AGOSTO DE 2018

Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas

VERSIÓN 1

PRESIDENCIA DE LA REPÚBLICA
Alfonso Prada Gil
Secretario General de la Presidencia de la República
Juan Pablo Charry Rozo
Secretario de Transparencia (e)

MINISTERIO DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Juan Sebastián Rozo Rengifo
Ministro
Elizabeth Blandón
Directora de Gobierno Digital

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA
Liliana Caballero Durán
Directora
María del Pilar García González
Directora de Gestión y Desempeño Institucional

Equipo de Trabajo

Presidencia de la República - Secretaria de Transparencia

Martha Ligia Ortega Santamaría

Ana Paulina Sabbagh Acevedo

María Victoria Sepúlveda Rincón

Ministerio de las Tecnologías de la Información y las Comunicaciones - Grupo Interno de Seguridad y Privacidad de la Información

Antonio Carrillo Rosas

Juan Carlos Valenzuela Buitrago

Senen Niño Gil

Ángela Cortés

Departamento Administrativo de la Función Pública – Dirección de Gestión Desempeño y Institucional, Grupo de Análisis y Política
Diana María Caldas Gualteros
Dolly Amaya Caballero
Eva Mercedes Rojas Valdés
Myrian Cubillos Benavides
Dorley Enrique León López
Edwin Arley Giraldo

ÍNDICE

PÁGINA

Introducción 5
Objetivos 6
Conceptos básicos 7
Antes de iniciar la metodología 9
Acerca de la metodología 11

Paso 1. Política Administración de Riesgos 12

Paso 2. Identificación de riesgos 14
2.1. Establecimiento del contexto 16
2.1.1. Contexto interno 16
2.1.2. Contexto externo 16
2.1.3. Contexto del proceso 16
2.1.4. Identificación de activos de seguridad de la información 18
2.2. Identificación de riesgos - técnicas para identificación de riesgos de gestión y corrupción 19
Tipología de los riesgos 24
Ejemplos descripción del riesgo 25

Paso 3. Valoración de riesgos 28
3.1. Análisis de riesgos 29
3.1.2. Cálculo de la probabilidad 30
3.1.3 Análisis del impacto (riesgos de gestión y corrupción) 34
Tratamiento del riesgo 37

3.2.1. Análisis preliminar (Riesgo Inherente) 45
3.2.2 Valoración de los controles (Diseño Controles) 46
Valoración de los controles 62
Análisis y Evaluación de los Controles para la Mitigación de los Riesgos. 66
3.2.3 Nivel de riesgo (Riesgo residual) 69
3.3 Monitoreo y revisión 71
Líneas de defensa frente al riesgo 71
Reporte Plan de tratamiento de riesgos 78
Indicadores - gestión del riesgo de seguridad digital 82
3.4 Seguimiento riesgos de corrupción 83
Comunicación y consulta 85
Información, comunicación y reporte 86

Referencias bibliográficas 87

Índice de tablas 88

Índice de esquemas 89

Listado de anexos 90

Introducción

El Consejo Asesor del Gobierno Nacional en materia de Control Interno consideró necesario unificar la metodología existente para la administración del riesgo de gestión y corrupción, con el fin de hacer más sencilla la utilización de esta herramienta gerencial para las entidades públicas y así, evitar duplicidades o reprocesos.

Igualmente, en respuesta a las conclusiones emitidas por la Contraloría General de la República que, producto de su labor como ente de control fiscal durante las últimas vigencias, encontró una marcada debilidad en el ejercicio del control interno efectuado por las entidades públicas, tanto del orden nacional como territorial. Es decir, se hizo evidente la importancia de fortalecer la metodología para diseñar y aplicar controles que permitan asegurar el logro de los objetivos.

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

El Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República y el Ministerio de Tecnologías de la Información y Comunicaciones presentan la “Guía para la Administración del Riesgo de Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas”, incluidos sus anexos, como una herramienta con enfoque preventivo, vanguardista y proactivo que permitirá el manejo del riesgo y corrupción, así como el control en todos los niveles de la entidad pública, brindando seguridad razonable frente al logro de sus objetivos.

Objetivos

- Unificar los lineamientos metodológicos en los aspectos comunes de las metodologías para la administración de todo tipo de riesgos y fortalecer el enfoque preventivo con el fin de facilitar a las entidades, la identificación y tratamiento de cada uno de ellos.

- Suministrar una metodología que permita a todas las entidades gestionar de manera efectiva los riesgos que afectan el logro de los objetivos estratégicos y de proceso.

- Ofrecer herramientas para identificar, analizar, evaluar los riesgos y determinar roles y responsabilidades de cada uno de los servidores de la entidad (Esquema de las Líneas de Defensa) en los riesgos de gestión y en los riesgos de corrupción el monitoreo y seguimiento.

- Suministrar lineamientos basados en una adecuada gestión del riesgo y control a los mismos, que permitan a la alta dirección de las entidades tener una seguridad razonable en el logro de sus objetivos.

Conceptos básicos relacionados con el riesgo

Riesgo de Gestión:

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

Riesgo de Seguridad Digital:

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

Riesgo de Corrupción:

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

Gestión del Riesgo:

Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

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.

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.

Probabilidad:

Se entiende como la posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de Frecuencia o Factibilidad.

Impacto:

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

Riesgo Inherente:

Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo Residual:

Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo.

Mapa de Riesgos:

Documento con la información resultante de la gestión del riesgo.

Fuente: ICONTEC INTERNACIONAL. (2011). *NORMA TÉCNICA COLOMBIANA NTC ISO 31000.* Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).
ICONTEC Internacional. (2011). NORMA TÉCNICA COLOMBIANA GTC 137. GESTIÓN DEL RIESGO. VOCABULARIO. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)
Presidencia de la República, Departamento Nacional de Planeación, Departamento Administrativo de la Función Pública. Estrategias para la construcción del plan anticorrupción y de atención al ciudadano. Bogotá. 2012. P8

Conceptos básicos relacionados con el riesgo

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.

Control:

Medida que modifica al riesgo (Procesos, políticas, dispositivos, prácticas u otras acciones)

Amenazas:

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

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:

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

Apetito al riesgo:

Magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

Tolerancia al riesgo:

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

Fuente: ICONTEC INTERNACIONAL. (2016). N*ORMA TÉCNICA COLOMBIANA NTC/ISO-IEC 27000*. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).
CONPES 3854 de 2016
Intosai: guía para las normas de control interno del sector público http://www.Intosai.org
Presidencia de la República, Departamento Nacional de Planeación, Departamento Administrativo de la Función Pública. Estrategias para la construcción del plan anticorrupción y atención al ciudadano. Bogotá. 2016. P.8

Antes de iniciar con la metodología

¿QUÉ ESTABLECE MIPG?

