



FUNCIÓN PÚBLICA

Guía para la Administración del Riesgo y el diseño de controles en entidades públicas

Versión 6

Dirección de Gestión y Desempeño Institucional
Noviembre 2022

Control de cambios al documento

Versión	Observación
Versión 1 Mayo de 2009	Creación Documento, basados en la Norma Técnica NTC5254
Versión 2 Septiembre de 2011	Se mantiene estructura conceptual, se actualizan lineamientos, acorde con la Norma ISO31000.
Versión 3 Octubre de 2014	Se mantiene estructura conceptual, se mejora visualmente mediante la inclusión de esquemas explicativos de los contenidos. Alineación con políticas de lucha contra la corrupción.
Versión 4 Octubre de 2018	Se mantiene estructura conceptual, se articulan las políticas de lucha contra la corrupción y seguridad de la información. Se define metodología para el diseño de controles.
Versión 5 Noviembre de 2020	Se mantiene estructura conceptual, con precisiones en los siguientes aspectos: 1. Ajustes en definición riesgo y otros conceptos relacionados con la gestión del riesgo. Se articula la institucionalidad de MIPG con la gestión del riesgo. 2. En paso 1: identificación del riesgo, se estructura propuesta para la redacción del riesgo. 3. Se amplían las tipologías de riesgo. 4. En paso 2 valoración del riesgo: se precisa análisis de probabilidad e impacto y sus tablas de referencia, así como el mapa de calor resultante. 5. Para el diseño y evaluación de los controles se ajusta tabla de calificación. 6. Se reubica y precisan las opciones de tratamiento del riesgo. 7. Se incluyen indicadores clave de riesgo. 8. Se precisan términos y uso relacionados con los planes de tratamiento del riesgo. 9. Se incluye en la caja de herramientas una matriz para el mapa de riesgos. 10. Se amplía el alcance de la seguridad digital a la seguridad de la información.
Versión 6 Noviembre de 2022	Se mantiene estructura conceptual para la administración del riesgo. Se incluye capítulo específico sobre riesgo fiscal, que se complementa con el Anexo denominado catalogo indicativo de puntos de riesgo fiscal para facilitar el análisis en el marco del modelo de operación por procesos.

César Augusto Manrique Soacha
Director

Jesús Hernando Amado Abril
Subdirector

Lidoska Julia Peralta Prieto
Secretaria General

Francisco Camargo Salas
Director de Empleo Público

Hugo Armando Pérez Ballesteros
Director de Desarrollo Organizacional

Hugo Armando Pérez Ballesteros
Director de Gestión y Desempeño Institucional (E)

Aura Isabel Mora
Directora de Participación, Transparencia y Servicio al Ciudadano

Armando López Cortés
Director Jurídico

Luz Stella Patiño Jurado
Jefe de Oficina de Control Interno

Bruce Vargas Vargas
Jefe Oficina de Tecnología de la Información y las Comunicaciones

Daniel Canal Franco
Jefe Oficina Asesora de Comunicaciones

Henry Humberto Villamarín Serrano
Jefe Oficina Asesora de Planeación

Elaborado por:
Departamento Administrativo de la Función Pública
-Myrian Cubillos Benavides
-Sandra Patricia Avellaneda Avendaño
-Eva Mercedes Rojas Valdés
- Damián Camilo Vargas Vargas

Secretaría de Transparencia (Contenidos 2018)
-Martha Ligia Ortega Santamaría
-Ana Paulina Sabbagh Acevedo
-María Victoria Sepúlveda Rincón

Grupo Interno de Seguridad y Privacidad de la Información – MinTIC
(Contenidos 2020)

-Ángela Janeth Cortés Hernández

-Danny Alejandro Garzón Aristizábal

Noviembre de 2022

Tabla de contenido

Presentación	9
Conceptos básicos relacionados con la gestión del riesgo	12
Antes de iniciar con la metodología.....	16
Institucionalidad.....	20
Beneficios	21
Acerca de la metodología.....	22
Paso 1: política de administración de riesgos	23
1.1 Lineamientos de la política de riesgos:	23
1.2 Marco conceptual para el apetito del riesgo:.....	26
Paso 2: identificación del riesgo	30
2.1 Análisis de objetivos estratégicos y de los procesos:.....	30
2.2 Identificación de los puntos de riesgo:	31
2.3 Identificación de áreas de impacto:	32
2.4 Identificación de áreas de factores de riesgo:.....	32
2.5 Descripción del riesgo.....	34
2.6 Clasificación del riesgo:	36
Paso 3: valoración del riesgo	39
3.1 Análisis de riesgos:	39
3.2 Evaluación de riesgos:	44
3.3 Estrategias para combatir el riesgo:	58
3.4 Herramientas para la gestión del riesgo:	59
3.5 Monitoreo y revisión:.....	61
4. Lineamientos para el análisis de riesgo fiscal	66
4.1 Control fiscal interno y prevención del riesgo fiscal:	66

4.2 Definición y elementos del riesgo fiscal:	68
4.3 Metodología y paso a paso para el levantamiento del mapa de riesgos fiscales:	69
5. Lineamientos sobre los riesgos relacionados con posibles actos de corrupción	83
6. Lineamientos riesgos de seguridad de la información	95
6.1. Identificación de los activos de seguridad de la información:	95
6.2. Identificación del riesgo:	98
6.3. Valoración del riesgo:	100
6.4 Controles asociados a la seguridad de la información	103
Referencias	106
Anexos.....	107

Índice de figuras

Figura 1 Esquema general del modelo integrado de planeación y gestión (MIPG)	16
Figura 2 Conocimiento y análisis de la entidad	18
Figura 3 Operatividad Institucionalidad para la Administración del Riesgo	20
Figura 4 Metodología para la administración del riesgo	22
Figura 5 Estructuración de la política de administración de riesgos	23
Figura 6 Definiciones de apetito, tolerancia y capacidad de riesgo	27
Figura 7 Análisis de objetivos	30
Figura 8 Desglose características SMART	31
Figura 9 Cadena de valor	32
Figura 10 Estructura propuesta para la redacción del riesgo	34
Figura 11 Ejemplo aplicado bajo la estructura propuesta para la redacción del riesgo	36
Figura 12 Relación ente factores de riesgo y clasificación del riesgo	38
Figura 13 Estructura para el desarrollo de la valoración del riesgo	39
Figura 14 Matriz de calor (niveles de severidad del riesgo)	44
Figura 15 Ejemplo aplicado bajo la estructura propuesta para la redacción del control	46
Figura 16 Ciclo del proceso y las tipologías de controles	46
Figura 17 Movimiento en la matriz de calor acorde con el tipo de control	49
Figura 18 Movimiento en la matriz de calor con el ejemplo propuesto	52
Figura 19 Estrategias para combatir el riesgo	58
Figura 20 Operatividad Esquema de líneas de defensa	64
Figura 21 Articulación modelo constitucional control fiscal y sistema de control interno	67
Figura 22 Conceptualización activos de información	95
Figura 23 Pasos para la identificación de activos	96
Figura 24 Formato de descripción del riesgo de seguridad de la información	99
Figura 25 Valoración del riesgo en seguridad de la información	102
Figura 26 Formato mapa riesgos seguridad de la información	105

Índice de tablas

Tabla 1 Factores de riesgo	33
Tabla 2 Clasificación de riesgos	37
Tabla 3 Actividades relacionadas con la gestión en entidades públicas	40
Tabla 4 Criterios para definir el nivel de probabilidad.....	41
Tabla 5 Criterios para definir el nivel de impacto	42
Tabla 6 Atributos de para el diseño del control	47
Tabla 7 Aplicación tabla atributos a ejemplo propuesto	50
Tabla 8 Aplicación de controles para establecer el riesgo residual	51
Tabla 9 Ejemplo mapa de riesgos acorde con el ejemplo propuesto	54
Tabla 10 Ejemplos indicadores clave de riesgo	60
Tabla 11 Preguntas orientadoras para puntos riesgo fiscal y causas inmediatas	70
Tabla 12 Ejemplos adicionales acorde con el objeto sobre el que recae el efecto dañoso	74
Tabla 13 Ejemplo identificación activos del proceso	97
Tabla 14 Tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo	98
Tabla 15 Controles para riesgos de seguridad de la información	104

Presentación

El Departamento Administrativo de la Función Pública, como entidad técnica, estratégica y transversal del Gobierno nacional, pone a disposición de las entidades la metodología para la administración del riesgo que incorpora el capítulo relacionado con riesgo fiscal.

El capítulo que se incluye presenta el paso a paso para la gestión del riesgo fiscal (Identificación, análisis y valoración), que debe vincularse al análisis general de los riesgos institucionales, a fin de contar con un esquema integral que facilite su seguimiento por parte de los líderes del proceso. La metodología que se propone a través del desarrollo de dicho capítulo, es de gran utilidad para gestionar de manera efectiva los recursos, bienes e intereses públicos, previniendo efectos dañosos, lo cual a la vez permite, mitigar la posibilidad de configuración de responsabilidades fiscales para los diferentes gestores públicos.

Como parte integral de la metodología propuesta para el análisis de riesgo fiscal, se pone a disposición, como insumo de referencia, un catálogo indicativo y enunciativo de puntos de riesgo fiscal y circunstancias Inmediatas, documento que se consolida a partir del análisis de investigaciones previas y del estudio detallado de información sobre:

- (i) Fallos con responsabilidad fiscal, en firme, emitidos en los últimos 3 años, por una muestra de 10 de las contralorías territoriales mejor calificadas en 2020, según el criterio de desempeño integral, el cual corresponde a evaluación realizada por la Auditoría General de la República.
- (ii) Muestra aleatoria de fallos con responsabilidad fiscal, en firme, emitidos por la Contraloría General de la República en los últimos 3 años.
- (iii) Listado de hallazgos fiscales por temáticas, consolidado por la Auditoría General de la República, 2021.

Se precisa que los desarrollos metodológicos generales que se despliegan en el primer capítulo se mantienen y se articulan en los pasos de política, identificación y valoración del riesgo, con el capítulo de riesgo fiscal.

Atendiendo lo anterior y dando inicio a la estructura metodológica, en el paso 1, *política de administración del riesgo*, se definen los lineamientos para su elaboración, en articulación con el esquema de líneas de defensa¹ eje articulador definido en la Dimensión 7 Control Interno del Modelo Integrado de Planeación y Gestión MIPG, teniendo en cuenta que se trata de un paso esencial en cabeza de la alta dirección de las entidades, en tanto se constituye en la base para la gestión del riesgo en todos los niveles organizacionales; en el paso 2, *identificación del riesgo*, se propone una estructura para la redacción adecuada del riesgo, lo que facilita el análisis de la causa raíz y se proponen una serie de premisas básicas para evitar errores o generalizaciones del riesgo que dificultan la aplicación de los pasos siguientes definidos en la metodología. En este mismo apartado se precisan los factores de riesgo y su relación con las tipologías de riesgo.

En el paso 3, *valoración del riesgo*, se establecen los criterios para el análisis de probabilidad e impacto del riesgo identificado y su respectivo nivel de severidad, en este apartado se propone la tabla para el análisis de probabilidad con un enfoque en la exposición al riesgo, análisis que le permite a los líderes de proceso contar con elementos objetivos para su definición; en cuanto a la tabla de impacto, se consideran la afectación económica y reputacional como aspectos principales frente a la posible materialización de los riesgos, en tal sentido, se ajusta la matriz de calor de acuerdo con la escala de severidad definida en 5 zonas (baja, moderada, alta y extrema), elementos que, en su conjunto, plantean un análisis más ácido, es decir de mayor profundidad y estricto, teniendo en cuenta el entorno cambiante en el cual se desenvuelven las entidades públicas del país.

¹ Estructura de asignación de responsabilidades y roles para la gestión del riesgo y el control, el cual se distribuye en diversos servidores de la entidad, no siendo ésta una tarea exclusiva de las oficinas de control interno.

En el análisis de controles de este mismo paso 2 de valoración se propone una estructura para su redacción, se mantienen los atributos propuestos en la versión 2018 en cuanto a su diseño y ejecución y se agrega una nueva tabla de análisis a partir de la cual se calcularán los movimientos en la matriz de calor. Este esquema les permitirá una reducción sustancial en los pasos, además de poder establecer la eficiencia de los controles identificados, lo que le facilita a los responsables su aplicación, así como el seguimiento y evaluación por parte de las oficinas de control interno y de los organismos de control.

En los capítulos finales se aclaran temas como las opciones de tratamiento del riesgo y los indicadores clave de riesgo, estos últimos como herramienta para la toma de decisiones y para determinar la efectividad en la gestión del riesgo.

Dando continuidad a la articulación requerida en el marco del Modelo Integrado de Planeación y Gestión MIPG, se mantienen los capítulos relacionados con las políticas de transparencia, acceso a la información pública y lucha contra la corrupción liderada por la Secretaría de Transparencia y la de seguridad de la información en cabeza del Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC) respectivamente.

Finalmente, en los anexos se adiciona el catálogo indicativo y enunciativo de puntos de riesgo fiscal y circunstancias Inmediatas que complementa el capítulo relacionado con riesgo fiscal; se mantienen los anexos sobre la matriz propuesta para la construcción del mapa de riesgos, el anexo 4 Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas del Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC) y el protocolo para la identificación de riesgos de corrupción, asociados a la prestación de trámites y servicios, en el marco de la política de racionalización de trámites, liderado por la dirección de participación, transparencia y servicio al ciudadano de Función Pública.

Conceptos básicos relacionados con la gestión del riesgo

A continuación, se relacionan una serie de conceptos, necesarios para la comprensión de la metodología que se desarrolla a partir del paso 1 política de administración del riesgo, hasta el paso 3 valoración del riesgo. De igual forma, se consideran aquellos relacionados con los capítulos 4, 5 y 6 sobre riesgo fiscal, riesgos de corrupción y de seguridad de la información respectivamente.

<p>Riesgo: Efecto que se 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, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.</p>	<p>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).</p>	<p>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</p>	<p>Riesgo fiscal: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial². (ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).</p>
<p>Gestión del Riesgo Fiscal: son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).</p>	<p>Gestor público: Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales³. A título de ejemplo, además de los gestores fiscales, son gestores públicos, entre otros (sin perjuicio de las</p>	<p>Gestor Fiscal: Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes</p>	<p>Recurso público: Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública. Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que</p>

² Concepto propuesto por Función Pública, a partir del análisis de fallos de responsabilidad fiscal y literatura investigada sobre el tema.

³ Esta definición de gestor público, es armónica con la evolución que ha tenido el alcance de quien puede ser potencial responsable fiscal (art. 4 Decreto 403 de 2020 y ar. 37 Ley 2195 de 2022). Adicionalmente, para mayor claridad, dentro del glosario se incluirá el concepto de gestor público, el cual se encuentra en armonía con la normativa actual sobre la materia

<p>Bien público: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:</p> <p>a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional.</p> <p>Ejemplos: Las calles, plazas, puentes, vías, parques etc.</p> <p>b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades.</p> <p>Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.</p>	<p>particularidades de cada entidad): los contratistas, los interventores, los supervisores y en general todos los servidores públicos.</p>	<p>públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique)⁴. A título de ejemplo son gestores fiscales, entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.</p>	<p>resultan del ejercicio de funciones públicas por particulares.</p>
<p>Intereses patrimoniales de naturaleza pública: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas.</p> <p>Ejemplos: Son algunos ejemplos de intereses patrimoniales de naturaleza pública, la rentabilidad proyectada de cualquier inversión pública, es decir antes de que se causen o generen efectivamente; la cobertura de garantías y pólizas; la participación accionaria pública en una empresa de economía mixta o en una empresa de servicios públicos con socio o socios públicos; los rendimientos financieros y frutos de recursos públicos cuando se proyectan, es decir antes de que se causen o generen efectivamente; así como, los intereses moratorios, indexaciones, actualización del dinero en el tiempo, estimación de pérdida de costo de oportunidad, cuando se trata de cobrar recursos públicos que un tercero debe:</p>		<p>Patrimonio público: se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C-340-07).</p>	<p>Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.</p>

⁴ Con la Ley 610 de 2000, específicamente el artículo 3°, hoy no sólo el gestor fiscal es responsable fiscal, sino que también la ley reconoce como potenciales generadores de daño fiscal y por lo tanto responsables fiscales, a los que concurrent, inciden o contribuyen directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública.

