

 IDERMETA	DIRECCIÓN GENERAL		
	RESOLUCIONES		
Versión: 001	Emisión y vigencia: 22-10-2018	Código: FORM-055	Página 1 de 4

RESOLUCIÓN No. 059
(18 de Mayo de 2021)

**“POR MEDIO DE LA CUAL SE ACTUALIZA LA POLÍTICA DE ADMINISTRACIÓN
DE RIESGOS EN EL INSTITUTO DE DEPORTE Y RECREACIÓN DEL META -
IDERMETA”**

**EL DIRECTOR GENERAL DEL INSTITUTO DE DEPORTES Y RECREACIÓN DEL
META**, en ejercicio de las facultades que le confiere los artículos 13 y 28 del Decreto
Ley 785 del 2005, los estatutos de la entidad y,

CONSIDERANDO:

La Constitución Política de 1991 en sus artículos 209 y 269, preceptuó la obligación para las Autoridades Administrativas de coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado, contando en todos sus órdenes con un Control Interno que se ejercerá en los términos que señale la Ley, diseñando y aplicando según su naturaleza métodos y procedimientos de control interno.

El artículo 6 de la Ley 87 de 1993, dispuso que el establecimiento y desarrollo del Sistema de Control Interno en los organismos y entidades públicas, será responsabilidad del representante legal o máximo directivo correspondiente. No obstante, la aplicación de los métodos y procedimientos al igual que la calidad, eficiencia y eficacia del Control Interno, también será responsabilidad de los jefes de cada una de las distintas dependencias de las entidades y organismos.

El literal f del Artículo 2 de la Ley 87 de 1993, establece como uno de los objetivos del Sistema de Control Interno 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 73 de la Ley 1474 de 2011 determinó que "Cada entidad del orden nacional, departamental y municipal deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano. Dicha estrategia contemplará, entre otras cosas, el mapa de riesgos de corrupción en la respectiva entidad, las medidas

 IDERMETA	DIRECCIÓN GENERAL		
	RESOLUCIONES		
Versión: 001	Emisión y vigencia: 22-10-2018	Código: FORM-055	Página 2 de 4

concretas para mitigar esos riesgos, las estrategias antitrámites y los mecanismos para mejorar la atención al ciudadano." Igualmente, determinó en el parágrafo de este artículo que en aquellas entidades donde se tenga implementado un sistema integral de administración de riesgos, se podrá validar la metodología de este sistema con la definida por el Programa Presidencial de Modernización, Eficiencia, Transparencia y Lucha contra la Corrupción.

El Decreto 1499 de 2017, por el cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

El Modelo MIPG, establece dentro de la Dimensión 2. Direccionamiento Estratégico y Planeación, como uno de sus elementos, la definición de la Política de Administración de Riesgos y la identificación y la valoración de los riesgos.

La Guía para la administración del Riesgo y el diseño de controles en las entidades públicas (Riesgos de Gestión, Riesgos de Corrupción y Riesgos de Seguridad de la información). Versión 5, emitida por el Departamento Administrativo de la Función Pública, establece la Política de Administración de Riesgos la implementación de la gestión del riesgo, es necesario que cada entidad haga un análisis de las estrategias, la formulación de objetivos y la implementación de esos objetivos en la toma de decisiones cotidiana, lo que permitirá una identificación del riesgo adecuada a las necesidades de cada organización, con un enfoque preventivo que permita la protección de los recursos, alcanzar mejores resultados y mejorar la prestación de servicios a sus usuarios aspectos fundamentales frente a la generación de valor público, eje fundamental en el quehacer de todas las organizaciones públicas.

El MIPG establece que la línea estratégica es propia del nivel directivo y se debe hacer desde el ejercicio de "Direccionamiento estratégico y de planeación", se deben emitir los lineamientos precisos para el tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales.

El día 27 de abril de 2021, en su acta N° 2, el Comité Institucional Coordinador de Control Interno, revisó y aprobó la política de administración de riesgos previamente revisados en mesas de trabajo con el direccionamiento del sistema integrado de gestión y en coordinación con los líderes de los procesos del Instituto. 

En mérito de lo anteriormente expuesto,

 IDERMETA	DIRECCIÓN GENERAL		
	RESOLUCIONES		
Versión: 001	Emisión y vigencia: 22-10-2018	Código: FORM-055	Página 3 de 4

RESUELVE:

ARTÍCULO PRIMERO: ADOPCIÓN. Adoptar la actualización de la Política de Administración de Riegos en el Instituto de Deporte y Recreación del Meta - IDERMETA, la cual se encuentra anexa al presente acto administrativo.

ARTÍCULO SEGUNDO: POLÍTICA ADMINISTRACIÓN DE RIESGOS. El Instituto de Deporte y Recreación del Meta - IDERMETA se compromete a administrar de forma eficiente, eficaz y efectiva los riesgos de gestión, corrupción y de seguridad digital identificados en los diferentes políticas, planes, programas, proyectos, procesos y puntos de control de la entidad, de manera que se determinen y ejecuten acciones correctivas, defectivas, preventivas o de mejora de forma oportuna para evitar la materialización de los riesgos, y actuar de forma inmediata ante las situaciones presentadas, con el fin de mitigar el impacto o posibles consecuencias sobre los resultados de la gestión institucional, en cumplimiento de la metodología establecida y la normatividad vigente.

El Modelo Integrado de Planeación y Gestión, y el Modelo Estándar de Control Interno, le corresponde monitorear y controlar los riesgos que puedan impedir el cumplimiento de las metas y objetivos organizacionales, de conformidad a la metodología establecida en las guías expedidas por el Departamento Administrativo de la Función Pública “Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano – Versión 2”, “Guía para la Gestión del Riesgo de Corrupción”, “Guía de Administración del Riesgo”, “Guía para la administración del riesgo y el diseño de controles en entidades públicas V5 2020 “ del DAFP, la Norma NTC ISO 31000:2011. Gestión del Riesgo.

ARTÍCULO TERCERO: METODOLOGÍA. Adóptese la metodología anexa “Mapa de riesgos” documento en formato Excel establecida por el instituto para la identificación, tratamiento, monitoreo y seguimiento de los riesgos, según los lineamientos definidos en la política de administración de riesgos del Instituto, Anexa al presente acto administrativo.

PARÁGRAFO. Las actualizaciones a la metodología anexa se realizarán de acuerdo al procedimiento de control de documentos implementado por el instituto y tendrá vigencia conforme al listado maestro de documentos.

