POLÍTICA Y METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS Y OPORTUNIDADES

DE-DR-001

Ministerio de Comercio, Industria y Turismo
Direccionamiento Estratégico
Marzo de 202X~~1~~

TABLA DE CONTENIDO

TÍTULO I. ASPECTOS GENERALES

1. OBJETIVO

Establecer los lineamientos y criterios que orienten al Ministerio de Comercio, Industria y Turismo (MinCIT) en la correcta identificación, valoración, tratamiento, monitoreo y seguimiento de los riesgos y la identificación, valoración y seguimiento de las oportunidades, 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, así como orientar en las acciones que conduzcan a disminuir la materialización de los riesgos.

2. ALCANCE

Esta política aplica desde el análisis del Marco Estratégico del Ministerio y de los Objetivos de cada Proceso, siguiendo con la identificación, valoración (análisis y evaluación), tratamiento (planificación y definición de acciones de mejora), monitoreo y seguimiento de los riesgos institucionales, así como la identificación, valoración y seguimiento de las oportunidades.

3. RESPONSABLES

Las responsabilidades para la administración del riesgo, se definieron con base en las líneas de defensa[1], se encuentran descritas en el Anexo 1 del presente documento.

4. DEFINICIONES[2]

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, h~~H~~ardware, información física o digital, recurso humano, entre otros, que tengan valor para la organización y que sean utilizados en el ~~que utiliza la organización~~ para funcionar~~funcionar~~ en el entorno digital.
- **Activo**: En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Administración del Riesgo:** Actividades encaminadas a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y monitoreo de los mismos de forma que se apoye el cumplimiento de los objetivos de la entidad.
- **Análisis de Riesgos:** Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo
- **Análisis del Riesgo:** Proceso que permite comprender la naturaleza del riesgo y determinar el nivel del riesgo NTC-ISO/IEC 27000:2017
-
-

Comentado [DYEV-C1]: Sugiero que en lo que respecta a la seguridad de la información y seguridad digital se haga referencia nó solamente a las definiciones de la de Riesgos del DAFP, sino también a la familia de normas 27XXX, por ejemplo 27000, 27001 y 27005.

Comentado [DYEV-C2]: La guía de Riesgos del DAFP lo define, sin embargo pongo en consideración que se utilice el termino operar.

Comentado [DYEV-C3]: Esta es una definición? Consultando los documentos de referencia, no existe ese término. Entiendo que se debe tener en cuenta por cuanto contempla las acciones para administración y gestión del riesgo, si es para contextualizar.

[1] Las responsabilidades para la administración del riesgo se definieron con base en las líneas de defensa descritas en el Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG, anexo 7 criterios diferenciales.
[2] Las definiciones son tomadas de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020.

- **Amenazas:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización NTC-ISO/IEC 27000:2017
- **Apetito de riesgo**: Es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito puede ser diferente para los distintos tipos de riesgo que la entidad debe o desea gestionar.
- **Capacidad de riesgo**: Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sea posible el logro de los objetivos de la entidad.
- **Causa:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
- **Causa raíz:** Causa principal o básica, correspondiente a las razones por las cuales se puede presentar el riesgo.
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **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:** Media que permite reducir o mitigar un riesgo.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.[3]
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad autorizada.[4]
- **Evaluación del riesgo:** Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo y su magnitud o ambos son aceptables o tolerables. NTC-ISO 31000:2011

- **Factores de riesgo:** Son las fuentes generadoras de riesgos.
- **Gestión del riesgo:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Identificación del riesgo:** Proceso de análisis para encontrar una potencial desviación de los objetivos.
- **Impacto:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** Propiedad de exactitud y completitud.[5]
- **Mapa de calor:** Plano en el que se presentan simultáneamente las escalas de medición de impacto y de probabilidad, y que, como producto de su combinación, mediante colorimetría representa la importancia (nivel de severidad o criticidad) del riesgo.
- **Mapa de riesgos:** Documento con la información resultante de la gestión del riesgo.
- **Materialización del Riesgo:** Ocurrencia o desarrollo del riesgo
- **Nivel de riesgo**: Es el valor que se determina a parir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento

Comentado [DYEV-C4]: La norma lo cita como CAUSA

Comentado [DYEV-C5]: La norma NTC-ISO/IEC 27000:2017 lo define como Medida que modifica un riesgo.

Con formato: Normal, Sin viñetas ni numeración

Comentado [DYEV-C6]: La norma NTC-ISO 31000_2011 la define como Gestión del riesgo. Actividades coordinadas para dirigir y controlar una organización
con respecto al riesgo.

Comentado [DYEV-C7]: Las normas ISO 31000, la 27000 y la 27005 no la definen en esos términos, si es una interpretación propongo la siguiente:

Se determinan las causas, fuentes del riesgo y los eventos con base al contexto del proceso, que pueden afectar el logro de los objetivos del mismo

Comentado [DYEV-C8]: La norma NTC-ISO/IEC 27005 la define como:
Cambio adverso en el nivel de los objetivos del negocio logrados

[3] ISO / IEC 27000.2018 (https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1.
[4] ISO / IEC 27000.2018 (https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1
[5] ISO / IEC 27000.2018 (https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1

traería sobre la capacidad institucional del alcanzar los objetivos.

- **Objetivo de proceso**: Son los resultados que se espera lograr para cumplir la misión y visión. Determina el cómo logro la política trazada y el aporte que se hace a los objetivos institucionales. Un objetivo es un enunciado que expresa una acción, por lo tanto debe iniciarse con un verbo fuerte como: establecer, identificar, recopilar, investigar, registrar, buscar. Los objetivos deben ser: medibles, realistas y se deben evitar frases subjetivas en su construcción
- **Oportunidad:** Eventos que permiten alcanzar un resultado esperado o aumentar los efectos deseables.
- **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.
- **Política de Administración del Riesgo:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.
- **Probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo. se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **Riesgo:** Efecto que causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, falla o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Riesgo de corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo de gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo de fraude:** Posibilidad de que la Entidad incurra en una pérdida financiera o de otro tipo cuando una persona (que puede ser empleado, un cliente, o una persona vinculada a la Entidad) que actúa individualmente o en colusión, obtiene una ventaja o beneficio injusto en forma deshonesta o engañosa.
- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 27000). Efecto de la incertidumbre sobre los objetivos.
  Nota 1 a la entrada: Un efecto es una desviación de lo esperado: positivo o negativo.
  Nota 2 a la entrada: Incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con, comprensión o conocimiento de un evento, su consecuencia o probabilidad.
  Nota 3 a la entrada: El riesgo se caracteriza a menudo por referencia a posibles "eventos" (como se define en la Guía ISO 73: 2009, 3.5.1.3) y "consecuencias" (como se define en la Guía ISO 73: 2009, 3.6.1.3), o una combinación de estos.
  Nota 4 a la entrada: El riesgo a menudo se expresa en términos de una combinación de las consecuencias de un evento (incluidos los cambios en las circunstancias) y la “probabilidad” asociada (como se define en la Guía ISO 73: 2009, 3.6.1.1) de ocurrencia.
  Nota 5 a la entrada: En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden expresarse como efecto de la incertidumbre sobre los objetivos de seguridad de la información.
  Nota 6 a la entrada: El riesgo de seguridad de la información está asociado con la posibilidad de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de

Comentado [DYEV-C9]: Cual es la fuente de esta defincón? Enla 27000 no la encontré y tampoco es así en la 27005

Comentado [DYEV-C10]: De acuerdo a la norma NTC-ISO/IEC 27000:2011, esta es una nota al margen pero referente al riesgo

Comentado [DYEV-C11]: Igual al anterior

activos de información y, por lo tanto, causen daños a una organización.[6]

Riesgos en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. NTC-ISP 27005:2009.
Nota: Se mide en términos de una combinación de la probabilidad de que sucede un evento y sus consecuencias.

- **Riesgo inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riego inherente, dentro de unas escalas de severidad.
- **Riesgo residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **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.
- **Tratamiento del riesgo:** Proceso para modificar el riesgo.
- **Valoración del Riesgo:** Establece la identificación y evaluación de los controles. En la etapa de valoración del riesgo se determina el riesgo residual.
- **Vulnerabilidad:** Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

5. CONDICIONES GENERALES

En el presente documento se establecen los siguientes parámetros:

- Los riesgos del Sistema de Gestión de Calidad se acogen al presente documento.
- Los riesgos de seguridad digital dando cumplimiento al Sistema de Gestión de Seguridad y Privacidad de la Información se acogen al presente documento.
- Los riesgos de gestión en materia de contratación se acogen a las Políticas de Colombia Compra Eficiente.
- Los riesgos de gestión de la operación del Proceso del Sistema de Gestión, el cual abarca los subprocesos de sistema de gestión de calidad, sistemas de gestión ambiental, sistema de gestión de seguridad y salud en el trabajo y sistema de seguridad y privacidad de la información, se acogen al presente documento.
- Los riesgos en materia de seguridad y salud en el trabajo (ocupacionales) dando cumplimiento al Sistema de Gestión de Seguridad y Salud en Trabajo se identifican e implementan de acuerdo con lo establecido en el **SG-PR-027 Procedimiento Gestión de Peligros y Riesgos.**
- Las responsabilidades para la administración del riesgo, se definen con base en las líneas de defensa.
- El Contexto de la Organización (cuestiones internas y externas) se define de acuerdo a lo establecido en el **DE-PR-014 Procedimiento Formulación y Seguimiento de la Planeación Estratégica Sectorial-PES**.
- Las oportunidades se identifican en el Contexto de la Organización, sin embargo, también se pueden identificar en los procesos.

[6] ISO / IEC 27000.2018 (https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1).