	<p>explotación de bienes públicos y/o recaudo de recursos públicos por un particular sin contrato o habilitación legal.</p>	<p>Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.</p> <p>Nota: Tratándose de riesgo fiscal, se usa el término circunstancia inmediata (Causa Inmediata, pero se asocia a la misma causa inmediata.</p>	<p>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.</p> <p>Nota: Tratándose de riesgo fiscal, el impacto siempre será económico y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos.</p>
<p>Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo</p>		<p>Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.</p> <p>Causa Raíz (Causa Eficiente o Causa Adecuada):⁵ Es el evento (acción u omisión) que de presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera. Así las cosas, la causa raíz se asocia con aquel hecho potencial generador del daño.</p>	
<p>Punto de Riesgo: Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública.</p> <p>Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han</p>	<p>Control: Medida que permite reducir o mitigar un riesgo.</p>	<p>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.</p>	<p>Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.</p>

⁵ Términos similares utilizados por la Contraloría General de la República. En el ámbito de la responsabilidad fiscal se usa el concepto de causa eficiente y acusa adecuada, refiriéndose en términos generales, al hecho generador del daño, es decir, aquel sin el cual el daño no se produciría.

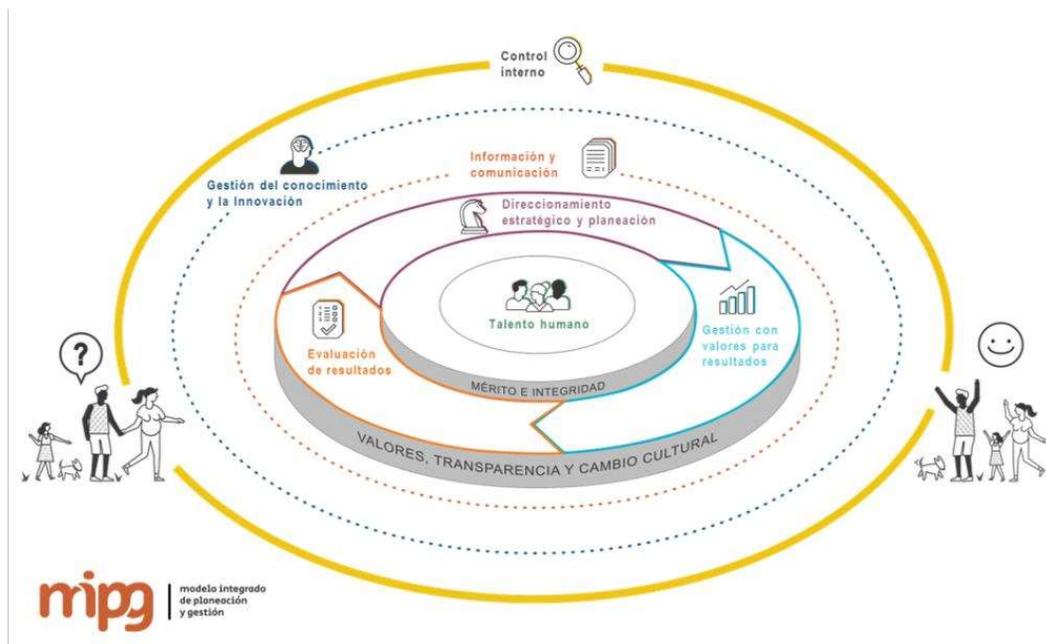
<p>presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales. Para facilitar el ejercicio de identificación de puntos de riesgo consulte el Anexo: Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas.</p>			
<p>Factores de Riesgo: Son las fuentes generadoras de riesgos.</p>	<p>Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados</p> <p>Activo: En el contexto de 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.</p>	<p>Integridad: Propiedad de exactitud y completitud.</p> <p>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 de Riesgo poder 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.</p>	<p>Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.</p> <p>Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.</p>
<p>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.</p>	<p>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.</p>	<p>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.</p>	

Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

Antes de iniciar con la metodología

El modelo integrado de planeación y gestión (MIPG) es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar las actividades de las entidades y organismos públicos, este modelo tiene el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en el servicio (Manual operativo MIPG, 2019, p. 6). El MIPG opera a través de 7 dimensiones (talento humano, direccionamiento estratégico, gestión con valores para el resultado, evaluación de resultados, información y comunicación, gestión del conocimiento y la innovación y, finalmente, control interno) que agrupan las políticas de gestión y desempeño institucional y que, implementadas de manera articulada e interrelacionada, permitirán que el modelo funcione y opere adecuadamente. La Figura 1 ilustra las 7 dimensiones del modelo:

Figura 1 Esquema general del modelo integrado de planeación y gestión (MIPG)



Fuente: Departamento Administrativo de la Función Pública, MIPG, 2017.

De acuerdo con el numeral 2.2.1 “política de planeación institucional” de la dimensión “Direccionamiento estratégico y planeación” del MIPG, para responder a la pregunta ¿cuáles son las prioridades identificadas por la entidad y señaladas

en los planes de desarrollo nacionales y territoriales?, se deben formular las metas de largo plazo, tangibles, medibles, audaces y coherentes con los problemas y necesidades que deben atender o satisfacer, evitando proposiciones genéricas que no permitan su cuantificación y definiendo los posibles riesgos asociados al cumplimiento de las prioridades.

En este sentido, es claro que la identificación y valoración de riesgos se integra en el desarrollo de la estrategia, la formulación de los objetivos de la entidad y la implementación de esos objetivos a través de la toma de decisiones cotidiana en cada uno de los procesos.

Este desarrollo se da en los diferentes niveles de la organización, por lo que cada entidad, de acuerdo con su esquema de direccionamiento estratégico, procesos, procedimientos, políticas de operación, sistemas de información, tendrá insumos esenciales para iniciar con la aplicación de la metodología propuesta para la administración del riesgo. En la Figura 2 se puede observar esta interrelación.

Figura 2 Conocimiento y análisis de la entidad

MODELO DE OPERACIÓN POR PROCESOS

El modelo de operación por procesos es el estándar organizacional que soporta la operación de la entidad pública, integrando las competencias constitucionales y legales que la rigen con el conjunto de planes y programas necesarios para el cumplimiento de su misión, visión y objetivos institucionales. Pretende determinar la mejor y más eficiente forma de ejecutar las operaciones de la entidad.

PLANEACIÓN INSTITUCIONAL

Las estrategias de la entidad, generalmente se definen por parte de la Alta Dirección y obedecen a la razón de ser que desarrolla la misma, a los planes que traza el Sectorial al cual pertenece (plan estratégico sectorial), a políticas específicas que define el Gobierno nacional, departamental, o municipal enmarcadas dentro del Plan Nacional de Desarrollo. En este contexto la entidad define su planeación institucional. La planeación institucional hace uso de los procesos estratégicos, misionales, de apoyo y de evaluación para materializarla o ejecutarla, por lo tanto la administración del riesgo no puede verse de forma aislada.

ASPECTOS

CADENA DE VALOR:

Es la interrelación de los procesos dirigidos a satisfacer las necesidades y requisitos de los usuarios.

MAPA O RED DE PROCESOS:

Es la representación gráfica de los procesos estratégicos, misionales, de apoyo y de evaluación y sus interacciones.

OBJETIVOS ESTRATÉGICOS

Identifican la finalidad hacia la cual deben dirigirse los recursos y esfuerzos para dar cumplimiento al mandato legal aplicable a cada entidad. El cumplimiento de estos objetivos institucionales se materializa a través de la ejecución de la planeación anual de cada entidad.



MISIÓN

Constituye la razón de ser de la entidad; sintetiza los principales propósitos estratégicos y los valores esenciales que deben ser conocidos, comprendidos y compartidos por todas las personas que hacen parte de la entidad.

VISIÓN

Es la proyección de la entidad a largo plazo, que permite establecer su direccionamiento, el rumbo, las metas y lograr su desarrollo. Debe ser construida y desarrollada por la Alta Dirección de manera participativa, en forma clara, amplia, positiva, coherente, convincente, comunicada y compartida por todos los miembros de la organización.

CARACTERIZACIÓN DE LOS PROCESOS:

Estructura que permite identificar los rasgos distintivos de los procesos. Establece su objetivo, la relación con los demás procesos, los insumos, los activos, su transformación a través de las actividades que desarrolla y las salidas del proceso, se identifican los proveedores y clientes o usuarios, que pueden ser internos o externos. Ver formato sugerido en el Anexo 1.

IMPORTANTE:

Para los objetivos de los procesos como punto de partida fundamental para la identificación del riesgo tenga en cuenta lo siguiente:

OBJETIVO DEL 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.

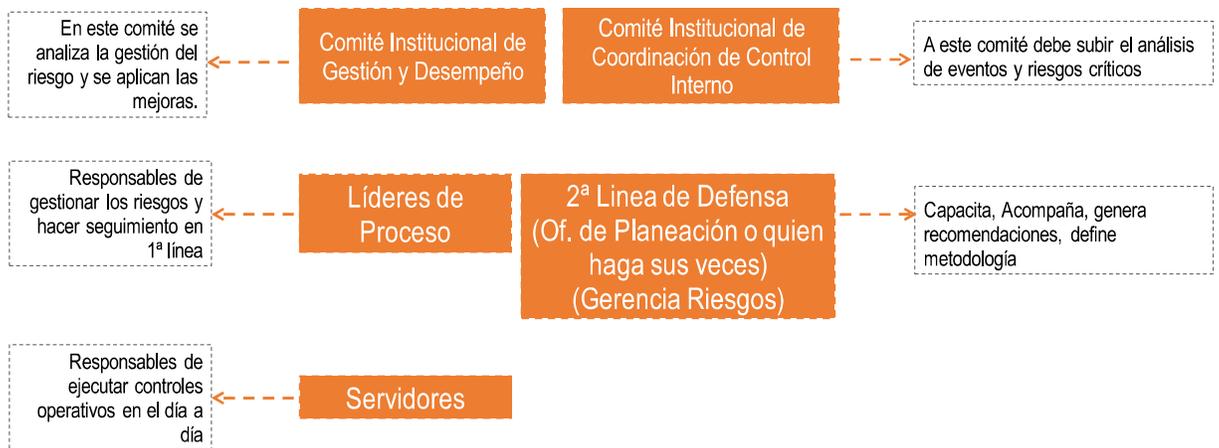
Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

Una vez determinados estos lineamientos básicos, es preciso analizar el contexto general de la entidad para establecer su complejidad, procesos y planeación institucional, entre otros aspectos, esto permite conocer y entender la entidad y su entorno, lo que determinará el análisis de riesgos y la aplicación de la metodología en general.

Institucionalidad

El modelo integrado de planeación y gestión (MIPG) define para su para su operación articulada la creación en todas las entidades del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, en este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:

Figura 3 Operatividad Institucionalidad para la Administración del Riesgo



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Nota: En entidades de alta complejidad se puede considerar la figura de gestores de riesgos. Se trata de personas clave en las áreas o procesos que ayudan al líder de proceso y a la 2ª línea de defensa en la gestión del riesgo, esta figura es opcional no obligatoria en su implementación.

Beneficios

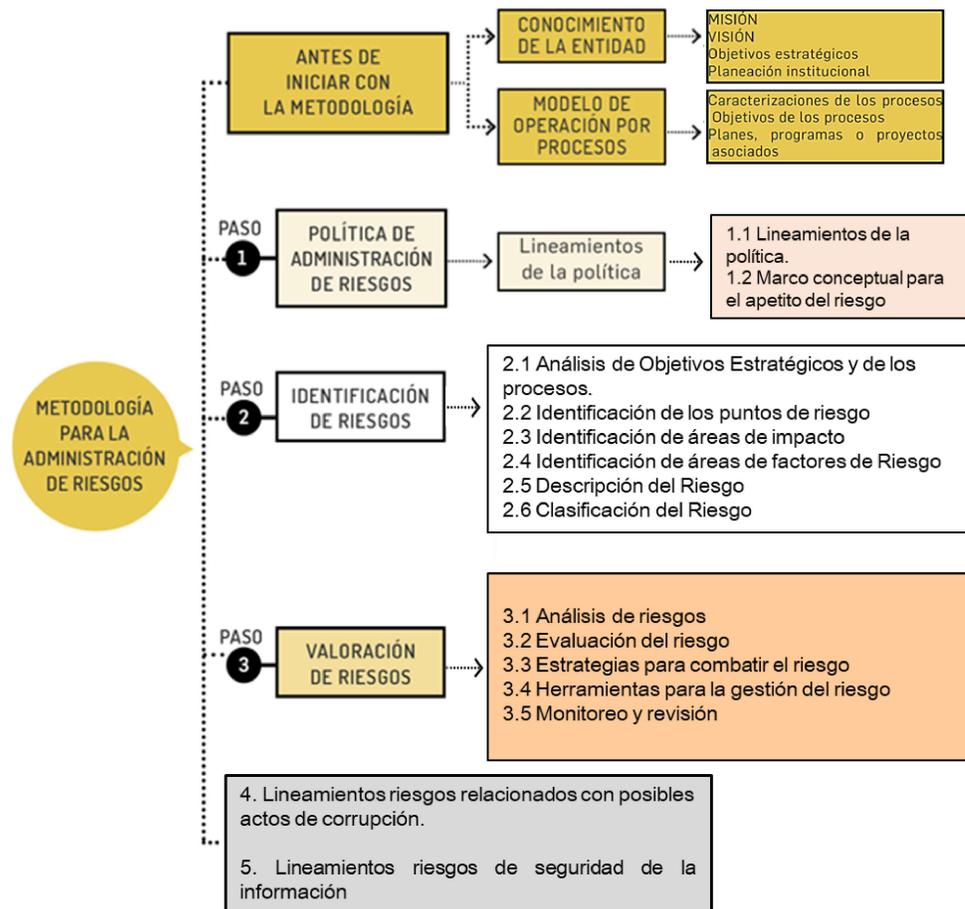
Considerando que la gestión del riesgo es un proceso efectuado por la alta dirección de la entidad y por todo el personal con el propósito de proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos, los principales beneficios para la entidad son los siguientes:

- Apoyo a la toma de decisiones
- Garantizar la operación normal de la organización
- Minimizar la probabilidad e impacto de los riesgos
- Mejoramiento en la calidad de procesos y sus servidores (calidad va de la mano con riesgos)
- Fortalecimiento de la cultura de control de la organización
- Incrementa la capacidad de la entidad para alcanzar sus objetivos
- Dota a la entidad de herramientas y controles para hacer una administración más eficaz y eficiente

Acerca de la metodología

La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada. A continuación se puede observar la estructura completa con sus desarrollos básicos:

Figura 4 Metodología para la administración del riesgo



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Paso 1: política de administración de riesgos

1.1 Lineamientos de la política de riesgos:

Figura 5 Estructuración de la política de administración de riesgos

¿QUÉ ES?

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.

¿QUIÉN LA ESTABLECE?

La Alta Dirección de la entidad
 Con el liderazgo del representante legal
 Con la participación del Comité Institucional de Coordinación de Control Interno



¿QUÉ SE DEBE TENER EN CUENTA?

Objetivos estratégicos de la entidad
 Niveles de responsabilidad frente al manejo de riesgos
 Mecanismos de comunicación utilizados para dar a conocer la política de riesgos en todos los niveles de la entidad

¿QUÉ DEBE CONTENER?

Objetivo:	Se debe establecer su alineación con los objetivos estratégicos de la entidad y gestionar los riesgos a un nivel aceptable.
Alcance:	La administración de riesgos debe ser extensible y aplicable a todos los procesos de la entidad. En el caso de los riesgos de seguridad digital, estos se deben gestionar de acuerdo con los criterios diferenciales descritos en el modelo de seguridad y privacidad de la información (ver caja de herramientas)
Niveles de aceptación al riesgo:	Decisión informada de tomar un riesgo particular (NTC GTC137, Numeral 3.7.1.6). Para riesgo de corrupción es inaceptable.
Niveles para calificar el impacto:	Esta tabla de análisis variará de acuerdo con la complejidad de cada entidad, será necesario considerar el sector al que pertenece (riesgo de la operación, los recursos humanos y físicos con los que cuenta, su capacidad financiera, usuarios a los que atiende, entre otros aspectos).
Tratamiento de riesgos:	Proceso para modificar el riesgo (NTC GTC137, Numeral 3.8.1.).
Periodicidad para el seguimiento de acuerdo con el nivel de riesgo residual.	

IMPORTANTE

El **MIPG** establece que esta es una tarea propia del equipo directivo y se debe hacer desde el ejercicio de **“Direccionamiento estratégico y de planeación”**. En este punto, se deben emitir los lineamientos precisos para el tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales.