ARTÍCULO CUARTO: OBLIGATORIEDAD. La política de administración de riegos del Instituto es de aplicación obligatoria por todos los niveles de autoridad, servidores públicos y demás personal vinculado a la entidad.

 IDERMETA	DIRECCIÓN GENERAL		
	RESOLUCIONES		
Versión: 001	Emisión y vigencia: 22-10-2018	Código: FORM-055	Página 4 de 4

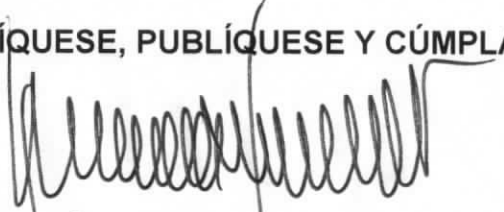
ARTÍCULO QUINTO: EVALUACIÓN. La evaluación de la eficacia de los controles establecidos para la mitigación de los Riesgos identificados, en el Mapa de Riesgos, estará bajo la responsabilidad de la Oficina Asesora de Control Interno.

ARTÍCULO SEXTO: PUBLICIDAD. El Mapa de Riesgos del Instituto, será socializado mediante los diferentes canales de información a todos los servidores públicos de Instituto, del mismo modo, será publicado en la Página Web y compartido a los correos institucionales.

ARTÍCULO SÉPTIMO: AJUSTES. La recepción de solicitudes de ajustes de los Mapas de Riesgos por Proceso y de Corrupción por parte de los líderes de proceso, sobre la modificación de actividades, fechas, responsables u otros será tramitada por la Oficina Asesora de Planeación y aprobada por el Comité Institucional de Gestión y Desempeño.

ARTÍCULO OCTAVO: La presente Resolución rige a partir de su expedición y deroga todas las disposiciones que le sean contrarias.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE


FABIÁN HERNÁN GONZALO TORRES CARRILLO
 Director General

NOMBRE Y APELLIDOS	CARGO	FIRMA
Revisó: Martha Bibiana Pan Merchán	Jefe Oficina Asesora de Planeación	
Revisó: Johan Mauricio García Guzmán	Contratista	
Elaboró: Gladys Ramírez Peña	Contratista	

CONTENIDO

	Pág.
1 POLÍTICA DE ADMINISTRACIÓN DEL RIESGO	3
2 ANTECEDENTES	3
3 INTRODUCCIÓN	4
4 OBJETIVOS.....	5
5 ALCANCE.....	5
6 GLOSARIO	5
7 RESPONSABILIDADES.....	7
7.1 Operatividad Institucionalidad para la Administración del Riesgo.....	10
8 METODOLOGIA PARA LA ADMINISTRACIÓN DE RIESGOS.....	11
9 IDENTIFICACIÓN DE RIESGOS.....	11
9.1 Análisis de objetivos estratégicos y de los procesos.....	11
9.2 Identificación de los puntos de riesgo	12
9.3 Identificación de áreas de impacto	12
9.4 Identificación de áreas de factores de riesgo	12
9.5 Descripción del riesgo	13
9.6 Clasificación del riesgo.....	14
10 VALORACIÓN DEL RIESGO	15
10.1 Análisis de riesgos.....	15
10.1.1 DETERMINAR LA PROBABILIDAD	15
10.1.2 DETERMINAR EL IMPACTO	15
10.2 Evaluación de riesgos.....	16
10.2.1 ANÁLISIS PRELIMINAR (RIESGO INHERENTE)	17
10.3 Matriz de calor	17
10.3.1 VALORACIÓN DE CONTROLES	17
10.4 Estrategias para combatir el riesgo.....	21
10.5 Monitoreo y revisión	21
11 LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN.....	22
11.1 Riesgo de corrupción.....	22
11.2 Valoración de riesgos	23
11.3 Valoración de los controles.....	25
12 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	26
12.1 Identificación de los activos de seguridad de la información.....	26
12.1.1 ¿CÓMO IDENTIFICAR LOS ACTIVOS?	26
12.1.2 EJEMPLO DE IDENTIFICACIÓN DE ACTIVOS	26
12.2 Identificación del riesgo	27
12.2.1 EJEMPLO DE AMENAZAS Y VULNERABILIDADES DE ACUERDO CON EL TIPO DE ACTIVO	27
12.3 Valoración del riesgo	28
12.4 Controles asociados a la seguridad de la Información.....	28
12.5 Materialización de los riesgos.....	28
13 MONITOREO Y SEGUIMIENTO DE RIESGOS	28
13.1 Primera línea de defensa	28
13.2 Segunda línea de defensa	28

13.3	Tercera línea de defensa.....	29
14	MAPA DE RIESGOS	29
14.1	Generalidades acerca de los riesgos de corrupción.....	30

ILUSTRACIONES

	Pág.
Ilustración 1 Estructura Dimensión Control Interno	4
Ilustración 2 Nivel de responsabilidad frente al riesgo.....	7
Ilustración 3 Operatividad de la administración del riesgo.....	10
Ilustración 4 Metodología de la administración de riesgos	11
Ilustración 5 Características SMART	12
Ilustración 6 Modelo de factores de riesgo.....	13
Ilustración 7 Estructura de riesgos.....	13
Ilustración 8 Clasificación de riesgos	14
Ilustración 9 Estructura de nivel de probabilidad	15
Ilustración 10 Estructura nivel de impacto.....	15
Ilustración 11 Aplicación de nivel de probabilidad	16
Ilustración 12 Aplicación nivel de impacto.....	16
Ilustración 13 Matriz o mapa de calor	17
Ilustración 14 Matriz de calor probabilidad - impacto.....	17
Ilustración 15 Redacción de controles	18
Ilustración 16 Tipología de controles y los procesos	19
Ilustración 17 Análisis y evaluación de los controles – Atributos	19
Ilustración 18 Determinación de riesgo residual.....	20
Ilustración 19 Estrategias para combatir el riesgo.....	21
Ilustración 20 Esquema de líneas de defensa.....	22
Ilustración 21 Componentes de riesgos de corrupción.....	23
Ilustración 22 Matriz: definición del riesgo de corrupción	23
Ilustración 23 Criterios para calificar la probabilidad	24
Ilustración 24 Criterios para calificar el impacto en riesgos de corrupción.....	24
Ilustración 25 Valoración controles riesgo de corrupción	25
Ilustración 26 Activos de seguridad de la información.....	26
Ilustración 27 Pasos para identificar activos	26
Ilustración 28 Identificación de activos.....	26
Ilustración 29 Amenazas y vulnerabilidades por tipo de activo.....	27
Ilustración 30 Identificación de riesgo de activos	27
Ilustración 31 Valoración de riesgo de activos	28

