	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 1 de 116

MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES

Coordinación: Nicolás Martínez Grau-Oficina de Planeación

abril 30 de 2024





	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 2 de 116

Tabla de contenido


1. PRESENTACIÓN:	5
2. Objetivos:.....	6
3. Alcance:	7
4. Glosarios y Siglas	7
5. Antes de Iniciar con el Manual Lo que se Tiene que Saber:	14
5.1 ¿Qué establece MIPG?.....	14
5.2 Acerca de la metodología	17
5.3 Institucionalidad	17
5.4 Beneficios	18
6. PASO 1: POLÍTICA DE ADMINISTRACIÓN DE RIESGOS.....	20
<i>1.1 Lineamientos de la Política</i>	20
6.1 Políticas de Gestión de Riesgos	21
6.2 Objetivo General	22
6.3 Objetivos Específicos	22
6.4 Metas De La Administración De Riesgos	23
6.5 Alcance De La Administración De Riesgos	23
6.6 Estrategias Para El Logro De Los Objetivos	23
6.8 Políticas Específicas	25
6.9 Criterios De Evaluación	26
6.10 Responsabilidades Y Roles	27
6.10.1 Roles	27
6.11 Niveles De Aceptación Del Riesgo (Residual)	28
6.11.1 Tratamiento del riesgo y monitoreo	28
6.11.2 ¿Cómo Se Define El Modelo De Las Líneas De Defensa?	29
6.11.3 ¿Quiénes Son Los Asignados Para Monitorear Y Revisar La Gestión De Riesgos?.....	29
6.12 Mapa De Riesgos	31
6.13 Seguimiento	32
6.14 Periodo De Revisión Del Riesgos Institucionales	33
6.15 Eliminación Riesgos Identificados	33
7. PASO 2: IDENTIFICACIÓN DEL RIESGO.....	34
7.1 Análisis Del Contexto Externo, Interno Y Del Proceso.....	36
7.1.1 Establecimiento Del Contexto	36
7.1.2 Establecimiento Del Contexto Interno.....	36



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 3 de 116


7.1.3	Establecimiento Del Contexto Externo	37
7.1.4	Establecimiento Del Contexto Del Proceso	37
7.2	Identificación De Los Puntos De Riesgo:	39
7.3	Identificación De Áreas De Impacto	40
7.4	Identificación de áreas de factores de riesgo	41
7.5	Descripción Del Riesgo	42
7.5.1	Desglosando La Estructura Propuesta Tenemos:.....	42
7.5.2	Premisas Para Una Adecuada Redacción Del Riesgo	43
7.6	Clasificación Del Riesgo:	44
8.	PASO 3: VALORACIÓN DEL RIESGO	45
8.1	Análisis De Riesgos:	46
8.1.1	Determinar La Probabilidad:	46
8.1.2	Determinar El Impacto:	47
8.2	Valoración De Controles:	52
8.2.1	Estructura Para La Descripción Del Control:.....	52
8.2.2	Responsable De Ejecutar El Control:	52
8.2.3	Acción:	52
8.2.4	Complemento:	52
8.2.5	Tipología De Controles Y Los Procesos	53
8.2.6	Control Preventivo:	54
8.2.7	Control Detectivo	54
8.2.8	Control Correctivo.....	54
8.3	Nivel De Riesgo (Riesgo Residual):	58
8.4	Estrategias Para Combatir El Riesgo:	63
8.5	Herramientas Para La Gestión Del Riesgo:	64
8.5.1	Gestión De Eventos:	65
8.5.2	Indicadores Clave De Riesgo:	65
8.6	Monitoreo y Revisión	67
8.6.1	Actividades De Control	67
8.6.2	Información y Comunicación	67



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 4 de 116

8.6.3 Actividades De Monitoreo	67
9. Lineamientos Para El Análisis De Riesgo Fiscal	73
9.1 Control Fiscal Interno y Prevención Del Riesgo Fiscal	73
9.2 Control Fiscal Interno (CFI):	73
9.3 Definición y Elementos Del Riesgo Fiscal.....	75
9.3.1 Efecto	75
9.3.2 Evento Potencial	75
9.4 Metodología y Paso A Paso Para El Levantamiento Del Mapa De Riesgos Fiscales.....	76
9.4.1 Paso 1: Identificación De Riesgos Fiscales	76
9.4.2 Identificación De Áreas De Impacto	79
9.4.3 Identificación De La Causa Raíz O Potencial Hecho Generador	80
9.4.4 Descripción del Riesgo Fiscal	81
Referencias	116



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 5 de 116


1. PRESENTACIÓN:

La Contraloría Distrital de Cartagena de Indias que en adelante se denominará CDC, en desarrollo de sus funciones constitucionales y legales, enfrenta diariamente situaciones o sucesos potenciales que en alguna medida podrían impactar negativamente la productividad, los resultados, la reputación e imagen, y por lo tanto el logro de los objetivos institucionales. Por tal razón, la Entidad debe gestionar los riesgos de gestión (de proceso u operativo, estratégicos, de seguridad digital, de continuidad de negocio, y los asociados al tratamiento de datos personales), de corrupción y los de seguridad y salud en el trabajo, con sujeción a la normativa sobre el particular, en armonía con las buenas prácticas en la materia, en aras de disminuir la probabilidad de ocurrencia de tales eventos o mitigar las consecuencias e impactos negativos. Algunos eventos pueden representar una oportunidad de mejora para la organización, pero si no se manejan y se controlan adecuadamente a tiempo, podrían generar consecuencias negativas e impedir el logro de los objetivos institucionales.

El artículo 2° de la Ley 87 de 1993, entre otros objetivos del Sistema de Control Interno institucional, señala los siguientes: “Proteger los recursos de la organización, buscando una adecuada administración ante posibles riesgos que los afecten; y definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos.”

El artículo 2.2.21.5.4 Gestión de Riesgos del Decreto 1083 de 2015, establece: “Como parte integral del fortalecimiento de los sistemas de control interno en las Entidades públicas, las autoridades correspondientes establecerán y aplicarán políticas de gestión de riesgos. Para tal efecto, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la Administración y las oficinas de control interno o quien haga sus veces, evaluando los aspectos tanto internos como externos que pueden llegar a representar amenazas para la consecución de los objetivos organizacionales, con miras a establecer acciones efectivas representadas en actividades de control,”



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 6 de 116


La CDC expone y adopta el siguiente Manual, tomando como referencia la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas¹, lo cual conduce a una gestión pública más eficiente y sirve para que se cumpla con los objetivos institucionales.

2. Objetivos:

- Fortalecer la gestión de riesgos de la Entidad, para optimizar la prevención, detección y corrección de desviaciones que puedan afectar el logro de los objetivos institucionales.
- Optimizar la gestión de riesgos de la Entidad, mediante la implementación del esquema de asignación de responsabilidades de las líneas de defensa (Línea Estratégica, Primera Línea de Defensa, Segunda Línea de Defensa y Tercera Línea de Defensa).
- Contribuir a la generación y fortalecimiento permanente de la cultura de gestión de riesgos y de control en la Entidad.
- Contribuir en la optimización de la toma de decisiones en la operación de los procesos institucionales, mediante el suministro de información pertinente generada en la gestión de riesgos.
- Contribuir en la reducción de la exposición (vulnerabilidad) de la Entidad frente a los eventos que puedan afectar el logro de sus objetivos.
- Optimizar el funcionamiento y eficacia del control interno, y por lo tanto el desempeño institucional, a partir del fortalecimiento de la gestión del riesgo.
- Contribuir al diseño e implementación del Programa Integral de Protección de Datos.
- Incluir en la gestión de riesgo los asociados al tratamiento de datos personales en el proceso de gestión de riesgos de la CDC, para su posterior desarrollo e implementación.

¹ Guía Para la Administración del Riesgo y el Diseño de Controles en Entidades Pública Versión 6 de 2022 DAFP



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 7 de 116

3. Alcance:

Este Manual deberá usarse en las operaciones de todas las Áreas y/ procesos, aplicado por todos los servidores públicos y Contratista que se encuentren ejecutando una actividad misional, de apoyo, Estratégica y de evaluación en lo de competencia de sus respectivos cargos, en especial por quienes ejerzan rol de líder de proceso.

4. Glosarios y Siglas

Aceptación del riesgo²: Decisión informada de tomar un riesgo particular.

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.

Alta Dirección³: Comprende los empleos a los cuales corresponden funciones de dirección general de formulación de políticas institucionales y de adopción de planes, programas y proyectos

Amenazas: Causa potencial de un incidente no deseado, el cuál puede ocasionar daño a un sistema o a una organización.

Análisis de Impacto del Negocio- BIA⁴: Proceso del análisis de actividades y el efecto que una interrupción del negocio podría tener sobre ellas. (ISO 22301).

Apetito por el riesgo⁵: Magnitud (cantidad) y tipo de riesgo que una organización está dispuesta a buscar o retener.


² Guía Técnica Colombiana GTC 137- Gestión del Riesgo vocabulario. Feb.16/11

³ Guía rol de las Unidades u oficinas de Control Interno, auditoría Interna o quien haga sus veces. DAFP dic/18

⁴ Guía para realizar el Análisis de Impacto del Negocio BIA. Ministerio de Tecnologías de la Información y las Comunicaciones. May 12/15

⁵ Guía Técnica Colombiana GTC 137- Gestión del Riesgo vocabulario. Feb.16/11.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 8 de 116

Causa del riesgo: Fuente interna o externa que sola o en combinación con otras puede ocasionar la materialización del riesgo. Usualmente también se denomina fuente de riesgo.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

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

CDC: Contraloría Distrital de Cartagena

Ciclo de vida del dato⁶: Significa reconocer cómo se produce el flujo de información en sus procesos y en sus actividades.

Clientes o grupos de valor de la CDC: Son los ciudadanos, grupos de ciudadanos y Entidades a quienes la CDC debe dirigir sus productos y servicios; es decir la ciudadanía, el Concejo Distrital de Cartagena. Los productos/servicios de la Entidad son las salidas de los procesos misionales destinadas a los Grupos de Valor de la entidad.

Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, Entidades o procesos no autorizados.


Consecuencia: Los efectos o situaciones resultantes de la materialización del riesgo que impactan el proceso, la Entidad, sus grupos de valor y/o a las demás partes interesadas. Usualmente también se denomina impacto.

Continuidad de Negocio: Capacidad de la organización para continuar la entrega de productos o servicios a los niveles predefinidos aceptables después de un evento perjudicial.

Control: Medida que mitiga y/o modifica el riesgo. Los controles incluyen procesos,

⁶ Superintendencia de Industria y Comercio, presentación sobre “El Principio de Responsabilidad demostrada en el Decreto 1377 de 2007”, jun/14.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 9 de 116

políticas, dispositivos, prácticas u otras acciones que varíen al riesgo. Los controles no siempre pueden ejercer el efecto modificador previsto o asumido.

Criterios de calificación del riesgo: Parámetros establecidos por la CDC para determinar la importancia (nivel de severidad o criticidad) del riesgo en función de su impacto y probabilidad.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables”.