Comentado [DYEV-C12]: De acuerdo a la norma NTC-ISO/IEC 27000:2011, esta es una nota al margen, pero referente al riesgo, pero en estos se le da alcance a la seguridad de la información.

Con formato: Fuente: Negrita, Color de fuente: Rojo

Con formato: Color de fuente: Rojo

Con formato: Color de fuente: Rojo

Comentado [DYEV-C13]: ¿Esta definición es una interpretación? No corresponde a la definición de la NTC-ISO/IEC 31000 ni a la 27000

6. COMUNICACIÓN Y DIVULGACIÓN

La Política y Metodología para la Administración de Riesgos busca crear conciencia en todos los servidores públicos del Ministerio de Comercio, Industria y Turismo, en los distintos niveles y vinculaciones, sobre la importancia de la gestión preventiva y el autocontrol en la ejecución de las actividades y se desarrolla en dos niveles, en los cuales se adelantan acciones o estrategias de comunicación y divulgación según su propósito:

- **A nivel institucional**: Comprende la divulgación y socialización de la Política y Metodología de Administración del Riesgo y el Mapa de Riesgos, la cual estará a cargo de la Oficina Asesora de Planeación Sectorial con el apoyo del Grupo de Comunicaciones. Esta estrategia incluye la publicación en la página web de la entidad, del Mapa de Riesgos de Corrupción y el resultado de los seguimientos.

  Así mismo, dentro de la estructura organizacional formalmente establecida se tiene el Grupo de Comunicaciones con enfoque interno y externo. A nivel interno, garantizan un adecuado flujo de la información a todos los niveles de la organización, mediante el uso de herramientas tecnológicas (como la Intranet, el correo institucional, las plataformas de interacción masiva como las aplicaciones del Office 365 con todas sus aplicaciones como TEAMS); así como con la estructura de enlaces en cada dependencia, para el despliegue de la información generada por cualquier medio.

- **A nivel de procesos**: Comprende la divulgación de los Mapas de Riesgos por Proceso al interior de los respectivos equipos de trabajo, está a cargo de los Responsables de cada Proceso con el apoyo de los gestores de calidad.

7. MARCO CONCEPTUAL PARA NIVELES DE ACEPTACION DEL RIESGO:

La entidad ha definido los niveles de aceptación teniendo en cuenta las siguientes fórmulas:

- **Nivel de riesgo**

  Riesgo inherente = Probabilidad inherente vs Impacto

  Riesgo Residual = Probabilidad inherente – (Probabilidad Inherente * Control) vs Impacto inherente – (Impacto Inherente * Control)

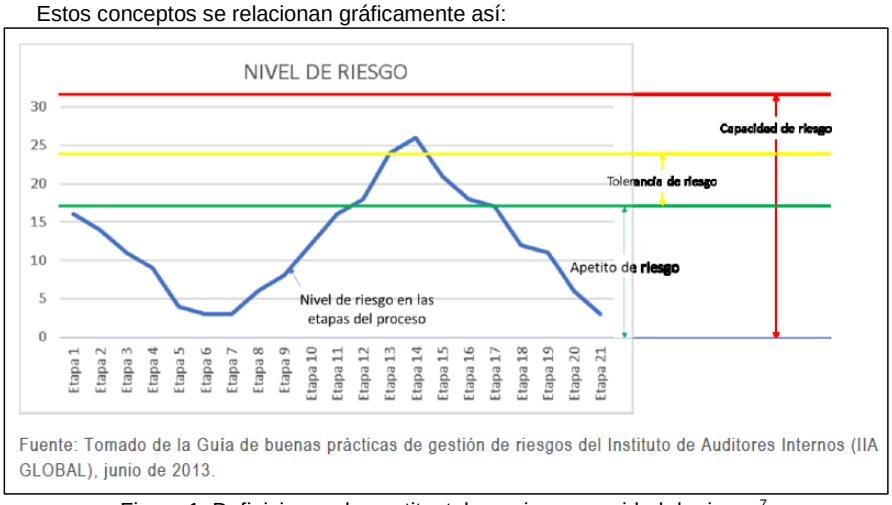
Tiendo en cuenta el apetito, la tolerancia y la capacidad del riesgo, para el ministerio los niveles de aceptación del riesgo residual son:

	UBICACIÓN EN EL MAPA DE CALOR (Riesgo Residual)	NIVELES DE ACEPTACION	FORMULA	ACCION A TOMAR
GESTIÓN	Bajo	Apetito del riesgo	# riesgos bajos / Total riesgos	Riesgos aceptado

	UBICACIÓN EN EL MAPA DE CALOR (Riesgo Residual)	NIVELES DE ACEPTACION	FORMULA	ACCION A TOMAR
	Moderado	Tolerancia del riesgo	# riesgos moderados y altos / Total riesgos	Riesgo tolerado sin plan de acción (acciones para abordar riesgos)
	Alto			Riesgo tolerado con plan de acción (acciones para abordar riesgos)
	Extremo	Capacidad del riesgo	# riesgos extremos / Total riesgos	Riesgo soportado con acciones correctivas
CORRUPCIÓN Y FRAUDE	**Moderado**	**Apetito al riesgo**	# riesgos bajos / Total riesgos	Riesgo tolerado sin plan de acción (acciones para abordar riesgos)
	Alto	**Tolerancia del riesgo**	# riesgos moderados y altos / Total riesgos	Riesgo tolerado con plan de acción (acciones para abordar riesgos)
	Extremo	**Capacidad de riesgo**	# riesgos extremos / Total riesgos	Riesgo soportado con acciones correctivas

Tabla 1. Clasificación de Niveles de Aceptación

Estos conceptos se relacionan gráficamente así:



Fuente: Tomado de la Guía de buenas prácticas de gestión de riesgos del Instituto de Auditores Internos (IIA GLOBAL), junio de 2013.

Figura 1: Definiciones de apetito, tolerancia y capacidad de riesgo[7].

[7] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020

TITULO II. IDENTIFICACIÓN DEL RIESGO

1. CONOCIMIENTO Y ANÁLISIS DE LA ENTIDAD:

Antes de iniciar con la metodología para administrar los riesgos es necesario comprender el contexto general del Ministerio (cuestiones internas y externas) y establecer el Marco Estratégico el cual se define para el Ministerio cada cuatro años.

El Marco Estratégico del Ministerio de Comerció Industria y Turismo parte de un análisis de contexto que permite reconocer en dónde se encuentra la entidad al revisar y establecer su direccionamiento para el siguiente periodo de gobierno. Este contexto se compone del **contexto externo (**factores: políticos, económicos, financieros, sociales, culturales, tecnológicos, ambientales, legales y reglamentarios), **contexto interno** (misión, visión, estructura organizacional, funciones y responsabilidades, políticas, planeación institucional, objetivos y estrategias implementadas, recursos con los que se cuenta (económicos, personas, procesos, sistemas, tecnología, información), cultura organizacional y relaciones con las partes involucradas) y **contexto del proceso** (objetivo y alcance del proceso, interrelación con otros procesos, planes, programas o proyectos asociados y activos de seguridad digital del proceso) y como resultado se definen los ejes estratégicos y el despliegue de estos. (Ver **Marco Estratégico MinCIT**.)

El conocimiento del contexto facilita la identificación de riesgos y oportunidades para el cumplimiento de los objetivos estratégicos.

2. CLASIFICACION DEL RIESGO

Los riesgos se clasifican así:

TIPO	CLASIFICACION	DESCRIPCIÓN
RIESGOS DE GESTION	**EJECUCION Y ADMINISTRACION DE PROCESOS**	Pérdidas derivadas de errores en la ejecución y administración de procesos.
	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.
	LEGALES	Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la entidad debido a su incumplimiento o desacato a la normativa vigente.

TIPO	CLASIFICACION	DESCRIPCIÓN	
RIESGOS DE SEGURIDAD DE LA INFORMACION		Pérdida de confidencialidad,	Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
		Pérdida de integridad	
		Pérdida de disponibilidad de los activos de información	
RIESGOS DE FRAUDE	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.	
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.	

Tabla 2. Clasificación de Riesgos[8]

3. DESCRIPCION DEL RIESGO:

Los **Riesgos se identifican a partir del Marco Estratégico del MINCIT**, o el documento que establezca el direccionamiento estratégico, que estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los **objetivos estratégicos o del proceso**.

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para las personas ajenas a él. A continuación se relaciona la estructura que facilita su redacción y claridad. Se inicia con la frase “POSIBILIDAD DE”.

Desglosando la estructura tenemos:

- **Impacto:** Aquí definimos el ¿Qué puede pasar?, los factores de impacto a los que puede estar expuesta la entidad -son:
  - Afectación Económica: afectación presupuestal de la entidad
  - Afectación Reputacional: afectación de la imagen de la entidad.

- **Causa inmediata:** nos responde al ¿Cómo puede pasar?, son las situaciones más evidentes por las cuales se puede materializar el riesgo.

- **Causa raíz:** nos dá respuesta al ¿Por qué puede pasar?. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

[8] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020.

Comentado [DYEV-C15]: En el informe de riesgos se articula la privacidad también, se debería nombrar desde este riesgo.
De la familia de la norma ISO 27000 recientemente salio la ICO/IEC 27701 que hace referencia a la privacidad de los datos https://tienda.icontec.org/gp-tecnicas-de-seguridad-ampliacion-de-las-ntc-iso-iec-27001-y-gtc-iso-iec-27002-para-la-gestion-de-la-privacidad-de-la-informacion-requisitos-y-directrices-ntc-iso-iec27701-2020.html

Tabla con formato

Comentado [DYEV-C14]:
1.Posibilidad de comprometer la integridad de la información institucional debido a fallas técnicas y operativas en el proceso.
2.Posibilidad de comprometer la confidencialidad de la información institucional debido a fallas técnicas y operativas en el proceso.
3.Posibilidad de comprometer la disponibilidad de la información debido a fallas técnicas y operativas en el proceso.
4.Posibilidad de no atender las necesidades de automatización de los procesos de la entidad, debido a capacidad limitada de los productos adquiridos
5.Posibilidad de tener Sistemas de información desatendidos o sin soporte debido a la imposibilidad de continuidad a los contratos de soporte y mantenimiento
6.Posibilidad de afectación de la confidencialidad, integridad y/o disponibilidad de la información por errores humanos

Comentado [DYEV-C16]: Los activos de información son un tipo de activo, en esta caso se debe hacer referencia no solo a los activos de información, sino a todos los tipos de activos, pues a través de ellos se transforma la información en todo ciclo de vida.