Adicional a los riesgos operativos, es importante identificar los riesgos de corrupción, los riesgos de contratación, los riesgos para la defensa jurídica, los riesgos de seguridad digital, entre otros.

La aceptación del riesgo puede ocurrir sin tratamiento del riesgo. Los riesgos aceptados están sujetos a monitoreo.

Tenga en cuenta que los riesgos de corrupción son inaceptables.

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

La política de administración del riesgo puede convertirse en un manual o guía de riesgos, es importante que este documento incluya mínimo los siguientes aspectos:

- ✓ La metodología a utilizar.
- ✓ Niveles de Responsabilidad y autoridad frente a la Administración del riesgo en la entidad (acorde con el esquema de líneas de defensa).
- ✓ Acorde con el punto anterior, incluir la periodicidad para el monitoreo y revisión de los riesgos, donde se determine el seguimiento a los controles establecidos.
- ✓ En caso de que la entidad haya dispuesto un software o herramienta para su desarrollo, deberá explicarse su manejo.
- ✓ Incluir los aspectos relevantes sobre los factores de riesgo estratégicos para la entidad, a partir de los cuales todos los procesos podrán iniciar con los análisis para el establecimiento del contexto.
- ✓ Incluir todos aquellos lineamientos que en cada paso de la metodología sean necesarios para que todos los procesos puedan iniciar con los análisis correspondientes.
- ✓ Incluir los niveles de riesgo aceptado para la entidad y su forma de manejo.

- ✓ Incluir las tablas de probabilidad e impacto institucional.
- ✓ Incorporar los lineamientos para el manejo de riesgo fiscal, aquellos relacionados con posibles actos de corrupción y el anexo metodológico para la gestión de riesgos de seguridad de la información, temas articulados en la presente guía.
- ✓ Otros aspectos que la entidad considere necesarios deberán ser incluidos, con el fin de generar orientaciones claras y precisas para todos los funcionarios, de modo tal que la gestión del riesgo sea efectiva y esté articulada con la estrategia de la entidad.

Dado que se plantea articular los niveles de autoridad y responsabilidad en el marco del esquema de líneas de defensa, a fin de facilitar la estructura para los seguimientos y monitoreos en todos los niveles organizacionales, frente a la gestión del riesgo se debe considerar el siguiente marco general para la definición de actividades o acciones propias de cada línea así:

- ✓ Desde la **Línea Estratégica (Alta Dirección)** se debe definir y aprobar la Política de Administración del Riesgo, en el marco del Comité Institucional de Coordinación de Control Interno, acorde con la cual, atendiendo la periodicidad para el seguimiento a riesgos críticos debe aplicar el monitoreo correspondiente haciendo uso de la información suministrada por las instancias de 2ª línea identificadas, con base en lo cual toma las acciones necesarias para intervenir situaciones detectadas como incumplimientos, retrasos e incluso posibles actuaciones irregulares, evitando consecuencias más graves para la entidad.
- ✓ Desde la **1ª línea de defensa** todos los servidores tienen una responsabilidad frente a la aplicación efectiva de los controles, por lo que se trata de un seguimiento permanente, esto incluye la aplicación de controles de gerencia operativa que corresponde a aquellos que son aplicados por servidores con personal a cargo (jefes, coordinadores u otro cargo).
- ✓ Desde la **2ª línea de defensa**, el Jefe de planeación o quien haga sus veces debe periódicamente hacer un seguimiento a todos los riesgos, permitiendo que se generen recomendaciones y posibles ajustes a los mapas de riesgos, de manera tal que las instancias de 1ª línea pueden establecer mejoras a los riesgos y controles, así mismo garantizar su aplicación efectiva, lo que implica que se deben incorporar ejercicios de asesoría y acompañamiento a los líderes de los procesos y sus equipos para la mejora de este tema.
- ✓ Finalmente, para la **3ª línea de defensa** que corresponde a la Oficina de Control Interno o quien hace sus veces, a través de sus procesos de seguimiento y evaluación,

especialmente a través de la auditoría interna deben establecer la efectividad de los controles para evitar la materialización de riesgos. De igual forma, en el marco de su Plan Anual de Auditoría puede proponer esquemas de asesoría y acompañamiento a la entidad, actividades que puede coordinar con la Oficina de Planeación o quien haga sus veces.

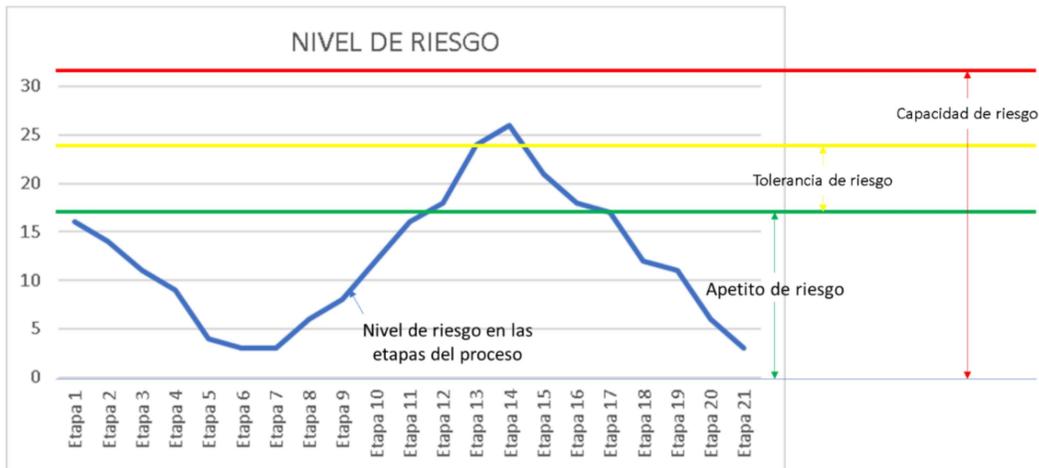
1.2 Marco conceptual para el apetito del riesgo:

Teniendo en cuenta que dentro de los lineamientos para la política de administración del riesgo se debe considerar el apetito del riesgo, a continuación se desarrolla conceptualmente este tema, a fin de contar con mayores elementos de juicio para su análisis en cada una de las entidades, iniciando con las siguientes definiciones:

- **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.
- **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 de riesgo 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.
- **Capacidad de riesgo:** es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

Gráficamente los anteriores conceptos se relacionan así:

Figura 6 Definiciones de apetito, tolerancia y capacidad de riesgo



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

Ahora bien, la norma IEC31010 Gestión del Riesgos – Técnicas de evaluación de riesgos (versión 2019) en su numeral 6.1.6.2 plantea lo siguiente:

“Criterios para decidir si el riesgo puede aceptarse

Los criterios para definir la naturaleza y alcance del riesgo que pueden aceptarse en la búsqueda de objetivos, a veces denominados apetito del riesgo, pueden definirse especificando una técnica para determinar la magnitud del riesgo o un parámetro relacionado con el riesgo, junto con un límite más allá del cual el riesgo se vuelve inaceptable. El límite establecido para el riesgo adverso inaceptable puede depender de posibles recompensas. La aceptabilidad del riesgo también puede definirse especificando la variación aceptable en medidas de desempeño específicas vinculadas a objetivos.

Se pueden especificar diferentes criterios según el tipo de consecuencia. Por ejemplo, los criterios de una organización para aceptar el riesgo financiero pueden diferir de los definidos para el riesgo para la vida humana. (...).”

Por su parte el Instituto de Auditores de España en su documento “Definición e implantación de Apetito de Riesgo” indica sobre el tema lo siguiente:

“(…) Cada organización puede optar por diferentes metodologías de cálculo, condicionadas por su sector de actividad e implantar modelos tanto cuantitativos como cualitativos. El uso de unos u otros normalmente depende del grado de estandarización que exista en el sector para la medición del apetito (condicionado en la mayoría de los casos por la existencia de regulación explícita al respecto, como es el caso del Sector Financiero). En los sectores en

los que no hay obligatoriedad ni modelos definidos, será cada empresa la que determine el método que desee seguir, en función principalmente de la naturaleza de los riesgos por medir. Para garantizar una gestión de riesgos integral y equilibrada, es recomendable combinar medidas cuantitativas con medidas cualitativas, así como tener en cuenta aquellos riesgos para los que la organización puede tener tolerancia cero.

Cabe destacar la existencia de dos posibles enfoques para la implantación del apetito de riesgo en las organizaciones:

- ✓ *El descendente o top down, basado en establecer el apetito de riesgo desde el más alto nivel organizativo, alineado con los objetivos estratégicos. Una vez validado formalmente por los órganos responsables, como el Consejo y/o la Comisión de Auditoría, se comunica al resto de la organización para alinear la gestión de riesgos de todas las áreas con el apetito de riesgo aprobado para toda la compañía, estableciendo niveles específicos de apetito para las distintas unidades que la componen.*
- ✓ *El enfoque ascendente o botton-up, por el contrario, define el apetito de riesgo al mínimo nivel de decisión dentro de una organización, para posteriormente ascender a lo más largo de la estructura organizativa hasta consolidarse en un apetito de riesgo global.*

(...)

En definitiva, desarrollar el apetito del riesgo no es un fin en sí mismo, ni debe consumir una cantidad desproporcionada de recursos. Cada organización deberá analizar su costo-beneficio y decidir si está justificada su implantación, así como el nivel de sofisticación que desea utilizar para sustentar el proceso de determinación de su apetito de riesgo. Bien definido y adecuadamente utilizado, el apetito de riesgo transforma métricas y métodos de evaluación de riesgos en decisiones de negocio y reporte. Además, establece los límites que forman un vínculo dinámico entre estrategia, objetivos y gestión de riesgos, lo que ayuda a optimizar la consecución de resultados y la creación de valor en las organizaciones. (...)

Teniendo en cuenta los anteriores lineamientos conceptuales, frente al apetito del riesgo cada organización debe establecer los criterios para su definición, considerando que pueden existir aspectos relacionados con la estrategia o bien estar planteados desde los procesos.

De igual forma, para su implantación debe mediar, en primer lugar, un lineamiento claro en la política de administración del riesgo de la entidad que permita definir el esquema y metodología, que tal como se ha explicado puede ser cualitativo o cuantitativo, o bien una combinación de ambos, de manera tal que por ejemplo, desde los procesos se puedan determinar cuáles riesgos de

zona baja pueden llegar a ser aceptados, pero que en cualquier caso deben ser monitoreados, a fin de garantizar que las condiciones bajo las cuales han sido analizados no han cambiado, si las condiciones cambian, es necesario volver a valorar y si es el caso determinar el manejo correspondiente a través de los controles que sean necesarios.

En todo caso la decisión de aceptar o no determinados riesgos que se ubiquen en zonas bajas es responsabilidad de la Alta Dirección, toda vez que es esta instancia la que define y aprueba la política de riesgos, donde se determinarán tales riesgos y su monitoreo correspondiente.

Lo anterior, indica que se trata de un análisis al más alto nivel, que exigen la aplicación integral de la metodología, lo que va a permitir hacer una evaluación del entorno, de las capacidades internas, así como de la estructura de operaciones para comprender y determinar con mayor claridad los aspectos aplicables en materia de riesgo aceptado, temas que se formalizarán a través de la política de administración del riesgo y se aplicará en la entidad en todos sus niveles y debe verse reflejada en los mapas de riesgo correspondientes al proceso, ya que si bien puede que no se apliquen acciones o controles específicos para esos niveles de aceptación, sí debe existir un monitoreo a fin de garantizar que las condiciones no han cambiado y que no se está superando los niveles de tolerancia establecidos. Así mismo, se requerirá un monitoreo por parte del Comité Institucional de Coordinación de Control Interno, donde la Línea Estratégica (alta dirección) evalúa la efectividad de la gestión del riesgo.

Nota Importante: Teniendo en cuenta la variedad de naturalezas jurídicas y complejidad de las diferentes entidades, frente a la definición del apetito del riesgo, cada organización podrá establecer su aplicabilidad o bien su exclusión, atendiendo un análisis interno de sus operaciones, usuarios, productos y servicios que ofrece, sector o entorno en el cual se desenvuelve, a fin de establecer si es viable su incorporación o definición.

Paso 2: identificación del riesgo

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos. Se aplican las siguientes fases:

2.1 Análisis de objetivos estratégicos y de los procesos: este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.

Figura 7 Análisis de objetivos

Análisis de objetivos estratégicos	Análisis de los objetivos de proceso
<p>La entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso.</p> <p>Es necesario revisar que los objetivos estratégicos se encuentren alineados con la Misión y la Visión Institucional, así como, analizar su adecuada formulación, es decir, que contengan las siguientes características mínimas: específico, medible, alcanzable, relevante y proyectado en el tiempo (SMART por sus siglas en inglés).</p>	<p>Los objetivos de proceso deben ser analizados con base en las características mínimas explicadas en el punto anterior, pero además, se debe revisar que los mismos estén alineados con la Misión y la Visión, es decir, asegurar que los objetivos de proceso contribuyan a los objetivos estratégicos.</p> <p>A continuación encontrará un ejemplo de análisis en el proceso de contratación:</p> <p>La entidad debe adquirir con oportunidad y calidad técnica, en no menos del 90%, los bienes y servicios requeridos para su continua operación.</p>

Fuente: Comité of Sponsoring Organizations of the Treadway Commission COSO Marco Integrado, Componente Evaluación de Riesgos, Principio, p. 73. 2013.

IMPORTANTE

Los objetivos deben incluir el "qué", "cómo", "para qué", "cuándo", "cuánto".

Si no están bien definidos los objetivos, no se puede continuar con la metodología de gestión del riesgo.

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

La entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión institucionales, así como su desdoble hacia los objetivos de los procesos. Se plantea la necesidad de analizar su adecuada formulación, es decir, que contengan unos atributos mínimos, para lo cual puede hacer uso de las características SMART⁶, cuya estructura se explica a continuación:

Figura 8 Desglose características SMART

- S** **Specific (específico):** Lo importante es resolver cuestiones como: qué, cuándo, cómo, dónde, con qué, quién. Considerar el orden y los necesarios para el cumplimiento de la misión.
- M** **Mensurable (medible):** Para ello es necesario involucrar algunos números en su definición, por ejemplo, porcentajes o cantidades exactas (cuando aplique).
- A** **Achievable (alcanzable):** Para hacer alcanzable un objetivo se necesita un previo análisis de lo que se ha hecho y logrado hasta el momento. Esto ayudará a saber si lo que se propone es posible o cómo resultaría mejor.
- R** **Relevant (relevante):** Considerar recursos, factores externos e información de actividades previas, a fin de contar con elementos de juicio para su determinación.
- T** **Timely (temporal):** Establecer un tiempo al objetivo ayudará a saber si lo que se está haciendo es lo óptimo para llegar a la meta, así mismo permite determinar el cumplimiento y mediciones finales.

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

2.2 Identificación de los puntos de riesgo: son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben

⁶ Hace referencia a las siglas en inglés que responden a: *specific* (específico); *mensurable* (medible); *achievable* (alcanzable); *relevant*; (relevante); *timely* (temporal)

mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

Figura 9 Cadena de valor



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2017.

2.3 Identificación de áreas de impacto: el área de impacto es 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.

2.4 Identificación de áreas de factores de riesgo: son las fuentes generadoras de riesgos. En la Tabla 1 encontrará un listado con ejemplo de factores de riesgo que puede tener una entidad.

Tabla 1 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
			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

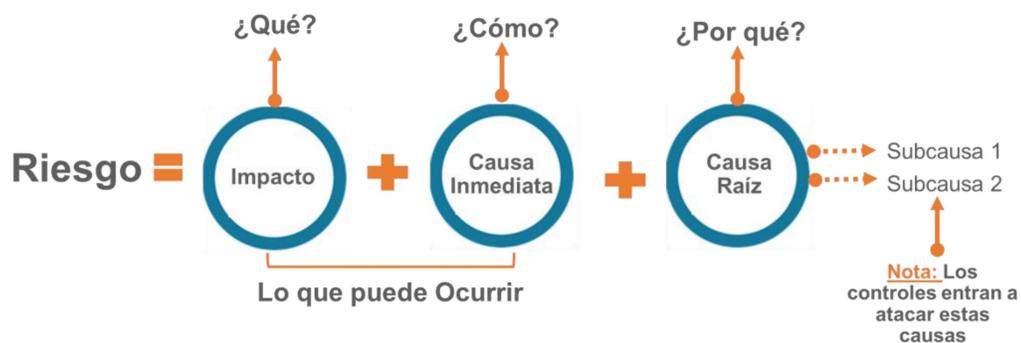
Factor	Definición		Descripción
Evento externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

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

NOTA: Los factores relacionados son una guía, cada entidad puede analizar los que considere de acuerdo con la complejidad propia de cada entidad y con sector en el que se desenvuelve, entre otros aspectos que puedan llegar a ser pertinentes para el análisis del contexto, e incluirlos como temas clave dentro de los lineamientos de la política de administración del riesgo.