Disponibilidad: La información puede ser accesible y utilizable por personas, procesos o Entidades autorizados en el momento que se necesite.

Análisis del contexto: Identificación de los aspectos internos y externos que se han de tomar en consideración cuando se gestione el riesgo.

Evento: Incidente o situación que ocurre o podría suceder en un lugar y durante un periodo de tiempo determinado. Puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie. Puede tener una o más causas y consecuencias. Puede ser algo previsto que llegue a ocurrir o algo no previsto que ocurre.

Factores de Riesgo: Son los agentes generadores asociados a las causas, con base en los cuales éstas son clasificadas. Específicamente para los riesgos de gestión, los principales factores internos son el recurso humano (cantidad, conocimiento, experiencia, cultura), los procesos/procedimientos, presupuesto, reglamentación interna, la tecnología y la infraestructura; y los factores externos más relevantes son los legales/reglamentarios, condiciones geográficas y de acceso a lugares dentro del alcance de las funciones y competencias de la Entidad, condiciones sociales, políticas, ambientales y de orden público; y los relacionados con la fuerza de la naturaleza, entre otros. En Seguridad y Salud en el Trabajo, los factores de riesgo se clasifican en: condiciones inseguras (instalaciones, equipos de trabajo, maquinaria y herramientas que no están en condiciones de ser usados y de realizar el trabajo para el cual fueron diseñadas y actos subestándar (acciones o decisiones humanas, que pueden causar una situación insegura o un incidente).



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 10 de 116

Frecuencia: Número de veces que ha ocurrido un evento en un tiempo dado.

Gestión de incidentes: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de Riesgos: Proceso dinámico e interactivo que le permite a la Contraloría Distrital de Cartagena de Indias identificar, evaluar y gestionar aquellos eventos internos y externos que puedan afectar o impedir el logro de sus objetivos institucionales

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Incidente de seguridad de la información: Un evento o series de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Propiedad de la exactitud y la integridad de la información, es decir que no ha sido modificada.


Mapa de calor: Plano en el que se presentan simultáneamente las escalas de medición de impacto y de probabilidad; y, como producto de su combinación, mediante colorimetría representa la importancia (nivel de severidad o criticidad) del riesgo.

Mapa de riesgos institucional por procesos: Información organizada (sistematizada) resultante de la aplicación del marco metodológico de la gestión de riesgos específicamente en lo correspondiente a la evaluación del riesgo (integra las etapas de identificación, análisis y valoración del riesgo) realizada para cada uno de los procesos institucionales.

MECI: Modelo Estándar de Control Interno para el Estado Colombiano

Nivel de riesgo: Magnitud de riesgo o de combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad²⁰. También se le conoce como nivel o grado de severidad, de criticidad o de importancia.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 11 de 116

Parte interesada: Persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la de corrupción que debe ser implementada por todas las Entidades del orden nacional, departamental y municipal.

Plan de contingencia: Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

Plan de continuidad de negocio: Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción.

Plan de manejo de riesgos Institucional-por procesos: Conjunto detallado e interrelacionado según se requiera de las acciones –por procesos– adoptadas por la Entidad para mitigar los riesgos residuales que lo ameriten. Tales Acciones corresponden al tratamiento del riesgo.


Probabilidad: Hace referencia a la medición de la posibilidad de que algo suceda, esté o no definido, medido o determinado objetiva o subjetivamente, cualitativa o cuantitativamente, y descrito utilizando términos generales o matemáticos (como la probabilidad numérica o la frecuencia en un periodo de tiempo determinado).

Propietario del riesgo: Persona o Entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 12 de 116

Riesgo de Gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

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

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).

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo Inherente: Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. También denominado riesgo absoluto.


Riesgo Residual: Nivel resultante del riesgo después de aplicar controles para su mitigación; es decir, el margen o residuo de riesgo que se mantiene.

Riesgos Estratégicos: Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la Entidad.

Riesgos de Imagen: Posibilidad de ocurrencia de eventos que afecten la percepción y la confianza de la ciudadanía y otras partes interesadas hacia el buen nombre la Entidad.

Riesgos de Cumplimiento: Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato de la normatividad legal y las obligaciones contractuales.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 13 de 116

Riesgos en Seguridad y Salud en el Trabajo (SST): Combinación de la probabilidad de que ocurran una o más exposiciones o eventos peligrosos y la severidad del daño que pueda ser causada por estos.


Tolerancia al riesgo: Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

Tratamiento de datos personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Tratamiento de Riesgo: Acciones o medidas para modificar el riesgo residual, las cuales son las siguientes (ERCA, por sus iniciales): Evitar el Riesgo, Reducirlo, Compartirlo o Aceptarlo. Con la formulación de este tipo de acciones se conforma el Plan de manejo de riesgos Institucional-por procesos.

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



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 14 de 116

5. Antes de Iniciar con el Manual Lo que se Tiene que Saber:

5.1 ¿Qué establece MIPG?


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).

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.

El numeral 2.2.1 “Política de Planeación institucional” de la dimensión “Direccionamiento Estratégico y Planeación” menciona que, 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.

De igual forma, se menciona en esta dimensión que, para llevar a cabo el ejercicio de planeación, la entidad debe documentar dicho ejercicio en donde se describa la parte conceptual u orientación estratégica; y la parte operativa en la que se señale de forma precisa los objetivos, las metas y resultados a lograr, las trayectorias de implantación o cursos de acción a seguir, cronogramas, responsables, indicadores para monitorear y evaluar su cumplimiento y los riesgos que pueden afectar tal cumplimiento y los controles para su mitigación.




	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 15 de 116

Importante: En atención a lo que establece COSO 2013 y COSO ERM 2017, los planes, programas o proyectos deben contemplar los riesgos para su ejecución y logro de sus objetivos.

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





	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 16 de 116

Enfoque N° 1 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. 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



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 17 de 116

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.

5.2 Acerca de la metodología

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, entender la entidad y el entorno, lo que determinará el análisis de riesgos y la aplicación de la metodología en general.

5.3 Institucionalidad

El modelo integrado de planeación y gestión (MIPG) define 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:



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 18 de 116

Enfoque N° 2 Operatividad Institucionalidad para la Administración del Riesgo




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

5.4 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:

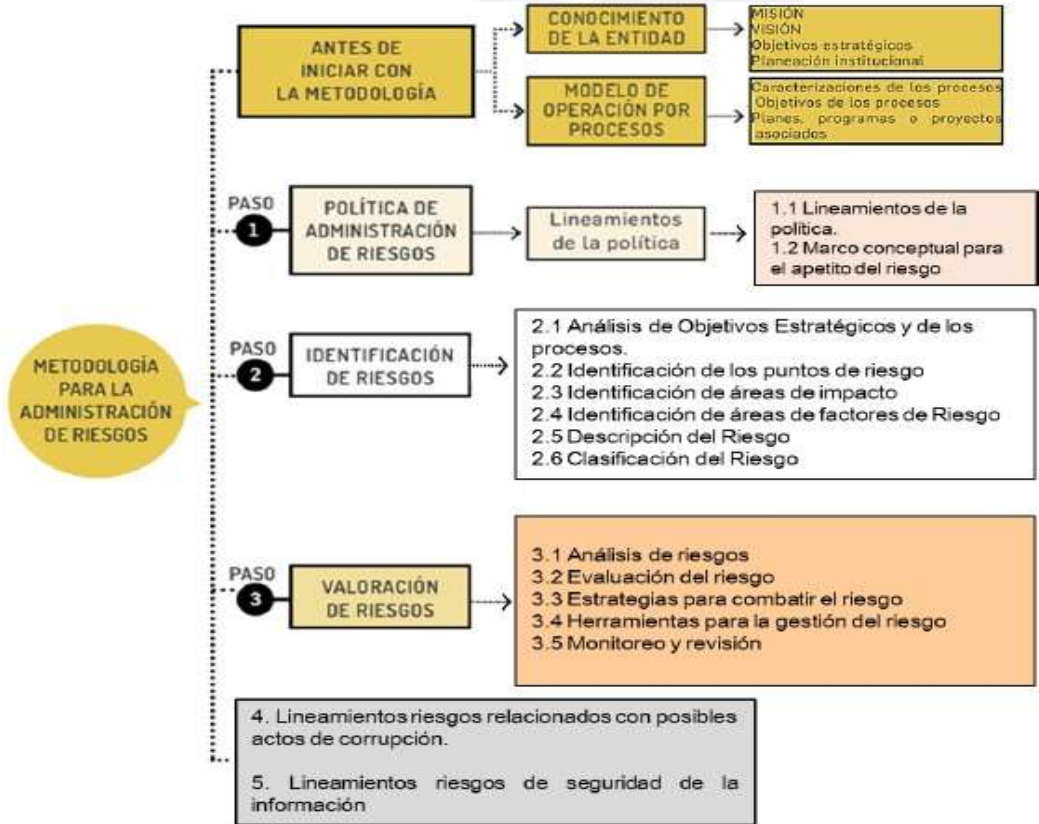
- Apoyo a la toma de decisiones.
- Garantizar la operación normal de la organización.
- Minimizar la probabilidad e impacto de los riesgos.
- Mejoramiento en la calidad de procesos y sus servidores (calidad va de la mano con el riesgo).
- Fortalecimiento de la cultura de control de la organización.
- 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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 19 de 116


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, el conocimiento de esta desde un punto de vista estratégico, de la aplicación de tres (3) pasos básicos para su desarrollo y 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:

Enfoque N° 3 Metodología para la Administración del Riesgo



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



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 20 de 116

6. PASO 1: POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

1.1 Lineamientos de la Política

Estructura 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.	



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 21 de 116

6.1 Políticas de Gestión de Riesgos

En la **CDC** la gestión del riesgo se realizará con sujeción a la operación del Sistema de Gestión en lo pertinente, a lo establecido en el presente Manual y en los demás documentos que sobre el particular se adopten.


Las políticas identifican las opciones para tratar y manejar los riesgos basadas en la valoración de riesgos, permiten tomar decisiones adecuadas y fijar los lineamientos de la Administración del riesgo, a su vez transmite la posición de la dirección y establecen las guías de acción necesarias a todos los servidores de la entidad. Estas se fundamentan en las medidas de respuesta que se derivan de las diferentes zonas de riesgo identificadas en la matriz de riesgo.

Para la consolidación de las Políticas de Administración de Riesgos se deben tener en cuenta todas las etapas consideradas en la Guía Metodológica de administración de riesgos.

Con la entrada en vigencia del decreto 1499 de 2017 del Modelo Integrado de Planeación y Gestión (MIPG), que integra los Sistemas de Gestión de la Calidad y de Desarrollo Administrativo, crea un único Sistema de Gestión y lo articula con el Sistema de Control Interno, el cual se actualiza y alinea con los mejores estándares internacionales como son el Modelo COSO 2013, COSO ERM 2017 y el Modelo de las Cuatro(4) Líneas de Defensa, con el fin de entregar a los ciudadanos, lo mejor de la gestión para producir cambios en las condiciones de vida, mayor valor público en términos de bienestar, prosperidad general y fortalecer la lucha contra la corrupción.

