TABLA DE CONTENIDO

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

INDICE DE ECUACIONES

INTRODUCCIÓN

Esta política establece los lineamientos generales, responsabilidades y mecanismos para la administración de los riesgos que permitan controlar y responder a los riesgos potenciales o que puedan desencadenar situaciones de corrupción en concordancia con las directrices en materia de gestión pública y el enfoque del Modelo de Planeación y Gestión MIPG.

Para la formulación de la Política se contó con la participación del Equipo Técnico de Gestión y Desempeño, y el liderazgo de la Alta Dirección, y con los lineamientos establecidos por el Departamento Administrativo de la Gestión Pública –DAFP-, tales como la Guía para la Administración del Riesgo de Gestión y Corrupción y Diseño de Controles en Entidades Públicas

1. INFORMACIÓN GENERAL

La política de administración de riesgos es la 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 que afectan el logro de los objetivos institucionales.

La política de administración de riesgos debe estar alineada con la planeación estratégica y contemplar las acciones para el manejo de los riesgos identificados, la cual articula los riesgos de gestión y corrupción y la estructura del Sistema de Gestión.

1.1 Normatividad y Documentos relacionados

- Decreto 1499 de 2017: “Por medio del 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”
- Ley 1474 de 2011: Estatuto Anticorrupción Artículo73. “Plan Anticorrupción y de Atención al Ciudadano” que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti trámites y los mecanismos para mejorar la atención al ciudadano

- Guía para la Administración del Riesgo de Gestión y Corrupción y Diseño de Controles en Entidades Públicas – DAFP – Versión 4
- Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5
- ISO 31000:2009 Norma Técnica Internacional Administración del Riesgo- Principios y orientaciones.
- Decreto 377 de 2018 "Por medio del cual se adopta el Modelo Integrado de Planeación y Gestión en la administración departamental y sus entes descentralizados y se derogan unas disposiciones"
- Decreto 378 de 2018 "Por el cual se conforma el Comité y equipo técnico institucional de gestión y desempeño en la administración departamental del Quindío y se derogan unas disposiciones"
- Decreto 634 de 2018 "Por medio del cual se modifica parcialmente el Decreto No. 378 de 2018 "Por el cual se conforma el Comité y Equipo Técnico Institucional de Gestión y Desempeño en la Administración Departamental del Quindío y se derogan unas disposiciones""
- Decreto 379 de 2018 "Por el cual se conforma el Comité Departamental de Gestión y Desempeño"
- Decreto 663 de 2018 "Por el cual se modifica parcialmente el Decreto No. 379 de 2018 "Por el cual se conforma el Comité Departamental de Gestión y Desempeño""
- Resolución 310 de 28 Noviembre de 2018 "Por la cual se conforma el Comité Técnico para la Racionalización de Trámites de la Administración Departamental del Quindío"
- Decreto No. 387 del 26 de junio de 2019 "Por medio del cual se compilan los Decretos 379 de 2018 y 663 de 2018 que conforman el Comité Departamental de Gestión y Desempeño y se dictan otras disposiciones"
- Decreto No. 388 de junio 26 de 2019 "Por medio del cual se compilan los Decretos 378 de 2018 y 634 de 2018 que conforman el Comité y el Equipo Técnico Institucional de Gestión y Desempeño en la Administración Departamental del Quindío y se dictan otras disposiciones"
- Resolución No. 3100 de Noviembre 28 de 2019 "Por la cual se conforma el Comité Técnico de racionalización de trámites de la Administración Departamental del Quindío"
- Decreto Nro. 644 del 11 de diciembre de 2019, "POR MEDIO DEL CUAL SE ACTUALIZA Y REGLAMENTA EL MODELO DE OPERACIÓN POR PROCESOS DE LA ADMINISTRACION CENTRAL DEL DEPARTAMENTO DEL QUINDIO "

1.2 Términos y Definiciones

Tabla 1. Conceptos básicos relacionados con la gestión del 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.	**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	**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.
Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo	**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.	**Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.	**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.	**Control:** Medida que permite reducir o mitigar 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
Factores de Riesgo: Son las fuentes generadoras de riesgos.	**Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados	**Integridad:** Propiedad de exactitud y completitud.	**Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad
Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.	**Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware,	**Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y	**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

	información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.	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**.**	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.
Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.	**Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.	**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.	**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.

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

2. Planificación de la Gestión del Riesgo

Para la gestión de sus riesgos, la Administración Departamental cuenta con un conjunto de elementos que garantizan su adecuado manejo, dentro de los que se incluyen los siguientes:

2.1 Política de Administración del Riesgo

La Política de Administración del Riesgo del Departamento del Quindío busca orientar la toma de decisiones y minimizar los efectos adversos de la materialización del riesgo al interior de la administración departamental, para dar continuidad a la gestión institucional y preservar la eficacia operativa de la entidad, así como la salvaguarda de sus bienes y el bienestar de sus colaboradores.

Todos los procesos y dependencias deben establecer la identificación, el análisis, la valoración y el tratamiento de los riesgos que pudieran afectar la misión y el cumplimiento de los objetivos institucionales en el marco de los programas, proyectos, planes, procesos y productos mediante:

a) La identificación y documentación de riesgos de gestión y corrupción de los programas, proyectos y planes
b) El establecimiento de acciones de control para detectar y prevenir los riesgos identificados
c) La actuación correctiva y oportuna ante la materialización de los riesgos identificados
d) Capacitar y entrenar al talento humano de la Entidad para una efectiva administración del riesgo.

La entidad establece las herramientas necesarias con la participación de los servidores públicos y contratistas para promover la integridad que permita controlar y responder a los acontecimientos potenciales o aquellos en los que puedan desencadenar situaciones de corrupción

Esta Política aplica a todos los procesos de la Gobernación del Quindío, desde las actividades de identificación de los riesgos incluyendo el análisis, valoración, monitoreo y seguimiento hasta la evaluación de los mismos

Para lograr lo anteriormente enunciado la Alta Dirección asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

El Departamento del Quindío define su política de administración del riesgo tomando como referente los lineamientos de la Guía para la administración del riesgo y diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública (DAFP) – Versión 5 para los riesgos de gestión y la Guía para la Administración del Riesgo de Gestión y Corrupción y Diseño de Controles en Entidades Públicas (DAFP) – Versión 4 para los riesgos de corrupción, según lo estipulado por la Secretaría de Transparencia, en el marco de la estructura del Sistema de Gestión.

2.1.1. Objetivo

Orientar la toma de decisiones y minimizar los efectos adversos de la materialización del riesgo al interior de la administración departamental del Quindío, para dar continuidad a la

gestión institucional y preservar la eficacia operativa de la entidad, así como la salvaguarda de sus bienes y el bienestar de sus colaboradores.

2.1.2. Alcance

Esta Política aplica a todos los procesos de la Administración departamental del Quindío, desde las actividades de identificación de los Riesgos incluyendo el análisis, valoración, monitoreo, hasta la evaluación y seguimiento de los mismos

.

2.1.3. Consideraciones Básicas

- La identificación y valoración de riesgos se integra en el desarrollo de la estrategia, la formulación de los objetivos de la entidad y la implementación de esos objetivos a través de la toma de decisiones cotidiana en cada uno de los procesos. Para la identificación y análisis de los riesgos en los procesos, se debe tener en cuenta el contexto interno y externo asociado al objetivo de cada proceso.

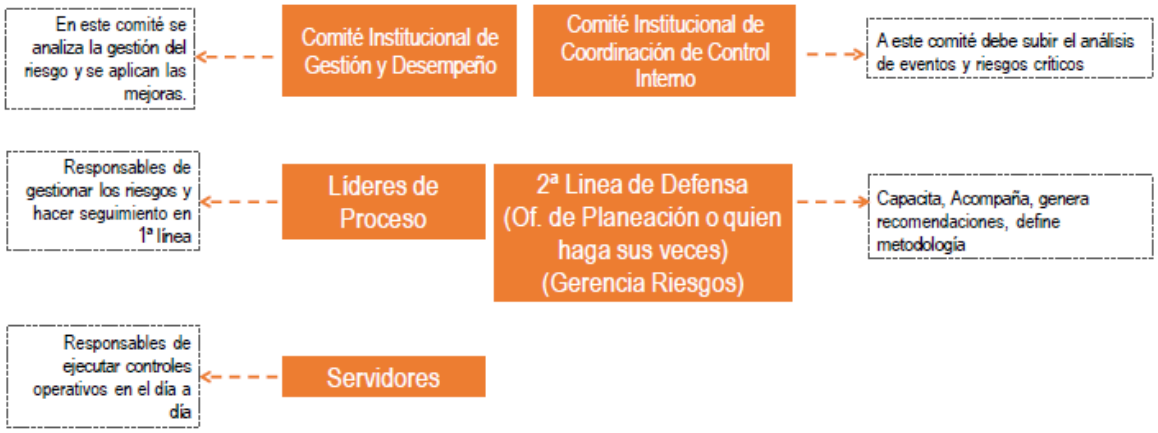
- De acuerdo con el esquema de direccionamiento estratégico, procesos, procedimientos, políticas de operación, sistemas de información, entre otros, la entidad tendrá insumos esenciales para iniciar con la aplicación de la metodología propuesta para la administración del riesgo.