El numeral 2.2.1 “Política de Planeación institucional” de la dimensión “Direccionamiento Estratégico y Planeación” menciona que, para responder a la pregunta ¿Cuáles son las prioridades identificadas por la entidad y señaladas en los planes de desarrollo nacionales y territoriales?, se deben formular las metas de largo plazo, tangibles, medibles, audaces y coherentes con los problemas y necesidades que deben atender o satisfacer, evitando proposiciones genéricas que no permitan su cuantificación y definiendo los posibles riesgos asociados al cumplimiento de las prioridades.

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

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

Antes de iniciar con la metodología

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

CONOCIMIENTO DE LA ENTIDAD

PLANEACIÓN INSTITUCIONAL

Las estrategias de la entidad, generalmente se definen por parte de la Alta Dirección y obedecen a la razón de ser que desarrolla la misma, a los planes que traza el Sectorial al cual pertenece (plan estratégico sectorial), a políticas específicas que define el Gobierno nacional, departamental, o municipal enmarcadas dentro del Plan Nacional de Desarrollo, en este contexto la entidad define su planeación institucional.

La planeación institucional hace uso de los procesos estratégicos, misionales, de apoyo y de evaluación para materializarla o ejecutarla, por lo tanto la administración del riesgo no puede verse de forma aislada.

MODELO DE OPERACIÓN POR PROCESOS

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

MISIÓN

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

VISIÓN

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

ASPECTOS

CADENA DE VALOR:

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

MAPA O RED DE PROCESOS:

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

CARACTERIZACIÓN DE LOS PROCESOS:

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

OBJETIVOS ESTRATÉGICOS

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

Importante:

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

OBJETIVO DEL PROCESO:

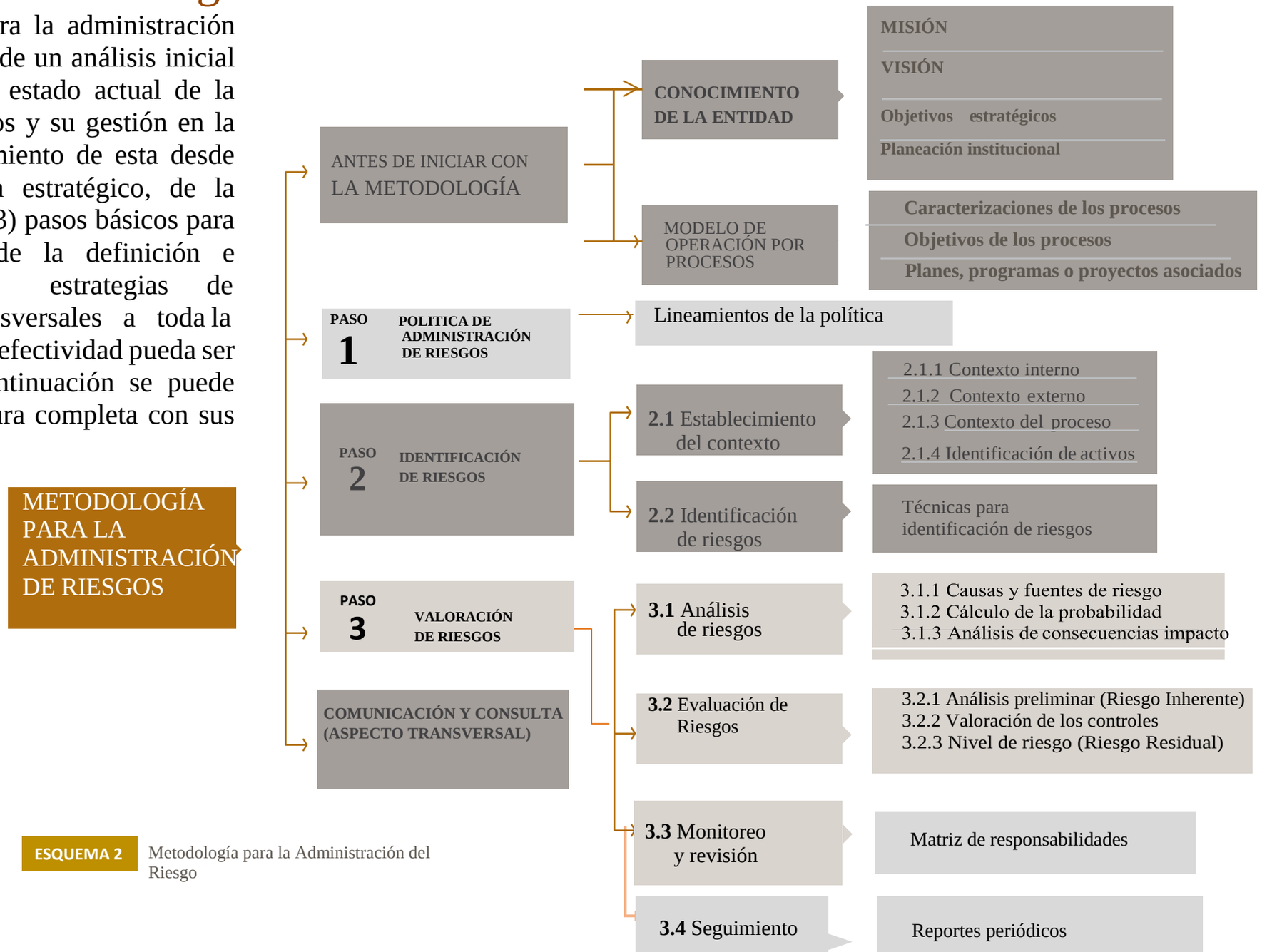
Son los resultados que se espera lograr para cumplir la misión y visión. Determina el cómo logro la política trazada y el aporte que se hace a los objetivos institucionales. Un objetivo es un enunciado que expresa una acción por lo tanto debe iniciarse con un verbo fuerte como: Establecer, identificar, recopilar, investigar, registrar, buscar.

Los objetivos deben ser: Medibles, realistas y se deben evitar frases subjetivas en su construcción.

ESQUEMA 1 Conocimiento y análisis de la entidad

Acerca de la metodología

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



ESQUEMA 2 Metodología para la Administración del Riesgo

Paso 1: Política de Administración de riesgos

Lineamientos de la Política

¿QUÉ ES?

Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo, (NTC ISO31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

¿QUÉ SE DEBE TENER EN CUENTA?

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

IMPORTANTE

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

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

La aceptación del riesgo puede ocurrir sin tratamiento del riesgo.
Los riesgos aceptados están sujetos a monitoreo.
Tenga en cuenta que los riesgos de corrupción son inaceptables

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

¿QUIÉN LA ESTABLECE?

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

¿QUÉ DEBE CONTENER?

Objetivo:	Se debe establecer su alineación con los objetivos estratégicos de la entidad y gestionar los riesgos a un nivel aceptable.
Alcance:	La administración de riesgos debe ser extensible y aplicable a todos los procesos de la entidad. En el caso de los riesgos de seguridad digital, estos se deben gestionar de acuerdo con los criterios diferenciales descritos en el Modelo de Seguridad y Privacidad de la Información (Ver Caja de Herramientas)
Niveles de aceptación al riesgo:	Decisión informada de tomar un riesgo particular. (NTC GTC137, Numeral 3.7.1.6) Para riesgo de corrupción es inaceptable.
Niveles para Calificar el Impacto:	Esta tabla de análisis variará de acuerdo con la complejidad de cada entidad, será necesario considerar el sector al que pertenece (riesgo de la operación, los recursos humanos y físicos con los que cuenta, su capacidad financiera, usuarios a los que atiende, entre otros aspectos). Ver Tabla Ilustrativa 3. Criterios para calificar el Impacto pág. 31
Tratamiento de riesgos:	Proceso para modificar el riesgo (NTC GTC137, Numeral 3.8.1.)
Periodicidad para el seguimiento de acuerdo al nivel de riesgo residual.	

ESQUEMA 3 Estructuración de la Política de Administración de Riesgos

La política de Administración del Riesgo puede adoptar la forma de un manual o guía de riesgos, donde se deben incluir mínimo los siguientes aspectos:

OBJETIVO:
Establece los principios básicos y el marco general de actuación para el control y la gestión de los riesgos de toda naturaleza a los que se enfrenta la entidad.

ALCANCE:
Establece el ámbito de aplicación de los lineamientos, el cual debe abarcar todos los procesos de la entidad. Se sugiere incluir a todas las seccionales o sedes que la entidad pueda tener en diferentes ubicaciones geográficas, con el fin de garantizar un adecuado conocimiento y control de los riesgos en todos los niveles organizacionales.

NIVELES DE ACEPTACIÓN DEL RIESGO O TOLERANCIA AL RIESGO:
Establece "los niveles aceptables de desviación relativa a la consecución de los objetivos" (NTC GTC 137 Numeral 3.7.16), los mismos están asociados a la estrategia de la entidad y pueden considerarse para cada uno de los procesos. Los riesgos de corrupción son inaceptables.

TÉRMINOS Y DEFINICIONES:
Relacionados con la administración del riesgo y con aquellos temas que el manual o guía desarrollen que sean relevantes para que todos los funcionarios entiendan su contenido y aplicación.

ESTRUCTURA PARA LA GESTIÓN DEL RIESGO:
Determina los siguientes aspectos:

- La metodología a utilizar.
- En caso de que la entidad haya dispuesto un software o herramienta para su desarrollo, deberá explicarse su manejo.
- Incluir los aspectos relevantes sobre los factores de riesgo estratégicos para la entidad, a partir de los cuales todos los procesos podrán iniciar con los análisis para el establecimiento del contexto.
- Incluir todos aquellos lineamientos que en cada paso de la metodología sean necesarios para que todos los procesos puedan iniciar con los análisis correspondientes.
- Incluir la periodicidad para el monitoreo y revisión de los riesgos, así como el seguimiento de los riesgos de corrupción,
- Incluir los niveles de riesgo aceptado para la entidad y su forma de manejo.
- Incluir la tabla de impactos institucional (Ver Tabla Ilustrativa 3. Niveles para calificar el impacto o consecuencias, pág. 31).
- Otros aspectos que la entidad considere necesarios deberán ser incluidos, con el fin de generar orientaciones claras y precisas para todos los funcionarios, de modo tal que la gestión del riesgo sea efectiva y esté articulada con la estrategia de la entidad.

IMPORTANTE
Los riesgos de corrupción no admiten aceptación del riesgo, siempre debe conducir a un tratamiento.
Todos los procesos son susceptibles frente a los riesgos de corrupción.

Paso 2: Identificación de riesgos

Análisis y definición de objetivos.

Le corresponde a la Segunda Línea de Defensa, el análisis de los objetivos de la entidad tanto del orden estratégico como de procesos

Análisis de objetivos estratégicos

La entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso.

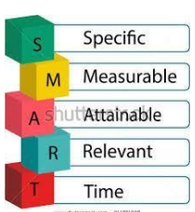
Es necesario revisar que los objetivos estratégicos se encuentren alineados con la Misión y la Visión Institucional, así como, analizar su adecuada formulación, es decir, que contengan las siguientes características mínimas: específico, medible, alcanzable, relevante y proyectado en el tiempo (SMART por sus siglas en inglés).

Análisis de los objetivos de proceso

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.

Ejemplo proceso contratación: “Adquirir con oportunidad y calidad técnica en no menos del 90%, los bienes y servicios requeridos por la entidad para su continua operación”.

Fuente: Comitte of Sponsoring Orgizations of the Treadway Commission COSO Marco Integrado, Componente Evaluación de Riesgos, Principio Pág. 73. 2013



IMPORTANTE

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

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

Paso 2: identificación de riesgos

IDENTIFICACIÓN DE RIESGOS

¿EN QUÉ CONSISTE?

En esta etapa se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas. (NTC ISO31000, Numeral 2.15).

ELEMENTOS QUE LO DESARROLLAN

ESTABLECIMIENTO DEL CONTEXTO

Definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo. (NTC ISO31000, Numeral 2.9). Se debe establecer el contexto interno, externo de la entidad y el contexto del proceso y sus activos de seguridad digital. Es posible hacer uso de herramientas y técnicas (consultar Anexo 2. Técnicas para Establecimiento del Contexto y Valoración del Riesgo).

IDENTIFICACIÓN DEL RIESGO

Se realiza determinando las causas, fuentes del riesgo y los eventos con base en el análisis de contexto para la entidad y del proceso, que pueden afectar el logro de los objetivos. Es importante centrarse en los riesgos más significativos para la entidad relacionados con los objetivos de los procesos, y los institucionales, en el caso de riesgos de corrupción se deben gestionar todos los riesgos, incluyendo los referentes a los trámites y servicios. (Ver anexo 3. Protocolo para la identificación de riesgos de corrupción asociados a la prestación de trámites y servicios)

IMPORTANTE

Debe analizarse en cada entidad el contexto particular al que se enfrentan los procesos ante los riesgos de corrupción, conforme a la misionalidad. Una buena práctica es analizar la gestión de riesgo de entidades semejantes.