La política de administración de riesgo establece las guías de acción necesarias a los Servidores Públicos de la Contraloría Distrital de Cartagena de Indias, para coordinar y administrar los eventos que pueden impedir el logro de los objetivos de la entidad.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 22 de 116

A continuación, se presentan las políticas de gestión de riesgo de gestión, en función de los roles y responsabilidades, niveles de aceptación del riesgo, de su tratamiento y monitoreo.


6.2 Objetivo General

Establecer las políticas para el manejo de Administración de Riesgos de la Contraloría Distrital de Cartagena de Indias, de acuerdo a los lineamientos establecidos por el Departamento Administrativo de la Función Pública, Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, con el fin de aplicar medidas necesarias que permitan administrar los riesgos identificados, prevenirlos y corregir las desviaciones que puedan afectar el logro de los objetivos institucionales y de proceso.

6.3 Objetivos Específicos

- Proteger los recursos de la Contraloría Distrital de Cartagena de Indias, resguardándolos contra la materialización de los riesgos.
- Revisar y ajustar dentro de los procesos y procedimientos las acciones de mitigación resultado de la administración del riesgo.
- Involucrar y comprometer a todos los servidores de la Contraloría Distrital de Cartagena de Indias, en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos.
- Asegurar el cumplimiento de normas, leyes y regulaciones.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 23 de 116

6.4 Metas De La Administración De Riesgos

Lograr una eficaz, eficiente y efectiva administración de las acciones conducentes a la mitigación, control y prevención de la materialización de los riesgos.


6.5 Alcance De La Administración De Riesgos

La administración de riesgos en la Contraloría Distrital de Cartagena de Indias, abarca la totalidad de los Procesos y/o Áreas funcionales diseñadas en el último rediseño de la organización (Acuerdo 045 de 2020) y procesos descritos en el “Mapa de procesos”.

6.6 Estrategias Para El Logro De Los Objetivos

- Evaluar periódicamente los eventos negativos tanto internos como externos que puedan afectar la administración de la Contraloría Distrital de Cartagena de Indias.
- Realizar seguimiento y evaluación por parte de la Oficina de Control Interno, (tercera línea de defensa) a las acciones de mitigación de los riesgos mediante las cuales se implementan o fortalecen los controles preventivos y correctivos, validando que la línea estratégica, la primera línea y segunda línea de defensa cumpla con sus responsabilidades.
- Fortalecer la cultura del autocontrol, involucrando a todos los servidores de la Entidad (comités de coordinación y seguimiento), en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos.
- Conformar los equipos Operativo MIPG en cada una de las Áreas y Procesos identificados para hacerle seguimiento al avance del FURAG y las recomendaciones propuestas por la Función Pública.
- Actualizar al personal de la Entidad, en desarrollo normativo y legal, en cumplimiento del principio de la autorregulación.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 24 de 116


6.7 Política General

Con el fin de garantizar el logro misional de la Contraloría Distrital de Cartagena de Indias, se ha definido que la Administración de Riesgos tendrá un carácter prioritario y estratégico asociado al Modelo de Operación por Procesos y El Modelo Integrado de Planeación y Gestión- (MIPG).

La Contraloría Distrital de Cartagena de Indias se compromete a ejercer el control efectivo de los eventos de riesgo que puedan impedir el cumplimiento de la misión, el logro de la visión, objetivos estratégicos y de proceso a través del diagnóstico, identificación, análisis, valoración y administración del riesgo, orientado al mejoramiento continuo de los procesos Estratégicos, misionales, de apoyo y de evaluación de la entidad.






	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 25 de 116

6.8 Políticas Específicas

Generar una visión sistémica acerca de la administración y evaluación de riesgos, consolidada en un ambiente de control que estimule la cultura de la identificación y prevención del riesgo, definiendo las políticas, propiciando los espacios y asignando los recursos necesarios, con canales directos de comunicación y el apoyo a todas los responsables de los procesos de la entidad que permitan propiciar las condiciones necesarias para la aplicación de las siguientes políticas:

- Fortalecer la implementación y desarrollo de la política de administración del riesgo, a través del adecuado tratamiento de los riesgos para garantizar el cumplimiento de la misión y los objetivos institucionales y de proceso, mejorando el desempeño de la entidad.
- Promover la cultura del autocontrol y de la identificación y prevención del riesgo.
- Diseñar los controles que le permitan a las áreas y procesos organizacionales lograr los objetivos estratégicos y operativos alineados con la Misión y Visión institucional.
- Identificar las acciones para administrar los riesgos con base en su valoración, que permitan tomar decisiones adecuadas para evitar, reducir, compartir, transferir o asumir los riesgos. Para el caso de los riesgos de corrupción los criterios de evaluación para la toma de decisiones adecuadas son eliminar o reducir, evitar o reducir el riesgo.
- El monitoreo está a cargo de los responsables de cada área y/o proceso, (Primera línea de defensa) y lo deben realizar mensualmente en los Comités Seguimiento, evaluando la eficacia de las acciones adelantadas durante dicho periodo y el registro de la materialización lo consignan en los formatos P02-F02 Y P02-F03 Seguimiento actividades de control, mapa de riesgos y Registro de materialización de riesgos para remitirlos bimestralmente (con corte a febrero 28, abril 30, junio 30, agosto 30, octubre 31 y diciembre 31) a la Coordinación de Planeación.
- Para el seguimiento a los riesgos de corrupción, el Jefe de Control Interno o quien haga sus veces, (Tercera Línea de Defensa) debe adelantar seguimiento al Mapa



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 26 de 116

de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

- La Oficina de Control Interno (Tercera Línea de Defensa) realizará seguimiento (tres) 3 veces al año, así: Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de mayo. Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de septiembre. Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de enero.
- La Coordinación de Planeación (Segunda Línea de Defensa) socializa a todos los Servidores públicos de la Contraloría Distrital de Cartagena de Indias, el Manual de Administración de Riesgos y Diseño de controles, que contiene la política General y específica para la Administración del Riesgo y Diseño de Controles, la cual debe ser actualizada periódicamente y comunicada a través de las herramientas de comunicación interna, como su publicación en la página WEB, ORBIS y correos institucionales.

6.9 Criterios De Evaluación


De acuerdo con la Metodología para la Administración de Riesgos adoptada y la matriz de riesgos generada para la entidad a partir de la aplicación de la metodología, se establecen los siguientes criterios de evaluación de los riesgos en cada una de las zonas así:

Los riesgos que se encuentran en **Zona Baja** implican que se debe Aceptar el riesgo, significa asumirlo, porque su frecuencia es muy baja y no representa ningún peligro para la entidad.

Los riesgos que se encuentran en **Zona Moderada** significan que se debe Reducir el riesgo, lo que implica tomar medidas encaminadas a disminuir tanto la frecuencia con medidas de prevención, como reducir la gravedad del impacto adoptando medidas de protección.

Los riesgos que se encuentran en **Zona Alta** significan que se debe Compartir el riesgo, reduce su efecto a través de la transferencia de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 27 de 116

Los riesgos que se encuentran **en Zona Extrema** significan que se debe Evitar o Eliminar el riesgo, cuando su frecuencia y gravedad son altas. Dándole un manejo prioritario a las acciones y recursos que se demanden para su gestión.

Los riesgos de corrupción se encuentran en la Zona Moderada, Zona Alta y Zona Extrema, debido a que el impacto siempre será negativo.


6.10 Responsabilidades Y Roles

La administración de riesgos es responsabilidad de todos los servidores públicos de Contraloría Distrital de Cartagena de Indias, la entidad debe asegurar el logro de sus objetivos, anticipándose a los eventos negativos relacionados con la gestión de la entidad. El Modelo Integrado de Planeación y Gestión- (MIPG) en la dimensión 7 “Control Interno” desarrolla a través de las Líneas de Defensa la responsabilidad de la gestión del riesgo y control.

6.10.1 Roles

- Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno de la Contraloría Distrital de Cartagena actuarán como máximo órgano de consulta, coordinación, asesoría, evaluación y decisión en materia de gestión de riesgo en la entidad. En tal virtud, le corresponderá, entre otros asuntos, aprobar las políticas institucionales en dicha materia y hacer seguimiento a su cumplimiento.
- La distribución de responsabilidades para la gestión de riesgos y ejercicio del control en la entidad se definirá de acuerdo con el esquema de las líneas de defensa previsto en el Modelo Integrado de Planeación y Gestión(MIPG) (estratégica, primera línea de defensa, segunda línea de defensa y tercera línea de defensa), como se indica en este Manual.
- La coordinación institucional de la gestión de riesgos la ejercerá el Coordinador de la Oficina de Planeación, de conformidad con las instrucciones del Contralor(a) Distrital de Cartagena de Indias, las directrices del Comité Institucional de Gestión y de Coordinación de Control Interno de la Contraloría Distrital de Cartagena de Indias, sin perjuicio de lo anterior; según la naturaleza del riesgo las siguientes instancias coordinarán la gestión de riesgo:



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 28 de 116

- Coordinador de la Oficina de Planeación: Riesgos de gestión (específicamente los riesgos de proceso u operativo y estratégicos) y los riesgos de corrupción
- Coordinador de Talento Humano: Riesgos de Salud y Seguridad en el Trabajo.

Las coordinaciones mencionadas les corresponden liderar, asesorar y acompañar a los responsables de la gestión de riesgos, en armonía con el esquema de las líneas de defensa. Así mismo, elaborar y formalizar la presentación de propuestas de documentos necesarios para la operación de la Gestión de riesgos diferentes a este Manual, de acuerdo con el procedimiento previsto en el Sistema de Gestión.

- Los servidores públicos que en virtud de la estructura organizacional y/o de Proceso deban ejercer el rol de líder de área y/o proceso cumplirán lo dispuesto en este Manual para dicho rol.


6.11 Niveles De Aceptación Del Riesgo (Residual)

- Se considerarán riesgos inaceptables (intolerables) los que sean clasificados como “Riesgo Extremo” y “Riesgo Alto”; y riesgos aceptables (tolerables) aquellos clasificados como “Riesgo Moderado” y “Riesgo Bajo”.
- La decisión excepcional de considerar aceptables riesgos de gestión cuyo nivel de severidad residual corresponda a Extremo o Alto será del Comité Institucional de Gestión y de Coordinación de Control Interno de la Contraloría Distrital de Cartagena de Indias.

6.11.1 Tratamiento del riesgo y monitoreo

- ✓ Se formulará plan de manejo (tratamiento) para aquellos riesgos de gestión inaceptables(intolerables); es decir, para los riesgos cuyo nivel de severidad residual sea Extremo o Alto.
- ✓ Frente a los riesgos de gestión aceptables (tolerables) cuyo nivel de severidad residual sea moderado será opcional la adopción de acciones de tratamiento.
- ✓ Cada año se actualizará el mapa de riesgo de gestión-por procesos, y el respectivo



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 29 de 116

- ✓ plan de manejo de riesgos bajo la coordinación de la Oficina de Planeación, sin perjuicio de la actualización extraordinaria cuando así se requiera en función de las necesidades institucionales, a solicitud del líder del proceso.
- ✓ Una vez aprobado el Plan de Manejo de Riesgos del proceso, cada líder de proceso, en su calidad respectivamente de responsables de la gestión de riesgos en lo de su competencia, mínimo dos veces durante su ejecución realizarán seguimiento al mismo.
- ✓ El monitoreo está a cargo de los responsables de cada proceso, (Primera línea de defensa) y lo realizan mensualmente en los Comités de Coordinación y Seguimiento, evaluando la eficacia de las acciones adelantadas durante dicho periodo y el registro de la materialización lo consignan en los formatos diseñados por la Oficina de Planeación y los remiten bimestralmente (con corte a febrero 28, abril 30, junio 30, agosto 30, octubre 31 y diciembre 31) a la Oficina de Planeación.

