En la tabla 8 se da continuación al ejemplo propuesto, donde se observan los cálculos requeridos para la aplicación de los controles.

Tabla 8. Aplicación de controles para establecer el riesgo residual

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2º control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = **25,2%**
	Probabilidad Residual	**25,2 %**			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	**80%**			

Fuente: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - V5", 2020

EJEMPLO (continuación)

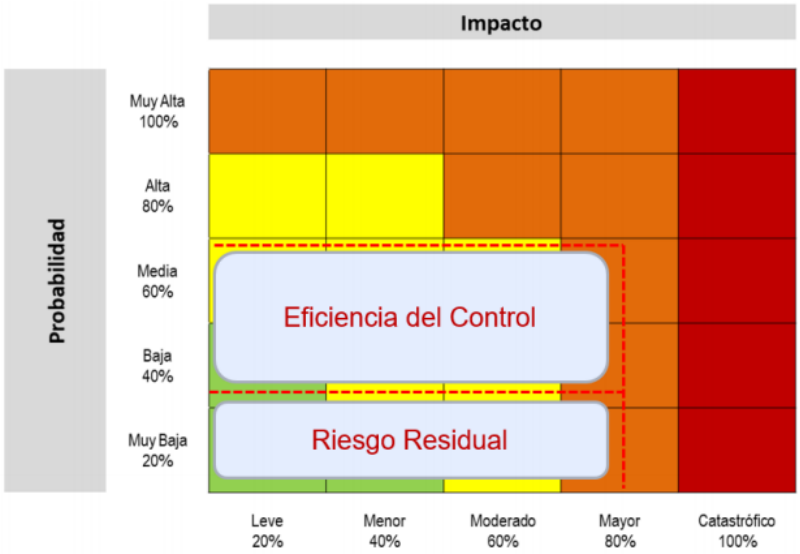
- ✓ **PROCESO:** gestión de recursos

- ✓ **OBJETIVO:** adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación
- ✓ **RIESGO IDENTIFICADO:** posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.
- ✓ **PROBABILIDAD RESIDUAL**= baja 25.2%
- ✓ **IMPACTO RESIDUAL:** mayor 80%
- ✓ **ZONA DE RIESGO RESIDUAL:** alta

Para este caso, si bien el riesgo se mantiene en zona alta, **se bajó el nivel de probabilidad de ocurrencia del riesgo.**

En la figura 9 se observa el movimiento en la matriz de calor correspondiente al ejemplo descrito.

Figura 9. Movimiento en la matriz de calor con el ejemplo propuesto



Fuente: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - V5", 2020

Nota: En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

10.3.3. Estrategias para combatir el riesgo (opciones de manejo transversales)

Consiste en decidir cómo actuar frente a un determinado nivel de riesgo, esta decisión puede ser **ACEPTAR, REDUCIR O EVITAR**.

Para procesos en funcionamiento la decisión se toma a partir del riesgo residual. Cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

En la figura 10 se aprecia las estrategias opciones de manejo y su relación con la necesidad de definir planes de acción en el mapa de riesgos.

Figura 10. Estrategias para combatir el riesgo

Fuente: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - V5", 2020

Los líderes de proceso deben evaluar las opciones existentes en materia de tratamiento de riesgo, partiendo de la política de administración de riesgos y teniendo en cuenta su importancia, los efectos que puede tener sobre la entidad, su probabilidad e impacto y la relación costo-beneficio de las medidas de tratamiento.

El tratamiento es una decisión que se toma frente a un determinado nivel de riesgo. Se analiza frente al Riesgo Residual.

Las opciones para el tratamiento del riesgo son:

- **ACEPTAR EL RIESGO:** Asumir el mismo conociendo los efectos de su posible materialización.
- **REDUCIR EL RIESGO**: Se determina tratarlo mediante transferencia o mitigación del mismo.
- **EVITAR EL RIESGO**: Se determina NO asumir la actividad que genera este riesgo.

Estrategia de reducción del riesgo

- **TRANSFERIR:** Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.
- **MITIGAR:** Después de realizar un análisis y considerar los niveles de riesgo se implementan controles que mitiguen el nivel de riesgo.

Frente al plan de acción referido para la opción de REDUCIR, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos (no necesariamente es un control adicional).
Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique:

i) Responsable,
ii) Fecha de implementación, y
iii) Fecha de seguimiento.

Nota: El plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca en el Plan de Continuidad de Negocio y se consideraría un control correctivo.

10.3.4. Herramientas para la gestión del riesgo

Como producto de la aplicación de la metodología, se contará con los mapas de riesgo. Además de esta herramienta, se tienen las siguientes:

a) **Gestión de eventos:** un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el

riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología.

Algunas fuentes para establecer una base histórica de eventos pueden ser la información suministrada por:

- Mesa de ayuda
- Las PQRD (peticiones, quejas, reclamos, denuncias)
- Oficina Jurídica
- Líneas internas de denuncia – Oficial de Transparencia

Este mecanismo genera información para que el evento no se vuelva a presentar, así mismo, permite el análisis de tendencia frente al desempeño de los controles así:

Desempeño del control= # eventos / frecuencia del riesgo (# veces que se hace la actividad)

b) Indicadores clave de riesgo-KRI: hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar. Un indicador clave de riesgo, o KRI, por su sigla en inglés (Key Risk Indicators), permite capturar la ocurrencia de un incidente que se asocia a un riesgo identificado previamente y que es considerado alto, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos. En la siguiente tabla se muestran algunos ejemplos de estos indicadores:

Figura 11. Ejemplos indicadores clave de riesgo

PROCESO ASOCIADO	INDICADOR	MÉTRICA
TIC	Tiempo de interrupción de aplicativos críticos en el mes	Número de horas de interrupción de aplicativos críticos al mes
FINANCIERA	Reportes emitidos al regulador fuera del tiempo establecido	Número de reportes mensuales remitidos fuera de términos
ATENCIÓN AL USUARIO	Reclamos de usuarios por incumplimiento a términos de ley o reiteraciones de solicitudes por conceptos no adecuados	% solicitudes mensuales fuera de términos % solicitudes reiteradas por tema
ADMINISTRATIVO Y FINANCIERA	Errores en transacciones y su impacto en la gestión presupuestal	Volumen de transacciones al mes sobre la capacidad disponible
TALENTO HUMANO	Rotación de personal	% de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses

Fuente: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - V5", 2020

11. LINEAMIENTOS SOBRE RIESGOS DE CORRUPCIÓN

Teniendo en cuenta que el Gobierno Nacional viene impulsando y desarrollando diferentes políticas públicas con miras a disminuir los niveles de corrupción en todos los ámbitos, la Secretaría de Transparencia de la Presidencia de la República en cumplimiento del artículo 73 de la Ley 1474 de 2011 diseñó una metodología para que todas las entidades determinen su Plan Anticorrupción y de Atención al ciudadano, la cual contempla como uno de sus componentes el levantamiento de los mapas de riesgos asociados a posibles hechos de corrupción.