Esta es la base para la definición de los controles.

El esquema para la redacción del riesgo es:

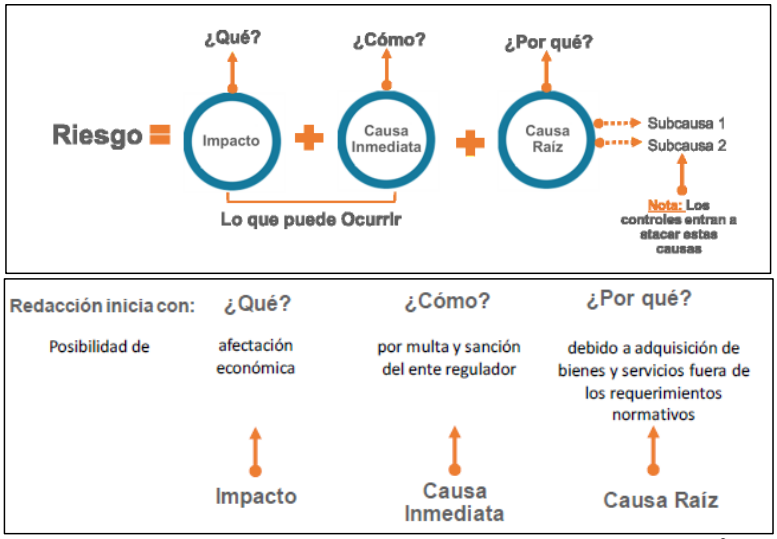


Figura 2. Estructura propuesta para la redacción del riesgo y ejemplo[9]

Recomendaciones:

- No describir como omisiones ni desviaciones de 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 causa transversales.
  Ejemplo: pérdida de expedientes.
- Evitar iniciar con palabras negativas como: “No…”, “Que no…”, o con palabras que denoten un factor de riesgo (causa) tales como: “ausencia de”, “falta de”, “poco(a)”, “escaso(a)”, “insuficiente”, “deficiente”, “debilidades en…”
- Generar en el lector o escucha la imagen del evento como si ya estuviera sucediendo.
- Pregúntese si el riesgo identificado está relacionado directamente con las características del objetivo. Si la respuesta es “no”, lo descrito puede ser la causa o la consecuencia del riesgo.

[9] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020.

3.1 Riesgos de Corrupción y Fraude

Corresponde al líder de proceso o proyecto la identificación de los riesgos de corrupción y fraude, que podrían afectar el logro de los objetivos de los procesos del Ministerio, los cuales están asociados al uso de poder y a la pérdida financiera.

Se puede determinar si un riesgo es de corrupción o fraude, si se marca con una X en la descripción del riesgo las situaciones señaladas en la siguiente tabla:

Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Perdida Financiera	Beneficio privado
Riesgo de **Corrupción**	X	X	X		X
Riesgo de **Fraude**			X	X	X

Tabla 3. Determinación del Riesgo de Corrupción y Fraude

3.2 Riesgos de Seguridad de la Información:

Corresponde al líder del Sistema de Gestión de Seguridad y Privacidad de la Información y al líder del proceso o proyecto la identificación de los riesgos de la Información. Estos se basan en la afectación de los tres, más de uno o algunos de los principios de la seguridad que comprometan ~~tres criterios en~~ un activo ~~de información~~ o un grupo de activos de información dentro del proceso "Confidencialidad, i~~I~~ntegridad ~~, confidencialidad~~ o disponibilidad".

Con formato: Normal, Derecha: 0 cm, No ajustar espacio entre texto latino y asiático, No ajustar espacio entre texto asiático y números, Punto de tabulación: No en 3,41 cm

Como se señaló anteriormente, existen tres 3 tipos de riesgos de seguridad de la información: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos de información. Para cada tipo de riesgo se seleccionan las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se pueda materializar.

Para el riesgo identificado se deben asociar el grupo de activos de información o activos de información específicos del proceso y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización Identificación de activos.

Comentado [DYEV-C17]: Creo que este término sobra, pues se desarrolla más adelante, ¿o sería un ítem a desarrollar?

Los siguientes son los pasos que sirven de guía para identificar los activos de información:

¿Cómo identificar los activos de información?:

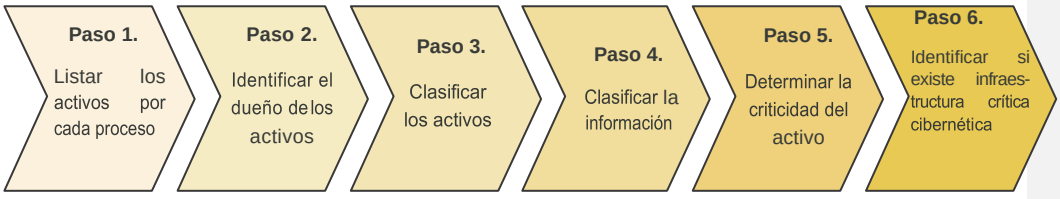


Figura 3. Identificación de activos de la información.

NOTA:

- La agrupación de activos debe ser del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.
- Para mayor información consultar Anexo 4. *Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas*, de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5 de diciembre de 2020.

TITULO III. VALORACIÓN DEL RIESGO

La valoración del riesgo consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial o propio de la actividad también llamado *"RIESGO INHERENTE"*.

1. ANALISIS DE RIESGO

Consiste en establecer la probabilidad de ocurrencia y el nivel de consecuencia o impacto del riesgo, con el fin de estimar su **probabilidad** de ocurrencia e **impacto/ consecuencia** si no se controla (RIESGO INHERENTE).

1.1. Determinar la PROBABILIDAD: se analiza a partir de la pregunta ¿qué tan posible es que ocurra el riesgo? Está asociada a la exposición al riesgo del proceso o actividad que se está analizando, se trata en este caso de un hecho que no se ha presentado pero es posible, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, o tratándose de hechos que se han materializado o frente a los cuales se cuenta con un historial de situaciones o eventos asociados al riesgo.

A ~~continuación~~continuación, se establecen los criterios para definir el nivel de probabilidad:

NIVEL	FRECUENCIA DE LA ACTIVIDAD	FRECUENCIA DE EVENTOS	PROBABILIDAD
MUY BAJA	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año.	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	20%
BAJA	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	El evento puede ocurrir en algún momento.	40%
MEDIA	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	El evento podrá ocurrir en algún momento.	60%
ALTA	La actividad que conlleva el riesgo se ejecuta de 500 veces al año y máximo 5.000 veces por año.	Es viable que el evento ocurra en la mayoría de las circunstancias.	80%
MUY ALTA	La actividad que conlleva el riesgo se ejecuta más de 5.000 veces por año.	Se espera que el evento ocurra en la mayoría de las circunstancias.	100%

Tabla 4. Criterios para definir el nivel de PROBABILIDAD de ocurrencia de los riesgos[10].

- Nota: En materia de tecnología (incluye disponibilidad de aplicativos) se tiene en cuenta 1 hora de funcionamiento = 1 vez.

[10] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020.

1.2. Determinar el IMPACTO/CONSECUENCIA: este se determina para establecer las consecuencias o efectos del riesgo, con el fin de estimar la zona de riesgo en caso de no controlarse (RIESGO INHERENTE). Para definir la tabla de criterios, las variables principales que se tienen en cuenta son impactos económicos y reputacionales.

Cuando se presente más de un impacto en un solo riesgo con diferentes niveles, se debe tomar el nivel más alto.

Para el Riesgos de **Corrupción y Fraude** se tiene en cuenta solamente los niveles "moderado", "mayor" y "catastrófico", dado que estos riesgos siempre serán significativos. En este orden de ideas, no se contemplan los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

NIVEL	VALOR IMPACTO / CONSECUENCIA RIESGOS	
	Riesgos de Gestión y de Seguridad de la Información	Riesgos de Corrupción y Fraude
LEVE	20%	N/A
MENOR	40%	
MODERADO	60%	60%
MAYOR	80%	80%
CATASTRÓFICO	100%	100%

Tabla 5. Criterios para definir el nivel de impacto/consecuencia riesgos de la entidad vs riesgos de corrupción y Fraude

El **impacto / consecuencia** se establece, de acuerdo con los siguientes criterios:

RIESGOS DE GESTION		
NIVEL	**CUANTITATIVAS - ECONOMICA**	**CUALITATIVAS - REPUTACIONAL**
CATASTROFICO 100%	-Impacto que afecte la ejecución presupuestal en un valor ≥50%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	-Interrupción de las operaciones de la entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR 80%	-Impacto que afecte la ejecución presupuestal en un valor ≥20%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%.	-Interrupción de las operaciones de la entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta.