Ilustración 1. Conocimiento y análisis de la entidad

Fuente: DAFP, 2020

- El modelo integrado de planeación y gestión (MIPG) define para su para su operación articulada, la creación 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:

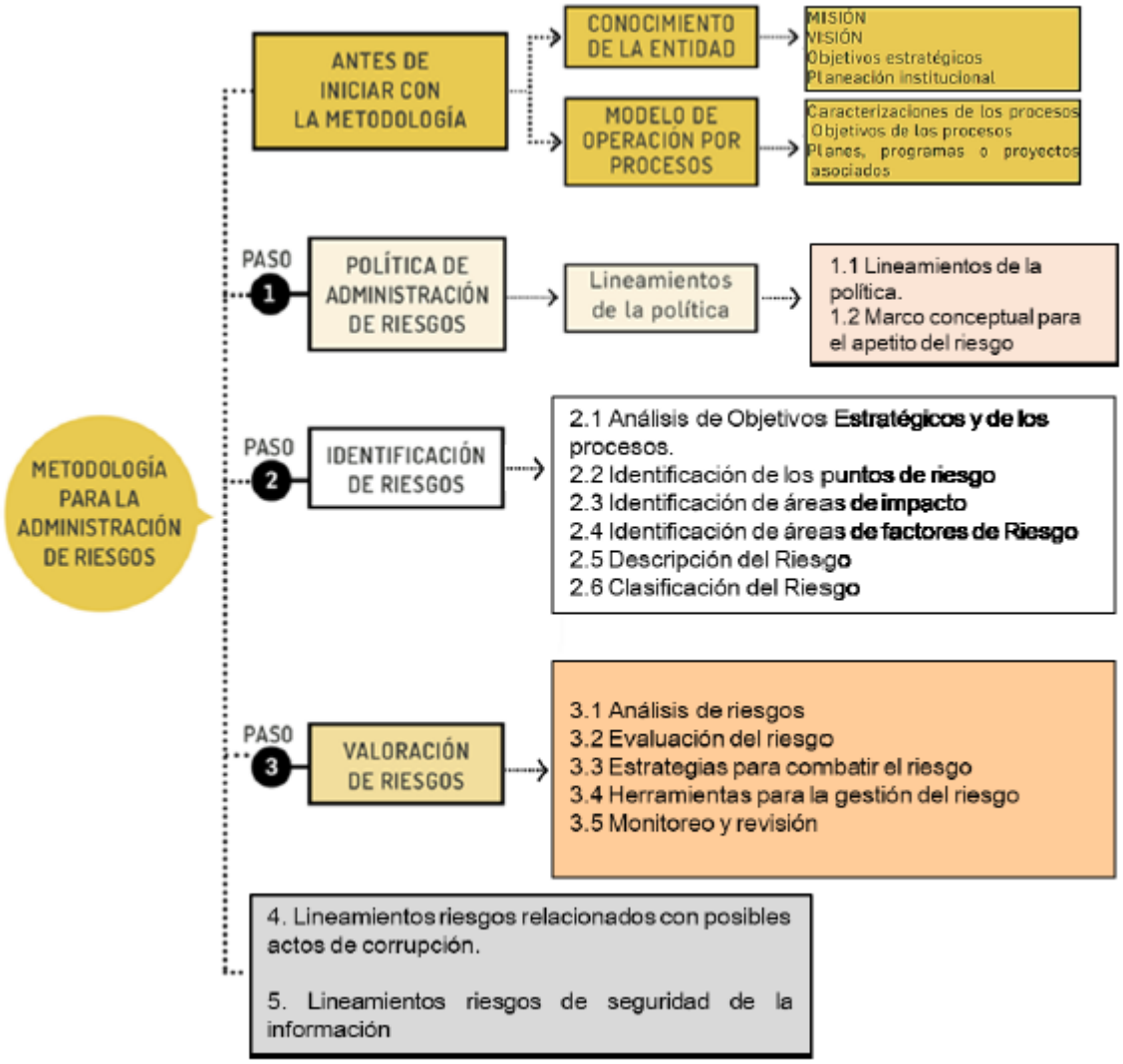
Ilustración 2. Operatividad Institucionalidad para la Administración del Riesgo



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

- 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 3. Metodología para la administración del riesgo



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

- Para la identificación y análisis de riesgos se pueden tomar como fuentes los planes de mejoramiento, los productos no conformes, encuestas de satisfacción, resultados de la gestión del proceso, entre otros.

- Los riesgos de corrupción se gestionan a través de los lineamientos establecidos por la Ley 1474 de 2011 y las estrategias para la construcción del plan anticorrupción y de atención al ciudadano.

- Para el análisis de los riesgos de corrupción se analizará de acuerdo a 5 niveles de probabilidad y 3 niveles de impacto (Catastrófico, Alto y Moderado) de acuerdo a la Guía para la Administración del Riesgo de Gestión y Corrupción y Diseño de Controles en Entidades Públicas – DAFP – Versión 4

- Para analizar la probabilidad e impacto de materialización de los riesgos (Riesgo inherente) se deben aplicar los criterios definidos en el presente documento.

- Las actividades de control que se establezcan para el tratamiento de los riesgos, deben evidenciar la gestión efectiva de los riesgos identificados, de tal manera que se puedan reducir las posibilidades de ocurrencia y los impactos que puedan llegar a generar, involucrando en su redacción las 6 variables: a) responsable, b) periodicidad, c) propósito, d) como se realiza (herramienta), e) que pasa con las observaciones o desviaciones y f) la evidencia del control

- El monitoreo de los riesgos se realiza de la siguiente forma: riesgos de gestión cada seis (6) meses, y riesgos de corrupción cada cuatro (4) meses.

- En los casos de que un riesgo se materialice, el líder de proceso debe establecer un plan de contingencia.

- Es responsabilidad de los lideres de los procesos, verificar el cumplimiento de los planes de tratamiento establecidos para los riesgos identificados, teniendo en cuenta tiempo y cronogramas establecidos.

2.1.4. Roles y Responsabilidades

Los roles y responsabilidades en la Gestión del Riesgo son de carácter participativo con los líderes de procesos, en el cual se determinaron los siguientes:

Tabla 2. Roles y responsabilidades en la Gestión del Riesgo

LINEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
Estratégica	Alta Dirección, el equipo directivo, Comité Institucional de Gestión y Desempeño y el	• Establecer y aprobar la Política de administración del riesgo • Establecer los lineamientos para la entidad en la identificación, valoración y monitoreo de los riesgos. • Revisar el cumplimiento de la Política de

	Comité Institucional de Coordinación de Control Interno	Administración de Riesgos de manera periódica y evaluar su impacto • Apoyar a los líderes de los procesos cuando se requiera en las actividades a realizar para que la gestión del riesgo sea eficaz en colaboración con los servidores públicos • Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles
Primera Línea	A cargo de los Gerentes públicos y líderes de procesos o gerentes operativos de programas y proyectos de la entidad	• Cumplir con los lineamientos establecidos en la política y aplicarlos. • Conocer el proceso e identificar los eventos del mismo. • Identificar y valorar los riesgos que pueden afectar los programas, planes y proyectos a su cargo y actualizarlo cuando se requiera • Revisar y aprobar la matriz de identificación y valoración del riesgo y el plan de tratamiento del riesgo a fin de minimizar la probabilidad de ocurrencia del riesgo. • Llevar a cabo las acciones asociadas a los controles establecidos para cada uno de los riesgos identificados en su proceso de acuerdo a la periodicidad establecida. Durante la aplicación de las acciones de seguimiento cada líder de proceso debe mantener la traza o documentación respectivas de todas las actividades realizadas. • Realizar de forma permanente el seguimiento a los controles establecidos en cada uno de los riesgos del proceso. • Informar a la secretaría de planeación (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo
Segunda Línea	Secretaría de Planeación Comité Institucional de Gestión y Desempeño	• Prestar asesoría a los procesos en la identificación y valoración de los riesgos institucionales y de corrupción, así como las acciones de contingencia que se requieran. • Consolidar el Mapa de riesgos Institucional y de Corrupción y presentarlo para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional • Evaluar que los riesgos sean consistentes con la

		presente política de la entidad y que sean monitoreados por la primera línea de defensa • Monitorear los riesgos identificados y controles establecidos por la primera línea de defensa acorde con la estructura de los temas a su cargo • Reportar a la Secretaría de Planeación, el seguimiento efectuado al mapa de riesgos a su cargo y proponer las acciones de mejora a que haya lugar • Acompañar al Equipo Técnico de Gestión y Desempeño en la identificación, análisis, y valoración del riesgo y definición de controles en los temas a su cargo
Tercera Línea	Equipo de Control Interno	• Asesorar de forma coordinada con la Secretaría de Planeación, a la primera y segunda línea de defensa en la identificación de los riesgos institucionales y diseño de controles • Verificar y analizar la idoneidad de los controles establecidos en los procesos, determinando si son o no adecuados para prevenir o mitigar los riesgos de los procesos. • Realizar seguimiento a los riesgos consolidados en los mapas de riesgos • Reportar el seguimiento a los riesgos identificados. • Recomendar mejoras a la política de administración del riesgo

3. ETAPAS DE LA GESTIÓN DEL RIESGO

La Administración Departamental ha determinado la siguiente metodología para el adecuado manejo de los riesgos:

Tabla 3. Metodología para el adecuado manejo de los riesgos en la Administración Departamental

3.1 Identificación del Contexto Estratégico

El contexto estratégico se establece a partir de la identificación y análisis de los factores internos, externos y del proceso. Los aspectos objeto del análisis interno o externo son definidos por el responsable del proceso o el equipo de trabajo designado teniendo en cuenta la naturaleza del proceso y las variables que permitan identificar los factores generadores de riesgo.