1 POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

El Instituto de Deporte y Recreación del Meta - IDERMETA se compromete a administrar de forma eficiente, eficaz y efectiva los riesgos de gestión, corrupción y de seguridad digital identificados en los diferentes políticas, planes, programas, proyectos, procesos y puntos de control de la entidad, de manera que se determinen y ejecuten acciones correctivas, defectivas, preventivas o de mejora de forma oportuna para evitar la materialización de los riesgos, y actuar de forma inmediata ante las situaciones presentadas, con el fin de mitigar el impacto o posibles consecuencias sobre los resultados de la gestión institucional, en cumplimiento de la metodología establecida y la normatividad vigente.

El Modelo Integrado de Planeación y Gestión, y el Modelo Estándar de Control Interno, le corresponde monitorear y controlar los riesgos que puedan impedir el cumplimiento de las metas y objetivos organizacionales, de conformidad a la metodología establecida en las guías expedidas por el Departamento Administrativo de la Función Pública "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano – Versión 2", "Guía para la Gestión del Riesgo de Corrupción", "Guía de Administración del Riesgo", "Guía para la administración del riesgo y el diseño de controles en entidades públicas V5 2020 " del DAFP, la Norma NTC ISO 31000:2011. Gestión del Riesgo.

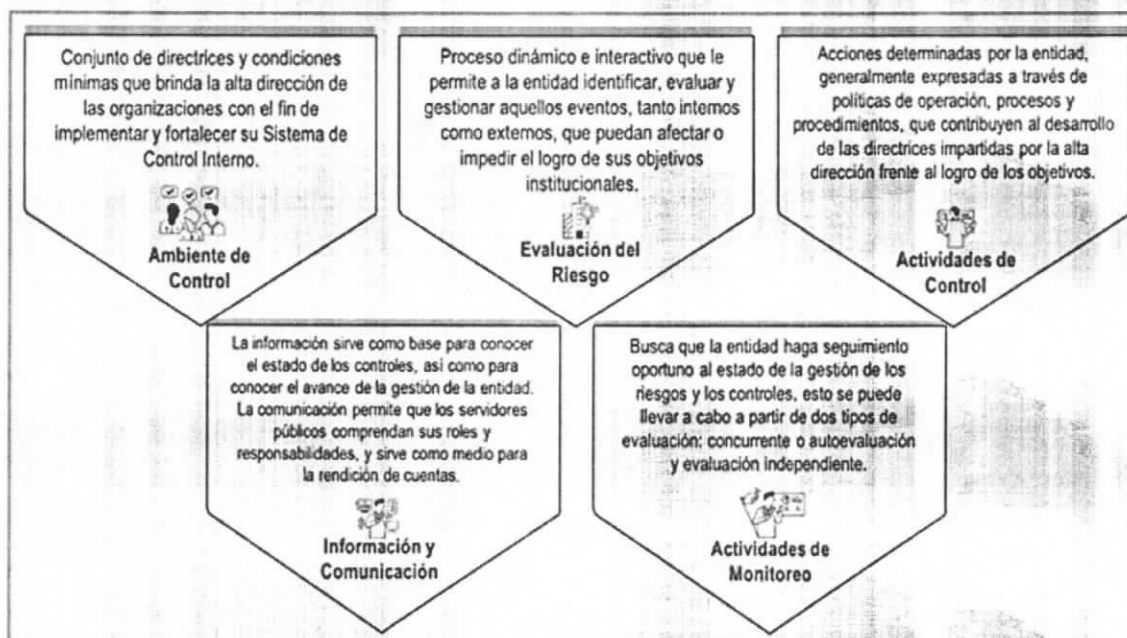
2 ANTECEDENTES

El sistema de control interno se inicia con la NTC GP 1000:2005, tiene actualización con la NTC GP 1000:2009, posteriormente el Decreto N° 943 de 2014, actualiza el Modelo Estándar de Control Interno, se produce una tercera versión del Sistema de Control Interno, manteniendo su estructura conceptual, mejorado visualmente mediante la inclusión de esquemas explicativos de los contenidos y se realiza alineación con políticas de lucha contra la corrupción.

El Decreto N° 1499 de 2017, estructura el Modelo Estándar de Control Interno en la dimensión N° siete 7, en cinco componentes:

1. Ambiente de Control
2. Evaluación del Riesgo
3. Actividades de Control
4. Información y Comunicación
5. Actividades de Monitoreo

Ilustración 1 Estructura Dimensión Control Interno



Fuente: adaptación MECI 2014 y COSO INTOSAI.

Por último, en el año 2020 después que las entidades atravesarán grandes retos y dificultades para el desarrollo de su gestión, ocasionado a la virtualidad que se hizo necesaria para el adecuado funcionamiento, debido a la contingencia generada por virus SARS-COV, se introducen cambios significativos en la administración del riesgo mediante la expedición de la guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, de diciembre de 2020, del Departamento Administrativo de la Función Pública.

3 INTRODUCCIÓN

El documento contiene la política de administración de riesgos del Instituto de Deporte y Recreación del Meta – IDERMETA, como herramienta de gestión, con el objeto de identificar y valorar los riesgos, establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos, con el objeto de garantizar y mejorar los indicadores de gestión y la evaluación del formulario único de reporte de avances de la gestión – FURAG.

La política de administración de riesgos, será adoptada, socializada e implementada a partir de su aprobación por el Comité Institucional de Coordinación de Control Interno.

El fin último del estado, es generar resultados que atiendan los planes de desarrollo y garanticen los derechos, resuelvan las necesidades y problemas de los

ciudadanos, para el caso que nos ocupa, la misionalidad del Instituto es la promoción y fomento, el desarrollo de políticas dirigidas al deporte, la recreación, la educación física, la educación extraescolar y el aprovechamiento del tiempo libre, para todos los habitantes del departamento del Meta, para el logro de esta meta, se hace necesario prever y precaver los riesgos de cualquier índole que pudieren afectar o trastocar el cumplimiento de los objetivos y metas fijadas en Plan de Acción Institucional, Plan de Desarrollo Departamental y Plan Nacional de Desarrollo.