2.5 Descripción del riesgo: la descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:

Figura 10 Estructura propuesta para la redacción del riesgo



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

La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

Desglosando la estructura propuesta tenemos:

- 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: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Ejemplo:

Proceso: gestión de recursos

Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

Alcance: inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquisidores) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas.

Atendiendo el esquema propuesto para la redacción del riesgo, tenemos:

Figura 11 Ejemplo aplicado bajo la estructura propuesta para la redacción del riesgo



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

Premisas 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.

Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes.

2.6 Clasificación del riesgo: permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

Tabla 2 Clasificación de riesgos

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 <i>hardware</i> , <i>software</i> , 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: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Teniendo en cuenta que en la Tabla 2 se definieron una serie de factores generadores de riesgo, para poder definir la clasificación de riesgos, su interrelación es la siguiente:

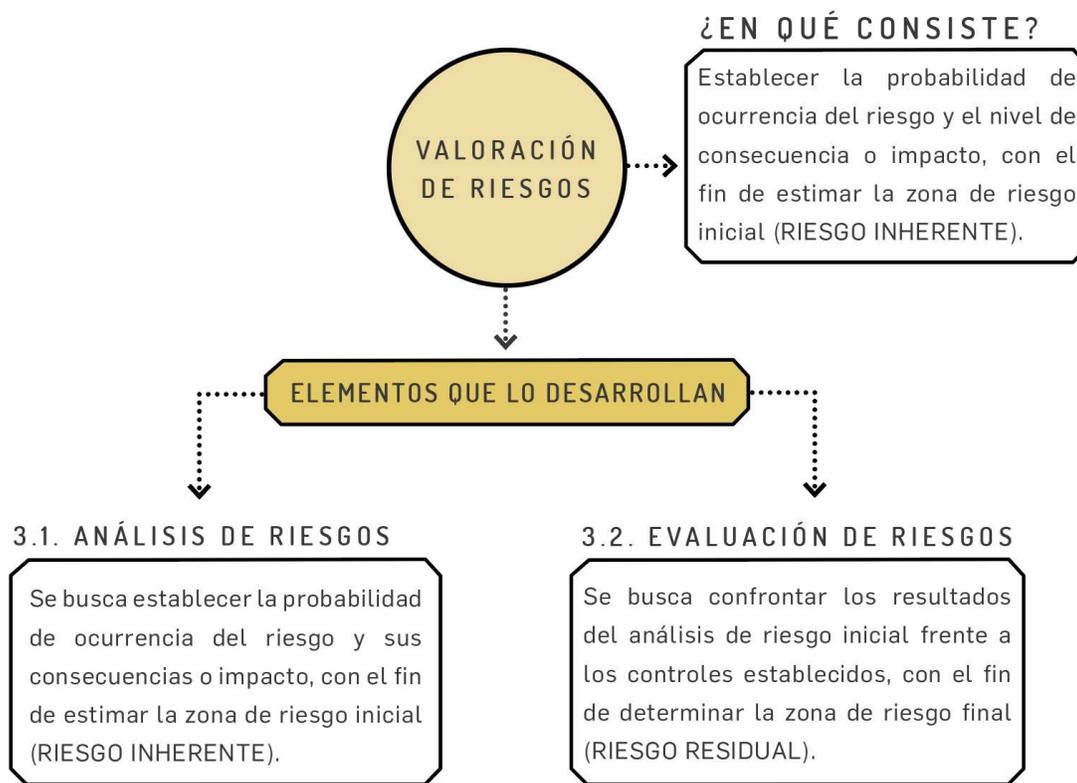
Figura 12 Relación ente factores de riesgo y clasificación del riesgo



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

Paso 3: valoración del riesgo

Figura 13 Estructura para el desarrollo de la valoración del riesgo



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

3.1 Análisis de riesgos: en este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

3.1.1 Determinar la probabilidad: se entiende como la posibilidad de ocurrencia del riesgo.

Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la **exposición al riesgo** del proceso o actividad que se esté analizando. De este

modo, la probabilidad inherente será el **número de veces que se pasa por el punto de riesgo en el periodo de 1 año.**

Bajo este esquema, la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, ya que bajo esta óptica, si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubicados en niveles bajos, situación que no es real frente a la gestión de las entidades públicas colombianas.

Como referente, a continuación se muestra una tabla de actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad:

Tabla 3 Actividades relacionadas con la gestión en entidades públicas

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
<p>*Tecnología (incluye disponibilidad de aplicativos), tesorería</p> <p>*Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez.</p> <p>Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60 días * 24 horas= 1440 horas.</p>	Diaria	Muy alta

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

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, la **exposición al riesgo** estará asociada al proceso o actividad que se esté analizando, es decir, al **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.

Tabla 4 Criterios para definir el nivel de probabilidad

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

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

Nota: Dependiendo del tamaño y complejidad de los procesos de la entidad, la tabla 4 podrá ser ajustada o adaptada a las necesidades de cada entidad.

3.1.2 Determinar el impacto:

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cabe señalar que en la versión 2018 de la Guía de administración del riesgo 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, todos estos temas se agrupan en impacto económico y reputacional en la versión 2020.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferente niveles se debe tomar el nivel 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 el más alto, en este caso sería el 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 darse en este tipo de análisis.

En la tabla 5 se establecen los criterios para definir el nivel de impacto.

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

Nota: Dependiendo del tamaño y complejidad de los procesos en la entidad, la tabla 5 podrá ser ajustada o adaptada a sus necesidades.

IMPORTANTE: Frente al análisis de probabilidad e impacto **no se utiliza criterio experto**, esto quiere decir 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, dicha situación se repite para el impacto, ya que 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.

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 afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.

N.º de veces que se ejecuta la actividad: la actividad de contratos se lleva a cabo 10 veces en el mes = 120 contratos en el año.

Cálculo afectación económica: de llegar a materializarse, tendría una afectación económica de 500 SMLMV.

Aplicando las tablas de probabilidad e impacto tenemos:

	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%

La actividad se realiza 120 veces al año, la probabilidad de ocurrencia del riesgo es **media**.

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

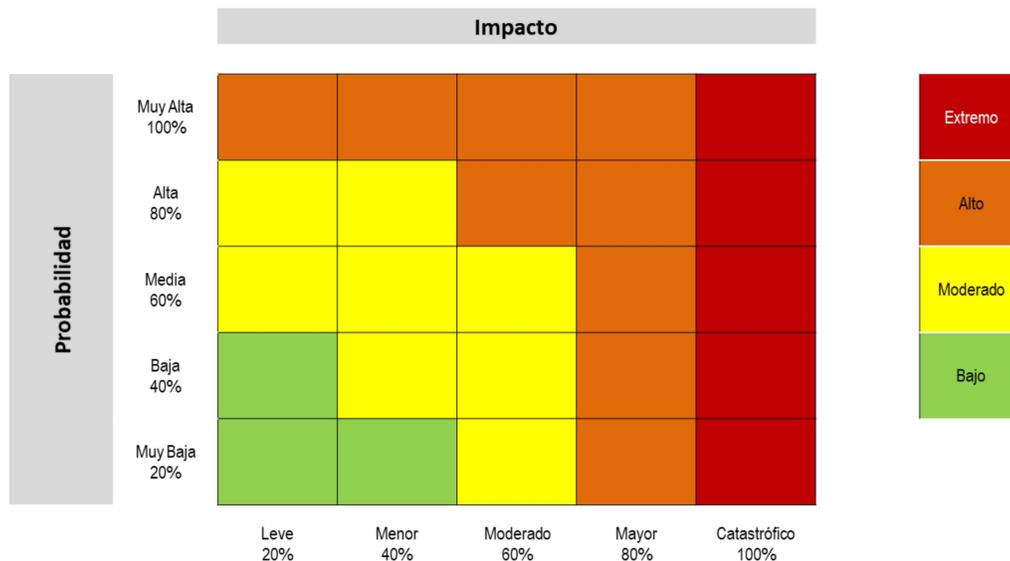
La afectación económica se calcula en 500SMLMV, el impacto del riesgo es **mayor**.

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

3.2 Evaluación de riesgos: 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).

3.2.1 Análisis preliminar (riesgo inherente): se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor (ver figura 14).

Figura 14 Matriz de calor (niveles de severidad del riesgo)



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

Ejemplo (continuación):

Proceso: gestión de recursos

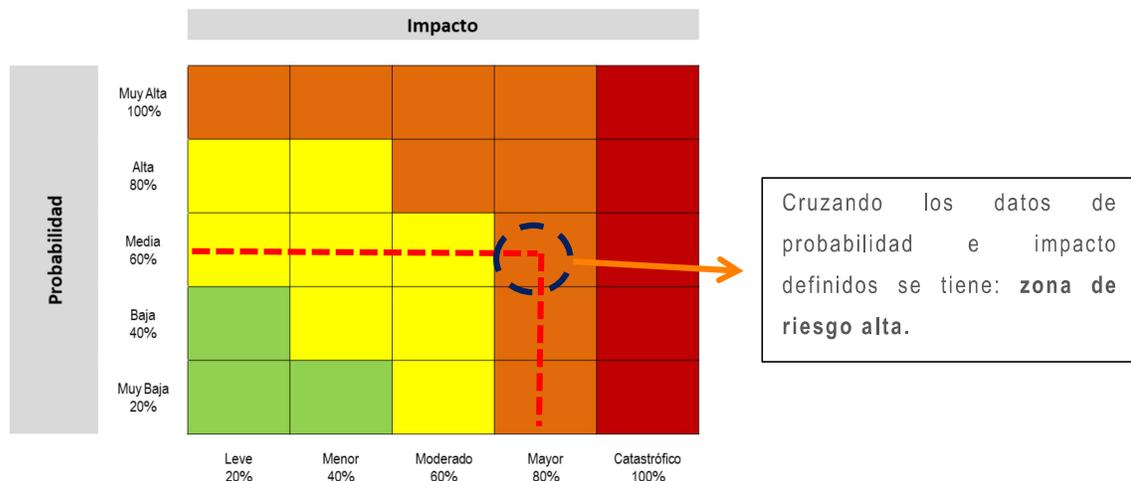
Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

Riesgo identificado: posibilidad de 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%

Aplicando la matriz de calor tenemos:



3.2.2 Valoración de controles: en primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

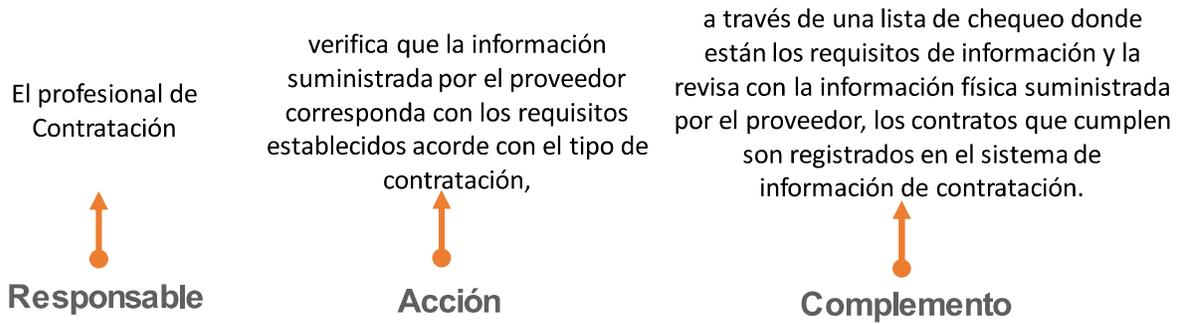
- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo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

3.2.2.1 Estructura para la descripción del control: para una adecuada redacción del control se propone 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 de que sean controles automáticos se identificará el sistema que realiza la actividad.
- **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.
- **Complemento:** corresponde a los detalles que permiten identificar claramente el objeto del control.

En la figura 15 se establece un ejemplo bajo esta estructura.

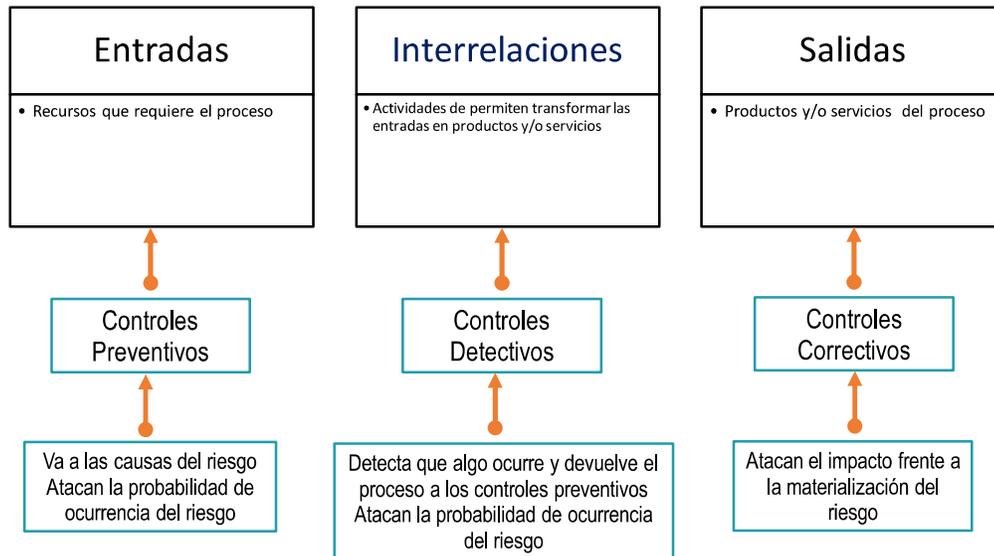
Figura 15 Ejemplo aplicado bajo la estructura propuesta para la redacción del control



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

3.2.2.2 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, en la figura 15 se consideran 3 fases globales del ciclo de un proceso así:

Figura 16 Ciclo del proceso y las tipologías de controles



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

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

- **Control preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las 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.

3.2.2.3 Análisis y evaluación de los controles – Atributos: A continuación se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la tabla 6 se puede observar la descripción y peso asociados a cada uno así:

Tabla 6 Atributos de para el diseño del control

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%

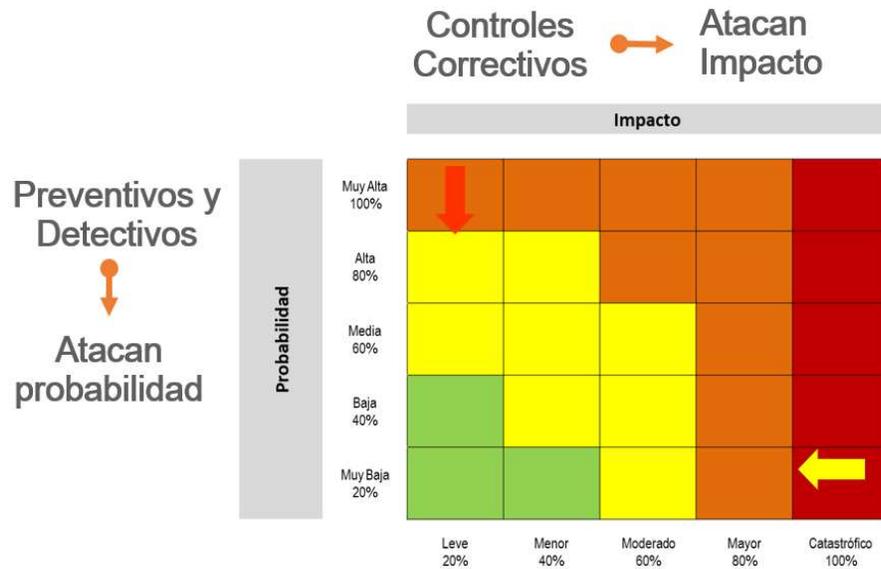
Características		Descripción	Peso	
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
*Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del 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: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 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 14 se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Figura 17 Movimiento en la matriz de calor acorde con el tipo de control



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 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 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 la tabla de atributos, esta le servirá como ejemplo para el análisis y valoración de los dos controles propuestos.