Entendiendo que los riesgos de corrupción se convierten en una tipología de riesgos que debe ser controlada por la entidad, éstos deben incorporarse en primera instancia en el mapa de riesgos del proceso, sobre el cual se han identificado, de modo tal que el responsable o líder del mismo pueda realizar el seguimiento correspondiente, en conjunto con los riesgos de gestión propios del proceso, lo que promueve que el responsable tenga una mirada integral de todos los riesgos que pueden llegar a afectar el desarrollo de su proceso.

Generalidades:

Teniendo en cuenta las definiciones dadas frente a la corrupción, esta guía define:

- ✓ Los hechos de corrupción son inaceptables e indeseables.
- ✓ El riesgo de corrupción debería tratar de evitarse, estableciendo controles para el hecho de corrupción.
- ✓ **Elaboración**: el mapa de riesgos de corrupción lo elabora anualmente cada responsable de proceso al interior del Ministerio, junto con su equipo de trabajo. El registro del mismo queda en el aplicativo SIG en el módulo de riesgos.
- ✓ **Consolidación:** la Subdirección de Desarrollo Organizacional, como administradora del Sistema Integrado de Gestión, será la encargada de consolidar el mapa de riesgos de corrupción.
- ✓ **Publicación del mapa de riesgos de corrupción:** se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año. La publicación será parcial y fundamentada en la elaboración del índice de información clasificada y reservada. En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014. En este caso se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la publicación.
- ✓ **Socialización:** Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación. Para lograr este propósito la Subdirección de Desarrollo Organizacional diseñará las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos de corrupción.
  Así mismo, se adelantarán las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de corrupción, dejando la evidencia del proceso de socialización y publicación de sus resultados.
- ✓ **Ajustes y modificaciones:** Después de su publicación y durante el respectivo año de vigencia, los líderes de proceso podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el Mapa de Riesgos de Corrupción realizando la solicitud correspondiente ante la Subdirección de

Desarrollo Organizacional. En este caso, deberán dejar por escrito los ajustes, modificaciones o inclusiones realizadas.

- ✓ **Monitoreo:** en concordancia con la cultura del autocontrol al interior del Ministerio, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción, de conformidad con la periodicidad definida en la circular de reportes de cada vigencia. En el tema concreto de los riesgos de soborno, el Oficial de Transparencia y el Equipo de Transparencia periódicamente harán monitoreo de los riesgos detectados y de los controles implementados
- ✓ **Seguimiento:** La Oficina de Control Interno realizará el seguimiento a la gestión de riesgos de corrupción. En este sentido, incluirá en sus procesos de auditoría interna, el análisis de las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción. Para los riesgos institucionales, de procesos y del SGSI, SGSST y SGA, las frecuencias de seguimiento y reporte de avances en el plan de tratamiento, por parte de los líderes y responsables de proceso se deben realizar de conformidad con lo establecido en la circular de reportes de la vigencia, de forma que permitan que el autocontrol realizado sea la base para la toma de decisiones, y que se logren introducir correctivos en el momento adecuado.
  Para el caso de los riesgos de corrupción, la periodicidad de su establecimiento, revisión, actualización y seguimiento se ejecutará de conformidad con las fechas establecidas por la guía denominada "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano". El seguimiento adelantado por la Oficina de Control Interno se debe publicar en la página Web del Ministerio.

11.1. Directrices de redacción para riesgos de corrupción

El riesgo de corrupción es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. "Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos" (Conpes N° 167 de 2013).

Es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

- Los riesgos de corrupción se establecen sobre procesos.

- 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.
- 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 como guía de la figura 12 lineamientos descripción riesgo de corrupción.

Figura 12 Lineamientos descripción riesgo de corrupción

Fuente: Elaboración propia SDO

IMPORTANTE: Los riesgos de corrupción y/o soborno, siempre deben gestionarse.

11.2. Identificación Riesgos de Soborno

Los riesgos de soborno están catalogados como riesgos de corrupción, es decir que los riesgos identificados como de soborno se deben evaluar frente a las siguientes directrices:

11.3. Riesgos de Corrupción y Soborno relacionados con los trámites

Siguiendo los estipulado en el “Protocolo para la identificación de riesgos de corrupción asociados a la prestación de trámites y servicios” del DAFP se estableció:

Los riesgos de corrupción y/o soborno en trámites se pueden presentar en dos momentos:

a) En el momento de efectuar el trámite propiamente dicho, cuando interactúan el ciudadano y el servidor (es decir de la ventanilla hacia afuera de la entidad por ejemplo cuando el ciudadano presenta un documento o efectúa un pago)

b) En el momento en que se ejecutan los procedimientos al interior de la entidad para dar cumplimiento al trámite (de la ventanilla hacia adentro. La entidad tiene procedimientos internos, como por ejemplo distribuir la documentación recibida entre las áreas internas cambiando el turno).

El riesgo de Corrupción y/o Soborno en relación con los trámites se puede llegar a materializar de acuerdo con la siguiente clasificación de las causas:

a) **Oportunidad:** Falta de controles internos y externos efectivos en los procesos, procedimientos y ausencia de controles en el desarrollo de los trámites.
   - Poca información al ciudadano
   - Desorganización en la información
   - Inexistencia de procesos y procedimientos claros
   - Confianza excesiva en los trabajadores (servidores públicos)
   - Pocas acciones de rendición de cuentas
   - Poca o débil vigilancia

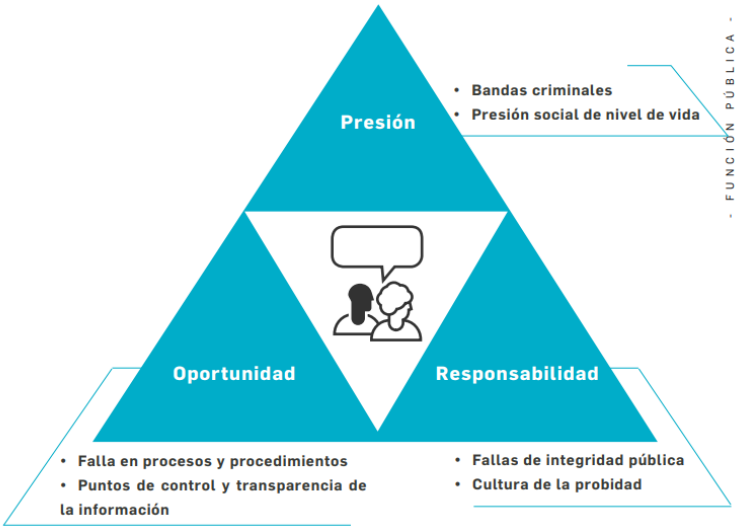
b) **Responsabilidad:** Las fallas éticas y de compromiso con lo público que afectan un desarrollo objetivo e imparcial en el manejo y regulación de los recursos públicos.
c) **Presión:** Existen factores externos e internos que afectan las conductas de integridad pública y propician riesgos de corrupción.