4 OBJETIVOS

- ✓ Adoptar una metodología que permita al Instituto gestionar de manera efectiva los riesgos que puedan afectar el logro de los objetivos Estratégicos, Misionales, de Apoyo y de Evaluación según los procesos documentados.
- ✓ Identificar, analizar, evaluar los riesgos de gestión, corrupción y de seguridad y privacidad de la información, según los roles y responsabilidades de cada uno de los servidores de la entidad, de acuerdo con el esquema de las líneas de defensa.
- ✓ Definir lineamientos basados en una adecuada gestión del riesgo, para permitir a la alta dirección del Instituto para la toma de decisiones y el logro los objetivos institucionales.
- ✓ Incentivar la toma de decisiones basada en los riesgos de la entidad.
- ✓ Promover y fomentar la cultura para la gestión del riesgo en el Instituto, mediante acciones y estrategias orientadas a un manejo adecuado de los riesgos por parte de los servidores públicos del Instituto.

5 ALCANCE

La presente política de administración del riesgo inicia su adopción, socialización termina con la implementación y la creación de la cultura para la gestión del riesgo en el Instituto de Deportes y Recreación del Meta – IDERMETA.

6 GLOSARIO

- **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.
- **AMENAZAS:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización

- **APETITO DE RIESGO:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **CAPACIDAD DE RIESGO:** Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
- **CAUSA:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **CAUSA INMEDIATA:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
- **CAUSA RAÍZ:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
- **CICCI:** Comité Institucional de Coordinación de Control Interno
- **CIGD:** Comité Institucional de Gestión y Desempeño.
- **CONFIDENCIALIDAD:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados
- **CONSECUENCIA:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **CONTINGENCIA:** Posible evento futuro, condición o eventualidad.
- **CONTINUIDAD:** Capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.
- **CONTROL:** Medida que permite reducir o mitigar un riesgo.
- **CRISIS (EMERGENCIA):** Ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.
- **DISPONIBILIDAD:** Propiedad de ser accesible y utilizable a demanda por una entidad, evento y sus consecuencias. (ISO/IEC 27000).
- **FACTORES DE RIESGO:** Son las fuentes generadoras de riesgos.
- **GUÍA:** Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - diciembre de 2020.
- **IMPACTO:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **INTEGRIDAD:** Propiedad de exactitud y completitud.
- **MAPA DE RIESGOS:** Documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.
- **MECI:** Modelo Estándar de Control Interno
- **MIPG:** Modelo Integrado de Planeación y Gestión
- **NIVEL DE RIESGO:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

- **PLAN ANTICORRUPCIÓN Y DE ATENCIÓN AL CIUDADANO:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **PROBABILIDAD:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **RESTABLECIMIENTO:** Capacidad de la Entidad para lograr una recuperación y mejora, cuando corresponda, de las operaciones, instalaciones o condiciones de vida una vez se supera la crisis.
- **RIESGO:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales¹.
- **RIESGO DE CORRUPCIÓN:** Posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **RIESGO DE 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
- **RIESGO INHERENTE:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad
- **RIESGO RESIDUAL:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **SGI:** Sistema Gestión Institucional
- **TIC:** Tecnologías de la Información y las Comunicaciones
- **TOLERANCIA DEL RIESGO:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.
- **VULNERABILIDAD:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

7 RESPONSABILIDADES

La responsabilidad está definida mediante las líneas de defensa y en la entidad se acogen según la siguiente tabla:

Ilustración 2 Nivel de responsabilidad frente al riesgo

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Línea Estratégica	➤ Director General ➤ Concejo Directivo	• Definir y aprobar el marco general para la administración del riesgo. • Analizar los riesgos, vulnerabilidades, amenazas y escenarios que afectan o

¹ 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.

	➤ Comité Institucional de Gestión y Desempeño ➤ Comité Institucional de Control Interno	puedan afectar la gestión de la entidad en los planes, programas, proyectos, dependencias y procesos y que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios. • Definir y aprobar la política para la administración del riesgo • Garantizar el cumplimiento de los planes de la entidad
Primera Línea	Líderes de Proceso Subdirectores – Jefe de Oficina Asesora de Planeación	• Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso. • Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • Revisar de acuerdo con su competencia y alcance la documentación de continuidad de negocio • Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados y los planes de preparación frente a la pérdida de continuidad de negocio. • Informar a la oficina de planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo. • Reportar en el SGI los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos.
Segunda Línea	Subdirectores - Jefe de Oficina Asesora de Planeación – Líderes de Proceso	• Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. • Consolidar el mapa de riesgos institucional, riesgos de mayor criticidad frente al logro de los objetivos y presentarlo para análisis y seguimiento ante el CIGD. • Actualizar la documentación que soporta la gestión del riesgo. • Presentar al CICC el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos

		identificados en las áreas en los diferentes niveles de operación de la entidad. • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. • Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos. • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. • Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean monitoreados por la primera línea de defensa. • Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. • Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos para su aprobación del CICCI. • Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada a la gestión del riesgo.
Tercera Línea	Control Interno	• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. • Asesorar a la primera línea de defensa de forma coordinada con la subgerencia, en la identificación de los riesgos y diseño de controles. • Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoría y reportar los resultados al CICCI. • Recomendar mejoras a la política de administración del riesgo.

De igual manera, la Oficina Asesora de Planeación lleva a cabo las siguientes acciones durante el acompañamiento para la identificación y administración del riesgo:

- Socializar anualmente la metodología de riesgos, los lineamientos de la primera línea de defensa frente al riesgo, objetivo del proceso, comunicación de los planes y proyectos del proceso asesorado.
- Capacitar al grupo de trabajo de cada dependencia en la herramienta SGI para la gestión del riesgo
- Liderar las mesas de trabajo de identificación del riesgo
- Liderar las mesas de trabajo para determinación del análisis de impacto del negocio, documentación de los escenarios de riesgo.
- Verificar que las acciones de control se documenten conforme a los requerimientos de la metodología
- Identificar claramente, junto con el equipo de trabajo, los responsables de las acciones y las fechas de realización, y registrarlas en el SGI
- Elaborar el mapa de riesgos de proceso con toda la información respectiva, a partir de la información construida con los equipos de trabajo
- Una vez aprobado, comunicar al líder del proceso los resultados de las mesas de identificación y recordar la importancia de socializarlos al interior de su dependencia
- Revisar que el cargue de información en el SGI esté acorde con lo aprobado
- Identificar, socializar y publicar el mapa de riesgos institucional a partir de los mapas de proceso, con los riesgos de gestión, corrupción y seguridad digital.