RIESGOS DE GESTION		
NIVEL	**CUANTITATIVAS - ECONOMICA**	**CUALITATIVAS - REPUTACIONAL**
	- Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
MODERADO 60%	-Impacto que afecte la ejecución presupuestal en un valor ≥5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el pre-supuesto total de la entidad en un valor ≥5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	-Interrupción de las operaciones de la entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
MENOR 40%	-Impacto que afecte la ejecución presupuestal en un valor ≥1%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el pre-supuesto total de la entidad en un valor ≥1%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	-Interrupción de las operaciones de la entidad por algunas horas. - Quejas de los usuarios relacionadas con la indebida aplicación de la Ley disciplinaria vigente, dentro de las actuaciones disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
LEVE 20%	-Impacto que afecte la ejecución presupuestal en un valor ≥0,5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las	-No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

RIESGOS DE GESTION		
NIVEL	**CUANTITATIVAS - ECONOMICA**	**CUALITATIVAS - REPUTACIONAL**
	cuales afectan en un valor ≥0,5% del presupuesto general de la entidad.	

Tabla 6. Criterios para definir el nivel de impacto/consecuencia – RIESGOS[11]

Para calificar el **impacto / consecuencia del riesgo de corrupción y fraude** se debe responder el siguiente cuestionario:

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

Tabla 7. Preguntas para calificar el impacto / consecuencia – RIESGO DE CORRUPCIÓN Y FRAUDE

De acuerdo con el resultado anterior, el número de preguntas contestadas afirmativamente permitirá ubicar el riesgo según la siguiente tabla y determinar el impacto / consecuencias del riesgo de corrupción y fraude:

DESCRIPTOR	CANTIDAD DE PREGUNTAS AFIRMATIVAS	IMPACTO / CONSECUENCIAS CUALITATIVO
CATASTRÓFICO 100%	DOCE a DIECINUEVE preguntas	Genera consecuencias desastrosas para la entidad
MAYOR 80%	SEIS a ONCE preguntas	Genera altas consecuencias sobre la entidad.
MODERADO 60%	UNA a CINCO pregunta(s)	Genera medianas consecuencias sobre la entidad

Tabla 8. Calificación impacto / consecuencia – RIESGO CORRUPCION Y FRAUDE

[11] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020.

RIESGO DE SEGURIDAD DE LA INFORMACION		
NIVEL	**CUANTITATIVAS - ECONOMICA**	**CUALITATIVAS - REPUTACIONAL**
CATASTRÓFICO 100%	-Afectación mayor o igual al 50% de la población. -Afectación mayor o igual al 50% del presupuesto anual de seguridad digital. -Afectación muy grave del medio ambiente que requiere de mayor o igual a 3 años de recuperación.	-Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. - Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. (Interrupción de las operaciones de la entidad por más de cinco (5) días. - Pérdida de información crítica para la entidad que no se puede recuperar) - Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MAYOR 80%	-Afectación en un valor igual o mayor al 20% e inferior al 50% de la población. -Afectación en un valor igual o mayor al 20% e inferior al 50% del presupuesto anual de seguridad digital. -Afectación importante del medio ambiente que requiere de 1 a 3 años de recuperación.	-Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. -Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. -Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MODERADO 60%	-Afectación en un valor igual o mayor al 10% y menor al 20% de la población. -Afectación en un valor igual o mayor al 10% y menor al 20% del presupuesto anual de seguridad digital. - Afectación leve del medio ambiente requiere de 3 meses a 1 año de recuperación.	-Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. -Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. -Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MENOR 40%	-Afectación en un valor igual o mayor al 1% y menor al 10% de la población. -Afectación en un valor igual o mayor al 1% y menor al 10% del presupuesto anual de seguridad digital. -Afectación leve del medio ambiente requiere de Afectación leve del medio ambiente requiere de 1 a 3 meses de recuperación.	-Afectación leve de la integridad. -Afectación leve de la disponibilidad. -Afectación leve de la confidencialidad.
LEVE 20%	-Afectación en un valor menor al 1% de la población. -Afectación en un valor menor al 1% del presupuesto anual de seguridad digital. -No hay afectación medioambiental.	-Sin afectación de la integridad. -Sin afectación de la disponibilidad. -Sin afectación de la confidencialidad.

Con formato: Color de fuente: Rojo

Comentado [DYEV-C18]: Estas son las variables corresponden a la guía de ICC.
¿Esta población está asociada al censo poblacional del país? O a qué tipo de población hace referencia (usuarios afectados)
Cadena de suministros – Inspección física simultánea.
Que se entiende como afectación grave

Tabla 9. Criterios para calificar el impacto / consecuencia – RIESGO DE SEGURIDAD DE LA INFORMACION

RIESGO DE SEGURIDAD DE LA INFORMACION			
NIVEL	**CUANTITATIVAS - ECONOMICA**	**CUALITATIVAS - REPUTACIONAL**	**Articulacion - Ciberseguridad Fuente: Propia**
CATASTRÓFICO **100%**	-Afectación mayor o igual al 50% de la población. -Afectación mayor o igual al 50% del presupuesto anual de seguridad digital. -Afectación muy grave del medio ambiente que requiere de mayor o igual a 3 años de recuperación.	-Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. - Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. (Interrupción de las operaciones de la entidad por más de cinco (5) días. - Pérdida de información crítica para la entidad que no se puede recuperar) - Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.	La amenaza está altamente motivada y es suficientemente capaz de llevarse a cabo, comprometiendo la confidencialidad, integridad y disponibilidad de la información y afectando de manera considerable la operación y la continuidad del negocio.
MAYOR **80%**	-Afectación en un valor igual o mayor al 20% e inferior al 50% de la población. -Afectación en un valor igual o mayor al 20% e inferior al 50% del presupuesto anual de seguridad digital. -Afectación importante del medio ambiente que requiere de 1 a 3 años de recuperación.	-Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. -Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. -Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.	La amenaza está motivada y podría llevarse a cabo afectando la confidencialidad, integridad y disponibiildad de la informacion..
MODERADO **60%**	-Afectación en un valor igual o mayor al 10% y menor al 20% de la población. -Afectación en un valor igual o mayor al 10% y menor al 20% del presupuesto anual de seguridad digital. - Afectación leve del medio ambiente requiere de 3 meses a 1 año de recuperación.	-Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. -Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. -Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.	La amenaza es posible y tiene la capacidad de afectar parcialmente la confidencialidad, integridad y disponibilidad de la informacion.
MENOR **40%**	-Afectación en un valor igual o mayor al 1% y menor al 10% de la población. -Afectación en un valor igual o mayor al 1% y menor al 10% del presupuesto anual de seguridad digital. -Afectación leve del medio ambiente requiere de Afectación leve del medio ambiente requiere de 1 a 3 meses de recuperación.	-Afectación leve de la integridad. -Afectación leve de la disponibilidad. -Afectación leve de la confidencialidad.	La amenaza afecta de manera ocasional la confidencialidad, integridad y disponibilidad de la Informacion.
LEVE **20%**	-Afectación en un valor menor al 1% de la población. -Afectación en un valor menor al 1% del presupuesto anual de seguridad digital. -No hay afectación medioambiental.	-Sin afectación de la integridad. -Sin afectación de la disponibilidad. -Sin afectación de la confidencialidad.	La amenaza no posee la suficiente capacidad para afectar la Confidencialidad, Integridad y disponibilidad de la Informacion.

2. EVALUACIÓN DEL RIESGO – NIVEL DE RIESGO INHERENTE (SEVERIDAD)

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE). Para establecer el nivel de riesgo inherente (sin aplicación de controles) y residual (con aplicación de controles) se utilizan los Mapas de Calor, que permiten ubicar el riesgo en la zona de acuerdo con la calificación de la **probabilidad** y el **impacto / consecuencia.**

Para todos los riesgos de **gestión y de seguridad de la información**, se definen cuatro zonas de severidad en el mapa de calor como se menciona a continuación:

IMPACTO

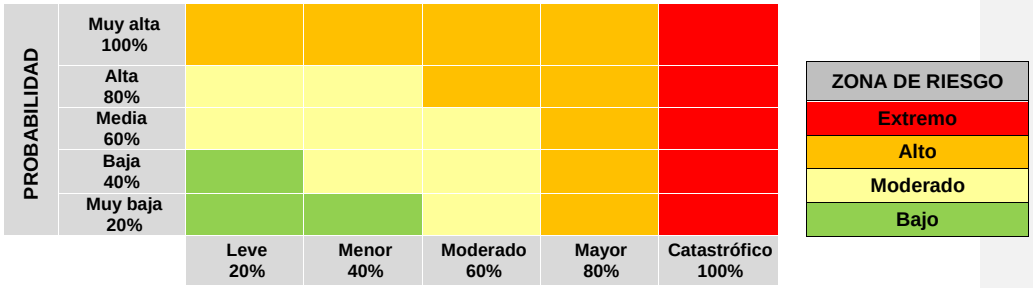


Figura 4. Mapa de Calor Riesgo Inherente[12]

- **Riesgo de Corrupción y Fraude**

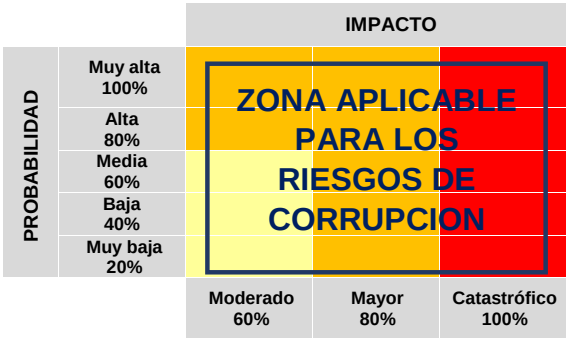


Figura 5. Mapa de calor para riesgos de corrupción y fraude[13]

3. DISEÑO Y VALORACIÓN DE CONTROLES

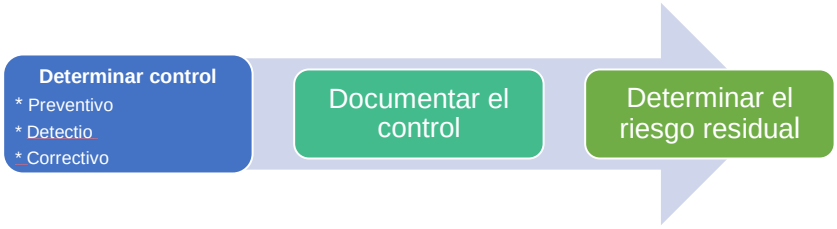
Los controles o actividades de control son medidas que permiten reducir o mitigar las causas que hacen que el riesgo se materialice, por eso la importancia en su diseño y evaluación.