Los siguientes son los pasos para identificar las causas relacionadas con los riesgos de corrupción y soborno en los trámites:

- PASO 1: Identificar si en el proceso se encuentran trámites que solicita el ciudadano y de estos cuales son propensos a riesgos de corrupción.
- PASO 2: Identificar los puntos sensibles o vulnerables dentro del procedimiento de los trámites, con ayuda del Triángulo de la Corrupción que propone el instructivo del protocolo para trámites.
- PASO 3: Analizar las debilidades que pueden ser causas de hechos de corrupción en las actividades asociadas al trámite en la entidad, así como las amenazas del entorno (factor externo).

Los trámites en general tienen alrededor de 12 actividades, de las cuales las cuatro (4) que se mencionan en el siguiente cuadro son las que presentan mayor riesgo de Corrupción y Soborno

Figura 13 Triángulo de la Corrupción



Fuente: IGA- Procuraduría General (AL, 2012) - basada en Donald R. Cressey.
Tomado de: DAFP 2018 – Anexo 3. Protocolo para la identificación de riesgos de corrupción asociados a la prestación de trámites y servicios

Figura 14 Etapas en los trámites propicias al riesgo

	TENGA EN CUENTA: ☆		
	Proceso	**Oportunidad que propicia el riesgo de corrupción**	
1	☆ Entidad divulga la información del trámite y los requisitos	Si no hay información clara previa a la gestión del trámite	Se pueden formar redes de tramitadores que incrementan los costos administrativos al usuario
3	☆ Usuario radica los documentos o presenta la solicitud	Si hay excesiva demanda y demora en tiempo de atención o se atiende por fuera de turnos	* Se busca tramitadores para agilizar el tiempo de radicación * Compra de turnos afectando la igualdad en la gestión del trámite
5	☆ Entidad revisa que los documentos estén completos	* Inexistencia de mecanismos que validen la veracidad de los requisitos acreditados * No hay criterios técnicos o jurídicos claros para determinar la calidad del requisito * No existen mecanismos de seguridad informática	* Buscan tramitadores para alterar o para adquirir documentación falsa * Buscan tramitadores para justificar la calidad del requisito por fuera de la norma técnica * Sobornos para borrar información institucional en beneficio propio
7	☆ Pago asociado al trámite	* Recepción directa de dinero sin mecanismos de registros * Inexistencia de sistemas de liquidación con auditorías * Certificaciones de pago sin mecanismos de verificación directos	* Apropiación de dineros públicos por servidores corruptos * Se realizan pagos por debajo de la tarifa oficial * Pago por sellos adulterados para simular pagos institucionales

Fuente: DAFP 2018 – Anexo 3. Protocolo para la identificación de riesgos de corrupción asociados a la prestación de trámites y servicios.

Para identificar las causas que pueden originar riesgos de corrupción y/o soborno se adaptó del protocolo para la identificación de riesgos de corrupción asociados a la prestación de trámites y servicios la siguiente herramienta:

Tabla 9: Priorización de las causas en relación con los Riesgos de Corrupción y/o Soborno

Denominación del Trámite	Posibles causas de hechos de corrupción en actividades asociadas al trámite	Respuesta (*seleccione con* X)		Nivel de criticidad de la causa	Priorización de la causa - Marque con X (Máx 3)	Redacte como Causa la selección de priorización
		SI	NO			
	1 ¿Los servidores del área de radicación efectúan registros manuales ?					
	2. ¿Los servidores del área de radicación manejan dinero de los usuarios o información privilegiada que pueda afectar la dinámica del mercado?					
	3 ¿Los servidores del área evidencian niveles de vida por encima del promedio del salario?					
	4 ¿El sistema de turnos es asignado manualmente con criterios de discrecionalidad del servidor?					
	5 ¿Existe una caja menor o cuentas para recibir dineros correspondientes a trámites?					
	6. ¿Existe exceso de procedimientos y participación de varios funcionarios que interviene en la relación con el ciudadano?					
	7. ¿Existe perdida de los documentos aportados por el usuario?					
	8. ¿Existen duda de legalidad de los requisitos acreditados por los ciudadanos?					
	9. ¿Se evidencia relaciones de amistad entre los servidores y tramitadores u oficinas especializadas en la gestión de trámites?					
	10. ¿Los niveles salariales de los funcionarios que atienden					

Denominación del Trámite	Posibles causas de hechos de corrupción en actividades asociadas al trámite	Respuesta (*seleccione con* X)		Nivel de criticidad de la causa	Priorización de la causa - Marque con X (Máx 3)	Redacte como Causa la selección de priorización
		SI	NO			
	los trámites, no se ajustan a la complejidad de su función?					
	11. ¿Hay deficiencia en los controles de la gestión de trámites a diario?					
	12. ¿Existe presiòn sobre la autonomía profesional para el análisis de requisitos y manipulación de decisiones por encima de la decisión técnica?					
	13. ¿Existen fases de análisis de los requisitos con excesiva reserva que impida la transparencia en el proceso?					
	14. ¿La Discrecionalidad está por encima de los parámetros técnicos que frenen el proceso?					
	15. ¿Se presenta interpretación subjetiva de las normas o reglamentos, por falta de bancos de conceptos técnicos y jurídicos?					
	16. ¿Existen actores de presión en el tema regulado por el trámite que puedan incidir en las decisiones institucionales?					
	17. ¿Existen servidores que tengan nexos con la temática que regulan?					
	18. ¿La complejidad de los procedimientos del trámite desborda la capacidad de comprensión del usuario?					
	19. ¿Existen espacios o puntos de encuentro entre el servidor y el usuario?					
	20. ¿Las diferentes etapas del trámite se realizan de manera presencial sin ayuda de los recursos tecnològicos?					
	21. ¿Falta información clara?					