Tabla 7 Aplicación tabla atributos 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	X	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	Tipo	Preventivo		
		Detectivo	X	15%
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin documentar		-
	Frecuencia	Continua	X	-
Aleatoria			-	

Controles y sus características				Peso
inconsistencias, devuelve el proceso al profesional de contratos asignado.	Evidencia	Con registro	X	-
		Sin registro		-
Total valoración control 2				30%

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

3.2.3 Nivel de riesgo (riesgo residual): es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que los 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.

Para mayor claridad, 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: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 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 26.8%

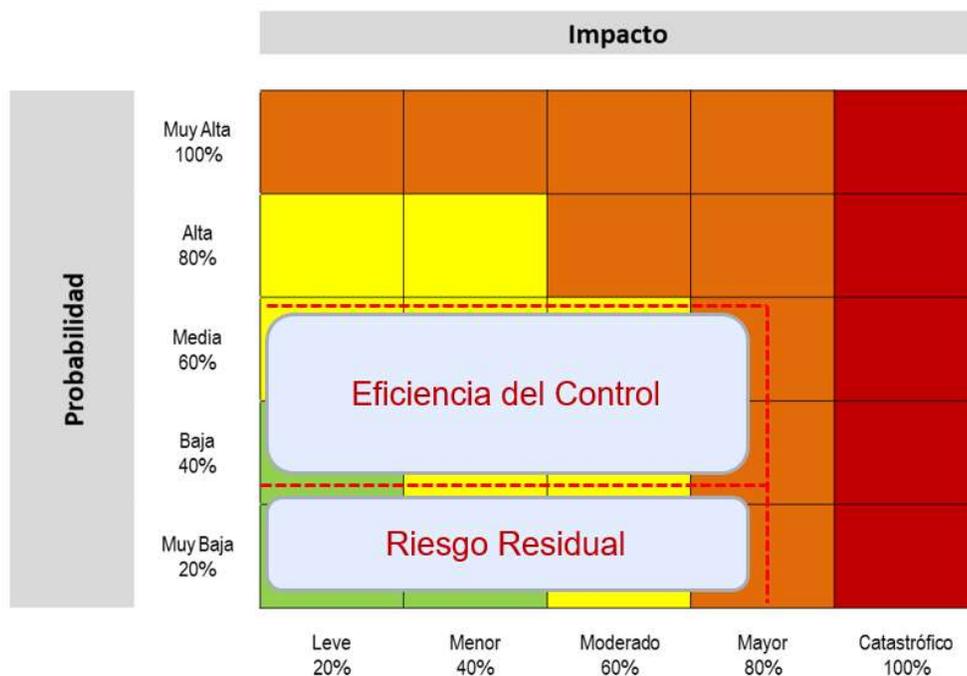
Impacto Residual: mayor 80%

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 18 se observa el movimiento en la matriz de calor.

Figura 18 Movimiento en la matriz de calor con el ejemplo propuesto



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

A continuación se podrá observar el formato propuesto para el mapa de riesgos, este incluye la matriz de calor correspondiente.

Formato mapa de riesgos

Parte 1 identificación del riesgo:

Tabla 9 Ejemplo mapa de riesgos acorde con el ejemplo propuesto

Gestión de recursos											
Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación											
Inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquisiciones) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas											
Referencia	Impacto	Causa inmediata	Causa raíz	Descripción del riesgo	Clasificación riesgo	Frecuencia	Probabilidad inherente	%	Impacto inherente	%	Zona de riesgo inherente
1	Afectación económica	Multa y sanción del organismo de control	Incumplimiento de los requisitos para contratación	Posibilidad de afectación económica por multa y sanciones del organismo de control debido la adquisición de bienes y servicios fuera de los requerimientos normativos.	Ejecución y administración de procesos	120	Moderada	60%	Mayor	80%	Alta

***Nota:** La columna referencia se sugiere para mantener el consecutivo de riesgos, así el riesgo salga del mapa no existirá otro riesgo con el mismo número. Una entidad puede ir en el riesgo 150, pero tener 70 riesgos, lo que permite llevar una traza de los riesgos. Esta información la debe administrar la oficina asesora de planeación o gerencia de riesgos.

Parte 2 Valoración del riesgo:

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	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.	X		Preventivo	Manual	40%	Documentado	Continua	Registro material	36%	Baja	25,2%	Mayor	80%	Alta	Reducir

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								
2	El jefe de 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.	X		Detectivo	Manual	30%	Documentado	Continua	Con registro	25,2%							

Parte 3 Planes de acción (para la opción de tratamiento reducir):

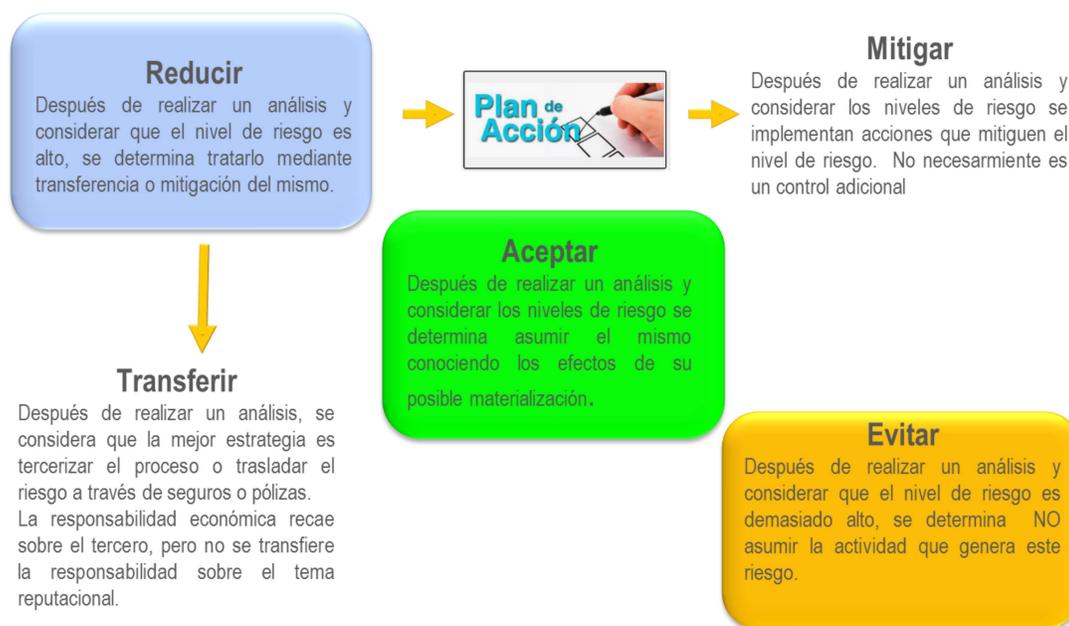
Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento	Seguimiento	Estado
Automatizar la lista de chequeo que utiliza el profesional de contratación, a fin de reducir la posibilidad de error humano y elevar la productividad del proceso.	Oficina de TIC	30/11/2020	30/06/2020	Se han adelantado las actividades de levantamiento de requerimientos funcionales para la automatización de la lista de chequeo.	En curso

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

3.3 Estrategias para combatir el riesgo: decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

En la figura 19 se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.

Figura 19 Estrategias para combatir el riesgo



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

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.

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 dentro del Plan de Continuidad de Negocio⁷ y se consideraría un control correctivo.

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:

3.4.1 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:

- Mesa de ayuda
- Las PQRD (peticiones, quejas, reclamos, denuncias)
- Oficina jurídica
- Líneas internas de denuncia

Este mecanismo genera información para que el evento no se vuelva a presentar, así mismo, es posible establecer el desempeño de los controles así:

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

3.4.2 Indicadores clave de riesgo: hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo

⁷ De acuerdo con la Guía para la preparación de las TIC para la continuidad del negocio emitida por el Ministerio TIC lo define como procedimientos documentados que guían y orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación una vez presentada o tras la interrupción para garantizar la continuidad de las funciones críticas del negocio.

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 tabla 9 se muestran algunos ejemplos de estos indicadores.

Tabla 10 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: Adaptado del listado de indicadores y métricas (www.riesgoscero.com) por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

3.5 Monitoreo y revisión: El modelo integrado de planeación y gestión (MIPG) desarrolla en la dimensión 7 el Modelo Estándar de Control Interno (MECI) y las líneas de defensa como eje articulador para identificar la responsabilidad de la gestión del riesgo y control. que está distribuida en diversos servidores de la entidad.

La estructura del MECI busca una alineación a las buenas prácticas de control referenciadas desde el Modelo COSO, razón por la cual la estructura del MECI se fundamenta en cinco componentes, a saber: (i) ambiente de control, (ii) Evaluación del riesgo, actividades de control, (iv) información y comunicación y (v) actividades de monitoreo. Al respecto, el Manual Operativo MIPG v4, frente a dichos componentes establece lo siguiente:

“(...) El propósito para cada uno de los compontes se despliega de la siguiente forma:

1. Ambiente de Control: *este componente busca asegurar un ambiente de control que le permita a la entidad disponer de las condiciones mínimas para el ejercicio del control interno. Requiere del compromiso, el liderazgo y los lineamientos de la alta dirección y del Comité Institucional de Coordinación de Control Interno.*

2. Evaluación del riesgo: *su propósito es identificar, evaluar y gestionar eventos potenciales, tanto internos como externos, que puedan afectar el logro de los objetivos institucionales.*

3. Actividades de control: *su propósito es permitir el control de los riesgos identificados y como mecanismo para apalancar el logro de los objetivos y forma parte integral de los procesos.*

4. Información y comunicación: *tiene como propósito utilizar la información de manera adecuada y comunicarla por los medios y en los tiempos oportunos. Para su desarrollo se deben diseñar políticas, directrices y mecanismos de consecución, captura, procesamiento y generación de datos dentro y en el entorno de cada entidad, que satisfagan la necesidad de divulgar los resultados, de mostrar mejoras en la gestión administrativa y procurar que la información y la comunicación de la entidad y de cada proceso sea adecuada a las necesidades específicas de los grupos de valor y grupos de interés.*

5. Actividades de monitoreo: *su propósito es desarrollar las actividades de supervisión continua (controles permanentes) en el día a día de las actividades, así como evaluaciones periódicas (autoevaluación, auditorías) que permiten valorar: (i) la efectividad del control interno de la entidad pública; (ii) la eficiencia, eficacia y efectividad de los procesos; (iii) el nivel de ejecución de los planes, programas y proyectos; (iv) los resultados de la gestión, con el propósito de detectar desviaciones, establecer tendencias, y generar recomendaciones para orientar las acciones de mejoramiento de la entidad pública. (...)*

En cuanto al esquema de líneas de defensa se define lo siguiente:

“(...)”

- ✓ **Línea estratégica de defensa:** *está conformada por la Alta Dirección en el marco del Comité Institucional de Coordinación de Control Interno. La responsabilidad de esta línea de defensa se centra en la emisión, revisión, validación y supervisión del cumplimiento de políticas en materia de control interno, gestión del riesgo, seguimientos a la gestión y auditoría interna para toda la entidad.*

- ✓ **Primera línea de defensa:** esta línea de defensa les corresponde a los servidores en sus diferentes niveles, quienes aplican las medidas de control interno en las operaciones del día a día de la entidad. Se debe precisar que cuando se trate de servidores que ostenten un cargo de responsabilidad (jefe) dentro de la estructura organizacional, se denominan controles de gerencia operativa, ya que son aplicados por líderes o responsables de proceso. Esta línea se encarga del mantenimiento efectivo de controles internos, por consiguiente, identifica, evalúa, controla y mitiga los riesgos.
- ✓ **Segunda línea de defensa:** esta línea de defensa está conformada por servidores que ocupan cargos del nivel directivo o asesor (media o alta gerencia), quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección.

Aquí se incluyen a los jefes de planeación, o quienes hagan sus veces; coordinadores de equipos de trabajo, coordinadores de sistemas de gestión, gerentes de riesgos (donde existan), líderes o coordinadores de contratación, financiera y de TIC, entre otros que se deberán definir acorde con la complejidad y misionalidad de cada organización. Esto le permite a la entidad hacer un seguimiento o autoevaluación permanente de la gestión, de manera que pueda orientar y generar alertas a las personas que hacen parte de la 1ª línea de defensa, así como a la Alta Dirección (Línea Estratégica)

Esta línea se asegura de que los controles y procesos de gestión del riesgo de la 1ª línea de defensa sean apropiados y funcionen correctamente, además, se encarga de supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas que permitan adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos.

Entre los parámetros a tener en cuenta, para definir esta línea son los siguientes:

- *Pertenecer a la media o alta gerencia: Dentro del Organigrama aquellos cargos que dependen del Representante Legal (Alta Gerencia), Para Media Gerencia, aquellos que se desprenden de los cargos anteriormente mencionados.*
 - *Responder ante la Alta Dirección: Aquel cargo que maneja un tema transversal para toda la entidad y responde ante el Representante Legal.*
 - *Evaluar y efectuar seguimiento a los controles aplicados por la 1ª línea de defensa.*
- ✓ **Tercera línea de defensa:** esta línea de defensa está conformada por la Oficina de Control Interno, quienes evalúan de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos o inadecuadamente cubiertos por la 2ª línea de defensa.
La interacción entre la 2ª línea de defensa (proveedores internos de aseguramiento) y la 3ª línea de defensa y estas con los proveedores externos de aseguramiento (organismos de control y otras instancias de supervisión o vigilancia) serán representadas en una matriz de doble entrada denominada mapa de aseguramiento⁸, herramienta considerada por el Instituto de Auditores como adecuada e idónea para coordinar las diferentes actividades de aseguramiento, visualizar el esfuerzo en común y mitigar los riesgos de una manera mucho más integral. (...)

Luego entonces, la Línea Estratégica debe definir lineamientos claros frente a la estructura de control, por lo que específicamente a través del componente Ambiente de Control debe generar los espacios para el análisis y seguimiento de

los temas relacionados con el Talento Humano, la Integridad y la Planeación Estratégica, claves para que se cuente con ambiente propicio o favorable al control. De igual forma, a través de los demás componentes del MECI, podrá tomar decisiones basados en hechos y datos, ya que los miembros de 2ª línea que se identifiquen aportarán información a tiempo, con evaluaciones en términos de control y riesgos, lo que facilitará tomar acciones que eviten situaciones no deseadas en la entidad en tiempo real.

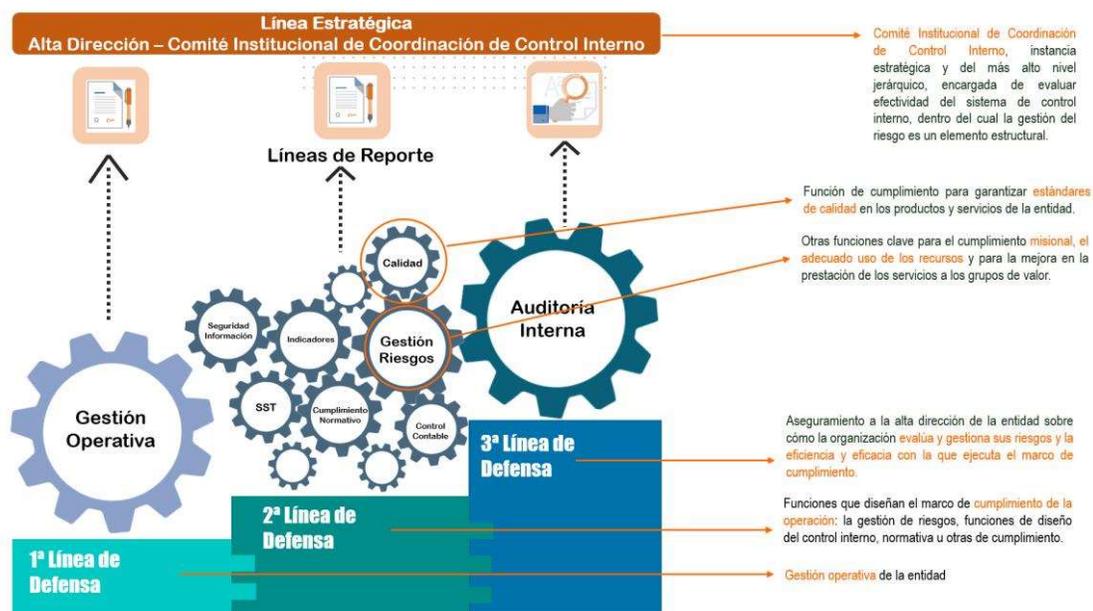
En cuanto a la 2ª Línea de Defensa, lleva a cabo autoevaluación permanente de las actividades llevadas a cabo por la 1ª línea de defensa, por lo que su objetivo principal es asegurar que la primera línea está diseñada y opera de manera efectiva, es decir, que las funciones de la segunda línea de defensa informan a la Alta Dirección y/o son parte de la Alta Dirección y generan información clave para la toma de decisiones en tiempos diferenciados respecto de los seguimientos y evaluaciones de la tercera línea de defensa y con respecto a temas o aspectos transversales en la entidad.