3.1 Determinación de controles

La identificación de los controles se realiza a cada riesgo a través de entrevistas con los líderes de procesos o servidores expertos en su quehacer, de igual forma son los responsables de implementar y monitorear dichos controles con el apoyo de su equipo de trabajo.

[12] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020.
[13] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020.

El propósito es comparar los resultados del análisis de riesgo inherente (sin controles) con los controles establecidos, para determinar la zona de riesgo final o *"riesgo residual"*, los pasos a seguir son:



- **Redacción de un control**

Al momento de definir las actividades de control por parte de los Líderes de los Procesos y sus equipos en trabajo (primera línea de defensa), es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitiguen las causas que generan la materialización del riesgo. Esto se debe tener en cuenta desde la redacción del mismo. Un control debe tener:

Figura 6. Etapas para la redacción de un control.

Ejemplo:

El profesional de Contratación cada vez que se va a realizar un contrato, 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. En caso de encontrar información faltante, requiere al proveedor a través de correo para el suministro de la información y poder continuar con el proceso de contratación. Como evidencia deja Lista de Chequeo diligenciada con la información de la carpeta del cliente, y correos solicitando la información faltante en los casos que aplique.

- **Tipología del Propósito de los Controles**

Se deben seleccionar actividades de **control preventivo, detectivo y correctivo** que por sí solos ayuden a la mitigación las **causas** que originan los riesgos. Para cada causa debe existir un control. Un control puede ser tan eficiente que ayude a mitigar varias causas.

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.

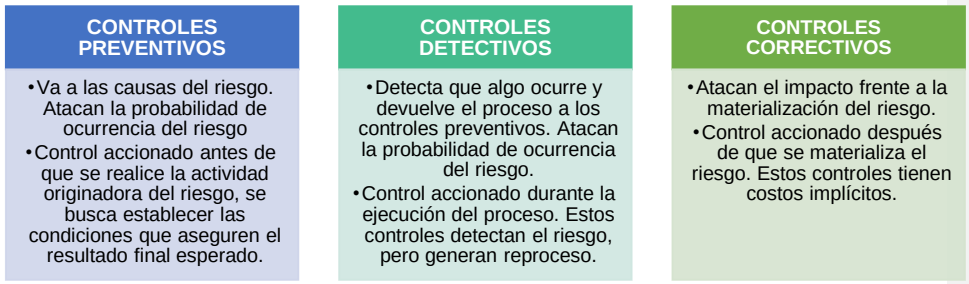


Figura 7. Tipologías de controles[14]

De acuerdo con la **forma** como se ejecutan los controles tenemos:

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

Es importante que para la adecuada mitigación de los riesgos no baste solo con que un control este bien diseñado, el control **debe ejecutarse por parte de los responsables tal como se diseñó.**

3.2 Análisis y evaluación de controles (Atributos)

A continuación se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. Los aspectos sin peso son atributos informativos que no tienen incidencia directa en la efectividad del control, sin embargo, permiten darle formalidad a éste.

Los aspectos de Tipo e Implementación, son atributos que tienen incidencia directa en la efectividad del control, su valoración suma máximo 50% y mínimo 25%.

CRITERIO DE EVALUACIÓN	DESCRIPCION	ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	PESO
1. Responsable	Adecuado	El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control	-
	Inadecuado		-
2. 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	-
3. Tipo	Prevenir	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
	Detectar	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%

[14] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020.

CRITERIO DE EVALUACIÓN	DESCRIPCION	ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	PESO
	Corregir	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
4. 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%
5. Estado de la documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
	Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
7. Evidencia de la ejecución del control	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.	-
TOTAL VALORACION CONTROL #_____ Máximo 50%, mínimo 25%			

Tabla 10. Atributos para el diseño de controles[15]

Nota: Siempre que se realicen ajustes a los controles se deben ajustar los documentos, y de igual forma si se hacen ajustes a los documentos del proceso se deben ajustar los controles involucrados.

4. NIVEL DE RIESGO RESIDUAL

Corresponde al resultado de **aplicar la efectividad de los controles** al riesgo inherente. A continuación se muestran las fórmulas para la aplicación de controles y establecer el riesgo residual:

Riesgo Residual = Probabilidad inherente – (Probabilidad Inherente * Control)
Impacto inherente – (Impacto Inherente * Control)

Nota:

- En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente (impacto inherente), es importante señalar que no es posible su movimiento en el mapa de calor para el impacto.
- Cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

La solidez del conjunto de controles se define acorde a la tabla10 por cada riesgo. Con la calificación obtenida se realiza un desplazamiento en el mapa de calor, así: si el control afecta la probabilidad se avanza hacia abajo. Si afecta el impacto se avanza a la izquierda:

[15] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020.

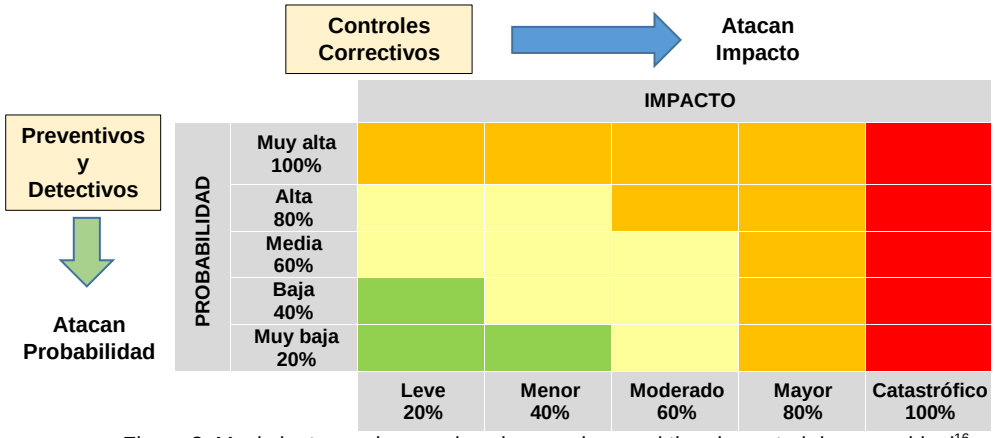


Figura 8. Movimiento en el mapa de calor acorde con el tipo de control riesgo residual[16]

Una vez realizado el análisis y evaluación de los controles se valora nuevamente la probabilidad e impacto/consecuencia del riesgo, determinando si los controles ayudan o no a la disminución probabilidad e impacto/consecuencia del riesgo y se procede a ubicar el **riesgo residual** en el **Mapa de Riesgo Residual.**

5. NIVELES DE ACEPTACIÓN DEL RIESGO RESIDUAL

De acuerdo con la valoración de cada riesgo residual y su ubicación en la zona de riesgo (extremo, alto, moderado, bajo) se establece su opción de manejo. Esto se define a partir del nivel del riesgo residual (con controles), de la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento.

Dependiendo del valor del riesgo residual, este se puede:

[16] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020.

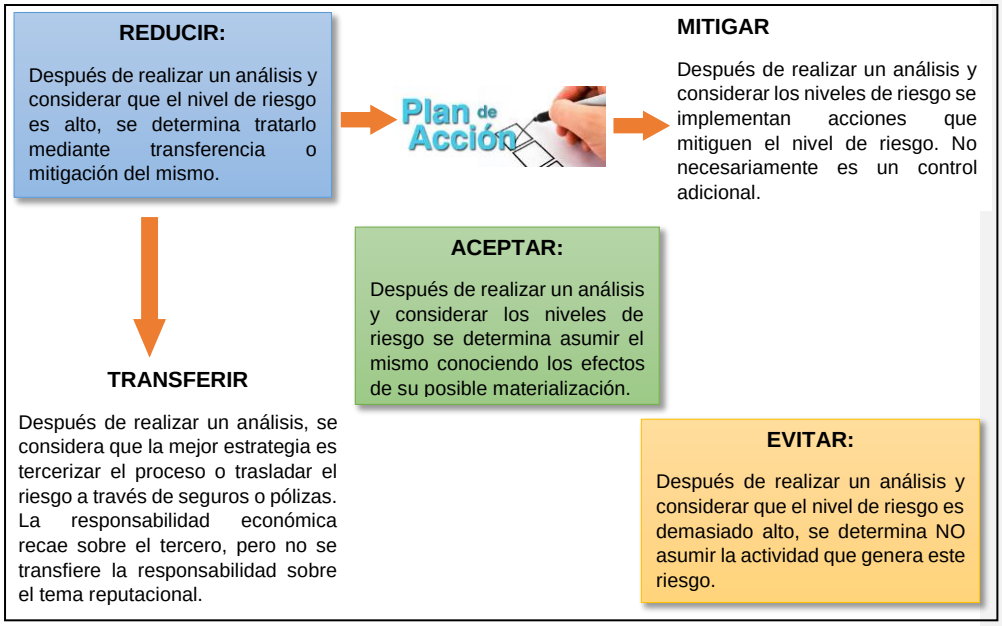


Figura 9. Criterios de aceptación del Riesgo Residual[17].