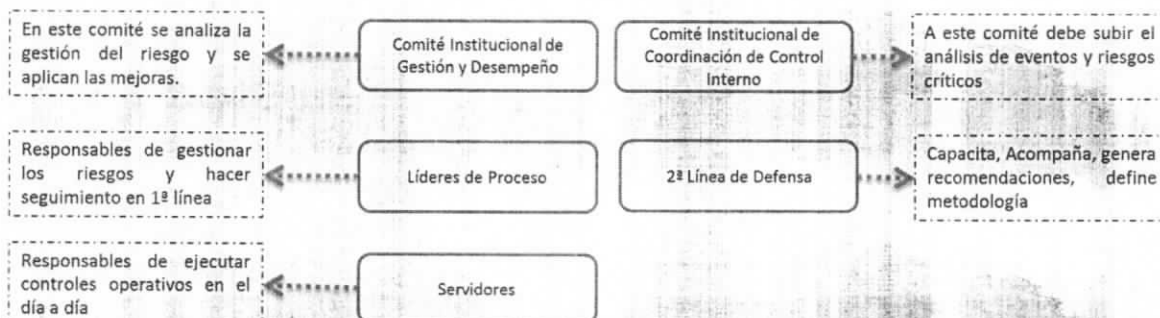
Por su parte, los líderes de proceso tienen la responsabilidad de:

- Asegurar que al interior de su grupo de trabajo se reconozca el concepto de “administración del riesgo”, la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa.
- Designar, el personal que se encargarán de la identificación, monitoreo, reporte y socialización del riesgo asociados.

Adicionalmente, la entidad construirá y socializará la matriz de responsabilidad y autoridad.

7.1 Operatividad Institucional para la Administración del Riesgo

Ilustración 3 Operatividad de la administración del riesgo



Fuente: Guía administración de riesgos V5 Función pública.

8 METODOLOGIA PARA LA ADMINISTRACIÓN DE RIESGOS

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

Ilustración 4 Metodología de la administración de riesgos



Fuente: Guía administración de riesgos V5 Función pública.

9 IDENTIFICACIÓN DE RIESGOS

Para la identificación de riesgos se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

Para dar cumplimiento a esta etapa, se requiere del desarrollo de las siguientes 6 fases:

9.1 Análisis de objetivos estratégicos y de los procesos

Los riesgos identificados en la entidad deben estar relacionados con impacto en el cumplimiento del objetivo estratégico o del proceso.

Es necesario que los objetivos estén alineados con la misión, visión y planeación estratégica de la entidad, además los objetivos estén bien definidos y se pueda continuar con la metodología de gestión de riesgos, estos deben responder al ¿Qué? ¿Cómo? ¿Para qué? ¿Cuándo? y ¿Cuánto? Asimismo, deben ser medibles, específicos, alcanzables, relevantes, con proyección en el tiempo, para lo cual puede hacer uso de las características SMART que se enuncia a continuación:

Ilustración 5 Características SMART

S	• Specific (específico): Lo importante es resolver las cuestiones como: que, cuando, como, donde, con que, quien. 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 como 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 esta haciendo es lo óptimo para llegar a la meta, asimismo permite determinar el cumplimiento y mediciones finales.

Fuente: Guía administración de riesgos V5 Función pública.

9.2 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.

9.3 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.

9.4 Identificación de áreas de factores de riesgo

Son las fuentes generadoras de riesgos. En la siguiente tabla se encuentra un listado con ejemplos de factores de riesgo que se puede tener en la entidad.

Ilustración 6 Modelo de factores de riesgo

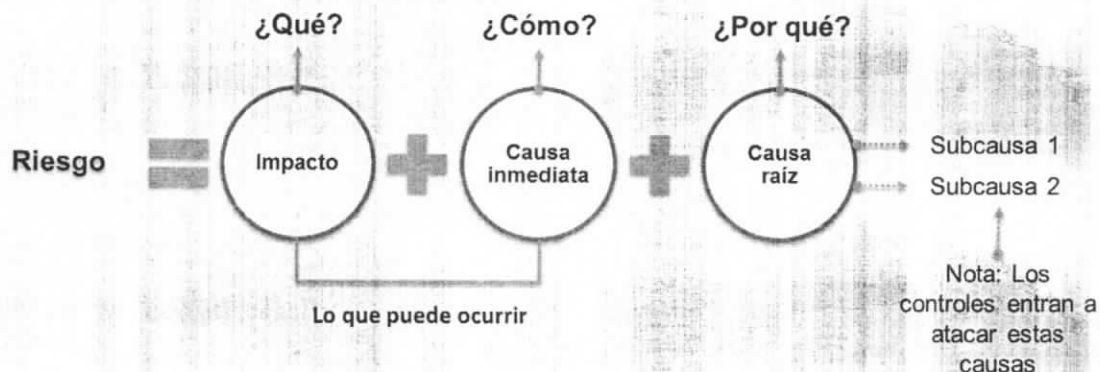
Factor	Definición	Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	Falta de procedimientos Errores de grabación, autorización Errores en cálculos para pagos internos y externos Falta de capacitación, temas relacionados con 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: Guía administración de riesgos V5 Función pública.

9.5 Descripción del riesgo

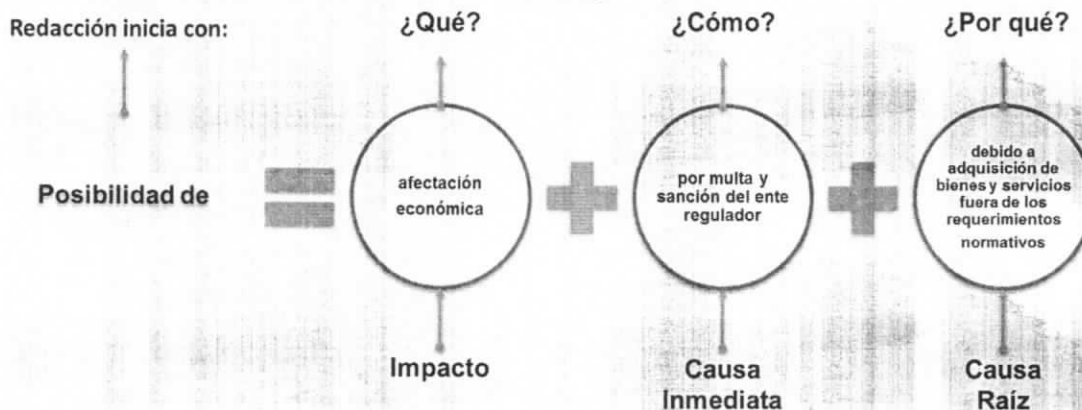
La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase posibilidad de y se analizan los siguientes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

Ilustración 7 Estructura de riesgos



causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

Ilustración 6 Modelo de redacción de riesgos



9.6 Clasificación del riesgo

Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

Ilustración 8 Clasificación de riesgos

Clasificación	Descripción
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 están involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Usuarios, productos y prácticas	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.
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.