Denominación del Trámite	Posibles causas de hechos de corrupción en actividades asociadas al trámite	Respuesta (*seleccione con* X)		Nivel de criticidad de la causa	Priorización de la causa - Marque con X (Máx 3)	Redacte como Causa la selección de priorización
		SI	NO			
	22. ¿Hay fallas en la cultura de la probidad (honradez)?					
	23. ¿Los sistemas de información carecen de controles?					
	24. ¿Se evidencia falsificación en los documentos?					
	25. ¿Hay debilidad en los canales de acceso a la publicidad de las condiciones del trámite?					
	26. ¿El proceso de radicación presencial es complejo?					
	27. ¿Se evidencia debilidad en los controles existentes en los procesos y procedimientos?					
	28. ¿Falta comportamientos de integridad de lo público del servidor que revisa?					
	29. ¿Falta controles administrativos en el proceso de revisión?					
	30. ¿Se evidencia falsificación o manipulación en la información?					
	31. ¿Falta control en el proceso financiero de pagos?					
	32. ¿Falta comportamientos de integridad de lo público del servidor que decide la solicitud?					
	33. ¿Se presentan fallas en el sistema de gestión documental para comunicar o notificar?					
	34. ¿Se presentan fallas en los canales de información?					

Fuente: Adaptación protocolo para la identificación de riesgos de corrupción asociados a la prestación de trámites y servicios del DAFP

11.4. Valoración de riesgos de corrupción y/o Soborno

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

Figura 15 Criterios para calificar la probabilidad en Riesgos de corrupción

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: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - V5", 2020

Figura 16 Matriz de priorización de probabilidad.

N.°	RIESGO	P1	P2	P3	P4	P5	P6	TOT	PROM	
1	Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad	Se espera que el evento ocurra en la mayoría de las circunstancias.	**5**	**4**	**3**	**5**	**3**	**4**	**24**	**4** PROBABLE
2	Otros riesgos identificados	Es viable que el evento ocurra en la mayoría de las circunstancias.								
3	Otros riesgos	El evento podrá ocurrir en algún momento.								
Convenciones: **N.°**: número consecutivo del riesgo - **P1**: participante 1 P... - **Tot**: total puntaje - **Prom.**: promedio										

Fuente: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – V4", 2018

En caso de que la entidad no cuente con datos históricos sobre el número de eventos que se hayan materializado en un periodo de tiempo, los integrantes del equipo de trabajo deben calificar en privado el nivel de probabilidad en términos de

factibilidad, utilizando la matriz de priorización de probabilidad definida en la Figura 16.

Análisis del 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 responder a 19 preguntas que se presentan en la figura 17.

Figura 17 Criterios para calificar Impacto en los Riesgos de corrupción

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
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.		10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		
CATASTRÓFICO :	Genera consecuencias desastrosas para la entidad		

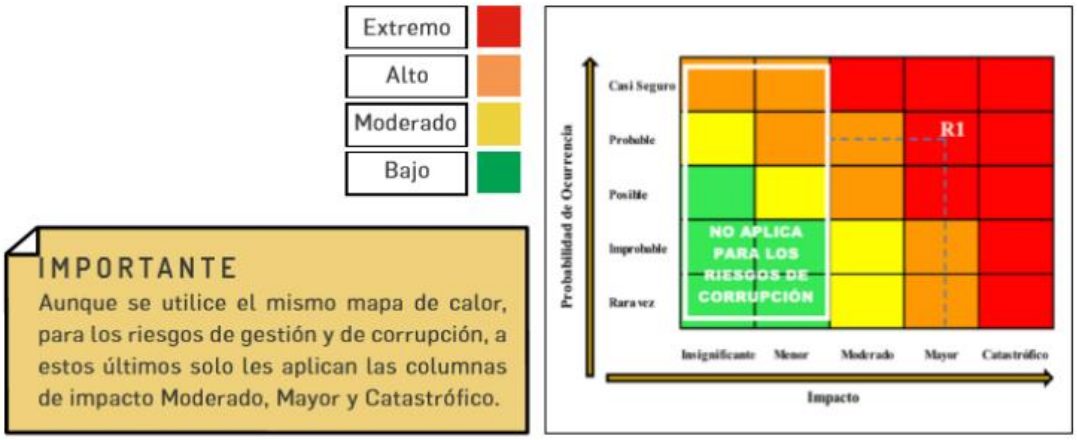
Nivel de impacto MAYOR

Fuente: "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - V5", 2020

Importante: 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.

Por último, ubique en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente.

Figura 18 Análisis del impacto Riesgos de Corrupción



Fuente: “Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - V5”, 2020

Valoración de controles: Se debe considerar lo establecido en el numeral 10 de esta guía, sin embargo, es muy importante considerar que los controles adicionales que sea pertinente establecer deben considerar la “anatomía” de la corrupción y su taxonomía.

El estudio anatómico de la corrupción debe considerar en la entidad su estructura funcional, incluyendo sus fuentes de acceso, el modelo de operación, los posibles delitos que pueden darse y los comportamientos culturalmente reconocidos como “malos”, que logren que, por el uso del poder, por acción u omisión se lleve a un particular a obtener beneficios que deberían estar al servicio de los intereses del Estado y la Comunidad.

Se entiende por taxonomía de la corrupción, la clasificación u ordenación en grupos de acciones de corrupción que se pueden dar en la Entidad. Este análisis

taxonómico de la corrupción debe hacerse en la Entidad y debe incluir las formas de corrupción en los escenarios legales y de integridad.

Algunas formas de corrupción asociadas a la ilegalidad:

Pueden ser formas de corrupción por incumplimiento legal las siguientes:

- ✓ Peculado en cualquiera de sus variantes.
- ✓ Delitos relacionados a la contratación, por ejemplo: Violación del régimen legal o constitucional de inhabilidades e incompatibilidades, Interés indebido en la celebración de contratos, Contrato sin cumplimiento de requisitos legales.
- ✓ Acuerdos restrictivos de la competencia.
- ✓ Tráfico de influencias del servidor público.
- ✓ Tráfico de influencias de particular.
- ✓ Prevaricato.
- ✓ Utilización de asunto sometido a secreto o reserva.
- ✓ Utilización indebida de información privilegiada.
- ✓ Intervención en Política.
- ✓ Hurto.
- ✓ Competencia desleal.

Las fuentes ilegales de la corrupción:

- ✓ Cohecho.
- ✓ Concusión.

Otras formas de corrupción asociadas al comportamiento inmoral:

En especial para las organizaciones privadas, pueden ser tipos de corrupción asociadas a “malos” comportamientos, algunos casos, por ejemplo:

- ✓ Alteración de propuestas comerciales.
- ✓ Abstención de presentación correcta de ofertas.
- ✓ Afectación deliberada de la buena reputación.
- ✓ Afectación de licencias de funcionamiento por abstención de cumplir las obligaciones.