3.1.1. Elaboración del Análisis Interno

En el análisis interno se determinan las características o aspectos esenciales del ambiente en el cual la entidad busca alcanzar sus objetivos; se pueden considerar factores como

- **Estratégicos:** Falta de lineamientos y demoras en la Planeación, mapa de procesos desactualizado, estructura organizacional no acordes con procesos, indicadores mal formulados que no aportan a la gestión para toma de decisiones, desconocimiento y

falta de aplicación de políticas de operación por parte de los servidores, Políticas, objetivos y estrategias implementadas

- **Personal:** Funciones y responsabilidades, desmotivación de los servidores, falta de incentivos, carrera administrativa sin posibilidades de ascenso, falta de capacitación para desarrollar proyectos, alta rotación, cultura organizacional

- **Tecnología:** Falta de interoperabilidad con otros sistemas, fallas en la infraestructura tecnológica, falta de recursos para el fortalecimiento tecnológico.

- **Comunicación Interna:** Falta de control sobre los canales establecidos, Falta de registros de resultados, demoras en cargar la información, poca efectividad en los canales internos.

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

- **Procesos:** Caracterización, PHVA, proveedores, entradas, salidas, gestión del conocimiento.

3.1.2. Elaboración del Análisis Externo

Se identifican los factores o circunstancias externas a la entidad, amenazas que pueden afectar el cumplimiento de planes, programas y el logro de los objetivos institucionales y de los procesos tales como:

- **Económicos:** Disminución del presupuesto por prioridades del Gobierno, Austeridad en el gasto.

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

- **Legales:** Cambios legales y normativos aplicables a la Entidad y a los procesos.

- **Sociales:** Cambio de gobierno con nuevos planes y proyectos de Desarrollo, falta de continuidad en los programas establecidos, desconocimiento de la Entidad por parte de otros órganos de gobierno.

- **Tecnológicos:** Sistemas de gestión ineficientes, falta de optimización de sistemas de gestión, falta de coordinación de necesidades de tecnología.

- **Medioambientales:** Contaminación por sustancias perjudiciales para la salud, mala práctica de clasificación de residuos.

- **Comunicación Externa:** Múltiples canales e interlocutores de la Entidad con los usuarios, Servicio telefónico insuficiente, falta de coordinación de canales y medios.

3.2 Identificación de los Riesgos

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

3.2.1. Análisis de objetivos estratégicos y de los procesos

Este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.

Ilustración 4. Análisis de objetivos

Análisis de Objetivos Estratégicos	Análisis de Objetivos de Proceso
La entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso. Es necesario revisar que los objetivos estratégicos se encuentren alineados con la Misión y la Visión Institucional, así como, analizar su adecuada Formulación. (Características SMART)	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.

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

3.2.2. Identificación de los puntos de riesgo

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

Ilustración 5. Cadena de valor publico

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

3.2.3. Identificación de áreas de impacto

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

3.2.4. Identificación de áreas de factores de riesgo

Son las fuentes generadoras de riesgos. En la Tabla 4 encontrará un listado con ejemplo de factores de riesgo que puede tener la entidad.

Tabla 4. 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 de 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

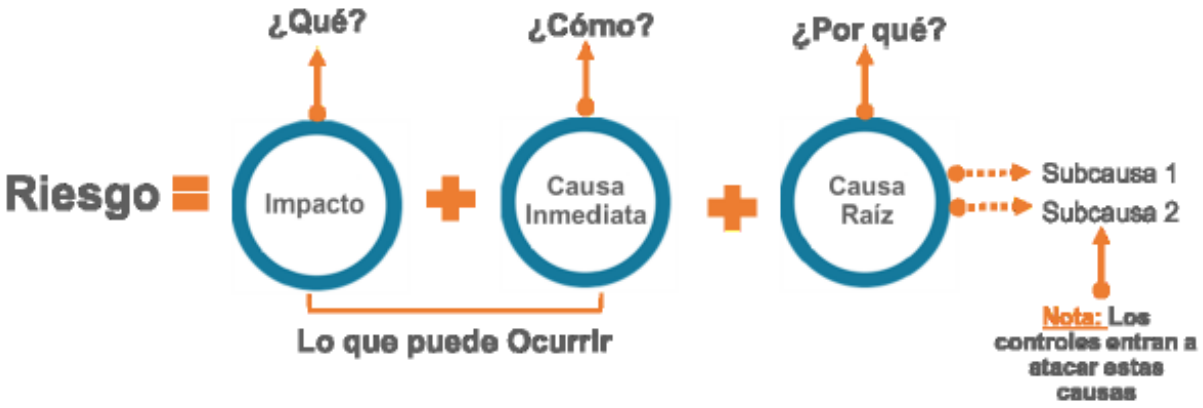
Evento externo	Situaciones externas que afectan la entidad.	▪ Suplantación de identidad ▪ Asalto a la oficina ▪ Atentados, vandalismo, orden público

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

3.2.5. Descripción del riesgo

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

Ilustración 6. Estructura propuesta para la redacción del riesgo



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

Esta es información esencial para la definición de controles en la etapa de valoración del riesgo. Desglosando la estructura propuesta tenemos:

- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo. (Ver numeral 3.2.3)

- **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.

3.2.6. Clasificación del riesgo

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

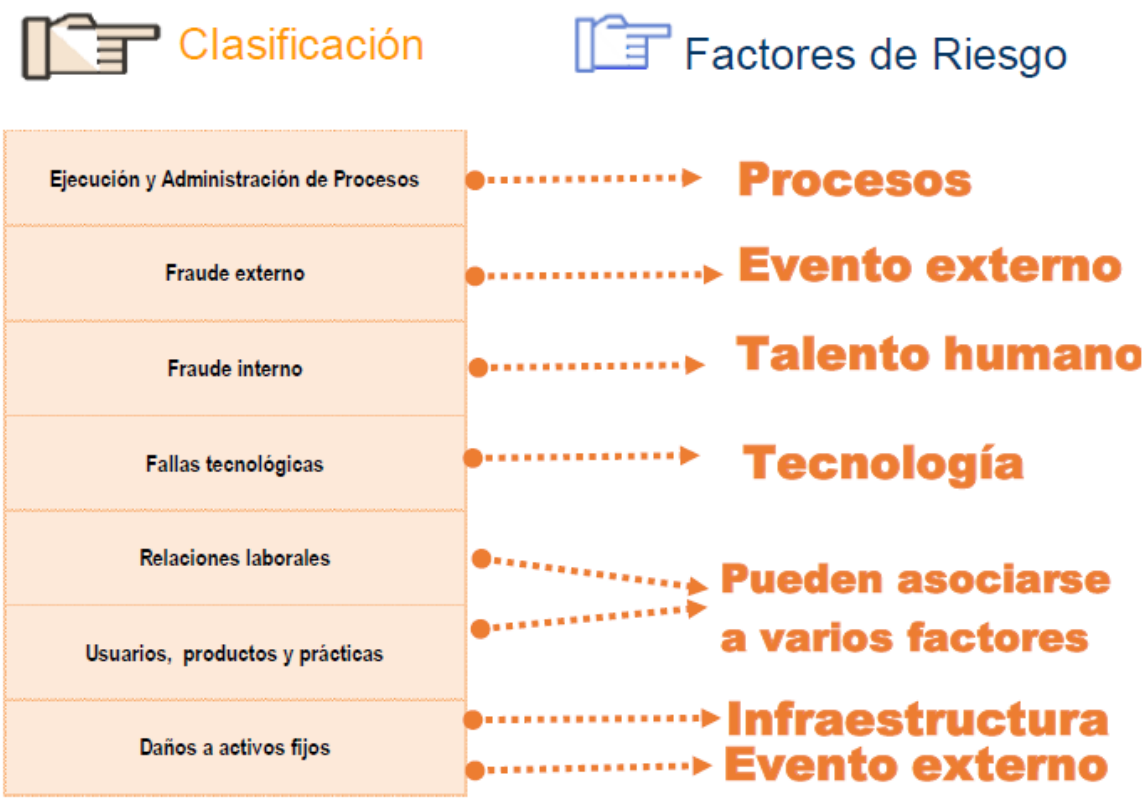
Tabla 5. Clasificación de riesgos

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público

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

Teniendo en cuenta que en la Tabla 4 se definieron una serie de factores generadores de riesgo, para poder definir la clasificación de riesgos, su interrelación es la siguiente:

Ilustración 7. Relación ente factores de riesgo y clasificación del riesgo

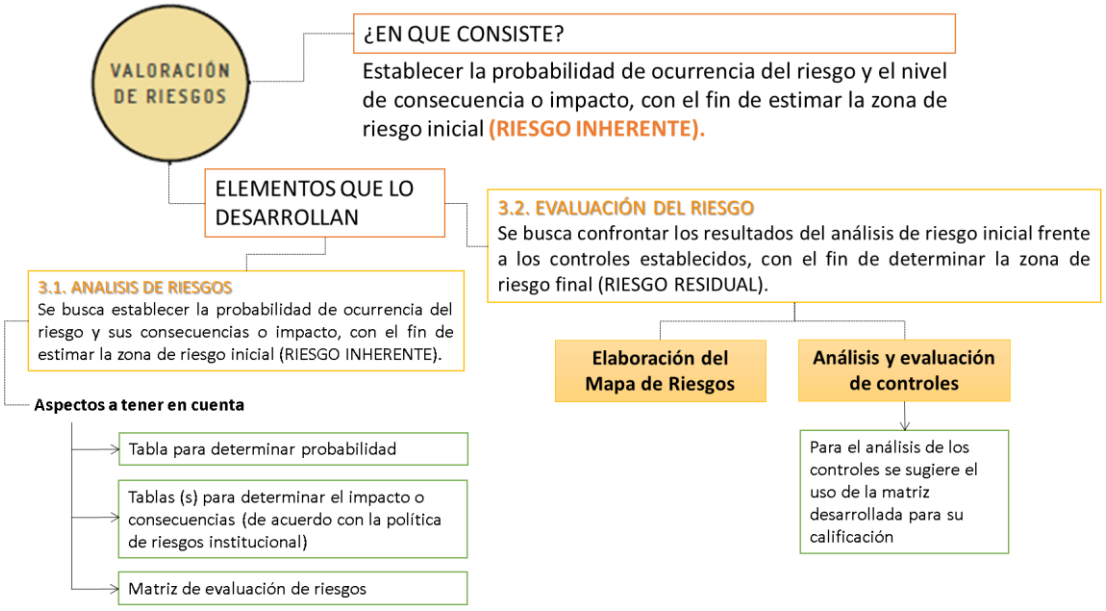


Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

3.3 Valoración del Riesgo

Se realiza el análisis de riesgos, a través de la estimación de la probabilidad de su ocurrencia y el impacto o consecuencias que puede causar su materialización, realizando la calificación y evaluación con el fin de estimar la zona de riesgo inicial o Riesgo inherente

Ilustración 8. Estructura para el desarrollo de la valoración del riesgo



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

3.3.1. Análisis de riesgos

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

3.3.1.1. Determinación de 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.

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 6. 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
Tecnología [1] (incluye disponibilidad de aplicativos), tesorería	Diaria	Muy alta

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

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, en la tabla 7 se establecen los criterios para definir el nivel de probabilidad:

Tabla 7. 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: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

3.3.1.2. Determinar el Impacto

Existen 2 áreas de impacto como se vio en el numeral 3.2.3, Económico y Reputacional. Cuando se presenten ambas áreas de impacto para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto,

[1] 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.

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. Para estimar el impacto, se utiliza la siguiente tabla:

Tabla 8. 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: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

El líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo.

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

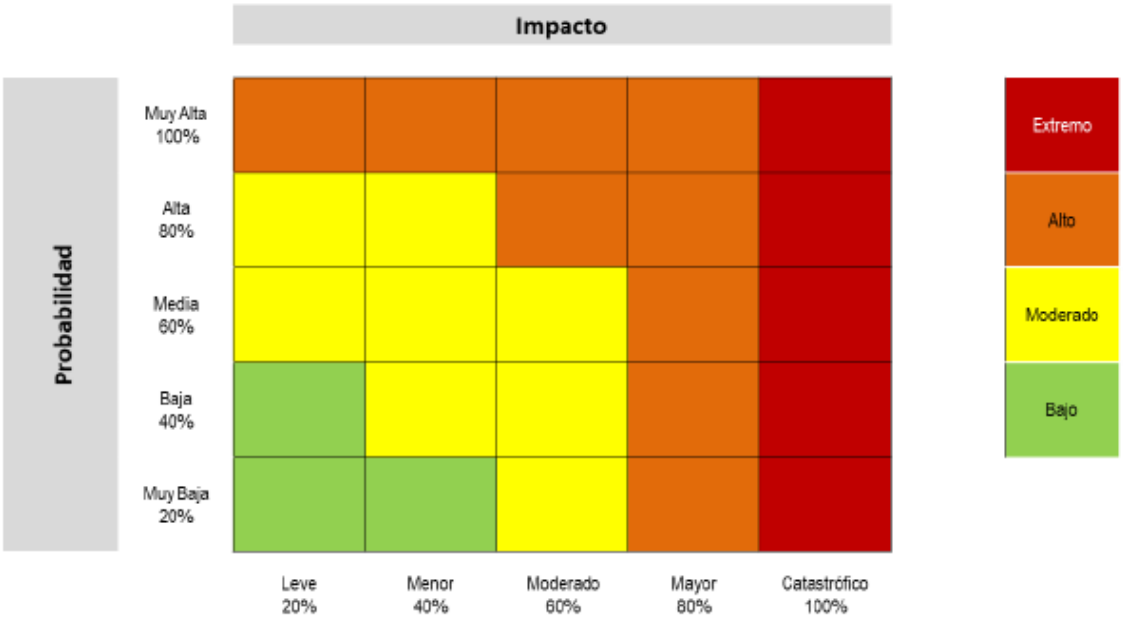
3.4 Evaluación de riesgos

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

3.4.1. 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 9. Matriz de calor (niveles de severidad del riesgo)



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

En ella se ubica la intersección entre la probabilidad inherente y el impacto inherente para determinar la Zona de riesgo

3.4.2. Valoración de controles

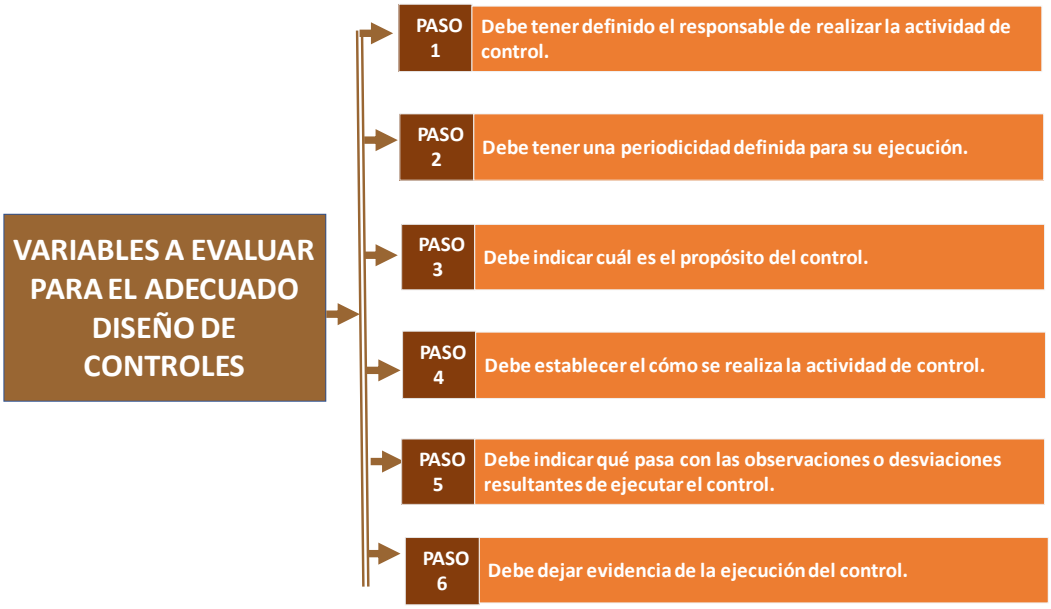
En primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- 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.

- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

3.4.2.1. 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:

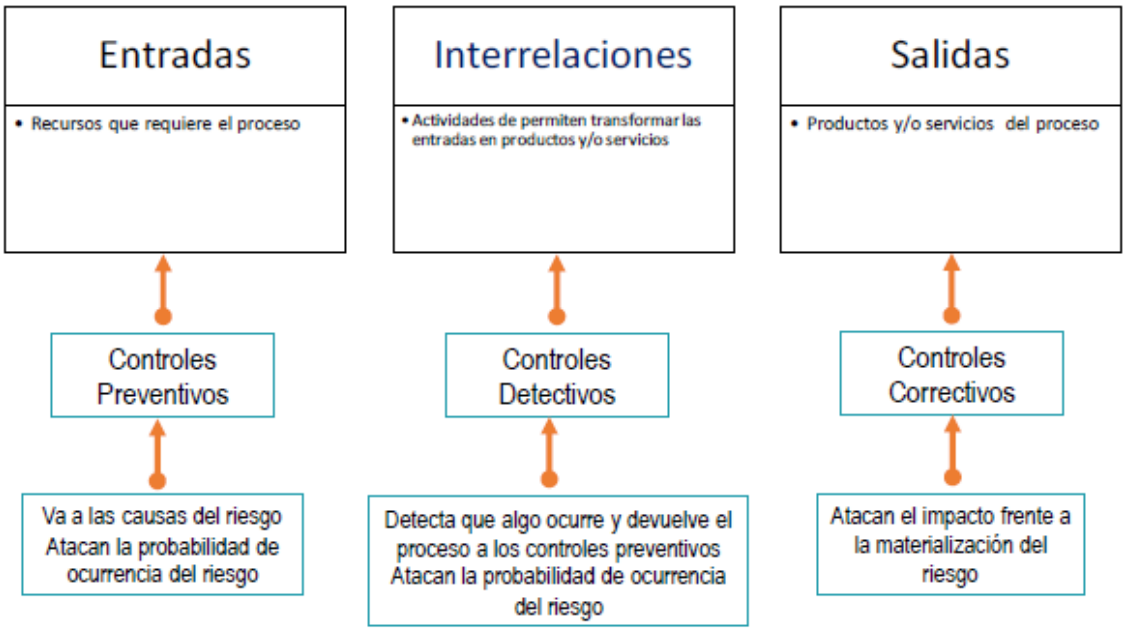


Fuente: Función Pública, 2018

3.4.2.2. Tipología de controles y los procesos

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

Ilustración 10. Ciclo del proceso y las tipologías de controles



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

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

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

- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

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

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

- **Control automático:** son ejecutados por un sistema.

3.4.2.3. Análisis y evaluación de los controles – Atributos

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la tabla 9 se puede observar la descripción y peso asociados a cada uno así:

Tabla 9. 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%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran	-

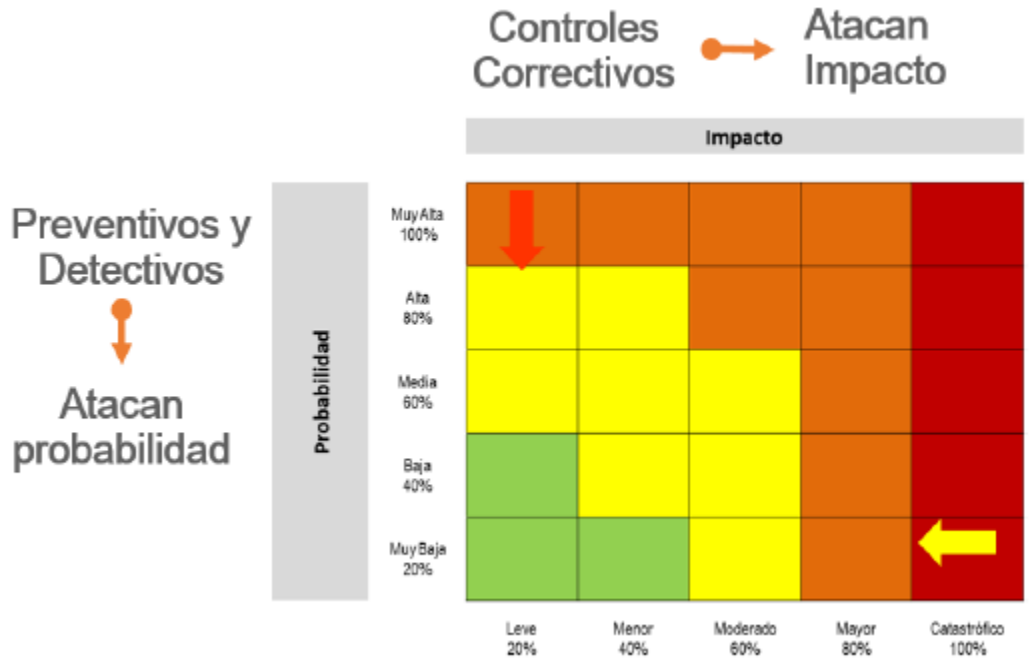
			documentados en ningún documento propio del proceso.	
	Frequencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Alectoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

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

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 siguiente, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Ilustración 11. Movimiento en la matriz de calor acorde con el tipo de control

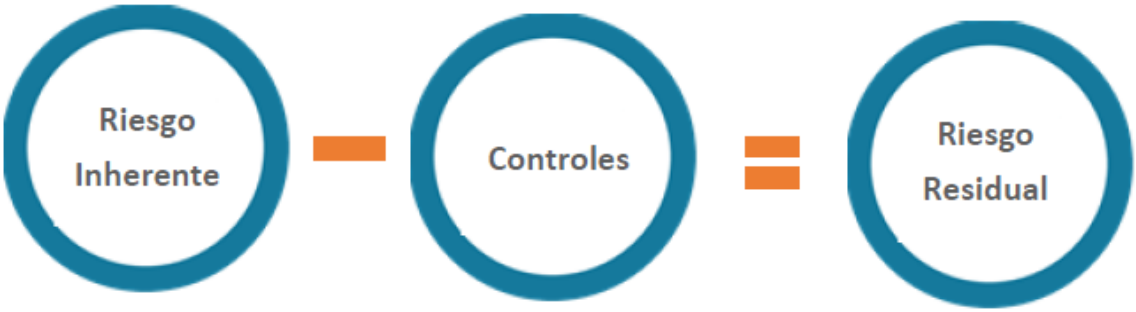


Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

3.4.3. Nivel de riesgo (riesgo residual)

Es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Ilustración 12. Riesgo residual



Ecuación 1. Cálculo del riesgo residual

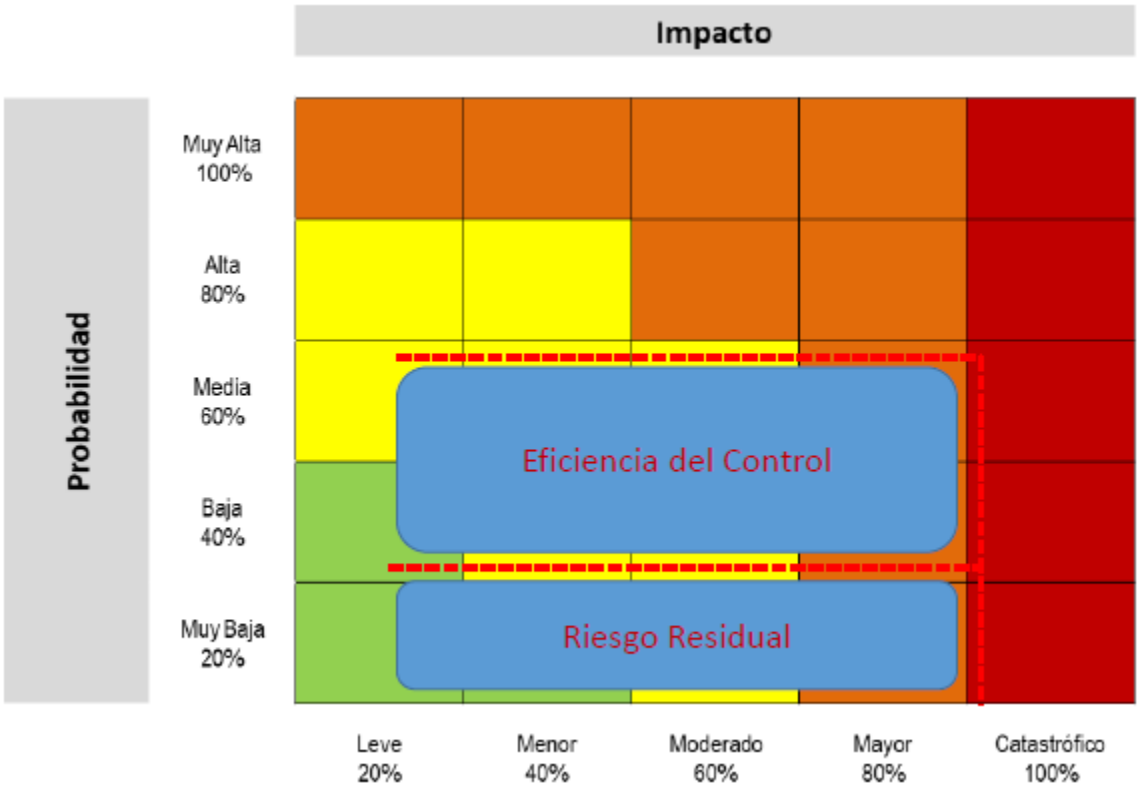
R. Residual = R. Inherente – (R.I. * Control)

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.