Dentro de esta 2ª línea se encuentran la Oficina Asesora de Planeación o quien haga sus veces quienes lideran temas estratégicos para la entidad, como sería el seguimiento a la planeación institucional y a la gestión del riesgo; así mismo, se deberán incluir otras instancias internas que lideren temas estratégicos y transversales relacionados con planes, programas y/o proyectos fundamentales para el cumplimiento misional, así como otras instancias de apoyo que son transversales y garantizan el manejo de los recursos y bienes de la entidad.

Por último, la 3ª línea de defensa la conforma la Oficina de Control Interno o quien haga sus veces en la entidad, quien, a través de sus procesos de seguimiento y evaluación, especialmente a través de la auditoría interna se pronuncian sobre la efectividad de los controles para evitar la materialización de riesgos. De igual forma, en cumplimiento de su rol de enfoque hacia la prevención se articulan con la oficina de planeación o quien haga sus veces, así como con las demás instancias de 2ª línea que se identifiquen, para compartir información y análisis de contraste que permita monitorear la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo de forma integral.

Este esquema se puede visualizar en la figura 20, donde se evidencia su interacción y complementariedad.

Figura 20 Operatividad Esquema de líneas de defensa



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

A continuación, en los capítulos 4, 5 y 6 se desarrollarán de manera específica los temas relacionados con riesgo fiscal, así como los riesgos asociados a posibles actos de corrupción y los de seguridad de la información de acuerdo con las políticas de transparencia, acceso a la información pública y lucha contra la corrupción liderada por la Secretaría de Transparencia y la de Gobierno Digital, específicamente frente a la seguridad de la información en cabeza del Ministerio de Tecnologías de la Información y Comunicaciones, esto teniendo en cuenta la integralidad frente a la gestión del riesgo y la articulación de dichas políticas en el marco del modelo integrado de planeación y gestión (MIPG).

En estos capítulos se vincula la estructura general definida en la metodología para la identificación, valoración y tratamiento de los riesgos, aspectos ya desarrollados a lo largo de la presente guía.

Específicamente se deben considerar los siguientes aspectos de acuerdo con los pasos de la metodología así:

1. En el paso *política de administración del riesgo* se deben incluir los lineamientos requeridos para el manejo de estas tipologías de riesgo.

Para el caso de los riesgos sobre seguridad de la información, se debe definir la incorporación del Anexo 4 modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas, de manera tal que los responsables analicen y establezcan, en el marco de sus procesos, los activos de información asociados y se identifiquen los riesgos correspondientes.

Para los riesgos asociados a posibles actos de corrupción se deben definir los lineamientos para su tratamiento. Es claro que este tipo de riesgos no admiten aceptación del riesgo; así mismo, las entidades deben incluir las matrices relacionadas con la redacción de este tipo de riesgos, las preguntas para la definición del nivel de impacto y la matriz de calor correspondiente, donde se precisan las zonas de severidad aplicables. Para esta tipología de riesgos se incluye el protocolo para la identificación de riesgos de corrupción, asociados a la prestación de trámites y servicios, en el marco de la política de racionalización de trámites, en los casos que aplique.

2. En la etapa de identificación del riesgo se enmarcan en los procesos, lo que exige el análisis frente a los objetivos, cadena de valor, factores generadores de riesgo (explicados en los primeros apartes de la presente guía). Estos lineamientos son aplicables a ambas tipologías de riesgos.

3. En la etapa de valoración del riesgo se asocian las tablas para el análisis de probabilidad, impacto niveles de severidad, así como para el diseño y evaluación de los controles identificados. En este caso, para los riesgos de corrupción se precisan algunas herramientas para la definición del impacto y las zonas de riesgo aplicables. En cuanto a los riesgos de seguridad de la información se incorporan las tablas de probabilidad, impacto y matriz de calor definidas en la metodología general.

4. Lineamientos para el análisis de riesgo fiscal

4.1 Control fiscal interno y prevención del riesgo

fiscal: la construcción de este capítulo tiene como finalidad prevenir la constitución del elemento medular de la responsabilidad fiscal, que es el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado (Decreto 403, 2020, art.6).

Las bases de la responsabilidad fiscal están consignadas en la Ley 610 de 2000. Para tener claro el ámbito normativo y jurídico, es necesario precisar que sus bases están sentadas en los artículos 267 y 268 de la Constitución Política de 1991, los cuales fueron modificados por el Acto Legislativo 04 de 2019 que se fundamentó en la necesidad de un ejercicio preventivo del control fiscal, que detuviera el daño fiscal e identificara riesgos fiscales; de esta manera, la administración y el gestor fiscal podrían adoptar las medidas respectivas para prevenir la concreción del daño patrimonial de naturaleza pública.

A partir de lo anterior, el control fiscal además de posterior y selectivo a través de las auditorías (control micro), es preventivo y concomitante, buscando con ello el control permanente al recurso público, para lo cual, una de las herramientas previstas es la articulación con el sistema de control interno, con lo cual surgen conceptos clave como:

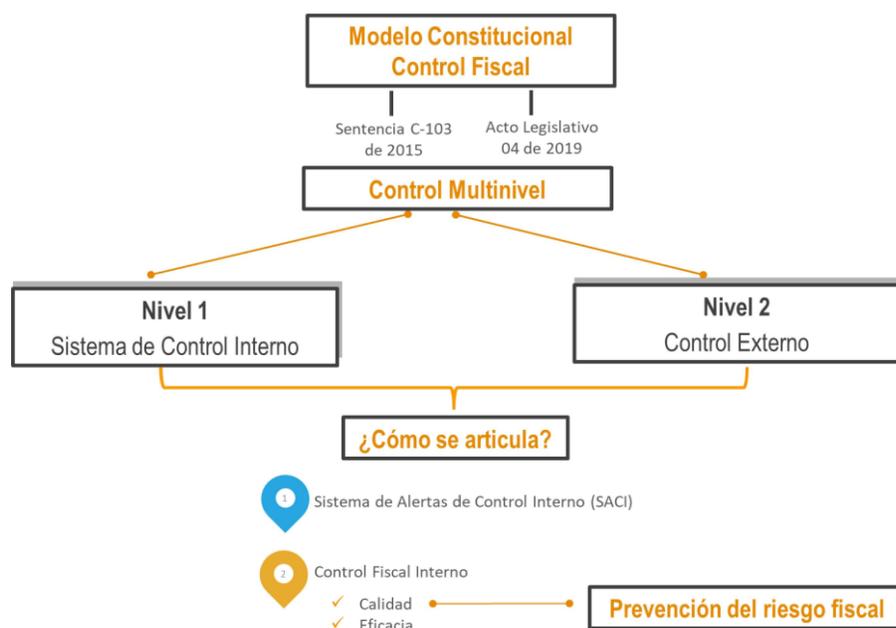
- Control fiscal Multinivel: Es la articulación entre el sistema de control interno (primer nivel de control) y el control externo (segundo nivel de control), con la participación activa del control social.

- Control fiscal Interno (CFI): Primer nivel para la vigilancia fiscal de los recursos públicos y para la prevención de riesgos fiscales y defensa del patrimonio público. El Control Fiscal Interno, hace parte del Sistema de Control Interno y es responsabilidad de todos los servidores públicos y de los particulares que administran recursos, bienes, e intereses patrimoniales de naturaleza pública y de las líneas de defensa, en lo que corresponde a cada una de ellas. El Control Fiscal Interno es evaluado por la Contraloría respectiva, siendo dicha evaluación determinante para el fenecimiento de la cuenta.

En el nuevo modelo constitucional el control externo adquiere un enfoque preventivo y a su vez el control interno potencia el enfoque preventivo, partiendo de la premisa de que el Sistema de Control Interno es fundamental para conjugar el logro de resultados, con la prevención de riesgos de gestión, corrupción y fiscales, así como, con la seguridad del gestor público (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros), a través de la prevención de responsabilidades.

La figura 21 muestra este despliegue y sus elementos de articulación que sustentan el desarrollo del presente capítulo.

Figura 21 Articulación modelo constitucional control fiscal y sistema de control interno



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

A continuación se presenta el paso a paso de la gestión del riesgo fiscal (Identificación, análisis y valoración), que debe vincularse al análisis general de los riesgos institucionales, a fin de contar con un esquema integral que facilite su seguimiento por parte de los líderes del proceso.

La metodología que se propone es de gran utilidad para gestionar de manera efectiva los recursos, bienes e intereses públicos, previniendo efectos dañosos, lo cual a la vez permite, mitigar la posibilidad de configuración de responsabilidades fiscales para los diferentes gestores públicos.

Como parte integral de la metodología propuesta se pone a disposición, como insumo de referencia, un Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas (ver anexo), el cual ha sido construido como resultado del análisis de precedentes (aproximadamente 130 fallos con responsabilidad fiscal de contralorías territoriales y de la Contraloría General de la República) y debe ser utilizado como marco de referencia para la identificación y valoración de riesgos fiscales, siempre atendiendo las particularidades, naturaleza, complejidad, recursos, usuarios o grupos de valor, portafolio de productos y servicios, sector en el cual se desenvuelva (contexto), así como otras condiciones específicas de cada entidad.

En consecuencia, cada entidad deberá analizar si existen, de acuerdo con su contexto y particularidades puntos de riesgos y circunstancias inmediatas diferentes a los identificados en dicho catálogo y tenerlas en cuenta en la identificación de sus riesgos fiscales.

4.2 Definición y elementos del riesgo fiscal: Teniendo en cuenta la estructura y elementos de la definición de riesgos que tiene la presente guía, la cual es armónica con la norma ISO 31000, se define riesgo fiscal, así:

Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

A continuación, se describen los elementos que componen la definición de riesgo fiscal:

Efecto: es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

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

Lo anterior se puede resumir de la siguiente manera:

$$\text{Riesgo Fiscal} = \text{Evento Potencial (Potencial Conducta)} + \text{Efecto dañoso}$$

Se debe tener especial cuidado en no confundir el riesgo fiscal, con el daño fiscal; por lo tanto, la definición debe estar orientada hacia el efecto de un evento potencial (potencial acción u omisión) sobre los recursos públicos y/o los bienes o intereses patrimoniales de naturaleza pública.

4.3 Metodología y paso a paso para el levantamiento del mapa de riesgos fiscales:

A continuación, se presenta el paso a paso para realizar de forma adecuada la identificación, clasificación, valoración y control del riesgo fiscal, que es fundamental para el resultado de la gestión de cada entidad y para la seguridad y prevención de responsabilidades de los gestores públicos (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros).

Paso 1: identificación de riesgos fiscales

Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal y las circunstancias Inmediatas. Los puntos de riesgos son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas⁹.

En conclusión, los puntos de riesgo fiscal son todas las actividades que representen gestión fiscal, así mismo, se deben tener en cuenta aquellas

⁹ Artículo 3 Ley 610 de 2000.

actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal.

Para las circunstancias inmediatas, se trata de aquella situación o actividad bajo la cual se presenta el riesgo, pero no constituyen la causa principal o básica - causa raíz- para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas.

Ahora bien, para poder identificar los puntos de riesgo y las circunstancias inmediatas, se recomienda realizar un taller entre personal del nivel directivo, asesores y aquellos servidores que por su conocimiento, experiencia o formación puedan aportar especial valor, en el que, basados en las anteriores definiciones, identifiquen los puntos de riesgo fiscal (actividades de gestión fiscal en las que potencialmente se genera riesgo fiscal) y circunstancias Inmediatas (situación por la que se presenta el riesgo, pero no constituye la causa principal del riesgo fiscal). Para este taller, puede usar las siguientes preguntas orientadoras:

Tabla 11 Preguntas orientadoras para puntos riesgo fiscal y causas inmediatas

Sirve para identificar	Preguntas y respuestas para la identificación
Puntos de riesgo fiscal	¿En qué procesos de la entidad se realiza gestión fiscal? (ver capítulo inicial la definición de gestión fiscal).
Puntos de riesgo fiscal y circunstancias inmediatas	<p>Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-.</p> <p>Nota 1: Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años.</p> <p>Nota 2: Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces.</p> <p>Nota 3: Los fallos con responsabilidad fiscal en firme son información pública, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañinos sobre los recursos, bienes o intereses patrimoniales del Estado.</p> <p>Nota 4: La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-, es una labor de la segunda línea de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces.</p>

Sirve para identificar	Preguntas y respuestas para la identificación
Circunstancias inmediatas	<p>En un ejercicio autocrítico, realista y objetivo, ¿Cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años?</p> <p>Nota: Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control.</p>
Puntos de riesgo fiscal y circunstancias inmediatas	<p>¿Qué puntos de riesgo fiscal y circunstancias inmediatas del “¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas” (anexo1), son aplicables a la entidad?</p>

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

Identificación de áreas de impacto

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.

Son ejemplo de efectos económicos que no son riesgos fiscales, los siguientes:

- (i) Los riesgos de daño antijurídico -riesgo de pago de condenas y conciliaciones.
- (ii) Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores públicos, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero (es decir, de alguien que no tenga la calidad de gestor público (ver definición de gestor público en el capítulo uno de conceptos básicos).

Otro aspecto, que es fundamental para definir de manera correcta el impacto al momento de identificar y redactar riesgos fiscales, es tener claro el concepto de patrimonio público, así como el de las tres expresiones de patrimonio público que se derivan del artículo 6 de la Ley 610 de 2000: (i) bienes públicos; (ii) recursos públicos o (iii) intereses patrimoniales de naturaleza pública (consultar definiciones en el capítulo uno de conceptos básicos).

Identificación de la causa raíz o potencial hecho generador

La causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015).

La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa/efecto. En este sentido, la determinación de la causa raíz o potencial hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio estatal.

Una adecuada gestión de riesgos fiscales exige que la identificación de causas sea especialmente objetiva y rigurosa, ya que los controles que se diseñen e implementen deben apuntarle a atacar dichas causas, para así lograr prevenir la ocurrencia de daños fiscales.

Siendo la causa raíz un elemento tan relevante para la eficaz gestión de riesgos fiscales, es importante tener claridad al respecto de qué es y qué no es una causa raíz o potencial hecho generador.

Es fundamental, entonces, tener claro que debe deslindarse el hecho que ocasiona el daño (hecho generador-causa raíz o causa adecuada), del daño propiamente dicho. En otras palabras, uno es el hecho generador -causa-, y otro es el daño -efecto- (Contraloría General de la República, 2021)¹⁰.

Ejemplo:

Una entidad X se atrasó en el pago del canon de arriendo de una de sus sedes, por 6 meses, generándose intereses moratorios por \$30 millones. Cuando llega un nuevo director este encuentra la deuda por concepto de canon y los intereses generados y procede a gestionar los recursos para el pago de capital e intereses y al mes de su posesión efectúa el pago.

¿Cuál es el daño? El daño fiscal corresponde al monto pagado por concepto de intereses moratorios

¿Cuál es el hecho generador? La omisión de pagó oportuno del canon de arrendamiento.

Conclusión: El hecho generador del daño no es el pago de los intereses moratorios, ya que el pagó es una acción diligente que da cumplimiento a una obligación adquirida y evita que se sigan generando intereses.

Descripción del Riesgo Fiscal

A continuación, se presenta la estructura de redacción de riesgos fiscales en la que se conjugan los elementos antes descritos; así mismo, se presentan algunos

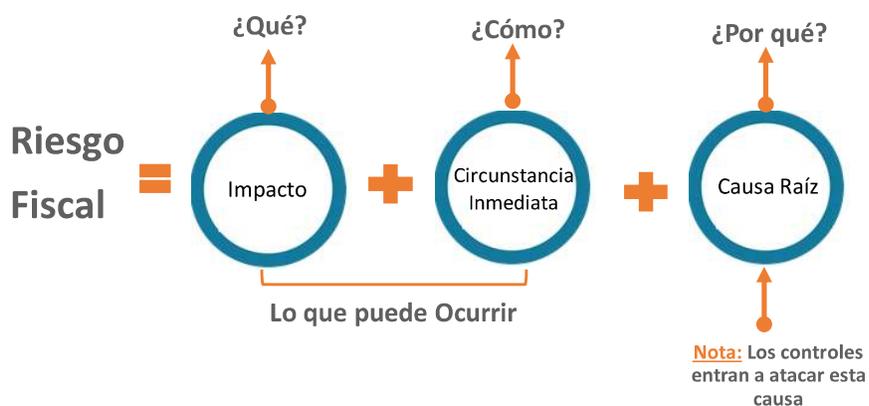
¹⁰ Concepto CGR-OJ-115-2021 de la Contraloría General de la República, pág. 13

ejemplos de riesgos fiscales identificados como resultado del estudio de fallos de contralorías territoriales y Contraloría General de la República.