A continuación, se desarrolla un ejemplo aplicando la metodología, atendiendo la siguiente información:

- ✓ **PROCESO:** Contratación.
- ✓ **OBJETIVO:** Ejecutar las etapas precontractual y contractual en las diferentes modalidades en esta materia, acorde con el Plan Anual de Adquisiciones aprobado para cada vigencia.
- ✓ **ALCANCE:** Inicia con el análisis de las contrataciones aprobadas en el plan anual de adquisiciones y termina con las compras y contrataciones requeridas y la asignación de supervisores o interventores (según aplique).
- ✓ **HECHO DE CORRUPCIÓN (TOMADO DE LA PROPUESTA DE RIESGOS TIPO):** Aplicar criterios de selección de contratistas que favorezcan de manera no objetiva ni imparcial la adjudicación, con el ánimo de obtener beneficios particulares.
- ✓ **Riesgo identificado:** Posibilidad de reducción de la capacidad financiera del Estado para atender el suministro de bienes y servicios que son requeridos por la inversión pública y el funcionamiento.
- ✓ **No. de veces que se ejecuta la actividad**: La actividad de contratos implican 20 en el mes = 240 contratos en el año.
- ✓ **Cálculo pérdida económica:** De llegar a materializarse tendría afectación económica de 1000 SMLMV.

Desarrollo del ejemplo:

No. Control	Descripción del Control	Afectación		Atributos						Probabilidad Residual (2 controles)	Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Final	Tratamiento
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia							
1	Para la etapa precontractual, el (la) Secretario(a) General en el marco del comité de contratación valida los estudios previos presentados por los líderes de proceso responsables, atendiendo la modalidad de contratación en cada caso, las decisiones tomadas son registradas en las actas del comité, firmadas por los miembros del mismo, permitiendo continuar las etapas subsiguientes de los procesos contractuales correspondientes.	X		Preventivo	Manual	40%	Documentado	Continua	Con Registro	36%	Muy Baja	25,2%	Mayor	80%	Alta	Reducir

12. MONITOREO (SDO) Y SEGUIMIENTO (OCI)

Una vez se han implementado el plan de manejo del riesgo, se debe realizar el monitoreo y seguimiento a los mismos, de conformidad con la dimensión del MIPG de “Control Interno”, que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles que se explicó en el apartado 8 de este documento.

A los riesgos de proceso y de corrupción se les hace monitoreo trimestral (SDO) y seguimiento trimestral (OCI).

Para los riesgos de los modelos referenciales que conforman el Sistema de Integrado de Gestión las frecuencias de seguimiento y reporte de avances en el plan de tratamiento, por parte de los líderes y responsables de proceso se deben realizar de conformidad con lo establecido en la circular de reportes de la vigencia, de forma que permitan que el autocontrol realizado sea la base para la toma de decisiones, y que se logren introducir correctivos en el momento adecuado.

Para el caso de los riesgos de corrupción, la periodicidad de su establecimiento, revisión, actualización, monitoreo y seguimiento se ejecutará de conformidad con las fechas establecidas por la guía denominada “Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano”. El seguimiento adelantado por la Oficina de Control Interno se debe publicar en la página Web del Ministerio.

13. ACTUALIZACIÓN DEL MAPA DE RIESGOS

El mapa de riesgos de la entidad debe ser actualizado cuando el proceso evaluado presente cambios organizacionales, como objetivo, alcance y/o actividades, o cuando el contexto estratégico presente un cambio significativo que requiere la revisión completa de los riesgos gestionados, teniendo como mínimo una revisión y/o actualización anual a partir de la última fecha de revisión.

Los riesgos identificados podrán ser actualizados de forma individual, cuando así se requiera, tomando como insumos las necesidades de ajuste identificadas en auditorías internas, revisión por la dirección, auditorías externas o resultado de las acciones de seguimiento y autocontrol ejecutadas por los líderes y responsables de proceso.

La actualización o ajuste estará a cargo de los líderes y responsables de procesos, quienes con el acompañamiento de la Subdirección de Desarrollo Organizacional y basados en las recomendaciones de seguimiento generadas por la Oficina de Control Interno, auditorías internas, revisión por la dirección o auditorías externas procederán a realizar los ajustes de los riesgos a su cargo.

14. COMUNICACIÓN Y CONSULTA

Teniendo en cuenta que la comunicación y consulta con las partes involucradas tanto internas como externas debe tener lugar durante todas las etapas del proceso para la gestión del riesgo, el Ministerio de Educación Nacional determina las siguientes actividades:

- El mapa de Riesgos deberá ser divulgado y estará cargado en el módulo de Riesgo del SIG para consulta al interior de la entidad.
- Los líderes y responsables de cada proceso deben divulgar y sensibilizar al interior de sus dependencias el mapa de riesgos junto con el plan de acción definido en el caso de que la opción del tratamiento del riesgo sea REDUCIR.
- La Subdirección de Desarrollo Organizacional y la Oficina de Control Interno, impulsarán a nivel institucional una cultura de gestión del riesgo, a través de capacitaciones, mesas de trabajo y asesorías, con el fin de mejorar el conocimiento y apropiación del pensamiento basado en riesgos.
- Las acciones de tratamiento de los riesgos priorizados que involucren partes interesadas o terceros serán dadas a conocer, por parte de los líderes y responsables de cada proceso.
- La consolidación del Mapa de Riesgos de Corrupción le corresponde realizarla a la Subdirección de Desarrollo Organizacional o quien haga sus veces, quien servirá de facilitador en el proceso de Gestión de Riesgos de Corrupción con las dependencias.
- La consulta y divulgación del Mapa de Riesgos de Corrupción a partes interesadas y comunidad en general se realizará a través de su publicación en la página Web del Ministerio.

15. GESTIÓN DEL RIESGO AMBIENTAL

15.1. Identificación de riesgos en el Sistema de Gestión Ambiental

En la identificación de las amenazas u oportunidades relacionadas con el **Sistema de Gestión Ambiental**, se deben tener en cuenta las fuentes que pueden producir

Riesgo para el ambiente y las fuentes que pueden producir **Riesgo para la entidad debido a temas relacionados con el ambiente.** A continuación se describe la aplicación para cada uno de ellos.