A partir de los criterios RAE (Reducir, Aceptar y Evitar), el Ministerio establece las siguientes acciones para los niveles de aceptación a los riesgos así:

CRITERIOS	ACCIONES
ACEPTAR	Se debe asumir el riesgo y el impacto de su materialización en caso que se presente.
EVITAR	Se debe eliminar, evitar o cambiar la actividad generadora del riesgo.
REDUCIR	Adoptar acciones para abordar riesgos encaminadas a reducir, mitigar o transferir el riesgo, no necesariamente las acciones es un control adicional.

Tabla 11. Acciones para los niveles de aceptación del Riesgo Residual

De acuerdo con la ubicación en la zona del riesgo residual se deben implementar los siguientes niveles de aceptación:

[17] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020

ZONA DE RIESGO	NIVEL DE ACEPTACIÓN DEL RIESGO RESIDUAL	
	Gestión y Seguridad de la Información	Corrupción y Fraude
Bajo	ACEPTAR - EVITAR	Ningún riesgo de corrupción podrá ser aceptado.
Moderado	EVITAR - REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO) - ACEPTAR	REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO) - EVITAR
Alto	EVITAR - REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO) Los riesgos ubicados en esta zona deben contar con un indicador de riesgo, para monitorear el comportamiento	EVITAR - REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO) Los riesgos ubicados en esta zona deben contar con un indicador de riesgo, para monitorear el comportamiento
Extremo	EVITAR - REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO) Los riesgos ubicados en esta zona deben contar con un indicador de riesgo, para monitorear el comportamiento	EVITAR - REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO) Los riesgos ubicados en esta zona deben contar con un indicador de riesgo, para monitorear el comportamiento

Tabla 12. Niveles de aceptación del Riesgo Residual.[18]

[18] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020

TÍTULO IV. MONITOREO Y SEGUIMIENTO A LOS RIESGOS

- **Monitoreo línea estratégica**[19]

La Alta Dirección y el Comité Institucional de Coordinación de Control Interno (CICCI), definen el marco general para la gestión del riesgo y el control, verifican el cumplimiento de los lineamientos establecidos de la presente política, analizan el resultado de las evaluaciones de la gestión del riesgo elaboradas por la segunda y tercera línea de defensa y definen ajustes o modificaciones a que haya lugar, monitorean permanentemente los cambios en el entorno (interno y externo) que puedan afectar la efectividad del SCI, monitorean el estado de los riesgos aceptados (apetito por el riesgo) con el fin de identificar cambios sustantivos que afecten el funcionamiento de la entidad.

- **Monitoreo primera línea de defensa:**

Los líderes de los procesos en conjunto con sus equipos monitorean y revisan periódicamente su Mapa de Riesgos y si es del caso lo ajustan. Según el resultado de la administración del riesgo, el líder del proceso solicita ajuste a los riesgos o controles a la Of. Asesora de Planeación Sectorial y elabora las acciones de mejora (acciones para abordar riesgos o acciones correctivas), según sea el caso, siguiendo la Guía de Acciones de Mejora.

El monitoreo a los riesgos lo empieza a realizar la primera línea de defensa (responsables de proceso y equipos de trabajo), mediante el uso de indicadores de gestión claves, que permiten realizar seguimiento a las actividades generadoras de riesgos. Los Responsables de los Procesos deben definir las actividades claves a medir en sus procesos y realizar un monitoreo para identificar si se materializó el riesgo o si hay mayor o menor exposición a determinados riesgos o si los controles se están implementando correctamente, según aplique. En caso de materialización o posible materialización de un riesgo se debe informa a la Of. Asesora de Planeación Sectorial (OAPS).

- **Monitoreo segunda línea de defensa:**

La Of. Asesora de Planeación Sectorial (OAPS), como segunda línea de defensa realiza monitoreo a los riesgos mediante entrevista con la primera línea de defensa u otros mecanismos que se consideren pertinentes utilizar. La frecuencia del monitoreo se establece en la siguiente tabla:

<table>
<tr><th rowspan="2">Zona de Riesgo Residual</th><th colspan="2">Periodicidad</th></tr>
<tr><th>Riesgos Gestión y Seguridad de la Información</th><th>Riesgos de Corrupción y Fraude</th></tr>
<tr><td>Bajo</td><td rowspan="2">SEMESTRAL</td><td rowspan="3">CUATRIMESTRAL</td></tr>
<tr><td>Moderado</td></tr>
<tr><td>Alto</td><td rowspan="2">CUATRIMESTRAL</td></tr>
<tr><td>Extremo</td><td></td></tr>
</table>

Tabla 13. Frecuencia de monitoreo de Riesgo Residual.

[19] Las responsabilidades para la administración del riesgo se definieron con base en las líneas de defensa descritas en el Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG, anexo 7 criterios diferenciales.

NOTA: Los monitoreos a la matriz de riesgos se dejan registrados en el formato DE-FM-022 Matriz de Riesgos.

Los resultados del monitoreo de los riesgos de Corrupción y Fraude se presenta en el Comité Institucional de Coordinación de Control Interno, teniendo en cuenta ~~los criterios~~los criterios RAE: Reducir (transfiriendo o implementar acciones para abordar riesgos dirigidas a mitigar el riesgo), Aceptar y Evitar.

Para el caso de los Riesgos de Corrupción y Fraude, la Oficina Asesora de Planeación Sectorial publica en la página web institucional antes del 31 de enero de cada vigencia, la DE-FM-022 Matriz de Riesgos, así como cada cuatrimestre los seguimientos realizados a estos.

- **Evaluación tercera línea de defensa:**

Por su parte la Oficina de Control Interno como tercera línea de defensa evalúa los riesgos a través de las auditorías, evaluaciones y seguimientos en desarrollo del plan anual de auditorías y seguimientos definidos para la vigencia.

1. ACCIONES ANTE LOS RIESGOS MATERIALIZADOS

Cuando se evidencian riesgos materializados identificados durante las actividades de monitoreo y seguimiento (autoevaluación por parte del líder del proceso, o de los líderes de los sistemas de gestión implementados auditorías internas y externas a los sistemas de gestión, auditorías de gestión y seguimientos de la Oficina de Control Interno, peticiones, quejas, reclamos, sugerencias o denuncias, PQRSD, entre otras), se deben aplicar las acciones descritas en la siguiente tabla:

RESPONSABLE	ACCIÓN
Primera Línea de Defensa (Líder de Proceso)	• Informar a la Oficina Asesora de Planeación Sectorial y al líder del sistema de gestión implementado, sobre el hecho encontrado que evidencia la materialización del riesgo. • Para la materialización de los riesgos de **corrupción y fraude**, una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción y fraude), tramitar la denuncia ante la instancia de control correspondiente. • Para los riesgos de **seguridad de la información** proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso). • Identificar las **acciones correctivas** necesarias y documentarlas en ISOlución / Módulo Mejora, de acuerdo con lo establecido en la Guía. • Efectuar el análisis de causas y determinar acciones correctivas. • Implementar y realizar seguimiento a las acciones correctivas formuladas • Revisar el riesgo materializado y actualizarlo. • Socializar la actualización del DE-FM-022 Matriz de Riesgos, derivada del tratamiento de los riesgos materializados.
Segunda Línea de Defensa (OAPS, Secretaria General y líderes de	• Asesorar a los líderes de los procesos para la documentación de las acciones correctivas en ISOlucion/Módulo Mejora. • Acompañar a los líderes de los procesos en la revisión del riesgo materializado y en la actualización del mapa de riesgos. • Llevar el listado de los riesgos materializados en el formato DE-FM-XXX

Comentado [DYEV-C19]: Para los riesgos de **seguridad de la información** reportar oportunamente el evento o incidente para la adecuada gestión e implementar la medidas pertinentes que permitan contenerlo y garantizar la continuidad del servicio.

RESPONSABLE	ACCIÓN
los Sistemas de Gestión)	Listado de Riesgos Materializados
Tercera Línea de Defensa (Oficina de Control Interno)	• Informar al Líder del Proceso del riesgo materializado. • Informar a la segunda línea de defensa del riesgo materializado, con el fin de facilitar el inicio de las acciones correctivas correspondientes con el líder del proceso y la revisión del riesgo materializado. • Recomendar al líder del proceso en la revisión, análisis y formulación de acciones correctivas. • Verificar que se tomaron las acciones correctivas pertinentes y la actualización del mapa riesgo. • Para el riesgo de corrupción y fraude, una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción y fraude materializado), realizar la denuncia ante la instancia de control correspondiente.

Tabla 14. Acciones ante los riesgos materializados.

TÍTULO V. DOCUMENTACIÓN DE LOS RIESGOS

El Ministerio cuenta con el formato **DE-FM-022 Matriz de Riesgos** donde se identifican, valoran, evalúan y administran los riesgos de gestión, seguridad de la información , de corrupción y de fraude, por tanto, toda información asociada con los riesgos será provista por este documento.

La elaboración, revisión y aprobación de los **RIESGOS** se realiza conforme a la siguiente tabla:

ELABORA	REVISA	APRUEBA
Profesional(es) asignado(s) del Área / Dependencia	Jefe de la Oficina de Planeación Sectorial	Directivo / Jefe / Coordinador del Área / Dependencia

TÍTULO VI. ADMINISTRACIÓN DE OPORTUNIDADES

1. IDENTIFICACIÓN DE LAS OPORTUNIDADES

Las **oportunidades se identifican a partir del Marco Estratégico del MINCIT**, o el documento que establezca el direccionamiento estratégico, que estará asociado a aquellos eventos que permitan alcanzar un resultado esperado o aumentar los efectos deseables en el cumplimiento de los **objetivos estratégicos**. En algunos casos, sin que sea obligatorio, las oportunidades se pueden identificar también en los procesos.