Opera una política de reducción máxima del 50% para los controles

La metodología acumulativa busca reducir los niveles de probabilidad e impacto residual, teniendo en cuenta la eficiencia del control

Ilustración 13. Movimiento en la matriz de calor



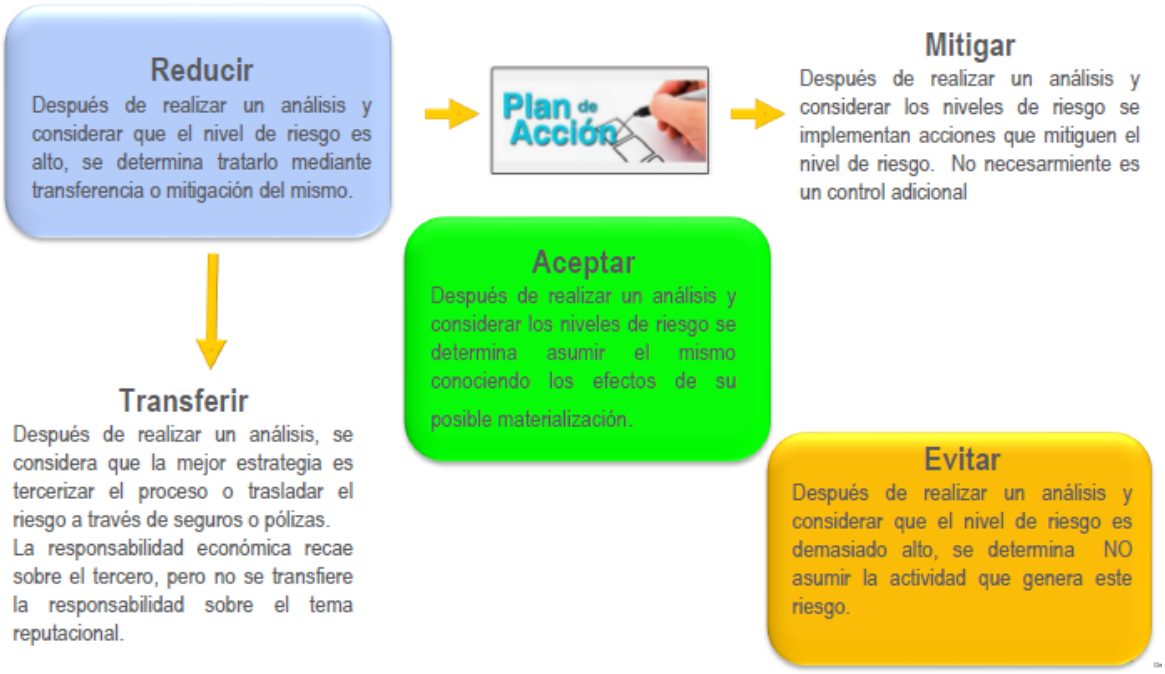
Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

3.5. Estrategias para combatir el riesgo

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

En la figura 14 se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.

Ilustración 14 Estrategias para combatir el riesgo



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

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

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

3.5.1. Nivel de Aceptacion del Riesgo

Tabla 10. Nivel de Aceptacion del Riesgo

Tipo de Riesgo	Zona de Riesgo	Nivel de Aceptación
Riesgos de Gestión	BAJA	Se ASUMIRÁ el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado y se realiza en el reporte mensual de su desempeño.
	MODERADA	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo, se hace seguimiento y se registra sus avances
	ALTA Y EXTREMA	Se establecen acciones de Control Preventivas y/o correctivas que permitan MITIGAR la materialización del riesgo. Se monitorea y se registra
Riesgos de Corrupción	BAJA	Ningún riesgo de corrupción podrá ser aceptado. Realizar seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos.
	MODERADA	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo. Realizar seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos y se registra su avance
	ALTA Y EXTREMA	Se adoptan medidas para: REDUCIR la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. EVITAR Se abandonan las actividades que dan

		lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo. TRANSFERIR O COMPARTIR una parte del riesgo para reducir la probabilidad o el impacto del mismo. Realizar seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos y se registra su avance

3.6. 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 11 se muestran algunos ejemplos de estos indicadores

Tabla 11. Ejemplos indicadores clave de riesgo

PROCESO ASOCIADO	INDICADOR	METRICA
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

También es posible establecer el desempeño de los controles así:

$$\textbf{Desempeño del control} = \frac{\#\ \text{eventos}}{\text{frecuencia del riesgo (\# veces que se hace la actividad)}}$$

3.7. MONITOREO Y REVISIÓN

El modelo integrado de plantación 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 de acuerdo a la figura 15.

Una vez analizado el nivel de riesgo residual y definido el tratamiento a implementar con el establecimiento de controles preventivos y detectivos, es necesario generar un reporte que consolide la información clave del proceso de gestión del riesgo.

En el formato de Matriz de Riesgos, se inicia con el registro del riesgo identificado, luego se especifica la clase de riesgo, las causas inmediata y raíz, así como la probabilidad e impacto que quedaron después de valorar los controles para determinar el riesgo residual

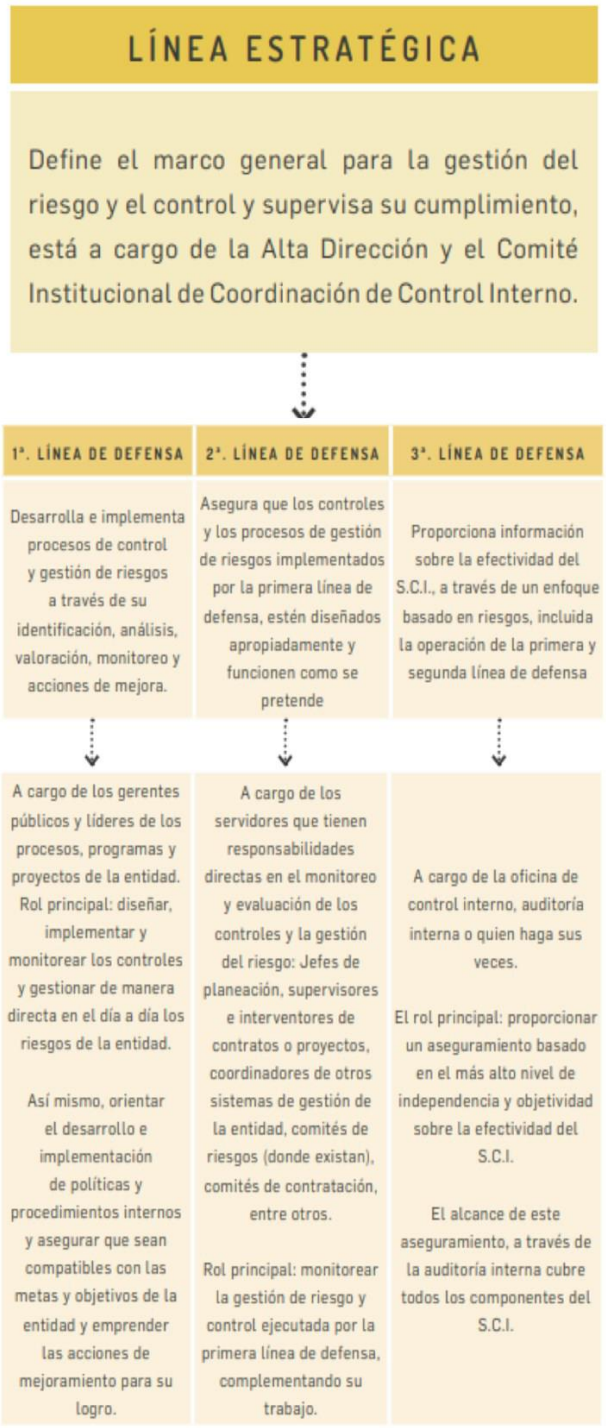
A partir de allí se deben analizar las estrategias DO y FA o estrategias formuladas en la etapa de establecimiento del contexto, que contrarresten las causas raíz, para colocarlas en las actividades de control del formato y con base en su contenido se establezca la opción de tratamiento a la que corresponden

Luego se relaciona el soporte con el que se evidenciará el cumplimiento de cada actividad, el responsable de adelantarla (relacionando el cargo y no el nombre), el tiempo específico para cumplir con la actividad o la periodicidad de ejecución.

Al final de todas las actividades de control establecidas para atacar las causas del riesgo, se debe relacionar el plan de acción, para ello es importante analizar las estrategias DA o estrategias de fuga provenientes de la Matriz DOFA, seleccionando la(s) más apropiada(s) para el riesgo identificado.

Por último, se formulan los indicadores clave de riesgo que permitan monitorear el cumplimiento (eficacia) e impacto (efectividad) de las actividades de control, siempre y cuando conduzcan a la toma de decisiones.

Ilustración 15. Esquema de líneas de defensa



4. RIESGOS DE CORRUPCIÓN Y SEGURIDAD DE LA INFORMACIÓN

De manera específica los temas relacionados con los riesgos asociados a posibles actos de corrupción y los de seguridad de la información se tratan 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), lo que ha permitido una coordinación adecuada con los líderes de política correspondientes.

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

- 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 la Guía de para la Administración del Riesgo de Gestión y diseño de Controles en Entidades Públicas - Versión 5, de manera tal que los responsables, en este caso la Secretaría TIC quien lidera el proceso, 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**, es claro que este tipo de riesgos no admiten aceptación del riesgo; así mismo, se incluyen 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.

- 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. Estos lineamientos son aplicables a ambas tipologías de riesgos.

- 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 riego aplicables. En cuanto a los riesgos de seguridad de la información se incorporan las tablas de probabilidad, impacto y matriz de calor definidas en la metodología general.