Para redactar un riesgo fiscal se debe tener en cuenta:

- ✓ Iniciar con la oración: *Posibilidad de*, debido a que nos estamos refiriendo al evento potencial.
- ✓ Impacto: Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).
- ✓ Circunstancia inmediata: Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.
- ✓ Causa Raíz: Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera¹¹.

De acuerdo con lo indicado, la estructura propuesta para la redacción de riesgos fiscales es la siguiente:



Ejemplo:

Proceso: Gestión de Recursos

Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada

¹¹ El control fiscal y la responsabilidad fiscal en Colombia. Luz Jimena Duque Botero y Fredy Céspedes Villa. Ibáñez 2018

vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.



¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efectos dañoso sobre bienes públicos	por pérdida, extravío o hurto de bienes muebles de la entidad.	a causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén

Como complemento a continuación se muestran otros ejemplos de redacción de riesgos fiscales, según el objeto sobre el cual recae la posibilidad de efecto dañoso, es decir efecto dañoso sobre bienes públicos, recursos públicos o sobre intereses patrimoniales de naturaleza pública.

Tabla 12 Ejemplos adicionales acorde con el objeto sobre el que recae el efecto dañoso

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la omisión en el cumplimiento de la licencia ambiental de los proyectos de infraestructura.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no tener incluidos todos los bienes muebles e inmuebles de la entidad en el contrato de seguro, a causa de la omisión en la actualización de bienes que cubren de dicho contrato.
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	Posibilidad de efecto dañoso sobre recursos públicos, por sobrecostos en contratos de la entidad, a causa de la omisión del deber de elaborar estudios de mercado.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no devolución al tesoro público de los rendimientos financieros generados por recursos de anticipo, a causa de la omisión por parte de la interventoría y/o supervisión de la interventoría al no exigir la devolución al contratista

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

Paso 2: Valoración del riesgo fiscal

Evaluación de riesgos

Se busca establecer la probabilidad inherente de ocurrencia del riesgo fiscal y sus consecuencias o impacto inherentes.

Probabilidad

La probabilidad es la posibilidad de ocurrencia del riesgo fiscal, se determina según al número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal.

Teniendo esto de presente, para definir el nivel de probabilidad, se ha de tener en cuenta la siguiente tabla definida en el numeral 3.1 de la presente guía:

	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%

Nota: Es necesario mencionar, que las frecuencias pueden variar según el tamaño y complejidad de los procesos de la entidad, así como sus necesidades, por lo que las frecuencias en cada nivel pueden ser adaptadas a las necesidades y complejidad de cada entidad.

Impacto

Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico, toda vez que el efecto dañoso siempre ha de recaer sobre un bien, recurso o interés patrimonial de naturaleza pública.

Toda potencial consecuencia económica sobre los bienes, recursos o intereses patrimoniales públicos, es relevante para la adecuada gestión fiscal y prevención de riesgos fiscales, sin perjuicio de ello, existen diferentes niveles de impacto, según la valoración del potencial efecto dañoso, es decir, del potencial daño fiscal, se aplicará la siguiente tabla definida en el numeral 3.1 de la presente guía:

	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

Nota: Es necesario mencionar, que los niveles en la afectación económica pueden variar según el tamaño y complejidad de los procesos de la entidad, así como sus necesidades, por lo que los rangos en cada nivel pueden ser adaptados a las necesidades y complejidad de cada entidad.

Determinación del nivel de riesgo inherente

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (riesgo inherente), se trata de determinar los niveles de severidad, para lo cual se aplica la matriz definida en el numeral 3.2 de la presente guía:

		Impacto																								
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%																				
Probabilidad	Muy Alta 100%						Extremo																			
	Alta 80%																									
	Media 60%																									
	Baja 40%																									
	Muy Baja 20%																									

Nota: Es necesario mencionar, que esta matriz de severidad está diseñada de acuerdo a estándares internacionales que permiten tener trazabilidad en los desplazamientos en cada zona, por lo que se recomienda no modificarla.

Ejemplo (continuación):

Proceso: Gestión de recursos

Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

Punto de Riesgo: Ingreso, custodia y salida de bienes muebles de la entidad

Riesgo Fiscal: Posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar (causa raíz).

Probabilidad: Las veces que se pasa por el punto de riesgo en un año es 365, puesto que todos los días del año de debe ejercer la custodia de los bienes muebles de la entidad. Para este ejemplo es importante tener en cuenta que los bienes muebles en cada entidad varía en cantidad y son de distinto valor en el inventario, se sugiere analizar el tipo de bien y el número de estos, a fin de acotar el nivel de probabilidad con un análisis más ácido que permita establecer controles diferenciados acorde con la naturaleza de diferentes grupos de bienes, ejemplo: equipos de cómputo, muebles y enseres, entre otros.

Aplicando las tablas de probabilidad e impacto tenemos:

	Frecuencia de la Actividad	Probabilidad	
Muy Baja	La actividad se realiza máximo 4 veces por año.	20%	
Baja	La actividad se realiza mínimo 5 veces al año y máximo 12 veces al año.	40%	
Moderada	La actividad se realiza mínimo 13 veces al año y máximo 365 veces al año.	60%	→
Alta	La actividad se realiza mínimo 365 veces al año y máximo 3660 veces al año.	80%	
Muy Alta	La actividad se realiza 3661 veces o más al año	100%	

La actividad se realiza 365 veces al año, la probabilidad de ocurrencia del riesgo es **media**.

Para determinar el impacto es necesario cuantificar el potencial efecto dañoso sobre el bien, recurso o interés patrimonial de naturaleza pública.

En este ejemplo el efecto dañoso sería del valor contable del inventario de bienes muebles que para el ejemplo se determina que es de \$2.500 millones de pesos, lo cual corresponde a 2.500 SMLMV. De acuerdo con la tabla para la definición del nivel de impacto, este riesgo tiene un nivel de impacto catastrófico

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

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

Probabilidad inherente= media 60%, **Impacto inherente:** catastrófico 100%

Zona de severidad o nivel de riesgo: De acuerdo con la tabla para la definición de zona severidad, al conjugar la calificación de probabilidad con la de impacto nos resulta un nivel de riesgo extremo.

		Impacto				
Probabilidad	Muy Alta 100%					
	Alta 80%					
	Media 60%					
	Baja 40%					
	Muy Baja 20%					
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

Cruzando los datos de probabilidad e impacto definidos se tiene: **zona de riesgo extrema**.

Paso 3. Valoración de controles

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos.

Tipologías de controles:

- ✓ Control Preventivo: Control accionado en la entrada del proceso y antes de que se realice la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles buscan establecer las condiciones que aseguren atacar la causa raíz y así evitar que el riesgo se concrete.
- ✓ Control Detectivo: Control accionado durante la ejecución de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles detectan el riesgo fiscal, pero generan reprocesos.
- ✓ Control Correctivo: Control accionado en la salida de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo) y después de que se materializa el riesgo fiscal. Estos controles tienen costos implícitos.

Para el análisis y evaluación de los controles se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. Se aplican los lineamientos para la redacción del control establecidos en el numeral 3.2.2.1 y tabla definida en el numeral 3.2.2.3 de la presente guía.

Ejemplo (continuación):

Proceso: Gestión de recursos

Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

Punto de Riesgo: Ingreso, custodia y salida de bienes muebles de la entidad

Riesgo Fiscal: Posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes e inventario del

almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar (causa raíz).

Probabilidad Inherente: Media 60%

Impacto Inherente: Catastrófico 100%

Zona de riesgo: Extrema

Controles Identificados:

- ✓ Control 1 Preventivo: El jefe de almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.
- ✓ Control 2 Detectivo: El coordinador administrativo verifica mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema (actualización y ubicación en el inventario), en caso de encontrar inconsistencias solicita al Jefe de Almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.
- ✓ Control 3 Correctivo: El director administrativo verifica la vigencia y actualización de la póliza de acuerdo a los bienes que ingresan a la entidad, en caso de presentarse un siniestro adelanta las reclamaciones respectivas ante el asegurador

Aplicando la tabla de valoración de controles tenemos:

Control 1	Criterios de efectividad			Peso
El jefe de almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
Total, Valoración Control 1 =40%				
Control 2	Criterios de efectividad			Peso
El coordinador administrativo verifica mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema (actualización y ubicación en el inventario), en caso de encontrar inconsistencias solicita al Jefe de Almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.	Tipo	Preventivo		
		Detectivo	x	15%
		Correctivo		
	Implementación	Automático		
		Manual	x	15%
Total, Valoración Control 2 = 30%				

Control 3	Criterios de efectividad			Peso
El director administrativo verifica la vigencia y actualización de la póliza de acuerdo a los bienes que ingresan a la entidad, en caso de presentarse un siniestro adelanta las reclamaciones respectivas ante el asegurador.	Tipo	Preventivo		
		Detectivo		
		Correctivo	x	10%
	Implementación	Automático		
		Manual	x	15%
Total, Valoración Control 3 = 25%				

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde a continuación se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles y su respectiva valoración, a fin de determinar el riesgo residual.

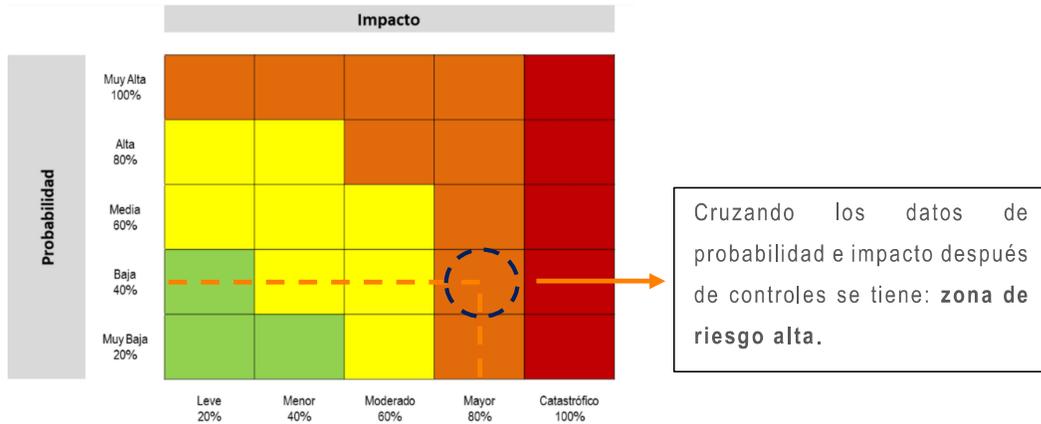
Nivel de riesgo (riesgo residual):

Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en cuenta que los 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.

Para mayor claridad a continuación, siguiendo con el ejemplo propuesto, se observan los cálculos requeridos para la aplicación de los tres controles definidos así:

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de efectos dañoso sobre bienes públicos (<i>área de impacto</i>), por pérdida, extravío o hurto de bienes muebles de la entidad (<i>circunstancia inmediata</i>), a causa de la omisión de cumplimiento del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar (<i>causa raíz</i>).	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	100%	Valoración control correctivo	25%	$100\% * 25\% = 25\%$ $100\% - 25\% = 75\%$
	Impacto Residual	75%			

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor, a continuación se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles y cálculo final:



La anterior información puede trasladarse a la matriz mapa de riesgo que hace parte de los anexos desarrollados para la presente guía.

5. Lineamientos sobre los riesgos relacionados con posibles actos de corrupción

Para la gestión de riesgos de corrupción, **continúan vigentes los lineamientos contenidos en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018**. Por lo anterior es necesario que para formular el mapa de riesgos de corrupción, se remita a dicho documento. Para mayor facilidad, a continuación se transcriben algunos de las pautas señaladas en la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018, que reiterando sigue vigente.

Por otra parte, es de resaltar que la Secretaría de Transparencia, en la actualidad está analizando la posibilidad de actualizar la metodología para la gestión de riesgos de corrupción.

Identificación de riesgos - técnicas para la identificación de riesgos

RIESGO DE CORRUPCIÓN

Definición de 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 concurren los **componentes de su definición**, así:

ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.

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 de la **matriz de definición de riesgo de corrupción**, que incorpora cada uno de los componentes de su definición.

De acuerdo con la siguiente matriz, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

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

Generalidades acerca de los riesgos de corrupción

- Entidades encargadas de gestionar el riesgo: lo deben adelantar las entidades del orden nacional, departamental y municipal.

- Se elabora anualmente por cada responsable de los procesos al interior de las entidades junto con su equipo.

- Consolidación: la oficina de planeación, quien haga sus veces, o a la de dependencia encargada de gestionar el riesgo le corresponde liderar el proceso de administración de estos. Adicionalmente, esta misma oficina 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.

Recuerde que las excepciones solo pueden estar establecidas en la ley, un decreto con fuerza de ley o un tratado internacional ratificado por el Congreso o en la Constitución.

- **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 oficina de planeación o quien haga sus veces, o la de gestión del riesgo deberá diseñar y poner en marcha 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, dicha oficina adelantará 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. Deberá dejarse la evidencia del proceso de socialización y publicarse sus resultados.

■ **Ajustes y modificaciones:** se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

■ **Monitoreo:** en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.

■ **Seguimiento:** el jefe de control interno o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

EJEMPLO

Información anonimizada:

N.º	Riesgo	Clasificación	Causa	Probabilidad	Impacto	Riesgo Residual	Opción de Manejo	Actividad de Control
1	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o para terceros...	Corrupción	Falta de...	Probable	Catastrófico	Catastrófico	Evitar	

Información anonimizada

¡IMPORTANTE

Tenga en cuenta que la información clasificada o reservada la señala la ley, un decreto con fuerza de ley o convenio internacional ratificado por el Congreso o en la Constitución.

Una resolución no puede calificar la información como clasificada o reservada.

IMPORTANTE

Los riesgos de corrupción, siempre deben gestionarse.

IMPORTANTE
En la descripción de los riesgos de corrupción deben concurrir TODOS los componentes de su definición:
Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.

Fuente: Secretaría de Transparencia de la Presidencia de la República

Valoración de riesgos

Cálculo de la probabilidad e impacto

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

Criterios para calificar la probabilidad

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

(Fuente DAFP)

Análisis del impacto

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo

Criterios para calificar el impacto en riesgos de corrupción

N.º	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.		

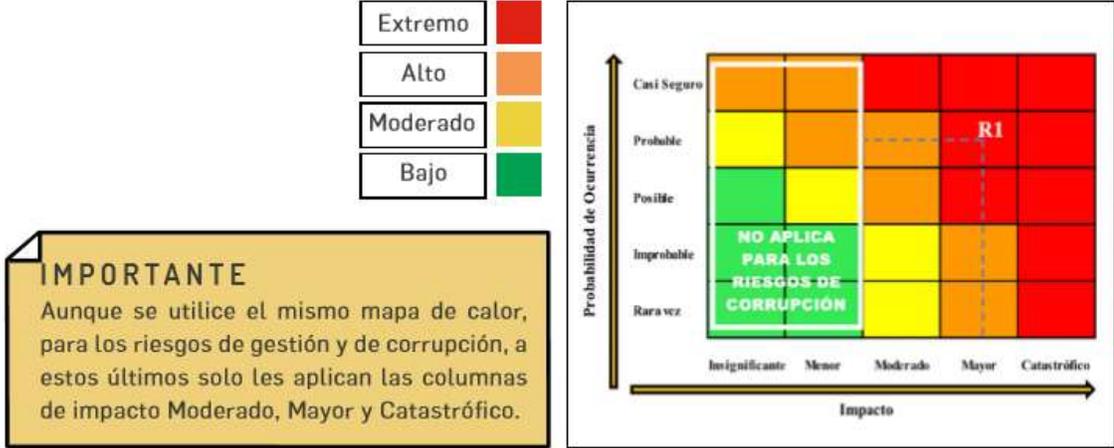
Nivel de
impacto
MAYOR

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

Análisis del impacto en riesgos de corrupción

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.