2. VALORACIÓN DE LAS OPORTUNIDADES

Para valorar las oportunidades se evalúa la **probabilidad de lograr la oportunidad** y el **beneficio potencial de la oportunidad**, de acuerdo con los criterios definidos en las tablas.

- **Probabilidad de lograr la oportunidad:** Se califica la probabilidad de que ocurra y las ocurrencias previas de la oportunidad; es decir que tan posible es que se pueda realizar la oportunidad y analizar si la oportunidad se ejecutó anteriormente.

  La probabilidad de que ocurra y las **ocurrencias previas** de la oportunidad se valoran bajo la escala que se relaciona en las siguientes tablas:

Calificación	PROBABILIDAD QUE OCURRA LA OPORTUNIDAD
1	No puede ocurrir / No aplicable
2	Poco probable que ocurra
3	Algo probable que ocurra
4	Probable que ocurra
5	Es muy probable que ocurra

Tabla 15. Criterios para calificar la probabilidad de que ocurra la oportunidad

Calificación	OCURRENCIAS PREVIAS DE LA OPORTUNIDAD
1	Nunca ha ocurrido
2	No ha ocurrido en los pasados 10 años
3	No ha ocurrido en los pasados 5 años
4	Ha ocurrido en el último año
5	Ha ocurrido en los pasados 5 años

Tabla 16. Criterios para calificar las ocurrencias previas de la oportunidad

- **Beneficio potencial de la oportunidad:** Mide las mejoras y resultados que se pueden obtener con la implementación de la oportunidad**.**

  El **beneficio potencial** se valora bajo la escala que se relaciona en la siguiente tabla:

	Mejora la calidad del servicio	Mejora la satisfacción de las partes interesadas	Mejora el procesos o los procesos involucrados	Mejora de la reputación de la organización	Aporta al mejoramiento del SIG y MIPG	Se cuenta con recursos económicos para su posible implementación o se pueden conseguir	
No Hay/ NA	1	1	1	1	1	No hay recursos económicos	1
Menor	2	2	2	2	2	Se pueden conseguir pero es demorado	2
Moderado	3	3	3	3	3	Se pueden conseguir fácilmente	3
Alto	4	4	4	4	4	Si hay recursos económicos	4
Muy alto	5	5	5	5	5	No aplica	5

Tabla 17. Criterios para calificar el beneficio potencial de la oportunidad

Una vez valorada la **probabilidad de lograr la oportunidad** y el **beneficio potencial de la oportunidad se determina el FACTOR DE OPORTUNIDAD.**

- **FACTOR DE OPORTUNIDAD**

El **factor de oportunidad** está dado por las oportunidades que una vez calificadas son susceptibles de implementación, de acuerdo con el resultado obtenido. Este factor es el resultado de la multiplicación de la **probabilidad de lograr la oportunidad** y el **beneficio potencial de la oportunidad.**

De acuerdo con el resultado obtenido en cada oportunidad, se implementan las acciones establecidas en la siguiente tabla:

Calificación	Descripción
300 -180	Implementar oportunidad
179 - 110	Es optativo implementar la oportunidad
109 - 1	No se implementa la oportunidad

Tabla 18. Criterios para determinar el factor de oportunidad

3. RESPONSABILIDADES

- Es responsabilidad de la Alta Dirección definir y valorar las oportunidades que se podrían tratar en el MinCIT.
- Es responsabilidad del responsable del proceso o dependencia definir y realizar seguimiento al plan de acción de las oportunidades identificadas.

- Es responsabilidad de la Of. Asesora de Planeación Sectorial acompañar a la Alta Dirección en la definición y valoración de las oportunidades.
- Es responsabilidad de la Of. Asesora de Planeación Sectorial realizar seguimiento general a la Matriz de Oportunidades y presentar los resultados en la Revisión por la Dirección.

4. DOCUMENTACIÓN DE LAS OPORTUNIDADES

El Ministerio cuenta con el formato **DE-FM-023 Matriz de Oportunidades** donde se identifican, valoran y se realiza seguimiento toda información asociada con las oportunidades será provista por este documento.

Los planes de acción dirigidos a implementar las oportunidades se documentan como Oportunidad de mejora en el software ISOlución.

La elaboración, revisión y aprobación de las **OPORTUNIDADES** se realiza conforme a la siguiente tabla:

ELABORA	REVISA	APRUEBA
Alta Dirección – Acta de Comité	Jefe de la Oficina de Planeación Sectorial	Directivo / Jefe / Coordinador del Área / Dependencia

HISTORIAL DE CAMBIOS

VERSIÓN	FECHA VIGENCIA	RAZÓN DE LA ACTUALIZACIÓN
00	28/07/2020	Versión inicial. • Los documentos de riesgos estaban asociados al Proceso de Sistema de Gestión, de acuerdo con el objetivo pertenecen al Proceso de Direccionamiento Estratégico, por tal razón se trasladan. • Se crean los formatos DE-FM-022 Matriz de Riesgos, DE-FM-023 Matriz de Oportunidades • Aprobado en Comité Institucional de Coordinación de Control Interno, mediante Acta 02, del 28 de julio de 2020 • Con la creación de este documento se **eliminan** los siguientes documentos, que hacían parte del proceso de Sistema de Gestión: SG-PR-017 Procedimiento Gestión del Riesgo_v2 ES-GU-001 Guía para la Administración del Riesgo_v2 SG-FM-043 Matriz de identificación y seguimiento a mapas de riesgo._v6 SG-FM-067 Formulación y Monitoreo Mapa de Riesgos de Corrupción_v10 SG-FM-042 Plan de Contingencia._v4 Resolución 1900 del 03 de octubre de 2016
01		Se hacen las siguientes actualizaciones al documento según los nuevos lineamientos de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020: - Actualización de definiciones: - Se incluye medición para: Apetito al riesgo, tolerancia al riesgo, Capacidad de riego. - Se modifica la forma como se debe describir el riesgo. - Se adicionan algunas recomendaciones para la redacción del riesgo. - Se modifica el cuadro de clasificación del riesgo - Se modifica la valoración en la tabla de probabilidad - Se modifica la valoración en la tabla de impacto - Se modifican los mapas de Calor - Se incluye el control correctivo - Se modifican las etapas para la redacción de un control - Se incluye control manual y control automático - Se modificó la tabla de calificación de atributos para el diseño de los controles - Se incluye la fórmula para hallar el nivel de riesgo residual - Se modifica la tabla de niveles de aceptación de riesgo residual - Se modifica la tabla para monitoreo de riesgo residual - Se incluye el formato DE-FM-XXX Listado de Riesgos Materializados

REVISIÓN Y APROBACIÓN DEL DOCUMENTO

	ELABORÓ	REVISÓ	APROBÓ
Nombre:	Ivonn Moreno Barrera – Profesional Especializado Of. Planeación Sectorial / Liliana Núñez M. - Of. Planeación Sectorial	Manuela Miranda	
Cargo:		Jefe Of. Asesora de Planeación Sectorial	
Fecha de vigencia del documento:			

BIBLIOGRAFIA

Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020 y anexos

ANEXO 1. RESPONSABILIDADES POR LÍNEA DE DEFENSA PARA LA ADMINISTRACIÓN DEL RIESGO[20]

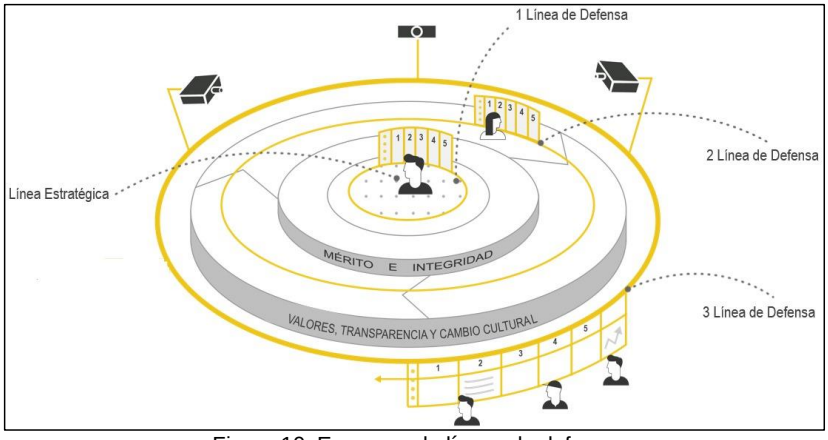


Figura 10. Esquema de líneas de defensa

En el ministerio las responsabilidades de carácter general por líneas de defensa para la administración de riesgos, se detallan a continuación:

LÍNEA	PROPÓSITO	RESPONSABLE	ACTIVIDADES
LINEA ESTRATÉGICA	Define el marco general para la gestión del riesgo y su control analiza los riesgos, monitorea la gestión y garantiza el cumplimiento de los planes estratégicos de la entidad (Objetivos, metas, indicadores)	**Al Ministro(a), equipo directivo (Secretario General, Viceministros, Directores) y al Comité Institucional de Coordinación de Control Interno les corresponde:**	**Por parte del Comité de Coordinación de Control Interno:** • Someter a aprobación del representante legal la política de administración del riesgo. • Revisar la exposición de la entidad a los riesgos de corrupción y fraude; si se cuenta con la línea de denuncia, monitorear el progreso de su tratamiento. • Verificar el cumplimiento de los lineamientos establecidos en la política de administración del riesgo, con énfasis en los de fraude y corrupción.
			Monitorear permanentemente los cambios en el entorno (interno y externo) que puedan afectar la efectividad del SCI.
			Monitorear el estado de los riesgos aceptados (apetito por el riesgo) con el fin de identificar cambios sustantivos que afecten el funcionamiento de la entidad.
			Monitorear al cumplimiento de la política de administración del riesgo de la entidad.
			Analizar el resultado de las evaluaciones de la gestión del riesgo, elaboradas por la segunda y tercera líneas de defensa,

[20] Las responsabilidades para la administración del riesgo se definieron con base en las líneas de defensa descritas en el Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG, anexo 7 criterios diferenciales.