6.11.2 ¿Cómo Se Define El Modelo De Las Líneas De Defensa?


Es un modelo de control que establece los roles y responsabilidades de todos los actores del riesgo y control en una entidad, este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos.

6.11.3 ¿Quiénes Son Los Asignados Para Monitorear Y Revisar La Gestión De Riesgos?

El monitoreo y revisión de la gestión de riesgos, está alineado con la dimensión del MIPG de “Control Interno”, que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en las diferentes Líneas de Defensas conformadas por diversos servidores públicos de la entidad como sigue:

Línea Estratégica. Define las políticas de gestión de riesgos y de control interno para la Contraloría Distrital de Cartagena de Indias y realiza el respectivo seguimiento a su cumplimiento. Instancias cargo de la Línea Estratégica. Contralor(a) Distrital de Cartagena de Indias, Secretario General, Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 30 de 116


Primera Línea de Defensa. Todos los servidores tienen una responsabilidad frente a la aplicación efectiva de los controles y por ende se encargan del mantenimiento efectivo de controles internos, ejecutar lo estipulado en el Manual de la gestión de riesgos -en todas sus etapas-, ejercer el control (inherente) en desarrollo de la gestión institucional bajo su responsabilidad, así como de la detección de deficiencias de control y de la implementación de las acciones de mejoras, correctivas, detectivas y preventivas que se requieran para garantizar el logro de los resultados esperados. En general debe gestionar los riesgos de los asuntos a su cargo. Las instancias a cargo de esta línea son todos los líderes de áreas y/o procesos, en los roles que cada uno desempeñe en la ejecución de las actividades, según la naturaleza de los respectivos cargos.

Segunda Línea de Defensa: Se encarga de coordinar a nivel institucional tanto la implementación, sostenibilidad y fortalecimiento del **MIPG**, como la gestión de riesgos; así mismo del monitoreo y evaluación del estado de los controles, para asegurar que sean apropiados y funcionen correctamente. Igualmente se encarga de funciones de cumplimiento, seguridad y calidad, entre otras similares, suministrando información sobre el particular a la primera línea de defensa y a la línea estratégica. Supervisa la implementación de prácticas de gestión del riesgo por parte de la primera línea y ayuda a distribuir la información adecuada sobre riesgos a todos los servidores de la Entidad. Asiste y guía a la línea estratégica y la primera línea de defensa en la gestión adecuada de los Riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar, tratar los riesgos, y realiza un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos. Instancia a cargo de esta línea de defensa, el Coordinador de la Oficina de Planeación, los supervisores del proceso auditor, supervisores e interventores de contratos.

Tercera Línea de Defensa: Se encarga de suministrar información sobre la efectividad del control interno y la operación de la primera y segunda líneas de defensa, con un enfoque basado en riesgos. Mediante la auditoría interna con dicho enfoque, proporciona aseguramiento sobre la eficacia de gobierno, gestión de riesgos y control interno a la alta dirección.

Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 31 de 116


sistema de gestión de riesgos, validando que la línea estratégica, la primer línea y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. Instancia a Cargo de la Tercera Línea de Defensa es la Oficina de Control Interno, responsable de la evaluación tanto de la gestión de riesgos como del diseño, aplicación y efectividad de los controles.

- La gestión de riesgos será responsabilidad de los líderes de área y/o procesos y de los demás directivos y servidores públicos de la Entidad, en lo que respecta a los riesgos específicos de los asuntos a su cargo. Dicha gestión también será responsabilidad de los contratistas (prestación de servicios) que actúen en representación de la Entidad, en el marco de las actividades que desarrollen en cumplimiento de sus obligaciones contractuales.
- La aprobación del mapa de riesgos del proceso y del respectivo plan de manejo es responsabilidad de los correspondientes líderes de procesos.
- Cada año se actualizará el mapa de riesgos de gestión-por procesos, según las directrices de la Oficina de Planeación bajo la coordinación, sin perjuicio de la actualización extraordinaria cuando así se requiera en función de las necesidades institucionales, a solicitud del líder del proceso. Los riesgos estratégicos se deben formular en cada cambio de administración y actualizarse cuando haya lugar a ello, con sujeción a las Directrices del Comité Institucional de Gestión y Desempeño y de Control Interno o del Coordinador de la Oficina de Planeación.
- La Oficina de Control Interno es responsable de la evaluación independiente tanto de la gestión de riesgos como la evaluación del diseño, aplicación y efectividad de los controles, de conformidad con la normatividad general, la reglamentación interna y procedimientos aplicables.

6.12 Mapa De Riesgos

El mapa de riesgos es la herramienta conceptual y metodológica que permite valorar y monitorear los riesgos al interior de la Contraloría y estará compuesto por los riesgos de Gestión, Corrupción y Seguridad Digital definidos conforme a la metodología adoptada por Contraloría Distrital de Cartagena de Indias.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 32 de 116

En caso de modificarse el contexto estratégico, los objetivos estratégicos o de Proceso, se deben ajustar o identificar nuevos riesgos. Para el ajuste o identificación de estos, las propuestas se harán por parte de los líderes de cada proceso (Primera Línea) siguiendo la metodología de administración de riesgos y se presentarán al área de Planeación, (Segunda Línea) la cual los consolidara y presentara posteriormente al Comité Institucional de Gestión y Desempeño para su aprobación.

Para el ajuste o identificación de nuevos riesgos, se realizará en el comité de Coordinación y Seguimiento de cada área y/o proceso correspondiente (Primera Línea), teniendo en cuenta la metodología de administración de riesgos y se remiten al área de Planeación, (Segunda Línea) para actualización del mapa de riesgos.

6.13 Seguimiento


El monitoreo y seguimiento es esencial para asegurar que las acciones se están llevando a cabo y evaluar la efectividad de cada uno de los controles existentes en términos de la materialización o no de los riesgos.

El monitoreo está a cargo de los responsables de los procesos, (Primera Línea) la cual se encargará de diseñar, implementar, monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad.

La oficina de planeación, (Segunda línea) monitoreara la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.

La Oficina de Control Interno, (Tercera Línea) Proporciona información sobre la efectividad del S.C.I., a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 33 de 116

6.14 Periodo De Revisión Del Riesgos Institucionales


Los riesgos asociados al logro de los objetivos de los procesos institucionales, se identifican y/o validan en cada vigencia por los líderes de proceso con sus respectivos equipos de trabajo con el acompañamiento de la Oficina de Planeación a través de la metodología propia de la CDC.

6.15 Eliminación Riesgos Identificados

Los riesgos que se encuentren en nivel de aceptación BAJO, que soporten documentación de sus controles en sus procedimientos y evidencien implementación de sus controles existentes y no presenten materialización durante los últimos 5 años, pueden ser considerados para su eliminación.





	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 34 de 116

7. PASO 2: IDENTIFICACIÓN DEL RIESGO

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.

Enfoque N°4 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.

La entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión Corporativa, 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 SMART, cuya estructura se explica a continuación:

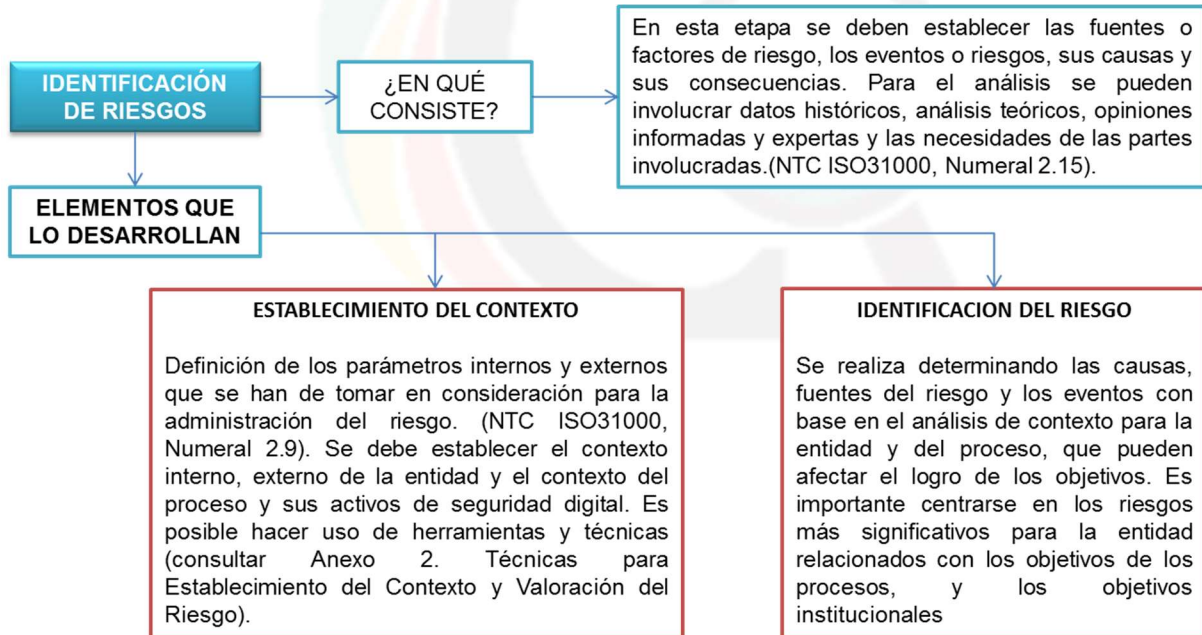


	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 35 de 116


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.

Enfoque N°5 Aspectos a desarrollar en la Identificación del Riesgo





	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 36 de 116

Importante: Debe analizarse en cada entidad el contexto particular al que se enfrentan los procesos ante los riesgos de todo tipo, conforme a la misionalidad institucional.

7.1 Análisis Del Contexto Externo, Interno Y Del Proceso

7.1.1 Establecimiento Del Contexto

Definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo (NTC-ISO 31000). A partir de los factores que se definan es posible establecer las causas de los riesgos a identificar.

7.1.2 Establecimiento Del Contexto Interno

Se determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos. Se pueden considerar los siguientes factores como:

Financieros: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.

Talento Humano: Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.


Procesos: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.

Tecnológicos: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.

Estratégicos: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.

Comunicación interna: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 37 de 116

7.1.3 Establecimiento Del Contexto Externo

Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad. Se pueden considerar factores como:

Económicos: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.

Políticos: Cambios de gobierno, legislación, políticas públicas, regulación.

Sociales: Demografía, responsabilidad social, orden público.

Tecnológicos: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.

Medioambientales: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.