ESQUEMA 4 Aspectos a desarrollar en la Identificación del Riesgo

2.1 Establecimiento del contexto

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

2.1.1 ESTABLECIMIENTO DEL CONTEXTO INTERNO

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

- Estructura organizacional
- Funciones y responsabilidades
- Políticas, objetivos y estrategias implementadas
- Recursos y conocimientos con que se cuenta (económicos, personas, procesos, sistemas, tecnología, información)
- Relaciones con las partes involucradas
- Cultura organizacional

2.1.2 ESTABLECIMIENTO DEL CONTEXTO EXTERNO

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

- Políticos
- Sociales y culturales
- Legales y reglamentarios
- Tecnológicos
- Financieros
- Económicos

ESTABLECIMIENTO DEL CONTEXTO

2.1.3 ESTABLECIMIENTO DEL CONTEXTO DEL PROCESO

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

- Objetivo del proceso
- Alcance del proceso
- Interrelación con otros procesos
- Procedimientos asociados
- Responsables del proceso
- Activos de seguridad digital del proceso

IMPORTANTE

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

ESQUEMA 5 Análisis del Contexto Externo, Interno y del Proceso

Tabla ilustrativa 1 - Factores para cada categoría del contexto

Contexto externo	**ECONÓMICOS:** disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	POLÍTICOS: cambios de gobierno, legislación, políticas públicas, regulación.
	SOCIALES: demografía, responsabilidad social, orden público.
	TECNOLÓGICOS: avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
	MEDIOAMBIENTALES: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	COMUNICACIÓN EXTERNA: mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad.
Contexto interno	**FINANCIEROS:** presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
	PERSONAL: competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
	PROCESOS: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	TECNOLOGÍA: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
	ESTRATÉGICOS: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
	COMUNICACIÓN INTERNA: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
Contexto del proceso	**DISEÑO DEL PROCESO:** claridad en la descripción del alcance y objetivo del proceso.
	INTERACCIONES CON OTROS PROCESOS: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	TRANSVERSALIDAD: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	PROCEDIMIENTOS ASOCIADOS: pertinencia en los procedimientos que desarrollan los procesos.
	RESPONSABLES DEL PROCESO: grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	COMUNICACIÓN ENTRE LOS PROCESOS: efectividad en los flujos de información determinados en la interacción de los procesos.
	ACTIVOS DE SEGURIDAD DIGITAL DEL PROCESO: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano. Ver conceptos básicos relacionados con el riesgo páginas 10 y 11.

IMPORTANTE

Los factores relacionados son una guía, cada entidad debe analizar los que considere de acuerdo con su complejidad, y al sector en el que se desenvuelve, entre otros aspectos e incluirlos como aspectos clave dentro de los lineamientos de la política de administración del riesgo

2.1.4 Identificación de activos de seguridad de la información

Identificación de activos

Le corresponde a la primera línea de defensa, realizar la identificación de activos en cada proceso.

IMPORTANTE
Todo lo que no está plenamente identificado, no está debidamente asegurado.

¿QUÉ SON LOS ACTIVOS?	¿POR QUÉ IDENTIFICAR 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.	De esta manera se puede determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, unos archivos, servidores web o aplicaciones claves para que la entidad pueda prestar sus servicios). Así la entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento tanto interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

¿CÓMO IDENTIFICAR LOS ACTIVOS?:

1. Paso 1. Listar los activos por cada proceso
2. Paso 2. Identificar el dueño de los activos
3. Paso 3. Clasificar los activos
4. Paso 4. Clasificar la información
5. Paso 5. Determinar la criticidad del activo
6. Paso 6. Identificar si existe infraestructura crítica cibernética

IMPORTANTE
Para realizar la identificación de activos (relacionados con seguridad digital), deberá remitirse a la sección **4.1.6 del Anexo 4 "Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas**", que hace parte de la presente guía.

2.2. Identificación de riesgos -técnicas para la identificación de riesgos.

Identificación de riesgos

La identificación del riesgo se realiza determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos. Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis del contexto externo, para ser tenidas en cuenta en el análisis y valoración del riesgo.

A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del Proceso o estratégicos.

Las preguntas claves para la identificación del riesgo permiten determinar:

¿QUÉ PUEDE SUCEDER? Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.

¿CÓMO PUEDE SUCEDER? Establecer las causas a partir de los factores determinados en el contexto

¿CUÁNDO PUEDE SUCEDER? Determinar de acuerdo al desarrollo del proceso

¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN? Determinar los posibles efectos por la materialización del riesgo

Preguntas clave para la identificación de riesgos

¿QUÉ PUEDE SUCEDER?

¿CÓMO PUEDE SUCEDER?

¿CUÁNDO PUEDE SUCEDER?

¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN?

IMPORTANTE
En la descripción del riesgo se deben tener en cuenta las respuestas a las preguntas arriba mencionadas.

ELABORACIÓN: Departamento Administrativo de la Función Pública

2.2 Identificación de riesgos -técnicas para la identificación de riesgos

Riesgo de corrupción

Definición de riesgo de corrupción:

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.

"*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 concurran los **componentes de su definición**, así:

Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.

Fuente: Secretaría de Transparencia de la Presidencia de la República

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.
Si en la descripción del riesgo, las casillas son contestadas todas afirmativamente, se trata de un riesgo de corrupción, así:

Matriz definición del riesgo de corrupción

Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado
Posibilidad de recibir o solicitar cualquier dadiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato	X	X	X	X

Fuente: Secretaría de Transparencia de la Presidencia de la República

Generalidades riesgos de corrupción

- Entidades encargadas de gestionar el riesgo: lo deben adelantar las entidades del orden nacional, departamental y municipal.
- Se elabora anualmente por cada responsable de los procesos al interior de las entidades, junto con su equipo.
- Consolidación: la oficina de planeación o quien haga sus veces, o a la de dependencia encargada de gestionar el riesgo le corresponde liderar el proceso de administración de estos. Adicionalmente, esta misma oficina será la encargada de consolidar el mapa de riesgos de corrupción.
- Publicación del mapa de riesgos de corrupción: se debe publicar en la página web de la entidad, en la sección particular de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.