10 VALORACIÓN DEL RIESGO

10.1 Análisis de riesgos

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

10.1.1 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.

En la siguiente tabla se establecen los criterios para definir el nivel de probabilidad.

Ilustración 9 Estructura de 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%

10.1.2 DETERMINAR EL IMPACTO

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 impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

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

Ilustración 10 Estructura nivel de impacto

	Afectación económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área del Instituto.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de Consejo Directivo y accionistas y/o de proveedores.

Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen del Instituto con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen del Instituto con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen del Instituto a nivel nacional, con efecto publicitario sostenido a nivel país

Ilustración 11 Aplicación de 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 20 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 21 a 50 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 51 veces al año y máximo 500 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 501 veces por año	100%

Ilustración 12 Aplicación nivel de impacto

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

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

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

10.2 Evaluación de riesgos

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

10.2.1 ANÁLISIS PRELIMINAR (RIESGO INHERENTE)

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor

Ilustración 13 Matriz o mapa de calor

		IMPACTO				
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%
probabilidad	Muy alta 100%					
	Alta 80%					
	Media 60%					
	Baja 40%					
	Muy baja 20%					

Extremo
Alto
Moderado
bajo

Fuente: Guía administración de riesgos V5 Función pública.

10.3 Matriz de calor

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%

Ilustración 14 Matriz de calor probabilidad - impacto

		IMPACTO				
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%
PROBABILIDAD	Muy alta 100%					
	Alta 80%					
	Media 60%					
	Baja 40%					
	Muy baja 20%					

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

10.3.1 VALORACIÓN DE CONTROLES

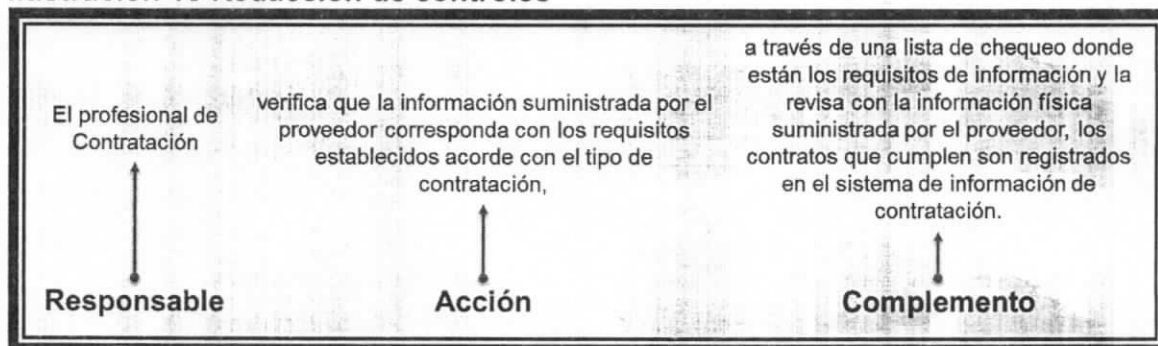
En primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- 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.

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

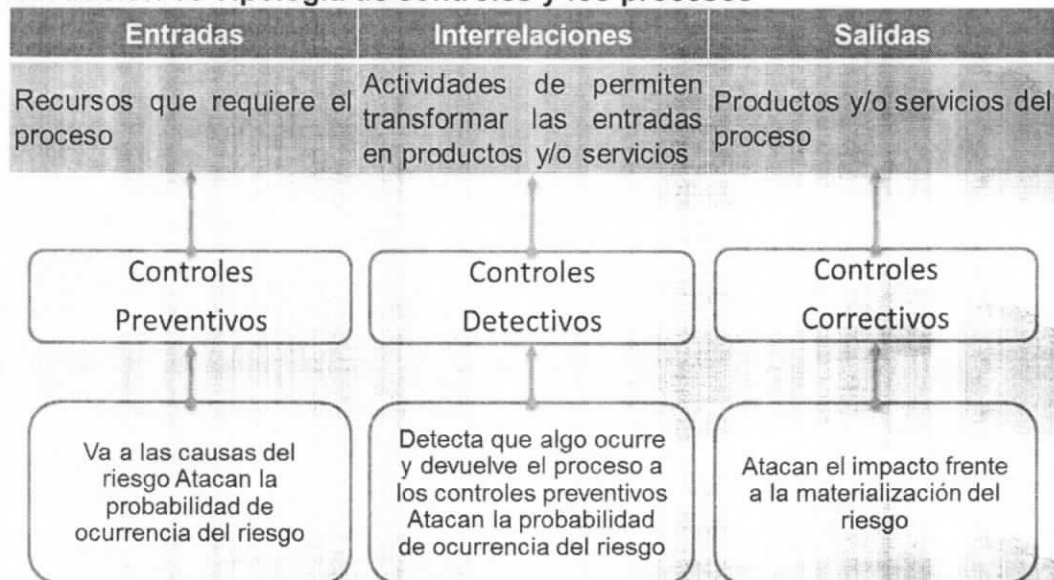
- Responsable de ejecutar el control: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.
- Complemento: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

Ilustración 15 Redacción de controles



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

Ilustración 16 Tipología de controles y los procesos



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

De acuerdo con la forma como se ejecutan:

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

Análisis y evaluación de los controles – Atributos: A continuación se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización.

Ilustración 17 Análisis y evaluación de los controles – Atributos

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	25%

Características			Descripción	Peso
*Atributos informativos			o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

*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, el movimiento se dará en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Ilustración 18 Determinación de riesgo residual

El resultado de aplicar la efectividad de los controles al riesgo inherente.