4.1 Generalidades de los Riesgos de corrupción

- 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.

4.2 Identificación del riesgo de corrupción.

4.2.1. Lineamientos para la identificación del riesgo de corrupción

Las preguntas clave para la identificación del riesgo son:

- ¿Qué puede suceder?
- ¿Cómo puede suceder?
- ¿Cuándo puede suceder?
- ¿Qué consecuencias tendría su materialización?

Ilustración 16. Descripción del riesgo de corrupción

Posibilidad de + recibir o solicitar cualquier dádiva o beneficio + a nombre propio o de terceros + con el fin de celebrar un contrato.

4.2.2. Valoración del riesgo

4.2.2.1. Determinación de la probabilidad

La determinación de la probabilidad (posibilidad de ocurrencia del riesgo) se debe llevar a cabo de acuerdo con lo establecido en el aparte 3.1.1.1 de esta política.

4.2.2.2. Determinación del impacto

Para la determinación del impacto frente a posibles materializaciones de riesgos de corrupción se analizarán únicamente los siguientes niveles i) moderado, ii) mayor, y iii) catastrófico, dado que estos riesgos siempre serán significativos, en tal sentido, no aplican los niveles de impacto insignificante y menor, que sí aplican para las demás tipologías de riesgos.

Ahora bien, para establecer estos niveles de impacto se deberán aplicar las siguientes preguntas frente al riesgo identificado

Tabla 12. Criterios para calificar el impacto en riesgos de corrupción

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA SÍ	RESPUESTA 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.		

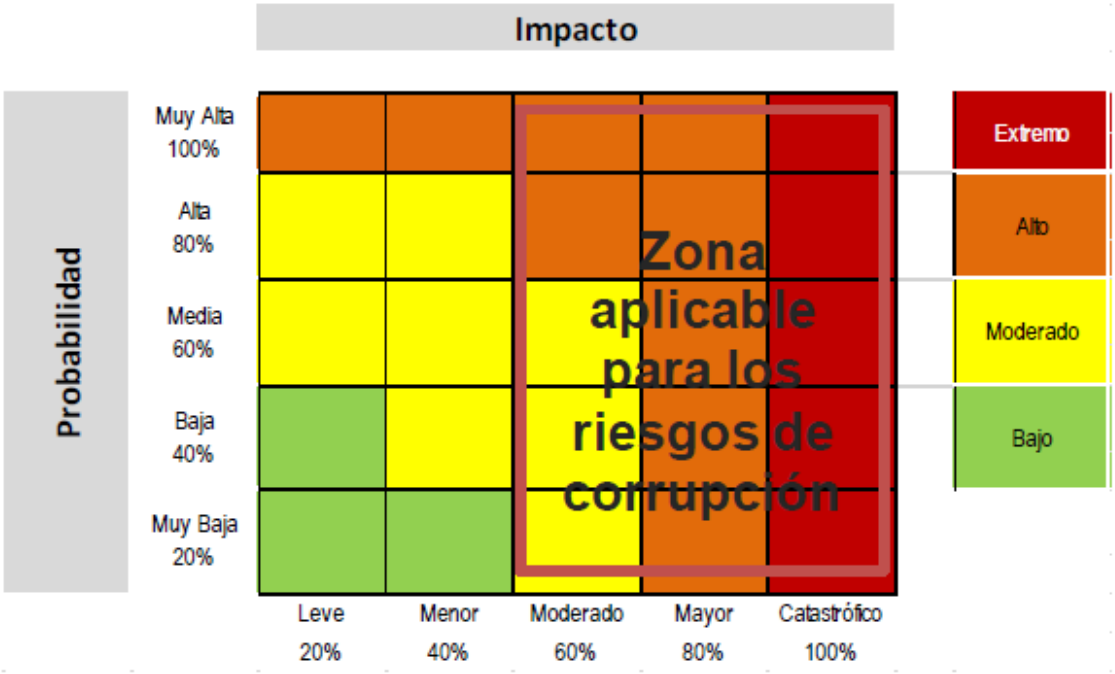
Nivel de impacto MAYOR

Fuente: Secretaría de Transparencia

4.2.2.3. Análisis preliminar (riesgo inherente)

En esta etapa se define el nivel de severidad para el riesgo de corrupción identificado, para lo cual se aplica la matriz de calor, teniendo en cuenta el ajuste frente a los niveles de impacto insignificante y menor mencionados en la determinación del impacto, lo que implica que las zonas de severidad para este tipo de riesgos se delimitan como se muestra a continuación:

Ilustración 17. Matriz de calor para riesgos de corrupción



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

4.2.2.4. Valoración de controles

Se evalúa si los controles están bien diseñados para mitigar el riesgo y si estos se ejecutan como fueron diseñados.

Para la evaluación del diseño de los controles existentes se debe tener en cuenta la siguiente escala de calificación:

Tabla 13. Análisis y Evaluación de los Controles para la Mitigación de los Riesgos de corrupción

Criterio de evaluación.	Aspecto a Evaluar en el Diseño del Control	Opción de respuesta al criterio de evaluación	Peso en la evaluación del diseño del control
1.1 Asignación del Responsable.	¿Existe un responsable asignado a la ejecución del control?	Asignado	15
		No Asignado	0
1.2 Segregación y Autoridad del Responsable.	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	15
		Inadecuado	0
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	15
		Inoportuna	0
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar Cotejar, Comparar, Revisar, ¿etc.?	Prevenir	15
		Detectar	10
		No es un Control	0
4. Como se realiza la actividad de control.	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	15
		No Confiable	0
5. Qué pasa con las observaciones o desviaciones.	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	15
		No se investigan y resuelven oportunamente.	0

6. Evidencia de la ejecución del control.	¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión?	Completa	10
		Incompleta	5
		No Existe	0

El resultado de cada variable de diseño, va a afectar la calificación del diseño del control, ya que deben cumplirse todas las variables, para que un control se evalué como bien diseñado.

Tabla 14. Calificación del Diseño del Control

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

El resultado de las calificaciones del control o promedio en el diseño de los controles, que este por debajo de 96 %, se debe establecer un plan de acción que permita tener un control o controles bien diseñados.

4.2.2.5. Evaluación de la Ejecución del Control

Aunque un control este bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo. No basta solo con tener controles bien diseñados, debe asegurare por parte de la primera línea de defensa que el control se ejecute. Al momento de determinar si el control se ejecuta, inicialmente es una confirmación por parte del responsable del proceso, y posteriormente se confirma con las actividades de evaluación realizadas por Control Interno

Tabla 15. Calificación de la Ejecución del control

Rango de Calificación de la Ejecución	Resultado - Peso de la Ejecución del control
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

4.2.2.6. Análisis y Evaluación de los Controles para la Mitigación de los Riesgos

Dado que la calificación de riesgos inherentes y residuales se realiza es al riesgo y no a cada causa, hay que consolidar el conjunto de los controles asociados a las causas, para evaluar si estos de manera individual y en conjunto si ayudan al tratamiento de los riesgos, considerando tanto el diseño y ejecución individual y promedio de los controles

En la evaluación del diseño y ejecución de los controles, las dos variables son importantes y significativas en el tratamiento de los riesgos y sus causas, por lo que siempre la calificación de la solidez de cada control, asumirá la calificación del diseño o ejecución con menor calificación entre fuerte, moderado y débil, tal como se detalla en la siguiente tabla:

Tabla 16. Solidez Individual de cada Control

Peso del diseño individual o promedio de los Controles. (DISEÑO)	El Control se ejecuta de manera consistente por los responsables. (EJECUCION)	Solidez individual de cada control Fuerte:100 Moderado:50 Debil:0	Aplica plan de acción para fortalecer el Control Si / NO
Fuerte Calificación Entre 96 y 100	**Fuerte** (Siempre se ejecuta)	Fuerte + Fuerte = Fuerte	No
	Moderado (Algunas veces)	Fuerte + Moderado = Moderado	Si
	Débil (No se ejecuta)	Fuerte + Débil = Débil	Si
Moderado Calificación Entre 86 y 95	**Fuerte** (Siempre se ejecuta)	Moderado + Fuerte = Moderado	Si
	Moderado (Algunas veces)	Moderado + Moderado = Moderado	Si
	Débil (No se ejecuta)	Moderado + Débil = Débil	Si
Débil Entre 0 y 85	**Fuerte** (Siempre se ejecuta)	Débil + Fuerte = Débil	Si
	Moderado (Algunas veces)	Débil + Moderado = Débil	Si
	Débil (No se ejecuta)	Débil + Débil = Débil	Si

4.2.2.7. Solidez del conjunto de controles para la adecuada mitigación del riesgo

Dado que un riesgo puede tener varias causas y a su vez varios controles y la calificación se realiza al riesgo, es importante evaluar el conjunto de controles asociados al riesgo.