La publicación será parcial, y fundamentada en la elaboración del Índice de Información Clasificada y Reservada. En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014)

En este caso, se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora no se hace visible en la publicación.

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

- **Socialización:** Los servidores públicos y contratistas de la entidad deben conocer su contenido antes de su publicación. Para lograr este propósito la oficina de planeación o quien haga sus veces o la de gestión del riesgo, deberá diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del Mapa de Riesgos de Corrupción.

Así mismo, dicha oficina adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de corrupción. Deberá dejarse la evidencia del proceso de socialización y publicarse sus resultados.

- **Ajustes y modificaciones:** 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 deberá dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

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

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

EJEMPLO

Información anonimizada

INFORMACIÓN ANONIMIZADA

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

IMPORTANTE
Tenga en cuenta que la Información clasificada o reservada la señala la ley, un decreto con fuerza de ley o convenio internacional ratificado por el Congreso o en la Constitución.
Una resolución no puede calificar la información como clasificada o reservada.

2.2 Identificación de riesgos

EJEMPLO REDACCIÓN DE RIESGOS

Evitar iniciar con palabras negativas como: “No…” “Que no…”, o con palabras que denoten un factor de riesgo (causa) tales como: “ausencia de”, “falta de”, “poco(a)”, “escaso(a)”, “insuficiente”, “deficiente”, “debilidades en…”

Objetivo del proceso: si el objetivo del proceso es “Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación”
Un **riesgo puede ser:** “Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad”.

Generar al lector o escucha, la imagen del evento como si ya estuviera sucediendo.

Redacción del riesgo

Ejemplo riesgo de corrupción:
Posibilidad de recibir o solicitar cualquier dadiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.

ESQUEMA 6 Redacción del riesgo

Fuente: Departamento Administrativo de la Función Pública

Importante
Pregúntese si el riesgo de gestión identificado está relacionado directamente con las características del objetivo. Si la respuesta es “no” este puede ser la causa o la consecuencia.

TIPOLOGÍA DE RIESGOS

Riesgos estratégicos: posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.

Riesgos gerenciales: posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.

Riesgos operativos: posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.

Riesgos financieros: posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.

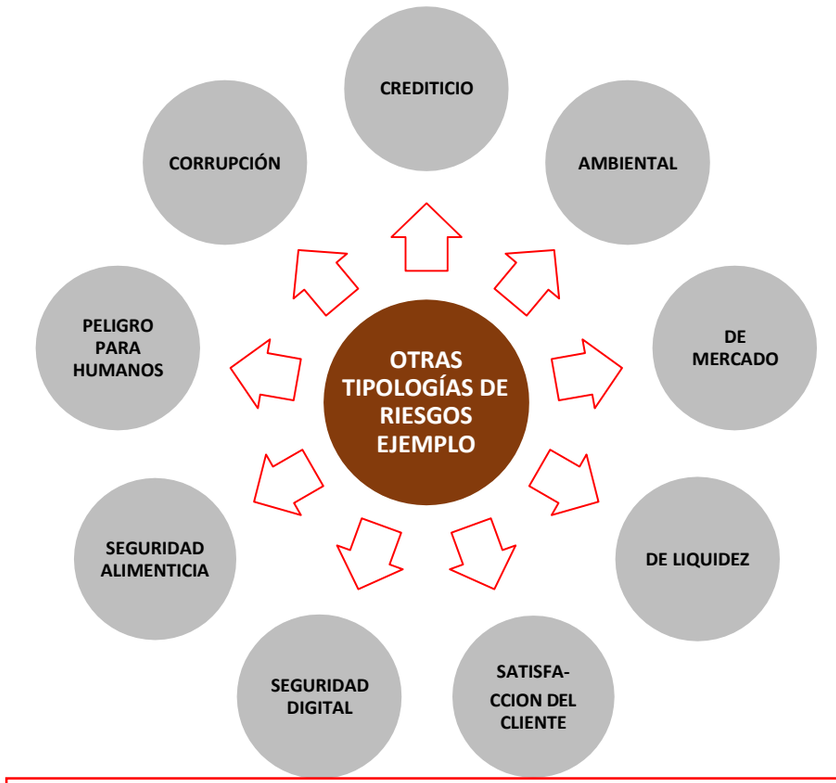
Riesgos tecnológicos: posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

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

Riesgo de imagen o reputacional: posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización, ante sus clientes y partes interesadas.

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

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



IMPORTANTE

La tipología de riesgos depende de la misión de cada entidad, de las normas que regulan su operación, de los sistemas de gestión que implemente, entre otros aspectos. Los riesgos de corrupción, siempre deben gestionarse.

Fuente: Departamento Administrativo de la Función Pública

Ejemplos descripción del riesgo

Formato de descripción del riesgo de gestión

RIESGO	DESCRIPCIÓN	TIPO	CAUSAS	CONSECUENCIAS
"Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad	La combinación de factores como, insuficiente capacitación del personal de contratos, cambios en la regulación contractual, inadecuadas políticas de operación y carencia de controles en el procedimiento de contratación, pueden ocasionar inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad, repercutiendo en la continuidad de su operación.	Operativo	Carencia de controles en el procedimiento de contratación Insuficiente capacitación del personal de contratos Desconocimiento de los cambios en la regulación contractual Inadecuadas políticas de operación	1. Parálisis en los procesos 2. Incumplimiento en la entrega de bienes y servicios a los grupos de valor 3. Demandas y demás acciones jurídicas 4. Detrimento de la imagen de la entidad ante sus grupos de valor 5. Investigaciones disciplinarias

IMPORTANTE

La descripción del riesgo consolida los pasos vistos en la metodología de gestión del riesgo y facilita su análisis.

Fuente: Departamento Administrativo de la Función Pública

Formato de descripción del riesgo de corrupción

RIESGO	DESCRIPCIÓN	TIPO	CAUSAS	CONSECUENCIAS
Posibilidad de recibir o solicitar cualquier dadiva o beneficio a nombre propio o de terceros con el fin celebrar un contrato.	Situaciones como: debilidades en la etapa de la planeación del contrato, la excesiva discrecionalidad, las presiones indebidas, la carencia de controles, la falta de conocimiento y/o experiencia, sumados a la falta de integridad pueden generar un riesgo de corrupción en la contratación, como por ejemplo "Exigencias de condiciones en los procesos de selección que solo cumple un determinado proponente".	Corrupción	Debilidades en la etapa de planeación, que faciliten la inclusión en los estudios previos, y/o en los pliegos de condiciones de requisitos orientados a favorecer a un proponente. Presiones indebidas Carencia de controles en el procedimiento de contratación Falta de conocimiento y/o experiencia del personal que maneja la contratación Excesiva discrecionalidad Adendas que modifican las condiciones generales del proceso de contratación para favorecer a un proponente	1. Pérdida de la imagen institucional 2. Demandas contra el estado 3. Pérdida de confianza en lo público 4. Investigaciones penales, disciplinarias y fiscales 5. Detrimento patrimonial 6. Obras inconclusas 7. Mala calidad de las obras 8. Enriquecimiento ilícito de contratistas y/o servidores públicos

IMPORTANTE

En la descripción de los riesgos de corrupción deben concurrir **TODOS** los componentes de su definición:

Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.