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%			

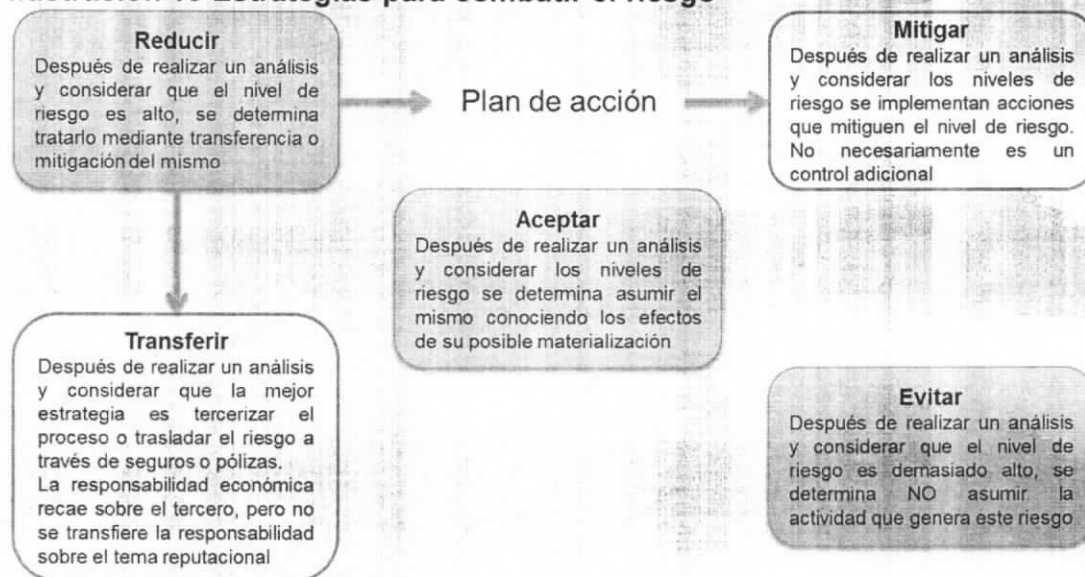
10.4 Estrategias para combatir el riesgo

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.

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.

Se define a partir de los planes de acción dentro del respectivo mapa de riesgos.

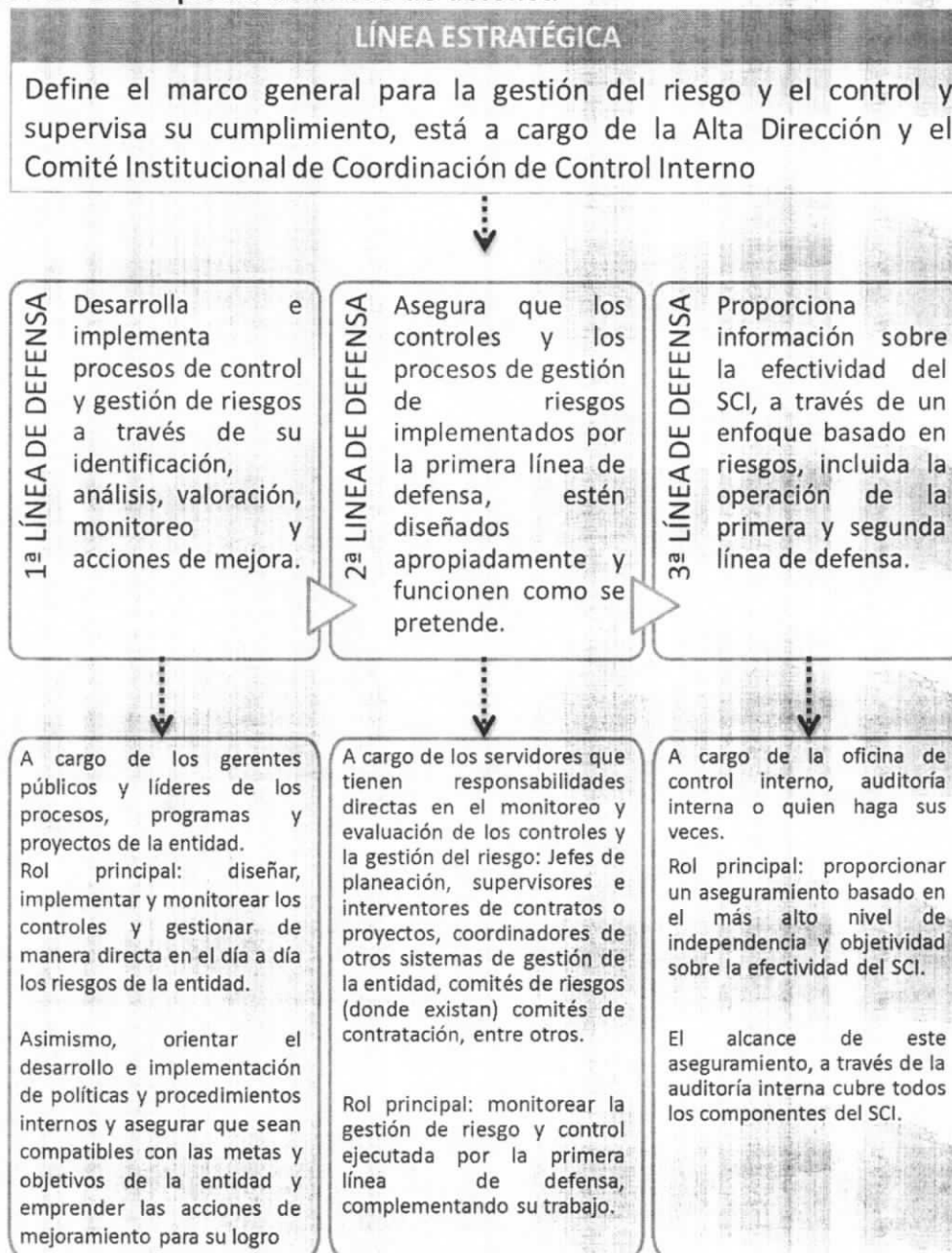
Ilustración 19 Estrategias para combatir el riesgo



10.5 Monitoreo y revisión

El Modelo Integrado de Planeación y Gestión (MIPG) desarrolla en la dimensión 7 control interno las líneas de defensa para identificar la responsabilidad de la gestión del riesgo y control que está distribuida en diversos servidores de la entidad como sigue:

Ilustración 20 Esquema de líneas de defensa



11 LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN

11.1 Riesgo de corrupción

Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

“Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos” (Conpes N° 167 de 2013).