15.2. Identificación de riesgos para el ambiente

Fuentes que pueden generar riesgo para el ambiente: El Ministerio de Educación Nacional cuenta con una ficha técnica que tiene por objetivo *"Establecer los lineamientos generales del procedimiento identificación, evaluación y determinación del nivel de significancia de los impactos ambientales generados por los procesos, las actividades y servicios desarrollados por el Ministerio de Educación Nacional* ***Identificación y valoración de aspectos e impactos*****"** y cuyo alcance inicia con la identificación de los aspectos ambientales, los impactos generados por los mismos, la valoración del impacto y finaliza con la determinación de significancia y el método de manejo de los impactos para su mitigación. Por lo anterior la identificación, valoración y análisis del riesgo ambiental se plasma en el formato **PM-FT-02 - Identificación y valoración de aspectos e impactos ambientales.**

Tabla 10. Fuente de amenazas u oportunidades comunes para la identificación de Riesgos para el ambiente - Sistema de Gestión Ambiental

Fuentes	Descripción
Resultados de la evaluación de los aspectos e impactos ambientales	Pueden crear riesgos u oportunidades asociados con impactos ambientales adversos, impactos ambientales beneficiosos y otros efectos para la entidad y estos se pueden determinar como parte de la evaluación de la significancia.
Resultados de la medición de las condiciones ambientales	Pueden crear riesgos u oportunidades asociados con impactos ambientales adversos, impactos ambientales beneficiosos y otros efectos para la entidad y estos se pueden determinar como parte de la evaluación de la significancia.
Situaciones de Emergencia	Pueden generar riesgos asociados a impactos ambientales adversos u otros efectos en la entidad, por ejemplo: - Internos, derrames químicos al medio ambiente debido al no entendimiento de los procedimientos. - Externos, incremento de inundaciones debido al cambio climático, que pueden afectar a las instalaciones de la entidad.

Fuente: Elaboración propia

15.3. Identificación de riesgos para la entidad debido a temas relacionados con el ambiente

Fuentes que pueden generar riesgo para la entidad debido a temas relacionados con el ambiente: Los riesgos asociados a estas fuentes se evaluan conforme la metodología descrita en la presente guía; teniendo en cuenta que son generados por las actividades que ejecuta la entidad relacionadas con la gestión ambiental, que si llegacen a presentarse pueden ocacionar incumplimiento legal, pérdidas de recursos, multas, reputación, costos por no asegurar y mantener los permisos y licencias para el desarrollo de las actividades operativas (Estos se identifican por medio de la Matriz de Riesgos descrita en la metodología de la presente guía).

Tabla 11. Fuente de amenazas u oportunidades comunes para la identificación de Riesgos para el ambiente - Sistema de Gestión Ambiental

Fuentes	Descripción
Resultado de la identificación y/o evaluación de las obligaciones de cumplimiento u otros requisitos	Estos pueden crear riesgos y oportunidades, tales como incumplimiento (que puede afectar a la reputación de la entidad o dar como resultado una acción legal) o ir más allá de sus requisitos legales y otros requisitos (que pueden mejorar la reputación de la entidad).
Requerimientos de partes interesadas (PQR Ambientales)	La entidad también puede tener riesgos relacionados con otras cuestiones, que incluyen las necesidades y expectativas de las partes interesadas.
Alcance del sistema de gestión ambiental	Se pueden identificar riesgos asociados al alance frente a la capacidad de la entidad para lograr los resultados previstos de su sistema de gestión ambiental.
Medición de indicadores de los procesos	Se pueden identificar riesgos asociados a los resultados de los indicadores ambientales frente a las acciones propuestas de ahorro y uso eficiente de los residuos en la entidad para lograr los resultados previstos de su sistema de gestión ambiental.
Factores relacionados a situaciones económicas, políticas	Riesgos que se pueden presentar por factores relacionados a situaciones económicas, políticas - Internos, falta de recursos disponibles para mantener un sistema de gestión ambiental eficaz, debido a limitaciones económicas. - Externo, Introducción de nueva tecnología subvencionada por el gobierno, que puede mejorar la calidad del aire.

Fuente: Elaboración propia

15.4. Análisis de riesgos ambientales

Esta etapa busca establecer tanto la probabilidad de ocurrencia del riesgo como la consecuencia o impacto; por lo anterior el análisis se lleva a cabo de la siguiente manera:

15.4.1. Análisis de riesgos para el ambiente

De acuerdo con la identificación de aspectos e impactos ambientales, se realiza el análisis y evaluación de acuerdo con la afectación que causa el aspecto e impacto ambiental con base en los criterios descritos en el documento para Identificar y valorar aspectos e impactos ambientales del MEN.

15.4.2. Análisis de riesgos para la entidad debido a temas relacionados con el ambiente

El análisis se realiza de acuerdo con lo descrito en el Análisis de Riesgos del presente documento.

15.5. Tratamiento del riesgo ambientales

El tratamiento de los riesgos involucra identificar las opciones para tratar los riesgos residuales priorizados o los impactos identificados como significativos.

Se identifican las acciones de acuerdo con el nivel de significancia identificada en la evaluación del impacto ambiental, descritas en la Matriz de Identificación y Valoración de Aspectos e Impactos Ambientales.

15.5.1. Tratamiento del riesgo para la entidad debido a temas relacionados con el ambiente

El tratamiento se realiza de acuerdo con lo descrito en el numeral de Evaluación del riesgo. Los planes de manejo se pueden enfocar en la implementación de los siguientes ítems:

- Programa de gestión integral de residuos
- Supervisión del cumplimiento de las obligaciones ambientales de los contratos
- Programa de uso eficiente y ahorro de energía

- Programa de uso eficiente y ahorro de agua
- Actividades de control operacional ambiental
- Planes de mantenimiento
- Plan de emergencias y Contingencias
- Plan de Gestión Integral de Residuos
- Otras que se identifiquen

16. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

16.1. Identificación de Riesgos de Seguridad de la Información

En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al Modelo de Seguridad y Privacidad de la Información (MSPI)[2], el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: Seguridad de la información, Arquitectura, Servicios ciudadanos digitales.
La identificación de los riesgos de seguridad de la información está determinada por las amenazas o vulnerabilidades relacionadas con los activos de información que tiene cada proceso bajo su responsabilidad.

Es importante considerar que las amenazas pueden causar daño temporal o permanente a los activos, procesos y sistemas de información de la entidad y algunas de ellas pueden afectar a más de un activo y pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

16.2. Identificación de activos de seguridad de la información

Activos de información: Un activo de información es cualquier elemento que tenga valor para la organización y que participe en el tratamiento de información, sin embargo, en el contexto de seguridad de la información son activos de información elementos tales como: hardware, software, red, personal, lugar y organización.