7.1.4 Establecimiento Del Contexto Del Proceso

Se determinan las características o aspectos esenciales del proceso y sus interrelaciones. Se pueden considerar factores como:

Diseño del proceso: Claridad en la descripción del alcance, Caracterización y objetivo del proceso.


Interacciones entre procesos: Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.

Transversalidad: Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.

Indicadores de Gestión: Variables que permiten medir el desempeño de los procesos.

Procedimientos asociados: Pertinencia en los procedimientos que desarrollan los procesos.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 38 de 116

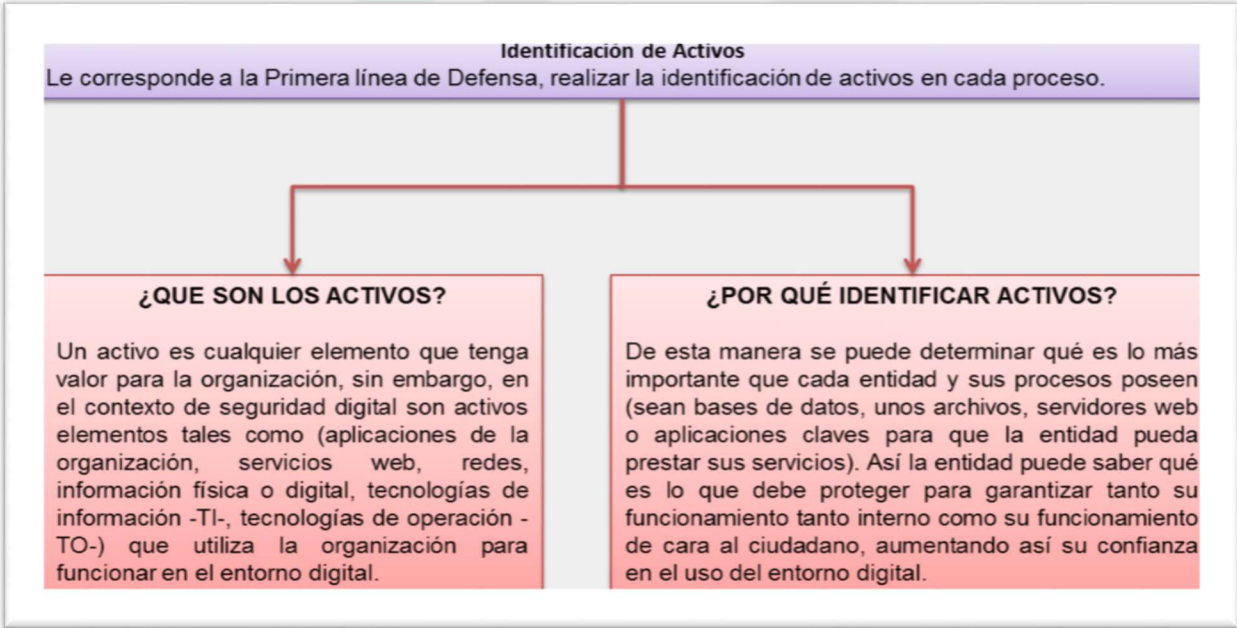
Responsables del proceso: Grado de autoridad y responsabilidad de los funcionarios frente al proceso.

Comunicación entre los procesos: Efectividad en los flujos de información determinados en la interacción de los procesos.

Activos de seguridad digital del proceso: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso


***Importante:** Como herramienta básica para el análisis del contexto del proceso se sugiere utilizar las caracterizaciones de estos, donde es posible contar con este panorama. Si estos documentos están desactualizados o no se han elaborado, es importante actualizarlos o elaborarlos antes de continuar con la metodología de administración del riesgo.*

Enfoque N°6 Identificación de Activos:



Importante: Todo lo que no está plenamente identificado, no está debidamente asegurado.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 39 de 116

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


Enfoque N° 7



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

En el desarrollo de la cadena de valor de una organización pública, existen elementos y actividades que podrían generar eventos de riesgos.




	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 40 de 116



















7.3 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.






	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 41 de 116

7.4 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*

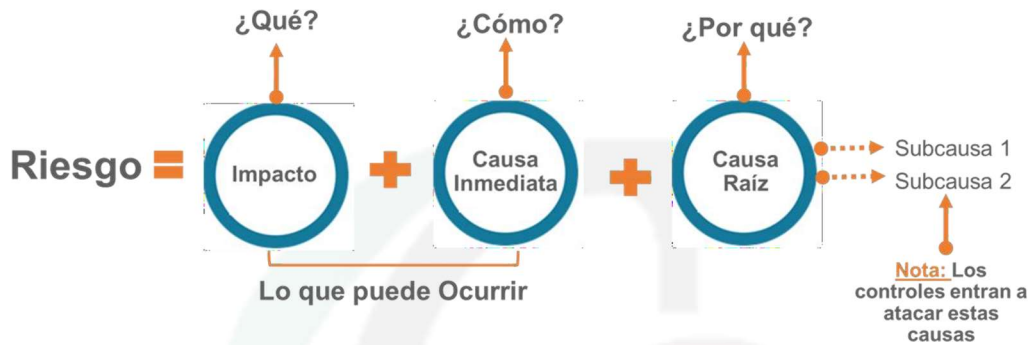
Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos internos y externos
			Falta de capacitación, temas relacionados 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
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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 42 de 116

7.5 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:



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.


7.5.1 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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 43 de 116

Ejemplo:

Proceso: gestión de recursos físicos y de Servicios

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 adquirentes) 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:

Ejemplo gráfico 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

7.5.2 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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 44 de 116

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

7.6 Clasificación Del Riesgo: permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

Tabla de Clasificación de los 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.

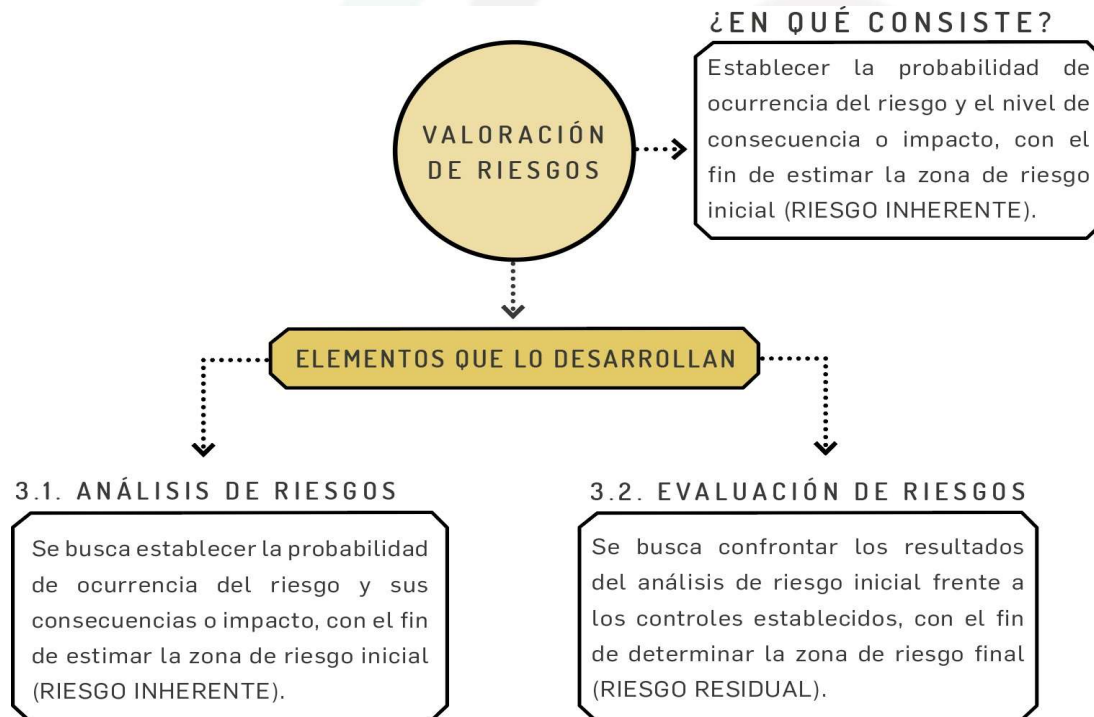
Teniendo en cuenta que en la Tabla se definieron una serie de factores generadores de riesgo, para poder definir la clasificación de riesgos, su interrelación es la siguiente:



Figura 12 Relación ente factores de riesgo y clasificación del riesgo




8. PASO 3: VALORACIÓN DEL RIESGO



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



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 46 de 116

8.1 Análisis De Riesgos: En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

8.1.1 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 de 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. 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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 47 de 116

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 anterior 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.

8.1.2 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 diferentes niveles se debe tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 48 de 116

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 siguiente tabla se establecen los criterios para definir el nivel de impacto.

Tabla de 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 yDesempeño Institucional de Función Pública, 2020.

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 ejecuta la actividad, cadena de valor del proceso, factores generadores y para la definición de los controles.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 49 de 116

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**.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 50 de 116

	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.

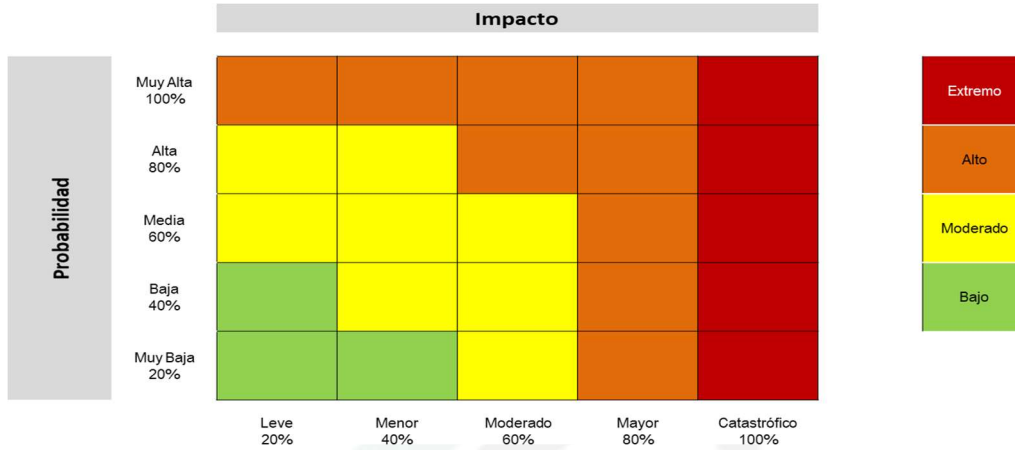
Probabilidad inherente= media 60%, **Impacto inherente:** mayor 80%

Evaluación de riesgos: a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto s, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

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 en la siguiente página).