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

Ilustración 21 Componentes de riesgos de corrupción



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:

Ilustración 22 Matriz: definición del riesgo de corrupción

Descripción del riesgo	Acción u omisión	Uso del poder	Desviación de 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

11.2 Valoración de riesgos

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.

Ilustración 23 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.

Ilustración 24 Criterios para calificar el impacto en riesgos de corrupción

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

Responder afirmativamente de SEIS A ONCE preguntas genera un impacto mayor			
Responder afirmativamente de DOCE A DIECINUEVE preguntas genera un impacto catastrófico.			
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad		
CATASTRÓFICO	Genera consecuencias desastrosas para la entidad		

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.

En este sentido se aplica la misma forma de ubicar la relación probabilidad – impacto en el mapa de calor.

11.3 Valoración de los controles

Ilustración 25 Valoración controles riesgo de corrupción

CRITERIO DE EVALUACIÓN	OPCIONES DE RESPUESTA AL CRITERIO DE EVALUACIÓN	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
1.1. Asignación de responsable	Asignado	15
	No Asignado	0
1.2. Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Prevenir	15
	Detectar	10
	No es un control	0
4. Cómo se realiza la actividad de control	Confiable	15
	No confiable	0
5. Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente	0
6. Evidencia de la ejecución del control	Completa	10
	Incompleta	5
	No existe	0

RANGO DE CALIFICACIÓN DEL DISEÑO	RESULTADO – PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
Fuerte	Calificación entre 96 y 100

Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

12 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

12.1 Identificación de los activos de seguridad de la información

Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

Ilustración 26 Activos de seguridad de la información

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: - Aplicaciones de la organización - 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	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). 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.

12.1.1 ¿CÓMO IDENTIFICAR LOS ACTIVOS?

Para lograr identificar de manera adecuada los riesgos de activos de información, se debe realizar los siguientes pasos:

Ilustración 27 Pasos para identificar activos



12.1.2 EJEMPLO DE IDENTIFICACIÓN DE ACTIVOS

Ilustración 28 Identificación de activos

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 de nómina	Jefe de oficina financiera	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA

**INSTITUTO DE DEPORTE Y RECREACIÓN DEL META****PROCESO EVALUACIÓN INDEPENDIENTE****POLÍTICA DE ADMINISTRACIÓN DE RIESGOS**

Código: PO-EVI-01

Vigencia: 27/04/2021

Versión: 1

Página 27 de 30

Gestión financiera	Aplicativo de nómina	de la entidad 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

12.2 Identificación del riesgo

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

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

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

12.2.1 EJEMPLO DE AMENAZAS Y VULNERABILIDADES DE ACUERDO CON EL TIPO DE ACTIVO**Ilustración 29 Amenazas y vulnerabilidades por 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

De esta manera se puede generar una identificación más precisa

Ilustración 30 Identificación de riesgo de activos

RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS / VULNERABILIDADES	CONSECUENCIAS
Pérdida de la integridad	Base de datos de nómina	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.

12.3 Valoración del riesgo

Para esta etapa se asociarán las tablas de probabilidad e impacto estarán definidas del mismo modo que los riesgos de gestión.

En este sentido la valoración estimada del ejemplo sería:

Ilustración 31 Valoración de riesgo de activos

RIESGO	ACTIVO	AMENAZA	CAUSAS / VULNERABILIDADES	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Perdida de la integridad	Base de datos de de	Modificación no autorizada	Falta de políticas de seguridad digital Ausencia de políticas de control de acceso Contraseñas sin protección Autenticación débil	4 Probable	4 Mayor	Extrema

12.4 Controles asociados a la seguridad de la Información

La entidad podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles que se encuentran en el anexo 4. "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", título 5 "Controles de referencia para la mitigación de riesgos de seguridad digital", siempre y cuando se ajusten al análisis de riesgos.

12.5 Materialización de los riesgos

Cuando un riesgo se materializa se debe presentar a Comité Institucional de Coordinación de Control Interno, para que el comité tome la decisión a que instancia se procede, porque un riesgo materializado no continua con tratamiento.

13 MONITOREO Y SEGUIMIENTO DE RIESGOS

13.1 Primera línea de defensa

El tratamiento o respuesta dada al riesgo, se debe realizar de forma planeada, por ello se requiere de la participación activa del personal vinculado a la entidad. Por tal motivo, los gerentes públicos y los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos y si es el caso ajustarlo.

13.2 Segunda línea de defensa

Le corresponde, igualmente, a la oficina de planeación adelantar el monitoreo, para este propósito se debe elaborar una matriz de monitoreo a riesgos. Dicho monitoreo será efectuado de forma periódica, en lo posible de forma mensual.

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.

13.3 Tercera línea de defensa

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

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

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.

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.

De acuerdo a los lineamientos para el seguimiento de riesgos de corrupción, la Oficina de Control Interno deberá realizar de forma cuatrimestral dentro de los días primeros días del mes siguiente el reporte de seguimiento a los riesgos de la entidad.

14 MAPA DE RIESGOS

A través del proceso de calidad articulará los formatos y documentos necesarios para la formulación, consolidación y seguimiento a los riesgos de gestión, corrupción y de seguridad digital identificados en los diferentes planes, programas, proyectos, dependencias y procesos de la entidad.

La metodología que aplica el Instituto es la definida en la guía de riesgos versión 5, para la construcción del mapa de riesgos y seguimiento de riesgos.

14.1 Generalidades acerca de los riesgos de corrupción

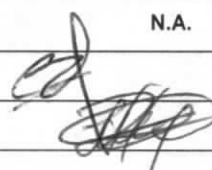
CONSTRUCCIÓN: Se elabora anualmente por cada responsable de los procesos al interior de la entidad, junto con su equipo.

AJUSTES Y MODIFICACIONES: después de su publicación y durante el respectivo año de vigencia, se podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción. 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 analicen las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción. Teniendo en cuenta la criticidad del tema y que se requiere su publicación en página web, las entidades podrán anonimizar la información relacionada con los controles establecidos que pueden tener relación con información clasificada o reservada.


FABIÁN HERNÁN GONZALO TORRES CARRILLO
 Director General

NOMBRE Y APELLIDOS	CARGO	FIRMA
Aprobó: Comité Institucional de Coordinación de Control Interno	Acta 27 de abril de 2021	N.A.
Revisó: Martha Bibiana Pan Merchán	Jefe Oficina Asesora de Planeación	
Elaboró: Johan Mauricio García Guzmán	Contratista	
Elaboró: Gladys Ramírez Peña	Contratista	