Ilustración 18. Solidez del conjunto de controles

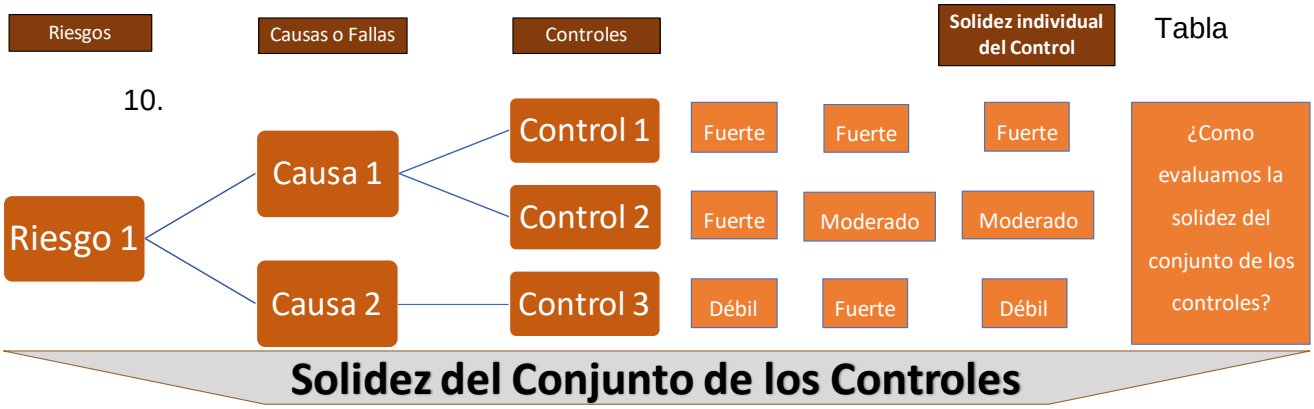


Tabla 10.

Tabla 17. Calificación de la solidez del conjunto de controles

Calificación de la Solidez del conjunto de controles.	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos la calificación está entre 50 y 99
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos la calificación es menor a 50.

4.2.2.8. Valoración del Riesgo Residual

- Desplazamiento del Riesgo Inherente para calcular el Riesgo Residual

Dado que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual, se realizará de acuerdo a la siguiente tabla:

Tabla 18. Desplazamiento del Riesgo Inherente para calcular el Riesgo Residual

Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos.				
Solidez del conjunto de los controles.	**Controles ayudan a disminuir la probabilidad**	**Controles ayudan a disminuir Impacto**	**# Columnas en la matriz de riesgo que se desplaza en el eje de la Probabilidad**	**# Columnas en la matriz de riesgo que se desplaza en el eje de Impacto**
Fuerte	**Directamente**	**Directamente**	**2**	**2**
Fuerte	**Directamente**	**Indirectamente**	**2**	**1**
Fuerte	**Directamente**	**No Disminuye**	**2**	**0**
Fuerte	**No disminuye**	**Directamente**	**0**	**2**
Moderado	**Directamente**	**Directamente**	**1**	**1**
Moderado	**Directamente**	**Indirectamente**	**1**	**0**
Moderado	**Directamente**	**No Disminuye**	**1**	**0**
Moderado	**No disminuye**	**Directamente**	**0**	**1**

Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, procedemos a la elaboración del mapa de riesgo residual (después de los controles).

La evaluación del riesgo se realiza de acuerdo a los resultados que se obtengan en la matriz, teniendo en cuenta la valoración del riesgo residual:

- Si el riesgo se ubica en la Zona de Riesgo Baja, permite a la entidad asumirlo, debido a que se encuentra en un nivel que puede controlado, sin necesidad de tomar otras medidas de control adicionales a las que se poseen.

- Si el riesgo se ubica en las Zonas Moderada o Alta, se deben tomar medidas de control adicionales a las actuales las cuales deben llevar a disminuir la probabilidad o la consecuencia o ambas para llevar en lo posible los riesgos a la zona baja.

- Si el riesgo se ubica en la Zona de Riesgo Extrema, se deben eliminar la (s) causa (as) que genera el riesgo e implementar controles preventivos para evitar la probabilidad de ocurrencia y disminuir el impacto. El tema debe ser abordado por la Alta Dirección.

4.3 Lineamientos riesgos de seguridad de la información

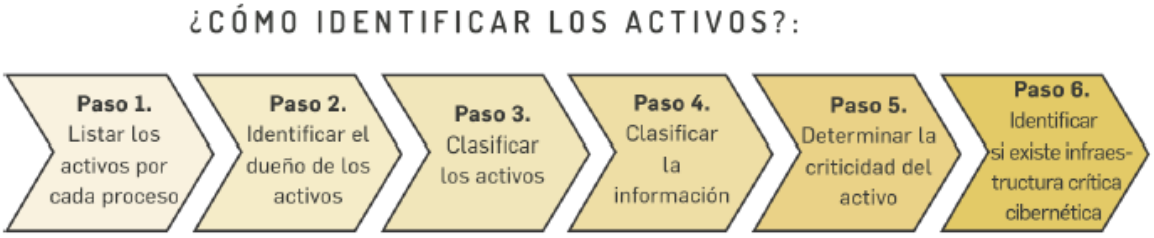
En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI)[2], el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

Tabla 19. Conceptualización activos de información

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización	Permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

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

Ilustración 19. Pasos para la identificación de activos



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

Tabla 20. Ejemplo identificación activos del proceso

Proceso	Activo	Descripción	Dueño del activo	Tipo del activo	Ley 1712 de 2014	Ley 1581 de 2012	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Gestión financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe de oficina financiera	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión financiera	Aplicativo de nómina	Servidor web que contiene el *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

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

4.3.1. Identificación del riesgo

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

- Pérdida de la confidencialidad

- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas de la Guía para la administración del riesgo y diseño de controles de las entidades públicas – Versión 5, 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

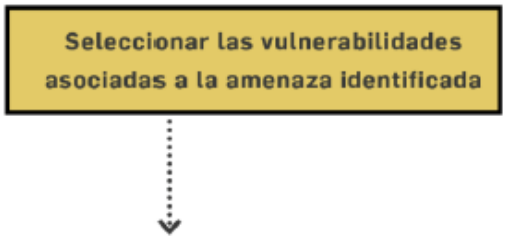
Tabla 21. Tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo

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.

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.

Ilustración 20. Formato de descripción del riesgo de seguridad de la información

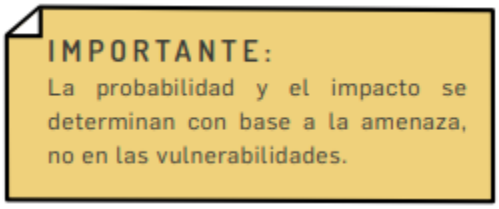


RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/ VULNERA-BILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políti-cas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar 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.

4.3.2. Valoración del riesgo

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas en la primera parte de la presente política.

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 la presente política.



4.3.3. Controles asociados a la seguridad de la información

La entidad podrá 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" de la Guía para la administración del riesgo y diseño de controles de las entidades públicas – Versión 5, siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

A continuación, se incluyen algunos ejemplos de controles y los dominios a los que pertenecen, la lista completa se encuentra en del documento maestro del modelo de seguridad y privacidad de la información (MSPI):

Tabla 22. 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 perdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del *software* 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

5. INFORMACIÓN, COMUNICACIÓN Y REPORTE

La comunicación de la Información y el reporte debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios. Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.

Por tanto, se debe hacer especial énfasis en la difusión, socialización, capacitación y/o entrenamiento de todos y cada uno de los pasos que componen la metodología de la administración del riesgo, asegurando que permee a la totalidad de la organización pública

Importante: Se debe conservar evidencia de la comunicación de la información y reporte de la administración del riesgo en todas sus etapas.

6. SEGUIMIENTO A LAS ACCIONES DE CONTROL DEL RIESGO EN CADA PROCESO

- ✓ Cuatrimestralmente, de debe verificar las acciones para los riesgos de corrupción y semestralmente para los riesgos de gestión; y registrar el avance junto con la evidencia en el Sistema de Gestión

- ✓ Analizar los resultados del seguimiento y establecer acciones inmediatas ante cualquier desviación

- ✓ Comunicar al líder del proceso las desviaciones del riesgo según el nivel de aceptación del riesgo

- ✓ Documentar las acciones de corrección o prevención en el plan de mejoramiento

- ✓ Revisar y actualizar el mapa de riesgo cuando se modifique las acciones o ubicación del riesgo

7. ANEXOS

- Formato mapa de riesgos parametrizado

8. BIBLIOGRAFÍA

- Departamento Administrativo de la Función Pública. Secretaría de Transparencia de la Presidencia de la República. (2018). *Guía de para la Administración del Riesgo de Gestión y Corrupción y Diseño de Controles en Entidades Públicas*. Versión 4. Gobierno de Colombia.

- Departamento Administrativo de la Función Pública. (2020). *Guía de para la Administración del Riesgo y Diseño de Controles en Entidades Públicas*. Versión 5. Gobierno de Colombia.

ELABORACION	REVISION	APROBACIÓN
Elaborado por: Martha Elena Giraldo Ramírez	Revisado por: José Duván Lizarazo	Aprobado por: Roberto Jairo Jaramillo Cárdenas
Cargo: Directora Técnica de Planeación	Cargo: Jefe de oficina de Control interno de Gestión	Cargo: Gobernador