Figura de Matriz de calor (Niveles de severidad del riesgo)



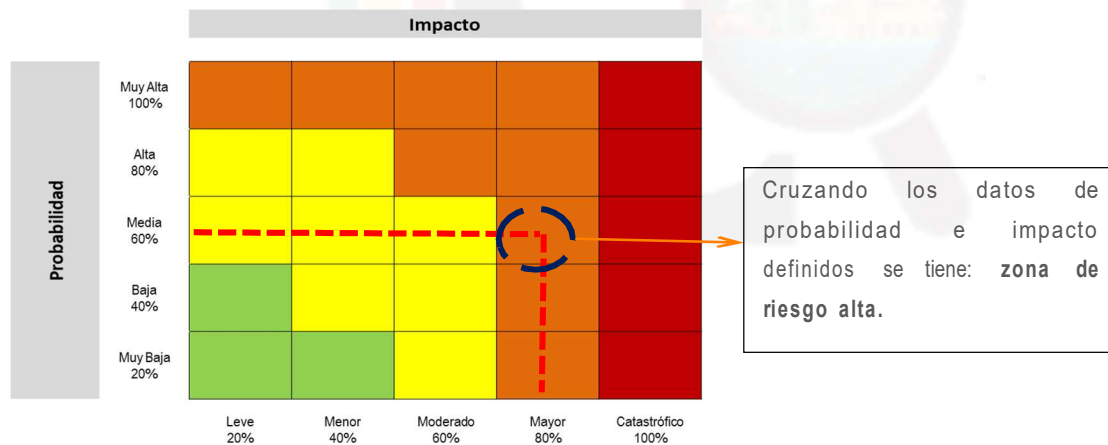
Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública

Conclusiones de ejemplo:


Probabilidad Inherente= moderada 60%

Impacto Inherente: mayor 80%

Aplicando la matriz de calor tenemos:





	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 52 de 116

8.2 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.

8.2.1 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:

8.2.2 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.

8.2.3 Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.

8.2.4 Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.




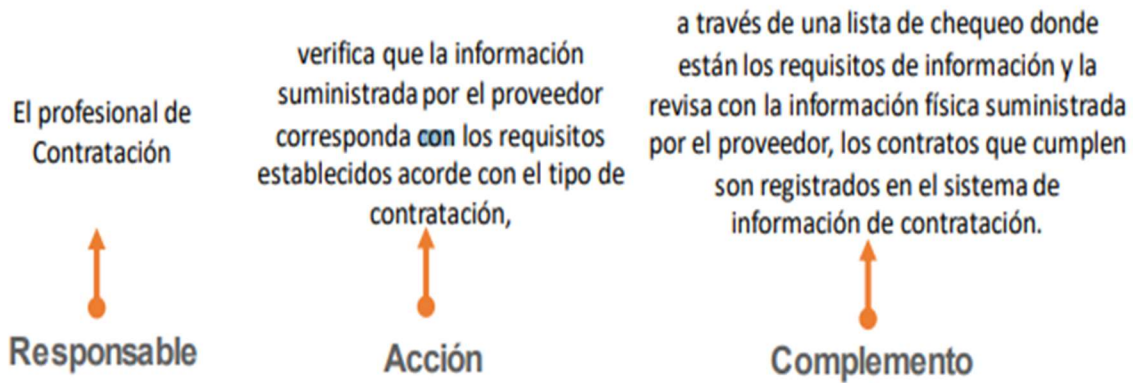
	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 53 de 116

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.

8.2.5 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 siguiente se consideran 3 fases globales del ciclo de un proceso así:




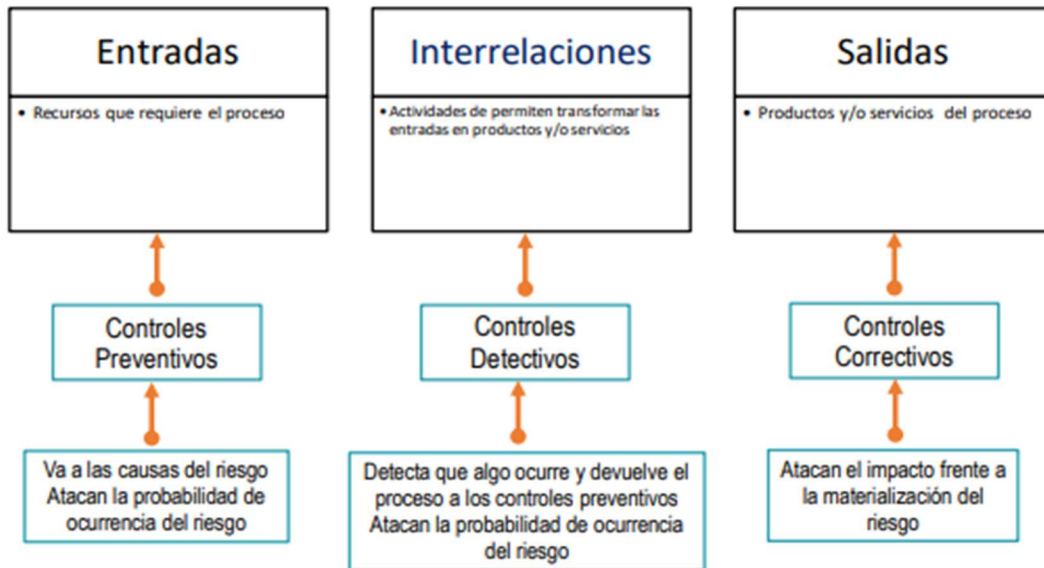
	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 54 de 116

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.

De acuerdo con lo anterior, tenemos las siguientes tipologías de controles:

8.2.6 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.

8.2.7 Control Detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

8.2.8 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.




	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 55 de 116

Tabla de 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
*Atributos Informativos	Documentación	Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
		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.	-



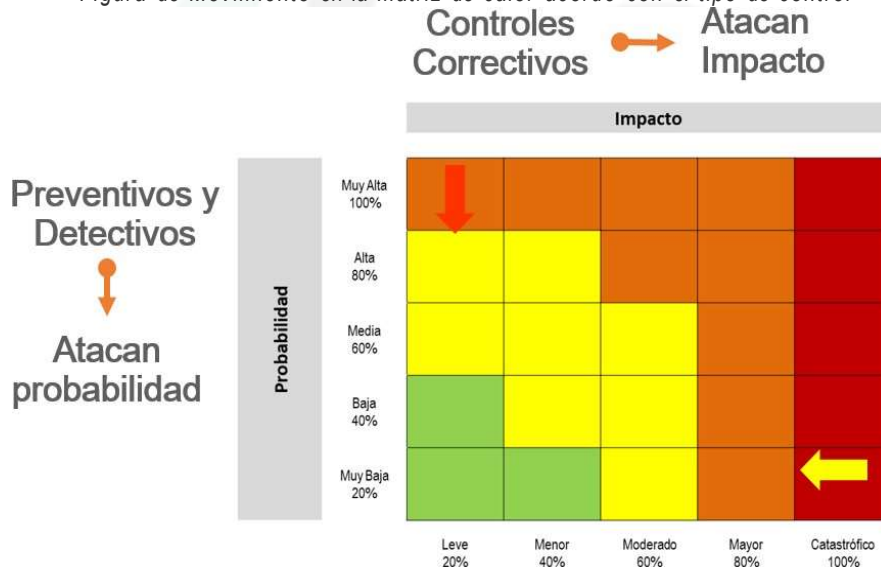
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

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 de 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

Ejemplo (continuación):

Proceso: gestión de recursos



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 57 de 116

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.

Controles y sus características			Peso	
<p style="text-align: center;">Control 1</p> <p>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 y la revisión con la información física suministrada por el</p>	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin documentar		-
	Frecuencia	Continua	X	-
Aleatoria			-	



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 58 de 116

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

8.3 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.




	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 59 de 116

Tabla de 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%			

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%

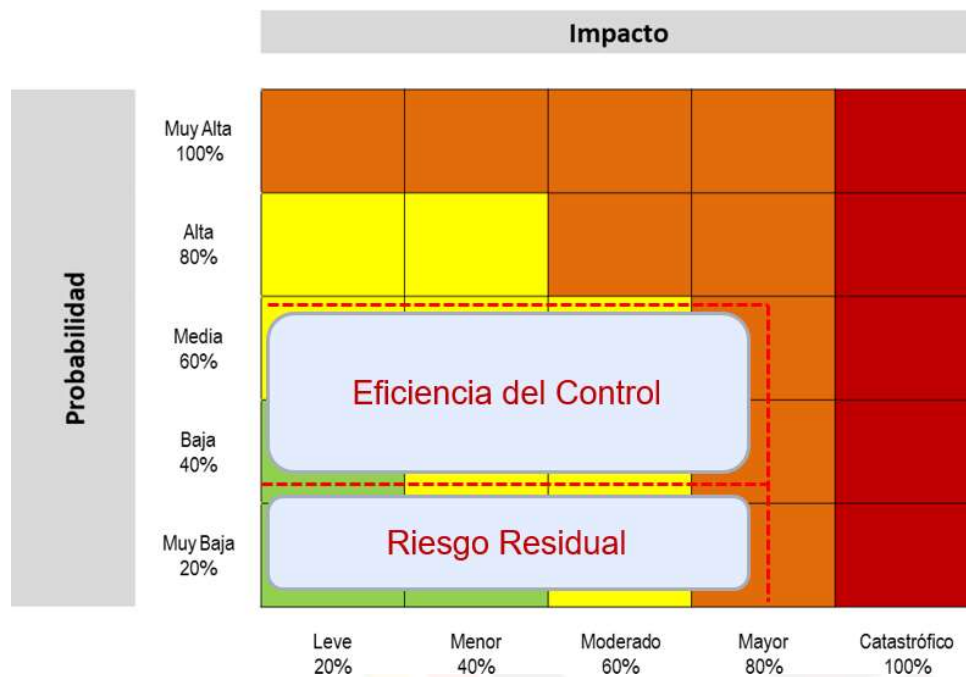
Zona de riesgo residual: alta

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



En la siguiente figura se observa el movimiento en la matriz de calor.

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



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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 61 de 116


Formato mapa de riesgos

Parte 1 identificación del riesgo:

Tabla de Ejemplo mapa de riesgos acorde con el ejemplo propuesto

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 adquisiciones) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas										
*Referen	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
<p>*Nota: La columna referencia se sugiere para mantener el consecutivo de riesgos, así el riesgo salga del mapa no existirá otro riesgo o 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.</p>											




	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 62 de 116

Parte 2 Valoración del riesgo:

No. control	Descripción del control	Afectación			Atributos				Probabilidad residual I/2	Probabilidad residual final	%	Impacto residual final	%	Zona de riesgo final	Tratamiento
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación	Frecuencia							
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%	25,2%	Mayor	80%	Alta	Reducir



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 63 de 116


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.