Fuente: Secretaría de Transparencia de la Presidencia de la República

Formato de descripción del riesgo de seguridad digital

Los riesgos de seguridad digital se basan en la afectación de 3 criterios en un activo o un grupo de activos dentro del proceso:

"Integridad, confidencialidad o disponibilidad"

Para el riesgo identificado 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

Seleccionar las **vulnerabilidades** asociadas a la **amenaza** identificada

ACTIVO	RIESGO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/VULNERABILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada causando la pérdida de la integridad de la base de datos de nómina.	Modificación no autorizada	Seguridad Digital	Falta de políticas de seguridad digital	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
					Ausencia de políticas de control de acceso	
					Contraseñas sin protección	
					Autenticación débil	

IMPORTANTE:

- Existirían tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.
- Los catálogos de amenazas y vulnerabilidades comunes se encuentran en la sección 4.1.7 del Anexo "Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas", el cual hace parte de la presente guía.
- NOTA 1: Tener en cuenta que la agrupación de activos debe ser del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.
- NOTA 2: Las entidades públicas deben incluir como mínimo los procesos y procedimientos establecidos en esta guía. Aquellas entidades que ya estén adelantando procesos relacionados con la gestión de este tipo de riesgo y que incorporen al menos lo dispuesto en estas guías podrán continuar bajo sus procedimientos. Si alguno de los aspectos contenidos en esta guía no está contemplado, deberá ser agregado a lo que manejan actualmente.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Paso 3. Valoración de riesgos

VALORACIÓN DE RIESGOS

¿En qué consiste?

Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

Elementos que lo desarrollan

3.1. Análisis de riesgos

Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

Aspectos a tener en cuenta

- Tabla para determinar probabilidad
- Tablas (s) para determinar el impacto o consecuencias (de acuerdo con la política de riesgos institucional)
- Matriz de Evaluación de riesgos

3.2. Evaluación de riesgos

Se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL).

Elaboración del mapa de riesgos

Análisis y evaluación de controles

Para el análisis de los controles se sugiere el uso de la matriz desarrollada para su calificación (ver Tabla Ilustrativa 6, pág. 63).

ESQUEMA 7 Valoración de Riesgos

3.1 Análisis de riesgos

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

3.1.1. ANÁLISIS DE CAUSAS

Los objetivos estratégicos y de proceso se desarrollan a través de actividades, pero no todas tienen la misma importancia, por tanto se debe establecer cuáles de ellas contribuyen mayormente al logro de los objetivos y estas son las actividades críticas o factores claves de éxito; estos factores se deben tener en cuenta al identificar las causas que originan la materialización de los riesgos. (Ver Anexo 5 Análisis y priorización de causas)

3.1.2 DETERMINAR PROBABILIDAD

Por PROBABILIDAD se entiende la posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de Frecuencia o Factibilidad.

Bajo el criterio de FRECUENCIA se analizan el # 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.

Bajo el criterio de FACTIBILIDAD se analiza 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 se dé.

Para su determinación se utiliza la tabla de probabilidad (ver Tabla Ilustrativa 2 - Probabilidad que se encuentra en la página 30)

PASOS CLAVES PARA EL ANALISIS DE RIESGO

ESTIMAR EL NIVEL DEL RIESGO INICIAL - INHERENTE

Se logra a través de la determinación de la probabilidad y el impacto que puede causar la materialización del riesgo, a través de las tablas establecidas en cada caso

Para su determinación se utiliza la Matriz de Calificación del Riesgo

3.1.3 DETERMINAR CONSECUENCIAS O NIVEL DE IMPACTO

Por IMPACTO se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Se tienen en cuenta las consecuencias potenciales establecidas en el paso 2 de Identificación del riesgo

Para su determinación se utiliza la tabla de niveles de impacto establecida en la Política de Riesgos (ver Tabla Ilustrativa 3 página 31).

ESQUEMA 8 Análisis de Riesgos

3.1.2. Cálculo de la probabilidad e impacto

Análisis de la Probabilidad

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda.

Tabla ilustrativa 2 Criterios parar 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.

En este paso los integrantes del equipo de trabajo, a menos que posean datos históricos sobre el número de eventos que se hayan materializado en un periodo de tiempo, deben calificar en privado, (para no generar polémica o influencia en el criterio de los otros), el nivel de probabilidad en términos de factibilidad, de forma similar a la priorización de causas, para definir el nivel de probabilidad de cada riesgo, de acuerdo con la tabla de criterios establecida.

Matriz de priorización probabilidad

Nr o	RIESGO	P1	P 2	P 3	P4	P5	P6	Tot	Prom
1	Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad	5	4	3	5	3	4	24	4 **PROBABLE**
2	Otros riesgos identificados								
3	Otros riesgos identificados								

Convenciones:

Nro: Número consecutivo del riesgo - P1: Participante 1 P… - Tot: Total puntaje -

Prom.: Promedio

IMPORTANTE

El análisis de frecuencia deberá ajustarse dependiendo del proceso y de la disponibilidad de datos históricos sobre el evento o riesgo identificado. En caso de no contar con datos históricos, se trabajará de acuerdo con la experiencia de los responsables que desarrollan el proceso y de sus factores internos y externos.

Tabla ilustrativa 3. Criterios para calificar el Impacto – riesgos de gestión

Nivel	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
CATASTRÓFICO	- Impacto que afecte la ejecución presupuestal en un valor ≥50% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de Información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MA YOR	- Impacto que afecte la ejecución presupuestal en un valor ≥20% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
MODERADO	- Impacto que afecte la ejecución presupuestal en un valor ≥5% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
MENOR	- Impacto que afecte la ejecución presupuestal en un valor ≥1% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por algunas horas. - Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
INSIGNIFICAN TE	- Impacto que afecte la ejecución presupuestal en un valor ≥0,5% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad.	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

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

IMPORTANTE
Cada entidad deberá adaptar los criterios de acuerdo a su complejidad.