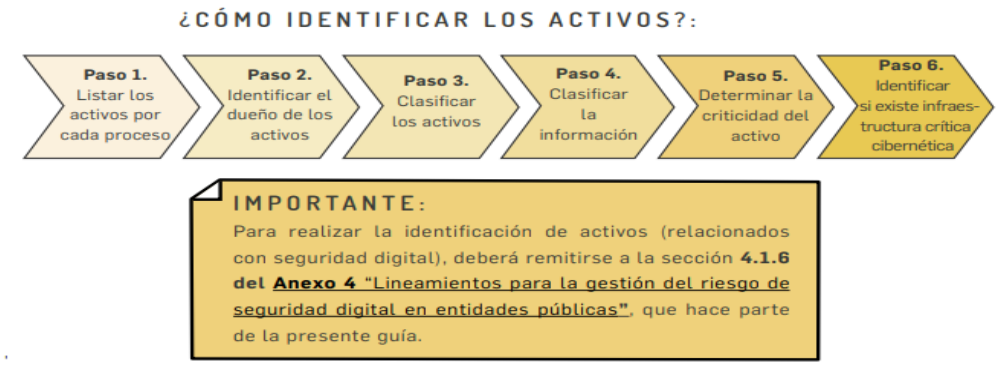
La entidad puede saber **qué es lo que debe proteger para garantizar su funcionamiento, tanto interno como su funcionamiento de cara al ciudadano**, aumentando así su confianza en el uso del entorno digital.

[2] Tomado de: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

Permite determinar **qué es lo más importante que la entidad y sus procesos poseen** (sean bases de datos, archivos, servidores web o aplicaciones claves para que la entidad pueda prestar sus servicios).

Cómo se identifican los activos de información:

Figura 19 Identificación de activos de información



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 4

16.3. Identificación del riesgo de seguridad de la información

Riesgos inherentes de seguridad de la información:

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

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto es necesario consultar el Anexo 4 "Modelo Nacional de Gestión de Riesgos de Seguridad de la Información para entidades públicas" donde se encuentran las siguientes tablas necesarias para este análisis:

- ✓ Tabla 5. Tabla de amenazas comunes
- ✓ Tabla 6. Tabla de amenazas dirigida por el hombre
- ✓ Tabla 7. Tabla de Vulnerabilidades Comunes

Nota Importante: La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.
En la Identificación de Riesgos – Tabla 12. Amenazas comunes para el Sistema de Gestión de Seguridad de la Información de esta Guía se detalla un listado de las amenazas para tener en cuenta cuando se está realizando la identificación de riesgos de seguridad de la información.

Las vulnerabilidades son fallas o debilidades que afectan la confidencialidad, integridad y disponibilidad de la información. En la Identificación de Riesgos - Tabla 13. Ejemplos vulnerabilidades y amenazas por tipo de activo se detallan las amenazas y vulnerabilidades más comunes que pueden afectar los principios de seguridad de la información en la Entidad.

En la identificación de las amenazas o vulnerabilidades relacionadas con el **Sistema de Gestión de Seguridad de la Información** es necesario tener en cuenta cuáles y cuantos activos de información tiene cada proceso bajo su responsabilidad. Es importante considerar que las amenazas pueden causar daño temporal o permanente a los activos, procesos y sistemas de soporte de la entidad. Algunas amenazas pueden afectar a más de un activo y pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

Con el fin de facilitar la identificación de estos riesgos, se describen una serie de amenazas comunes para el Sistema de Gestión de Seguridad de la Información, con el fin de orientar la identificación de los riesgos relacionados:

Tabla 12. Amenazas comunes para el Sistema de Gestión de Seguridad de la Información

TIPO	AMENAZA
Daño Físico	Fuego
	Agua
	Accidente
	Destrucción del equipo
	Polvo, corrosión, congelamiento
Eventos Naturales	Fenómenos climáticos
	Fenómenos volcánicos
	Fenómenos meteorológicos
Pérdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado
	Pérdida de suministro de energía
	Falla en equipo de telecomunicaciones

TIPO	AMENAZA
Perturbación debida a la radiación	Radiación electromagnética
	Radiación térmica
	Impulsos electromagnéticos
Compromiso de la información	Interceptación de señales
	Espionaje remoto
	Hurto de medios o documentos
	Hurto de equipos
	Recuperación de medios reciclados o desechados
	Divulgación no autorizada
	Datos provenientes de fuentes no confiables
	Manipulación con software
	Manipulación con hardware
	Detección de información
Fallas Técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento del sistema de información
Acciones no autorizadas	Uso no autorizado dele equipo
	Copia fraudulenta del software
	Uso de software falso o copiado
	Corrupción de los datos
	Procesamiento ilegal de datos
Compromiso de las funciones	Error en el uso
	Abuso de derechos
	Falsificación de derechos
	Negación de acciones
	Incumplimiento en la disponibilidad del personal

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC 2018.

Las vulnerabilidades del Sistema de Gestión de Seguridad de la Información son fallas o debilidades que afectan la confidencialidad, integridad y disponibilidad de los sistemas. La identificación podrá obtenerse de pruebas de vulnerabilidad, visitas, entrevistas y/o basados en los criterios que la entidad vea necesarios.

Las posibles amenazas y vulnerabilidades que ocasionan la aparición de un riesgo sobre un activo de información se relacionan a continuación, teniendo en cuenta el tipo de activo:

Tabla 13. Ejemplos vulnerabilidades y amenazas por tipo de activo

TIPO DE ACTIVO	EJEMPLO DE VULNERABILIDADES	EJEMPLO DE AMENAZAS
HARDWARE	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de temperatura	Pérdida del suministro de energía
	Almacenamiento sin protección	Hurto de medios o documentos
SOFTWARE	Ausencia de logs de auditoria	Abuso de derechos
	Ausencia de documentación	Error en el uso
	Tablas de contraseñas sin protección	Falsificación de derechos
	Ausencia de control de cambios eficaz	Manipulación con software
RED	Arquitectura de red insegura	Espionaje remoto
	Envío de contraseñas en texto claro	Espionaje remoto
	Gestión inadecuada de la red	Saturación del sistema de información
PERSONAL	Ausencia de personal	Incumplimiento en la disponibilidad del personal
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de políticas para el uso correcto del correo electrónico	Uso no autorizado del equipo
ORGANIZACIÓN	Ausencia de auditorias	Abuso de derechos
	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de derechos
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimientos para el manejo de la información	Error en el uso

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC 2018.

16.4. Controles asociados a la seguridad de la información

En el Ministerio de Educación Nacional se podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del 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", siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado será necesario considerar las características de Diseño y Ejecución definidas para su valoración.