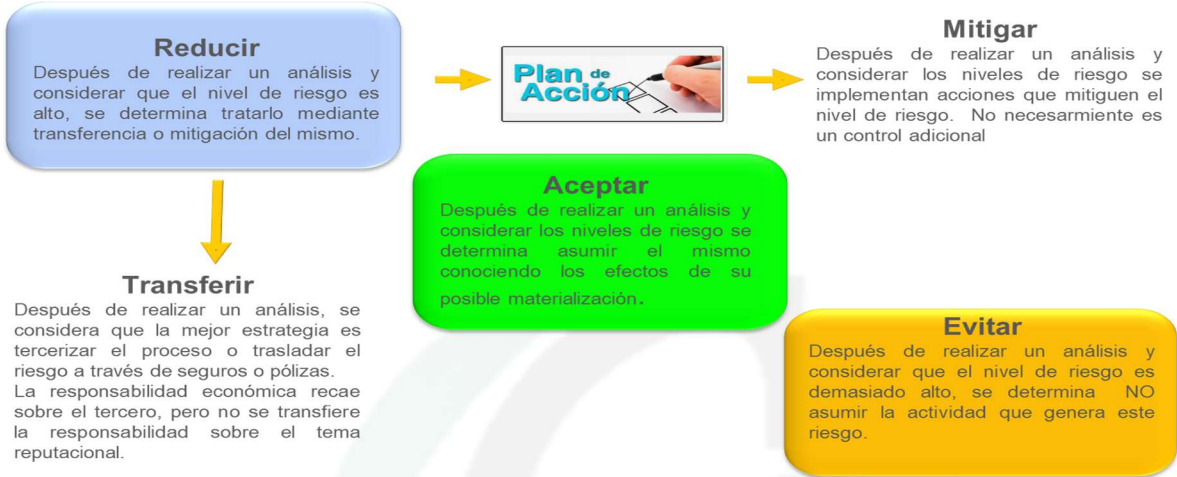
8.4 Estrategias Para Combatir El Riesgo: Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 64 de 116

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

Figura de Estrategias para combatir el riesgo



Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos.


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 Negocio ⁷ y se consideraría un control correctivo.

8.5 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:

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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 65 de 116

8.5.1 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 PQRDSF (peticiones, quejas, reclamos, denuncias, sugerencias y felicitaciones)
- 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)

8.5.2 Indicadores Clave De Riesgo: Hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar.

Un indicador clave de riesgo, o KRI, por su sigla en inglés (Key Risk Indicators), permite capturar la ocurrencia de un incidente que se asocia a un riesgo identificado previamente y que es considerado alto, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos. En la tabla 9 se muestran algunos ejemplos de estos indicadores.





	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 66 de 116

Tabla de 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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 67 de 116

8.6 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 componentes se despliega de la siguiente forma:

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.


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.

8.6.1 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.

8.6.2 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.

8.6.3 Actividades De Monitoreo : su propósito es desarrollar las actividades de supervisión continua (controles permanentes) en el día a día de las actividades, así como



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 68 de 116

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,



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 69 de 116

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:

Pertener 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 aseguramiento, 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



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 70 de 116

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.




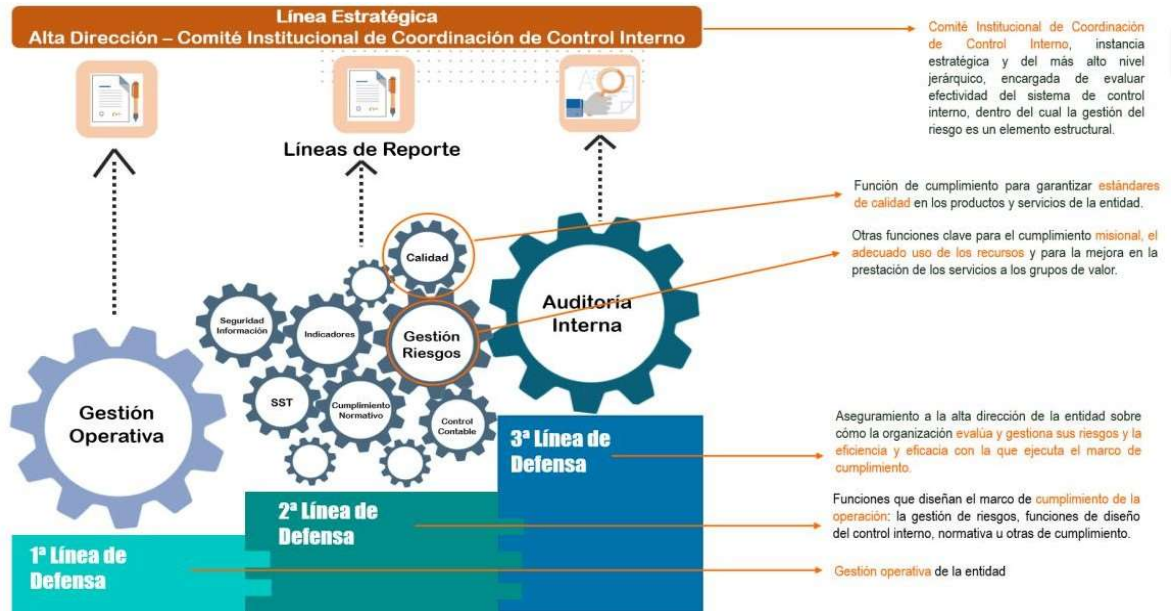
	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 71 de 116

Figura de Operatividad Esquema de líneas de defensa



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


A continuación, 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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 72 de 116

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.

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.




	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 73 de 116

9. Lineamientos Para El Análisis De Riesgo Fiscal

9.1 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.

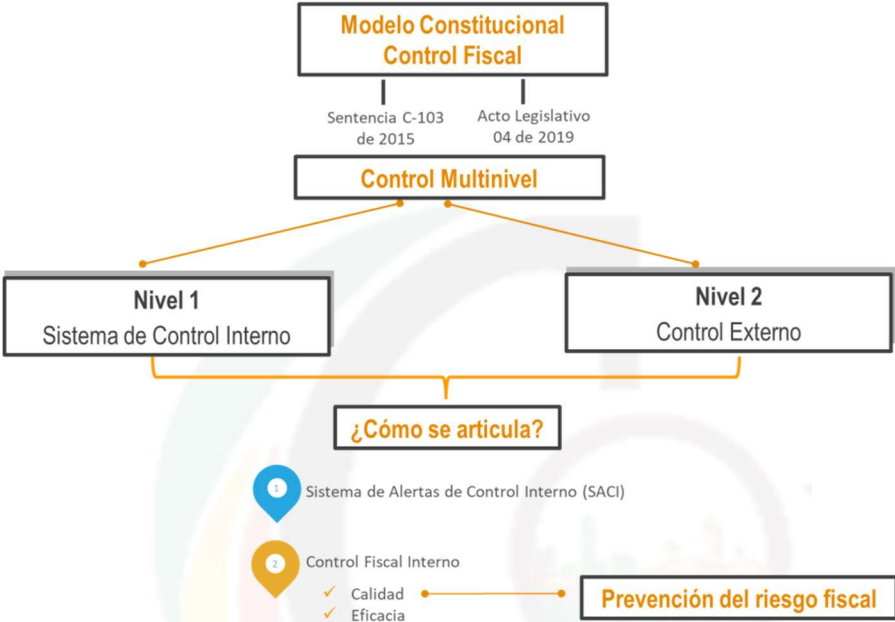
9.2 Control Fiscal Interno (CFI): Primer nivel para la vigilancia fiscal de los recursos públicos y para la prevención de riesgos fiscales y defensa del patrimonio público. El Control Fiscal Interno, hace parte del Sistema de Control Interno y es responsabilidad de todos los servidores públicos y de 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,



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 74 de 116

estructuradores y responsables de la planeación contractual, supervisores, responsables de labor es de cobro, entre otros), a través de la prevención de responsabilidades.

Figura de 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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 75 de 116

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.

9.3 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:

9.3.1 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.

9.3.2 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 este Manual, el evento potencial es equivalente a la causa raíz.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 76 de 116

Lo anterior se puede resumir de la siguiente manera:

<p>Riesgo Fiscal = Evento Potencial (Potencial Conducta)</p> <p>+</p> <p>Efecto dañoso</p>

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.

9.4 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).


9.4.1 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 rentas 9.

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



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 77 de 116

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:







	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 78 de 116

Tabla de 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><i>Nota 1:</i> Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años. <i>Nota 2:</i> 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><i>Nota 3:</i> 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 dañosos sobre los recursos, bienes o intereses patrimoniales del Estado. <i>Nota 4:</i> 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>



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 79 de 116

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	¿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?

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

9.4.2 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).



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 80 de 116

9.4.3 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 pago oportuno del canon de arrendamiento.

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



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 81 de 116

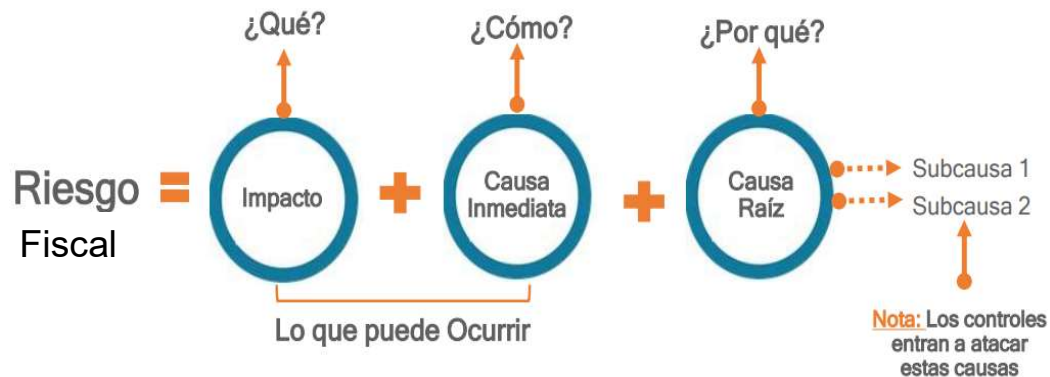
9.4.4 Descripción del Riesgo Fiscal

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 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 genera.

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





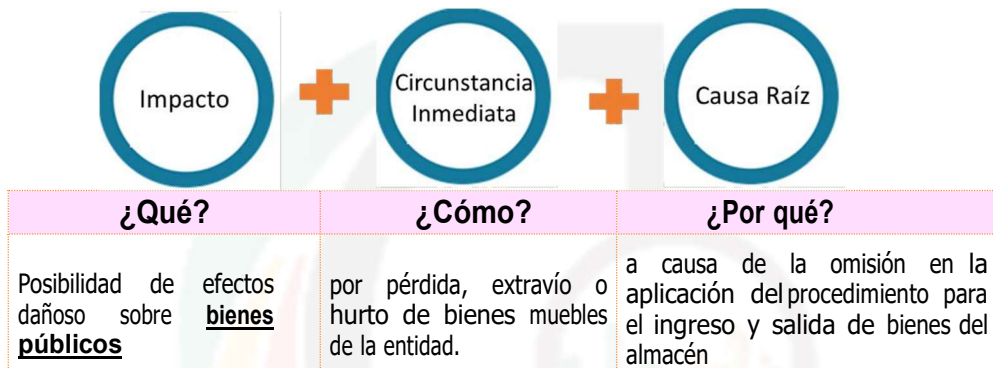
	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 82 de 116

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




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 de Ejemplos adicionales acorde con el objeto sobre el que recae el efecto dañoso

Bienes Públicos	Recursos públicos	Intereses patrimoniales denaturaleza 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 denaturaleza 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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 83 de 116

Bienes Públicos	Recursos públicos	Intereses patrimoniales denaturaleza 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 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 denaturaleza 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:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que con lleva 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%



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 84 de 116

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:

	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

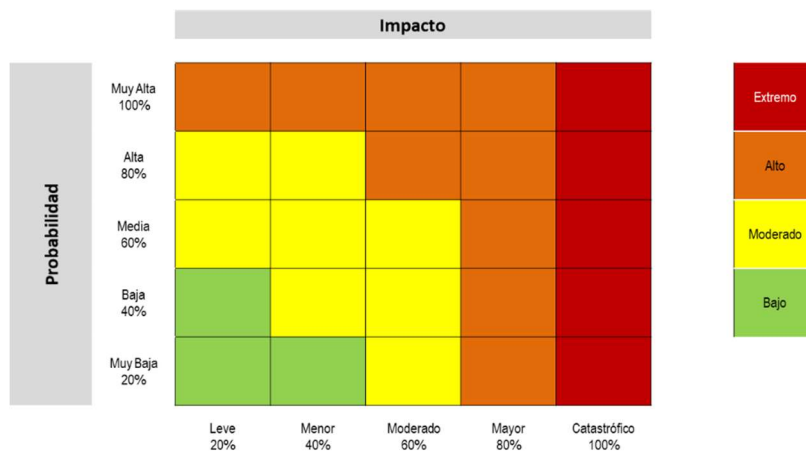
Nota: Es necesario mencionar, que los niveles en la afectación económica pueden variar según el tamaño y complejidad de los procesos de la entidad, así como sus necesidades, por lo que los rangos en cada nivel pueden ser adaptados a las necesidades y complejidad de cada entidad.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 85 de 116

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 siguiente matriz:



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),




	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 86 de 116

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 varían 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 moderada.