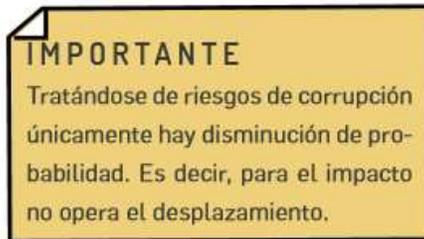
Fuente: Secretaría de Transparencia de la Presidencia de la República.

Valoración de los controles – diseño de controles

Tenga en cuenta para el diseño de controles, los parámetros señalados en la **versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de 2018, continúan vigentes**, por lo tanto se sugiere remitirse a dicho documento.

Nivel del riesgo (riesgo residual)

Desplazamiento del riesgo inherente para calcular el riesgo residual



Tratamiento del riesgo

¿Qué es tratamiento del riesgo?

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta 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. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:



Fuente: DAFFP

ACEPTAR EL RIESGO

IMPORTANTE
En el caso de riesgos de corrupción, estos no pueden ser aceptados.

EVITAR EL RIESGO

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

Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento es simple, la menos arriesgada y menos costosa, pero es un obstáculo para el desarrollo de las actividades de la entidad y, por lo tanto, hay situaciones donde no es una opción

COMPARTIR EL RIESGO

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

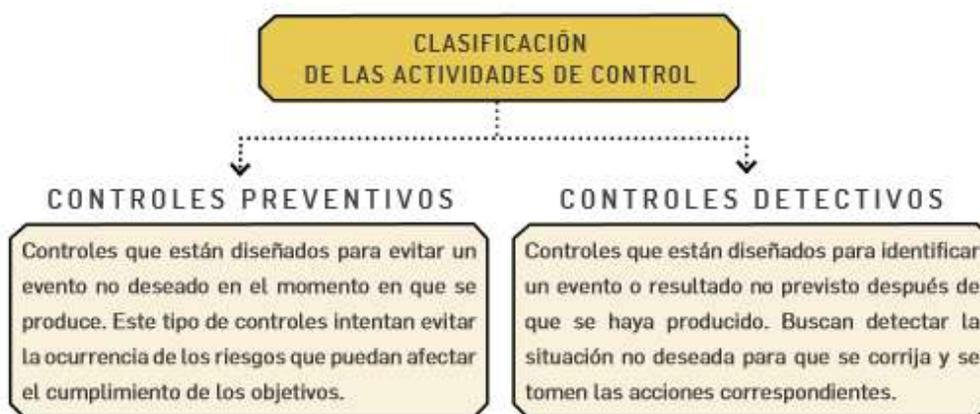
REDUCIR EL RIESGO

El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.

Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

Tratamiento del riesgo – rol de la primera línea de defensa

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente su efectividad depende, de qué tanto se están logrando los objetivos estratégicos y de proceso de la entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control.



(Fuente DAFP)

Monitoreo de riesgos de corrupción

Los gerentes públicos y los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y

si es el caso ajustarlo (primera línea de defensa). Le corresponde, igualmente, a la oficina de planeación adelantar el monitoreo (segunda línea de defensa), para este propósito se sugiere elaborar una matriz. Dicho monitoreo será en los tiempos que determine la entidad.

Su importancia radica en la necesidad de llevar a cabo un seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es, por sus propias características, una actividad difícil de detectar.

Para tal efecto deben atender a los lineamientos y las actividades descritas en la primera y segunda línea de defensa de este documento.

Reporte de la gestión del riesgo de corrupción

De igual forma, se debe reportar en el mapa y plan de tratamiento de riesgos los riesgos de corrupción, de tal manera que se comunique toda la información necesaria para su comprensión y tratamiento adecuado

Seguimiento de riesgos de corrupción

GESTION RIESGOS DE CORRUPCIÓN

* Seguimiento: El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

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

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

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

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano. (Ver anexo 6. matriz de seguimiento a los riesgos de corrupción)

En especial deberá adelantar las siguientes actividades:

* Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.

* Seguimiento a la gestión del riesgo.

* Revisión de los riesgos y su evolución.

* Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

Acciones a seguir en caso de materialización de riesgos de corrupción

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

- 1) Informar a las autoridades de la ocurrencia del hecho de corrupción.
- 2) Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
- 3) Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
- 4) Llevar a cabo un monitoreo permanente.

La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

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

6. Lineamientos 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)¹², 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.

6.1. Identificación de los activos de seguridad de la información: como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

Figura 22 Conceptualización activos de información

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización	Permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).

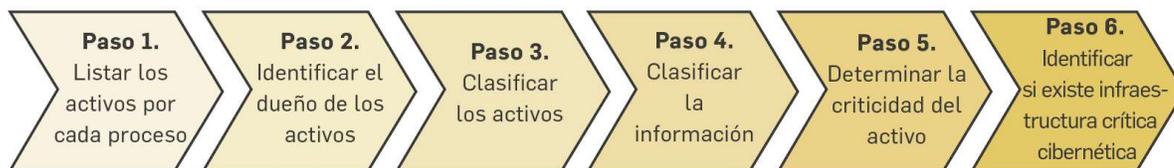
¹² Tomado de: <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>

¿Qué son los activos?	¿Por qué identificar los activos?
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano , aumentando así su confianza en el uso del entorno digital.

Fuente: Actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública y Ministerio TIC, 2020

Figura 23 Pasos para la identificación de activos

¿CÓMO IDENTIFICAR LOS ACTIVOS?:



Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

Nota: para realizar la identificación de activos deberá remitirse a la sección 3.1.6 del anexo 4 “Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas” que hace parte de los anexos de la presente guía.

Tabla 13 Ejemplo identificación activos del proceso

Proceso	Activo	Descripción	Dueño del activo	Tipo del activo	Ley 1712 de 2014	Ley 1581 de 2012	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Gestión financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe de oficina financiera	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión financiera	Aplicativo de nómina	Servidor web que contiene el <i>front office</i> de la entidad	Jefe de oficina financiera	Software	N/A	N/A	BAJA	MEDIA	BAJA	MEDIA
Gestión financiera	Cuentas de cobro	Formatos de cobro diligenciados	Jefe de oficina financiera	Información	Información pública	No contiene datos personales	BAJA	BAJA	BAJA	BAJA

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

6.2. Identificación del riesgo: se podrán identificar los siguientes tres (3) 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: 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.

Tabla 14 Tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo

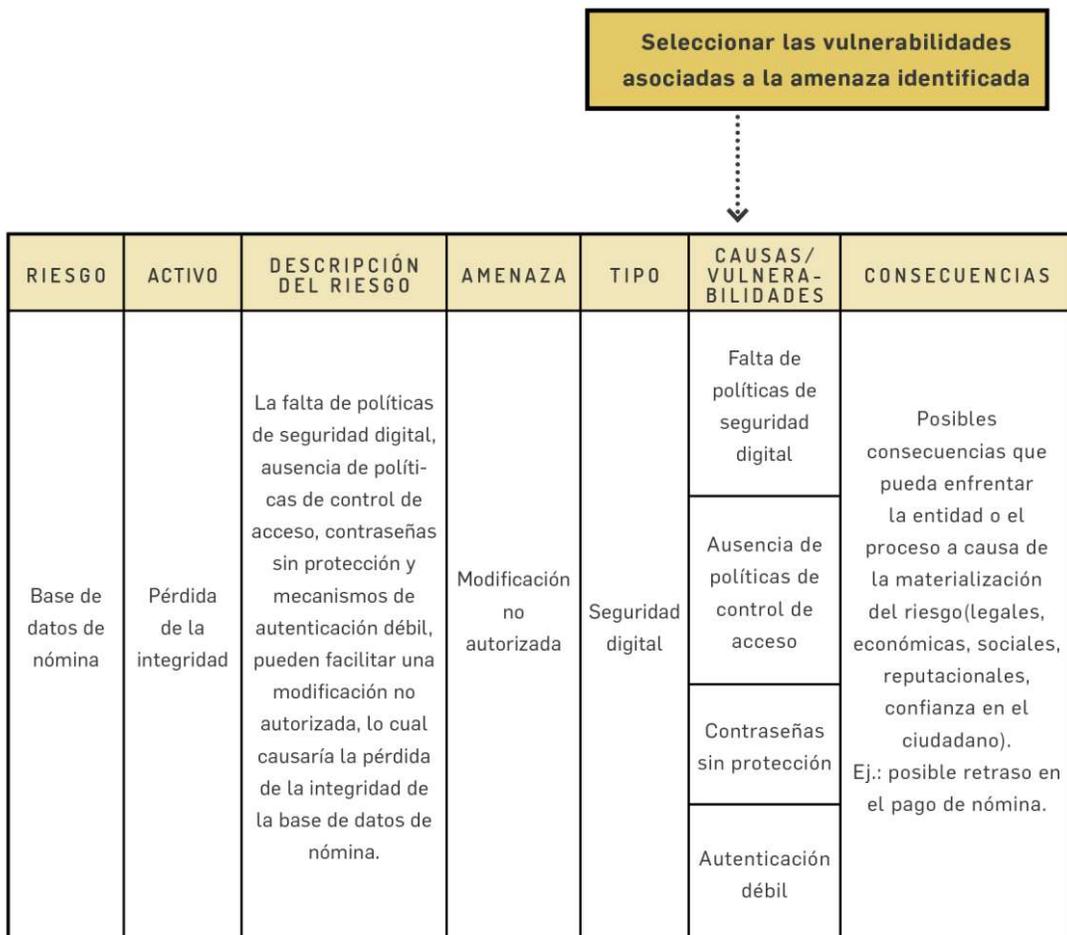
Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

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

En la figura 23 se observa un ejemplo de identificación del riesgo sobre un activo como es la base de datos de nómina.

Figura 24 Formato de descripción del riesgo de seguridad de la información



IMPORTANTE

- * Existirán tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.
- * Los catálogos de amenazas y vulnerabilidades comunes se encuentran en la sección 4.1.7. del **anexo “Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas”**, el cual hace parte de la presente guía.
- * **NOTA 1:** tener en cuenta que 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.
- * **NOTA 2:** las entidades públicas deben incluir como mínimo los procesos y procedimientos establecidos en esta guía. Aquellas entidades que ya estén adelantando procesos relacionados con la gestión de este tipo de riesgo y que incorporen al menos lo dispuesto en estas guías podrán continuar bajo sus procedimientos. Si alguno de los aspectos contenidos en esta guía no está contemplado, deberá ser agregado a los que manejan actualmente.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

6.3. Valoración del riesgo: Para esta etapa se asociarán las tablas de probabilidad e impacto definidas en la primera parte de la presente guía.

En este sentido, se debe considerar para este análisis la tabla 4 definida en el aparte 3.1.1, la cual se retoma a continuación:

	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%

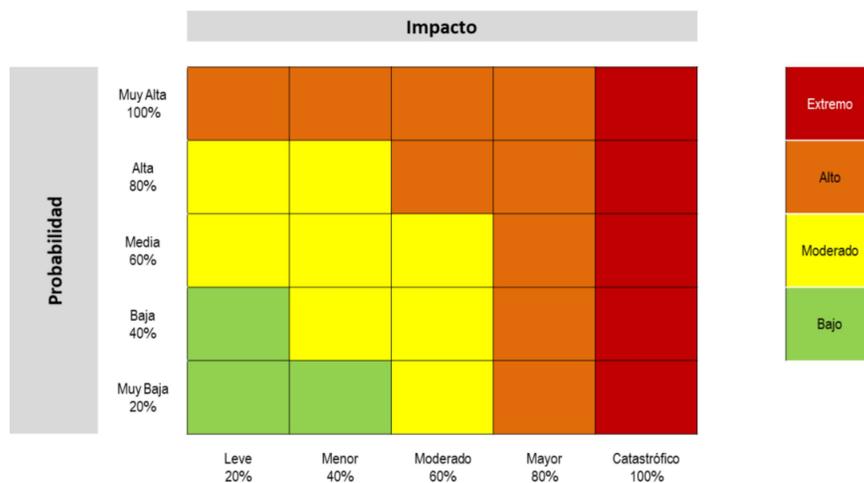
La determinación del impacto se debe llevar a cabo de acuerdo con lo establecido en el aparte 3.1.2 de la presente guía, entendiendo que el impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo.

En este sentido, se debe considerar para este análisis la tabla 5 definida en el aparte 3.1.2, que se retoma a continuación:

	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

Para el análisis preliminar (riesgo inherente), en esta etapa se define el nivel de severidad para el riesgo de seguridad de la información identificado, para ello,

se aplica la matriz de calor establecida en el numeral 3.2.1 de la presente guía, que se retoma a continuación:



En la figura 24 se observa un ejemplo aplicando la etapa de valoración del riesgo sobre un activo como es la base de datos de nómina.

Figura 25 Valoración del riesgo en seguridad de la información

IMPORTANTE

Cada entidad deberá adaptar los criterios a su realidad. El nivel de impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.

La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.

La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

RIESGO	ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Pérdida de la Confidencialidad	Base de datos de nómina	Modificación no autorizada	Ausencia de políticas de control de acceso	4-Probable	4- Mayor	Extrema
			Contraseñas sin protección			
			Ausencia de mecanismos de identificación y autenticación de usuarios			
			Ausencia de bloqueo de sesión			

Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. Agosto 2004.

Extremo	
Alto	
Moderado	
Bajo	

IMPORTANTE:
La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

6.4 Controles asociados a la seguridad de la información

Las entidades públicas 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 el documento maestro del modelo de seguridad y privacidad de la información (MSPI):

Tabla 15 Controles para riesgos de seguridad de la información

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 deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían 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 debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberían 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, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la pérdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del <i>software</i> y de las imágenes de los sistemas, 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.

Figura 26 Formato mapa riesgos seguridad de la información

N.	RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
2	Pérdida de la integridad	Base de datos de nómina	Seguridad digital	Modificación no autorizada	Ausencia de políticas de control de acceso	Probable	Menor	Moderado	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	EFICACIA: Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 EFFECTIVIDAD: Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
			Contraseñas sin protección	Reducir	A.9.4.3 Sistema de gestión de contraseñas				Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018			
			Ausencia de mecanismos de identificación y autenticación de usuarios	Reducir	A 9.4.2 Procedimiento de ingreso seguro				Procedimiento para ingreso seguro	Oficina TI	Tercer trimestre de 2018			
			"Ausencia de bloqueo	Reducir	A.11.2.8 Equipos de usuario desatendidos				Configuraciones para bloqueo automático de sesión	Oficina TI	Tercer trimestre de 2018			

*En este ejemplo el responsable de las actividades de control fue la Oficina de TI, sin embargo existen actividades para el área de personal, recursos físicos o cada oficina en particular. El análisis de riesgos determinará los controles y los responsables en cada caso.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

Referencias

Celis, Ó. B. (2012). Gestión Integral de Riesgos. Bogotá D.C.: Consorcio Gráfico Ltda.

COSO Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise Risk Management. Integrating with Strategy and Performance. Durham: Association of International Certified Professional Accountants.

ICONTEC Internacional. (2011). NORMA TÉCNICA COLOMBIANA GTC 137. GESTIÓN DEL RIESGO. VOCABULARIO. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

ICONTEC Internacional. (2011). NORMA TÉCNICA COLOMBIANA NTC ISO 31000. GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRECTRICES. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

Instituto de Auditores Internos de Colombia. (2017). MARCO INTERNACIONAL PARA LA PRÁCTICA PROFESIONAL DE LA AUDITORÍA INTERNA. Bogotá D.C. <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>

TIPOLOGÍAS DE CORRUPCIÓN. Oficina de las Naciones Unidas contra la Droga y el Delito –UNODC– y la Alcaldía Mayor de Bogotá – 2015.

<https://www.icbf.gov.co/cuales-son-los-delitos-que-tienen-relacion-con-hechos-de-corrupcion>

Anexos

A continuación se relacionan las herramientas y documentos complementarios, los cuales podrá descargar en el siguiente link: <https://www.funcionpublica.gov.co/web/mipg/como-opera-mipg>, ingresa a la *Dimensión Control Interno*, en la pestaña *Herramientas e Instrumentos Técnicos*.



1. Formatos matriz mapa de riesgos parametrizado (se incluye buena práctica Gobernación del Meta)



2. Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas



3. Protocolo Identificación Riesgos corrupción en Tramites.



4. Documentos Buenas prácticas para el análisis de riesgos de fraude y corrupción



5. Matriz de seguimiento a riesgos de corrupción.



6. Catálogo indicativo puntos riesgo fiscal