Tabla ilustrativa 4. Criterios para calificar el Impacto – riesgos de seguridad digital

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
INSIGNIFICANTE	**1**	Afectación ≥X% de la **población** Afectación ≥X% del **presupuesto** anual de la entidad No hay **Afectación medioambiental**	Sin afectación de la integridad Sin afectación de la disponibilidad Sin afectación de la confidencialidad
MENOR	**2**	Afectación ≥X% de la población Afectación ≥X% del presupuesto anual de la entidad Afectación leve del Medio Ambiente requiere de ≥X días de recuperación	Afectación leve de la integridad Afectación leve de la disponibilidad Afectación leve de la confidencialidad
MODERADO	**3**	Afectación ≥X% de la población Afectación ≥X% del presupuesto anual de la entidad Afectación leve del Medio Ambiente requiere de ≥X semanas de recuperación	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros
MAYOR	**4**	Afectación ≥X% de la población Afectación ≥X% del presupuesto anual de la entidad Afectación importante del Medio Ambiente que requiere de ≥X meses de recuperación	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros
CATASTRÓFICO	**5**	Afectación ≥X% de la población Afectación ≥X% del presupuesto anual de la entidad Afectación muy grave del Medio Ambiente que requiere de ≥X años de recuperación	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros Afectación muy grave confidencialidad de la información debido al interés particular de los empleados y terceros

FUENTE: Ministerio de Tecnologías de la Información y las Comunicaciones

IMPORTANTE

Cada entidad deberá adaptar los criterios a su realidad.

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

Las variables de confidencialidad, integridad y disponibilidad se definen de acuerdo con el Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.

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

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

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

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

Extremo	
Alto	
Moderado	
Bajo	

FUENTE: Ministerio de Tecnologías de la Información y las Comunicaciones

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

3.1.3 Análisis del impacto

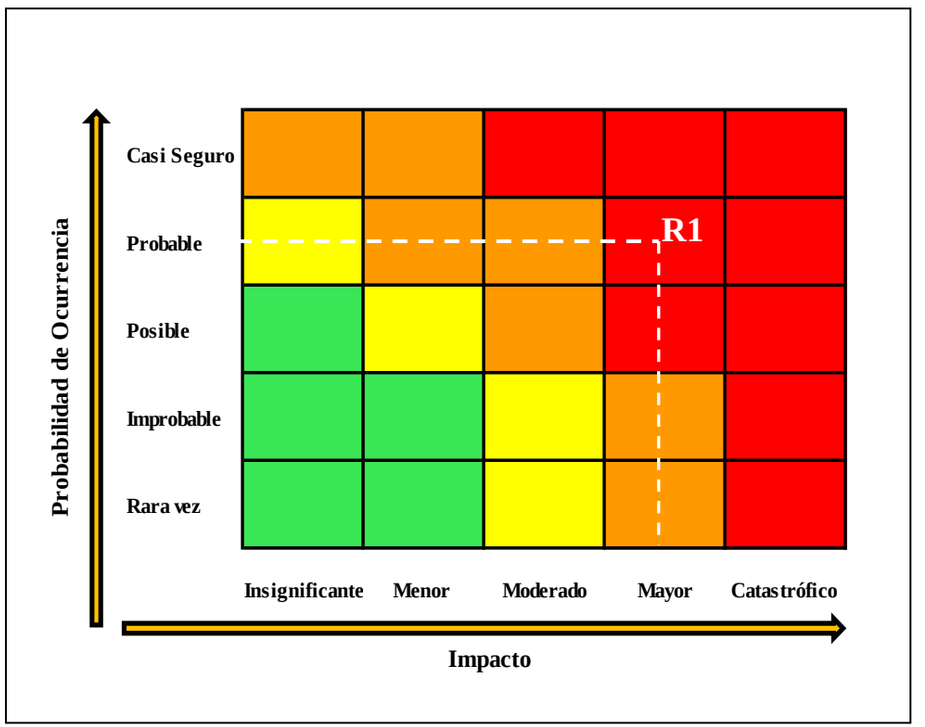
El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo. Para el ejemplo que venimos explicando, el impacto fue identificado como **mayor** por cuanto genera interrupción de las operaciones por más de dos días.

Mapa de calor

Se toma la calificación de probabilidad (resultante de la tabla Matriz de priorización de probabilidad), en el ejemplo: **probable** y la calificación de impacto, para nuestro ejemplo: **mayor;** ubique la calificación de probabilidad en la fila y la de impacto en la columnas correspondientes, establezca el punto de intercepción de las dos y este punto corresponderá al nivel de riesgo, que para el ejemplo es nivel extremo – color rojo (**R1**) determinando así el riesgo inherente.

IMPORTANTE
Matriz de criticidad de 5x5 significa que para ubicar el nivel de riesgo se cuenta con 5 niveles en probabilidad y 5 niveles en impacto.

Mapa de calor (riesgo inherente)



Fuente: Adaptado de Instituto de Auditores de Auditores Internos. COSO ERM. 2017.

Tabla ilustrativa 5. Criterios para calificar el Impacto - Riesgos de Corrupción

Nro	PREGUNTA: Si el riesgo de corrupción se materializa podría...	Respuesta	
		SI	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 o servicios o los 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 UNO 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 de la Presidencia de la República

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

3.1.3 Análisis del impacto en riesgos de corrupción

Para los riesgos de corrupción, **el análisis de impacto** se realizará teniendo en cuenta solamente los niveles moderado, mayor y catastrófico, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que si aplican para los demás riesgos.

De acuerdo a la tabla de criterios para calificar el impacto de la página anterior, nuestro ejemplo tiene en nivel de impacto **MAYOR**. La **probabilidad** de los riesgos de corrupción se califica con los mismos cinco niveles de los demás riesgos.