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, como se observa en la siguiente tabla:



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

	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 500 SMLMV, el impacto del riesgo es catastrófico.

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 extremo.**



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 88 de 116

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.

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: Extremo



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 89 de 116





	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 90 de 116

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		15%
		Manual	X	
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		15%
		Detectivo	x	
		Correctivo		
	Implementación	Automático		15%
		Manual	x	
Total, Valoración Control 2 = 30%				



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 91 de 116





	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 92 de 116

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.

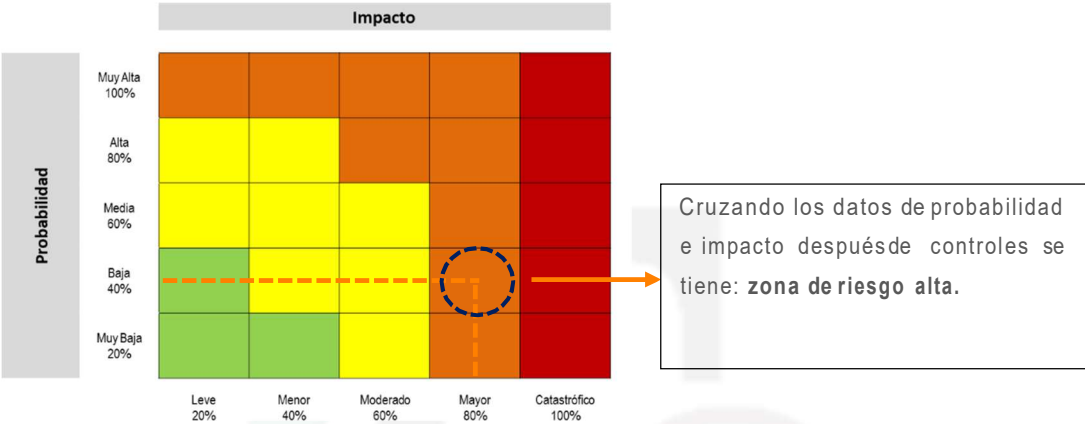
Para mayor claridad a continuación, siguiendo con el ejemplo propuesto, se observan los cálculos requeridos para la aplicación de los tres controles definidos así:

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
P osibilidad 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 C ausa 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 hayalugar (<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%			



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 93 de 116

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:



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:



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 94 de 116

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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 95 de 116

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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 96 de 116

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	[Redacted]

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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 97 de 116

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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 98 de 116

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



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 99 de 116

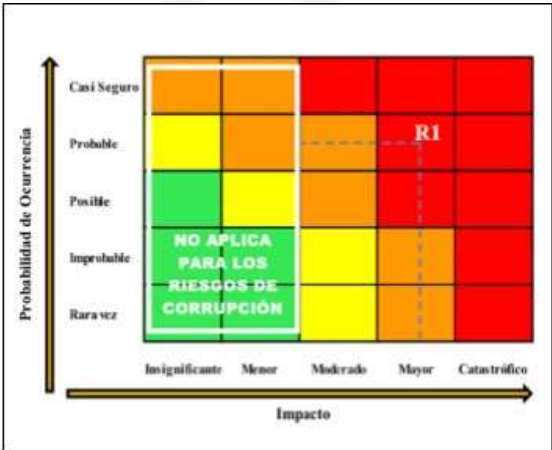
IMPORTANTE
 Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico.
 Por cada riesgo de corrupción identificado, se debe diligenciar una tabla de estas.

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.


Extremo	
Alto	
Moderado	
Bajo	

IMPORTANTE
 Aunque se utilice el mismo mapa de calor, para los riesgos de gestión y de corrupción, a estos últimos solo les aplican las columnas de impacto Moderado, Mayor y Catastrófico.



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



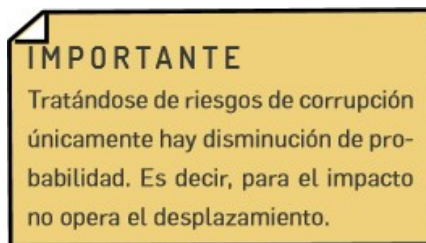
	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 100 de 116

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:



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 101 de 116



Fuente: DAFP

ACEPTAR EL RIESGO

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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 102 de 116

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.

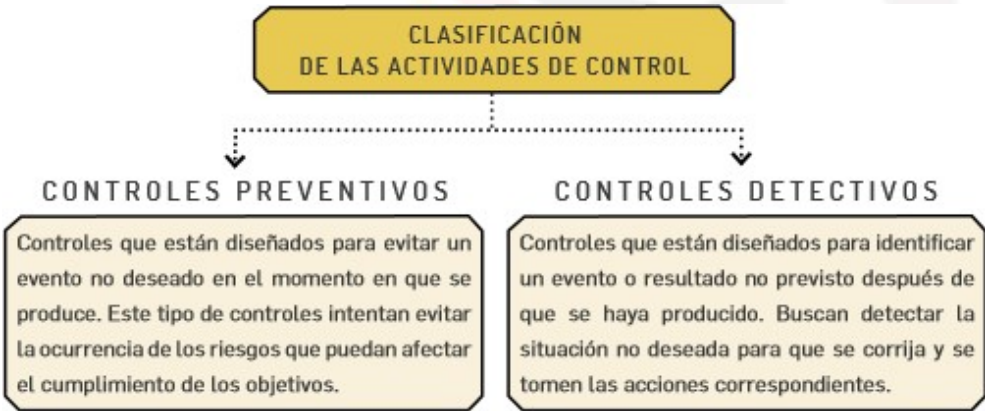
REDUCIR EL RIESGO

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.





	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 103 de 116

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

GESTIÓN 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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 104 de 116

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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 105 de 116

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), 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.

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?
<p>Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como:</p> <ul style="list-style-type: none"> -Aplicaciones de la organización 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 	<p>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).</p> <p>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.</p>

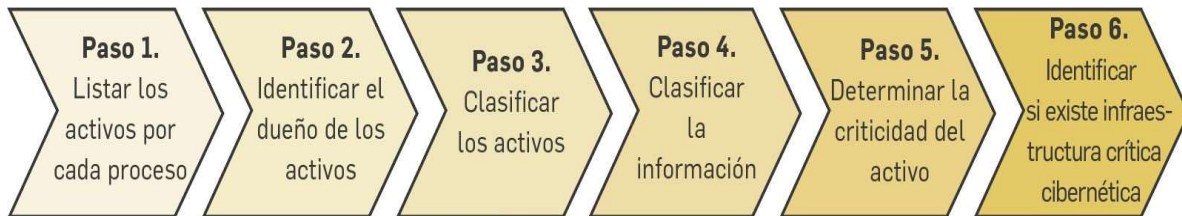
Fuente: Actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública y Ministerio TIC, 2020



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 106 de 116

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 su completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Gestión financiera	Base de datos de nómina	Base de datos con información denómina 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 front office 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

Identificación del riesgo: se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 107 de 116

- 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
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

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





	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 108 de 116

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



RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/VULNERABILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina.	Modificación no autorizada	Seguridad digital	Falta de políticas de seguridad digital Ausencia de políticas de control de acceso Contraseñas sin protección Autenticación débil	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo (legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 109 de 116

IMPORTANTE


- * Existirían 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.

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:

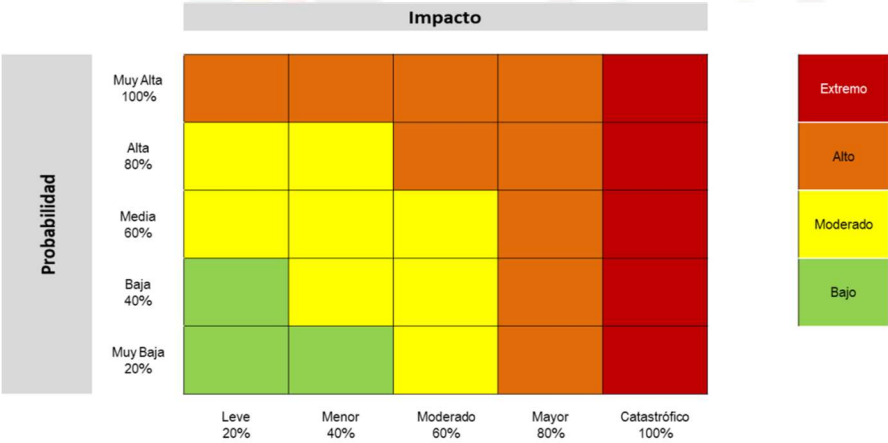


	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 110 de 116

La determinación del impacto se debe llevar a cabo de acuerdo con lo establecido en el aparte 3.1.2 del presente Manual, 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 <i>v/o de proveedores.</i>
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 del presente Manual, 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.




	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 111 de 116

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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 112 de 116

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.

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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 113 de 116

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.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 114 de 116


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.




	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 115 de 116

Conclusiones:

El presente Manual fue diseñado con el propósito de ser utilizados por las áreas y/o procesos de la CDC como una herramienta de gestión, que permita identificar los eventos potenciales que puedan impedir el logro de los objetivos operativos, tácticos y estratégicos; diseñar los controles para mitigar la materialización de estos posibles eventos negativos, perfilar y transmitir las estrategias organizacionales para el mejoramiento continuo de las áreas y/o procesos de la entidad; para un efectivo control y vigilancia fiscal en el Distrito de Cartagena de Indias.



	MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES	Código: P02-M01
		Fecha: 30/04/2024
		Versión: 1.0
		Página: 116 de 116

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>