A continuación, se incluyen algunos ejemplos de controles y los dominios a los que pertenecen, la lista completa se encuentra en del documento maestro del Modelo de Seguridad y Privacidad de la Información – MSPI:

Procedimientos operacionales y responsabilidades	**Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.**
Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	**Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.**
Controles contra códigos maliciosos	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
Copias de respaldo	**Objetivo: Proteger contra la pérdida de datos.**

Procedimientos operacionales y responsabilidades	Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
Respaldo de información	Control: Se deben hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC 2018.

16.5. Tratamiento para los Riesgos de Seguridad de la Información

Para el tratamiento de los riesgos de seguridad de la información se utilizará la metodología propuesta en la presente Guía.

Es importante señalar que para el análisis y valoración de controles de Seguridad de la Información se debe consultar el formato Declaración de Aplicabilidad ISO 27002:2013, en el cual se encuentra la lista de controles de seguridad de la información que podría implementar el Ministerio con el fin de mitigar los riesgos que pueden afectar la integridad, disponibilidad y confidencialidad de la información.

17. RIESGOS DE SEGURIDAD Y SALUD EN EL TRABAJO - SGSST

17.1. Identificación de peligros, SGSST.

En la identificación de los peligros, la valoración de los riesgos y la determinación de controles relacionadas con el **Sistema de Gestión de Seguridad y Salud en el Trabajo**, se deben tener en cuenta las fuentes que pueden producir **peligros para los colaboradores del Ministerio de Educación.**

A continuación se describe la aplicación para cada uno de ellos.

Matriz de Peligros del SGSST

El Ministerio de Educación Nacional cuenta con una ficha técnica que tiene por objetivo *"*Establecer los lineamientos para elaborar, revisar y actualizar la Matriz de Identificación de Peligros, valoración de riesgos y determinación de controles del

MEN, ***Matriz de identificación de peligros, valoración de riegos y determinación de controles"*** y cuyo alcance inicia con la identificación de los peligros en Seguridad y Salud en el Trabajo, las valoración de los riesgos y la determinación de los controles. Por lo anterior la identificación de peligros, valoración de riesgos y determinación de controles se plasma en el formato correspondiente dentro del Sistema Integrado de Gestión.

Medidas de prevención y control SGSST

De acuerdo con lo establecido en el Decreto 1072 de 2015 en su artículo 2.2.4.6.24, las medidas de prevención y control deben adoptarse con base en el análisis de pertinencia, teniendo en cuenta el siguiente esquema de jerarquización:

1. **Eliminación del peligro/riesgo**: Medida que se toma para suprimir (hacer desaparecer) el peligro/riesgo;

2. **Sustitución:** Medida que se toma a fin de remplazar un peligro por otro que no genere riesgo o que genere menos riesgo;

3. **Controles de Ingeniería:** Medidas técnicas para el control del peligro/riesgo en su origen (fuente) o en el medio, tales como el confinamiento (encerramiento) de un peligro o un proceso de trabajo, aislamiento de un proceso peligroso o del trabajador y la ventilación (general y localizada), entre otros;

4. **Controles Administrativos:** Medidas que tienen como fin reducir el tiempo de exposición al peligro, tales como la rotación de personal, cambios en la duración o tipo de la jornada de trabajo. incluyen también la señalización, advertencia, demarcación de zonas de riesgo, implementación de sistemas de alarma, diseño e implementación de procedimientos y trabajos seguros, controles de acceso a áreas de riesgo, permisos de trabajo, entre otros; y,

5. **Equipos y Elementos de Protección Personal y Colectivo:** Medidas basadas en el uso de dispositivos, accesorios y vestimentas por parte de los trabajadores, con el fin de protegerlos contra posibles daños a su salud o su integridad física derivados de la exposición a los peligros en el lugar de trabajo. El empleador deberá suministrar elementos y equipos de protección personal (EPP) que cumplan con las disposiciones legales vigentes. Los EPP deben usarse de manera complementaria a las anteriores medidas de control y nunca de manera aislada, y de acuerdo con la identificación de peligros y evaluación y valoración de los riesgos.

Como complemento de este documento está disponible el procedimiento de Gestión del riesgo.

Control de Cambios		
Versión	**Fecha de entrada en vigencia**	**Naturaleza del cambio**
01	Rige a partir de su publicación en el SIG	Migración total del documento soporte D-DS-ME-AR-00-01 denominado Guía de Administración de Riesgos, a la Guía PM-GU-01 denominada Guía de administración del riesgo. El cambio en la codificación obedece a la actualización en el mapa de procesos y en el formato de documentación del Ministerio de Educación Nacional. El documento soporte D-DS-ME-AR-00-01 llegó hasta la versión 02 cuya última actualización bajo este código fue del 10/10/2017, por tal motivo este documento conserva el flujo de aprobación de dicha versión.
02	25/10/2018	Se actualiza el logo y los colores de este documento de acuerdo con el nuevo manual de imagen institucional generado por la Presidencia de la República para todas las entidades del Gobierno, lineamiento recibido de la Oficina Asesora de Comunicaciones el 31-08-2018. Al ser este un ajuste de forma y no de contenido conserva el flujo de aprobación de la versión anterior y no requiere aprobación por parte del líder del proceso.
03	06-02-2019	El documento PM-GU-01 incorporó los lineamientos establecidos en el 2018 por Función Pública en la “Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, Riesgos de Gestión, Corrupción y Seguridad Digital. V4”
04	31-03-2021	Se incorporan los lineamientos establecidos en Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - diciembre de 2020. De igual forma se incorporó la metodología para el análisis de riesgos de soborno.
05	31-12-2021	Se actualiza la Guía incluyendo el ajuste a la política de administración del riesgo, aprobada por el Comité Coordinador de Control interno y el contenido específico de la misma. Se realizan precisiones que incluyen la unificación de la información relacionada a la identificación de riesgos de corrupción incluidos los riesgos de soborno
06	Rige a partir de su publicación en el SIG	Se actualiza la Guía realizando ajustes en su contenido así: 1. Actualización normativa en la introducción. 2. Se ajustó la definición de apetito del riesgo. 3. Se ajustaron las figuras y las fuentes de estas.

Control de Cambios		
Versión	**Fecha de entrada en vigencia**	**Naturaleza del cambio**
		4. Se incorporaron algunas responsabilidades de las líneas de defensa establecida en la guía V5 del DAFP. 5. Se ajustó el numeral 10.2. Identificación de riesgos de gestión.

Registro de aprobación					
Elaboró		**Revisó**		**Aprobó**	
Nombre	William H. Otálora C.	**Nombre**	María Helena Ordoñez	**Nombre**	Edna del Pilar Páez García
Cargo	Profesional especializado SDO /	**Cargo**	Jede Oficina de Control Interno	**Cargo**	Subdirectora de Desarrollo Organizacional.