LÍNEA	PROPÓSITO	RESPONSABLE	ACTIVIDADES
			para determinar el estado del SCI y definir los ajustes o modificaciones a que haya lugar.
PRIMERA LINEA DE DEFENSA	Desarrolla e implementa los procesos de control y gestión de riesgos, y detecta deficiencias (a través de su identificación, análisis, valoración, monitoreo, el control de una base del día a día de acciones de mejora.)	**Líderes de los Procesos y sus equipos de trabajo (en general servidores públicos en todos los niveles del Ministerio), les corresponde:**	Identificar los activos de información de su proceso.
			Identificar, valorar y definir la opción de tratamiento de los riesgos (gestión, corrupción, seguridad digital, fraude, financieros, entre otros) que pueden afectar el logro de los objetivos de los procesos, programas o proyectos en los cuales participe, acorde con la política de administración del riesgo.
			Identificar cambios que incidan en los riesgos y proponer los ajustes correspondientes.
			Identificar la posibilidad de fraude en los procesos, programas o proyectos en los cuales participe e informar oportunamente.
			Revisar en coordinación con la segunda línea de defensa en la identificación de riesgos.
			Definir y diseñar los controles que aplican (manuales o apoyados en TI) para gestionar ~~a~~ los riesgos, identificando: los responsables y su adecuada segregación de funciones, propósito, periodicidad, tratamiento en caso de desviaciones, forma de ejecutar el control y evidencias de su ejecución. (Ver Guía de Administración del Riesgo de Gestión, Corrupción y Seguridad Digital y Diseño de Controles para Entidades Públicas).
			Elaborar los mapas de riesgo, que incluyan los riesgos de gestión, corrupción, fraude y de seguridad digital, entre otros.
			Identificar cambios en los riesgos establecidos y proponer ajustes a los controles.
			Efectuar seguimiento a los riesgos y la efectividad de los controles de los procesos, determinar y proponer posibles mejoras en los mismos.
			Cumplir con las políticas y lineamientos para generar y comunicar la información relevante, de manera accesible, oportuna, confiable, íntegra y segura, que facilite las acciones de control en la entidad.
SEGUNDA LINEA DE DEFENSA	*Soporta y guía la línea estratégica *Supervisa, asegura y monitorea de manera independiente la pertinencia y eficacia en el cumplimiento de la gestión de riesgos de la primera línea que pueda afectar el cumplimiento de los objetivos	**El Jefe de la Oficina Asesora de Planeación Sectorial y líderes de los Sistemas de Gestión implementados en el Ministerio**	Evaluar y proponer modificaciones frente al diseño y desarrollo de la política para la Gestión de Riesgos, con el fin de mantenerla actualizada.
			Generar reportes periódicamente al Comité Institucional de Coordinación de Control Interno acerca del cumplimiento de las metas y los objetivos en relación a la gestión integral del riesgo.
			Evaluar y proponer estrategias de Gestión de Riesgos al Comité Institucional de Coordinación de Control Interno.
			Revisar las exposiciones al riesgo con los grupos de valor, proveedores, sectores económicos, áreas geográficas y tipos de riesgo (monitoreo del contexto estratégico).
			Supervisar y controlar el cumplimiento y la aplicación de políticas, límites y metodologías para gestionar los riesgos.
			Verificar en el marco de la política de riesgos institucional, que la identificación y valoración del riesgo de la primera línea sea adecuada frente al logro de objetivos y metas.

LÍNEA	PROPÓSITO	RESPONSABLE	ACTIVIDADES
	estratégicos o de los procesos. *Ayuda a los responsables de riesgos a distribuir la información adecuada sobre el riesgo a todos los servidores de la entidad.		Verificar la adecuada identificación de los riesgos relacionados con fraude y corrupción.
			Generar recomendaciones a las instancias correspondientes (primera, segunda, y línea estratégica), a partir de la información relacionada con la verificación a la identificación y valoración del riesgo.
			Analizar y verificar la adecuada identificación de los riesgos en relación con los objetivos institucionales o estratégicos y de los procesos, definidos desde el Direccionamiento Estratégico.
			Revisar en coordinación con la primera línea de defensa en la identificación de riesgos.
			Asegurar que los riesgos son monitoreados acorde con la política de administración de riesgo establecida para la entidad.
			Verificar el diseño y ejecución de los controles que mitigan los riesgos estratégicos o institucionales.
			Verificar el diseño y ejecución de los controles que mitigan los riesgos de fraude y corrupción.
			Hacer seguimiento a los mapas de riesgo y verificar su actualización de acuerdo a los cambios establecidos en la Política de Riesgos Institucional.
			El Oficial de Seguridad de la Información verifica el desarrollo y mantenimiento de controles de Tecnológicos y de seguridad y privacidad de la información
			Revisar en coordinación con la tercera línea de defensa la efectividad de los controles.
			Verificar que el diseño del control establecido por la primera línea de defensa sea pertinente frente a los riesgos identificados, analizando: los responsables y su adecuada segregación de funciones, propósito, periodicidad, tratamiento en caso de desviaciones, forma de ejecutar el control y evidencias de su ejecución, y efectuar las recomendaciones a que haya lugar ante las instancias correspondientes (primera, segunda, y línea estratégica).
			Verificar que los responsables estén ejecutando los controles tal como han sido diseñados.
			Verificar que los controles contribuyen a la mitigación de riesgos hasta niveles aceptables.
			Evaluar la gestión del riesgo de la entidad con énfasis en: *La exposición al riesgo, acorde con los lineamientos y la política institucional, *El cumplimiento legal y regulatorio, *Logro de los objetivos estratégicos o institucionales, *Confiabilidad de la información financiera y no financiera.
			Como resultado de la evaluación de la gestión del Riesgo comunica las deficiencias a la alta dirección o a las partes responsables para tomar las medidas correctivas, según corresponda.
			Revisar con la primera línea la adecuada formulación de los planes de mejoramiento y generar recomendaciones (análisis de causas, acciones, responsables y tiempos).

LÍNEA	PROPÓSITO	RESPONSABLE	ACTIVIDADES
			Verificar el avance y cumplimiento de las acciones incluidas en los planes de mejoramiento producto de las autoevaluaciones.
TERCERA LINEA DE DEFENSA	Provee aseguramiento independiente y objetivo sobre la efectividad en el cumplimiento de las responsabilidades de la línea estratégica, la primera y segunda línea de defensa con relación a la gestión de riesgos; a través de (evaluación) auditorías internas de control a la alta dirección de la entidad, en donde se valida que la gestión de riesgos es adecuada al logro de los objetivos institucionales y de los procesos	**Al Jefe de Control Interno, le corresponde:**	Verificar y evaluar que la entidad haya definido una política de administración del riesgo, atendiendo los lineamientos establecidos en la metodología adoptada por la entidad (Rol Enfoque hacia la prevención).
			Evaluar y alertar oportunamente sobre cambios que afecten la exposición de la entidad a los riesgos de corrupción y fraude. (Rol Enfoque hacia la prevención).
			Evaluar el cumplimiento de la política de administración del riesgo en todos los niveles de la entidad. (Rol Evaluación de la Gestión del Riesgo).
			Identificar y alertar al Comité de Coordinación de Control Interno posibles cambios que pueden afectar la evaluación y tratamiento del riesgo. (Rol Evaluación de la Gestión del Riesgo).
			Evaluar las actividades adelantadas por la segunda línea de defensa frente a la gestión del riesgo (oficina de planeación, direcciones o gerencias de riesgo), específicamente frente al análisis de contexto y de identificación del riesgo y de ser necesario asesorarlas, a fin de incorporar las mejoras correspondientes. (Rol Evaluación de la Gestión del Riesgo).
			Evaluar la efectividad de los controles, a partir de resultado del análisis del diseño, ejecución y la no materialización de los riesgos, y generar los informes ante las instancias correspondientes (primera, segunda, y línea estratégica). Se incluyen los controles tecnológicos y relacionados con riesgos de seguridad digital, los de fraude y de corrupción. (Rol de Evaluación de la Gestión del Riesgo).
			Evaluar que el diseño del control establecido sea adecuado frente a los riesgos identificados, analizando: los responsables y su adecuada segregación de funciones, propósito, periodicidad, tratamiento en caso de desviaciones, forma de ejecutar el control y evidencias de su ejecución, y generar los informes ante las instancias correspondientes (primera, segunda, y línea estratégica). Se incluyen los controles tecnológicos y relacionados con riesgos de seguridad digital, los de fraude y de corrupción. (Rol de Evaluación de la Gestión del Riesgo).
			Evaluar que los mapas de riesgos se encuentren actualizados. (Rol de Evaluación de la Gestión del Riesgo).
			Evaluar en coordinación con la segunda línea de defensa la efectividad de los controles. (Rol de Evaluación y Seguimiento).
			Establecer y ejecutar el plan anual de auditoría basado en riesgos, priorizando aquellos procesos de mayor exposición, así como la verificación del funcionamiento de los componentes de control interno e informar las deficiencias de forma oportuna a las partes responsables de aplicar las medidas correctivas (Línea estratégica, primera y segunda línea de defensa). (Rol de Evaluación y Seguimiento)

LÍNEA	PROPÓSITO	RESPONSABLE	ACTIVIDADES
			Evaluar la efectividad de las acciones desarrolladas por la segunda línea de defensa en aspectos como: cobertura de riesgos, cumplimientos de la planificación, mecanismos y herramientas aplicadas, entre otros, y generar observaciones y recomendaciones para la mejora. (Rol de Evaluación y Seguimiento).