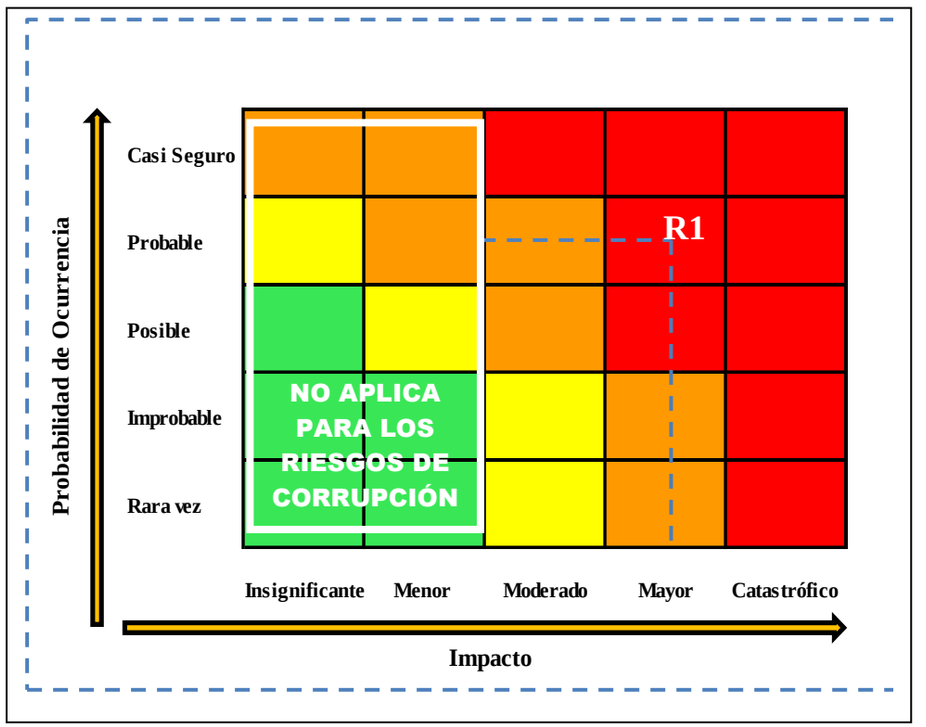
Por ultimo ubique en el mapa de calor el punto de intercepción resultante de la probabilidad y el impacto para establecer el nivel del riego inherente, para el ejemplo corresponde a: **EXTREMO**

R1

Importante

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

Mapa de calor (riesgo inherente)



Fuente: Secretaría de Transparencia de la Presidencia de la República

Tratamiento del riesgo

¿Qué es tratamiento del riesgo?

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de Corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto del riesgo, y la relación costo beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo, derive en un riesgo residual que supere los niveles aceptables para la dirección, se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción, la respuesta será evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Tratamiento del Riesgo

Aceptar el riesgo.

No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado)

Reducir el riesgo

Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.

Evitar el riesgo

Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.

Compartir el riesgo

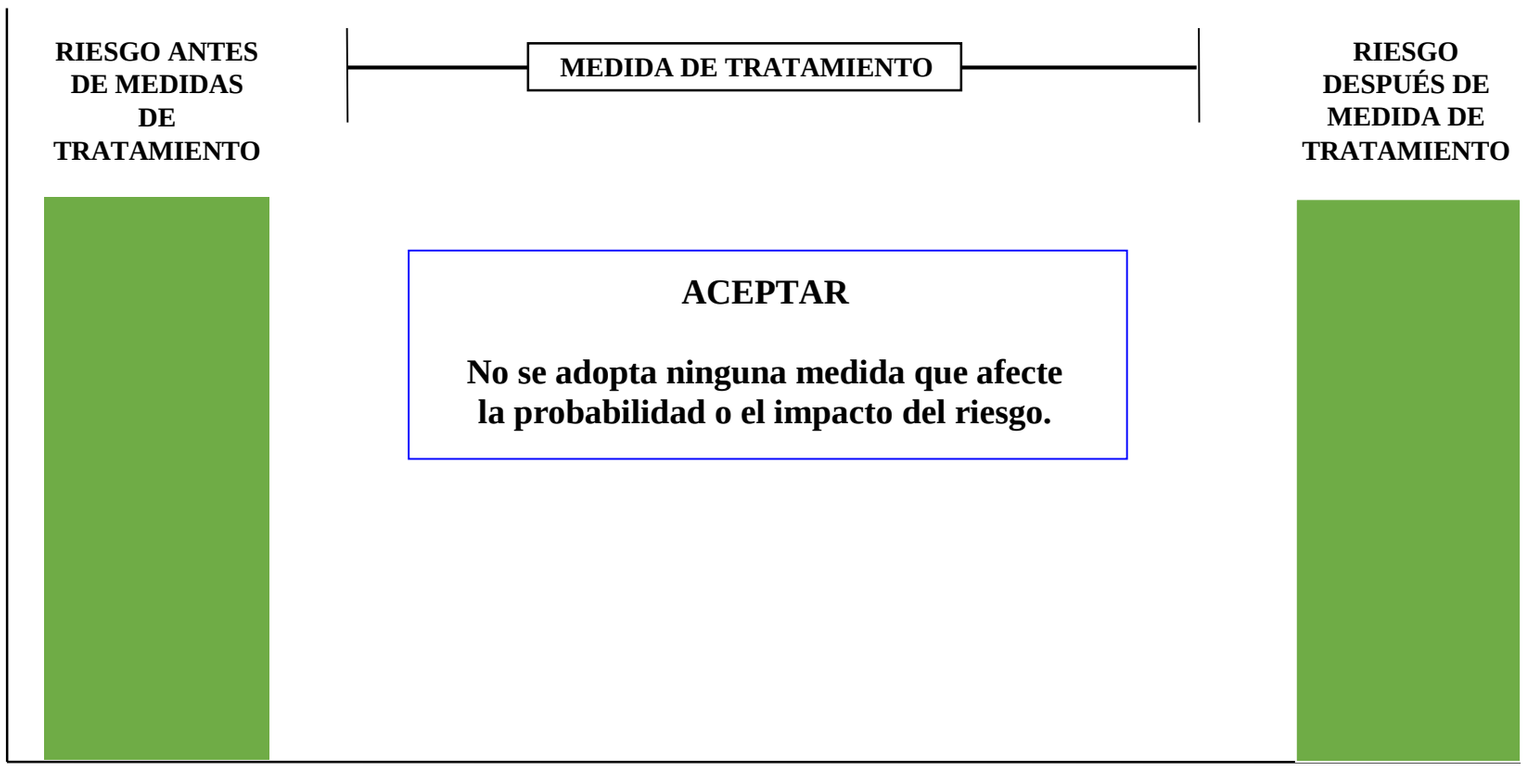
Se reduce la probabilidad o el impacto del riesgo, transfiriendo o compartiendo una parte del riesgo. Los riesgos de corrupción, se pueden compartir pero no se puede transferir su responsabilidad.

Aceptar el riesgo

Si el nivel de riesgo cumple con los criterios de aceptación de riesgo, no es necesario poner controles y el riesgo puede ser aceptado.

Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo.

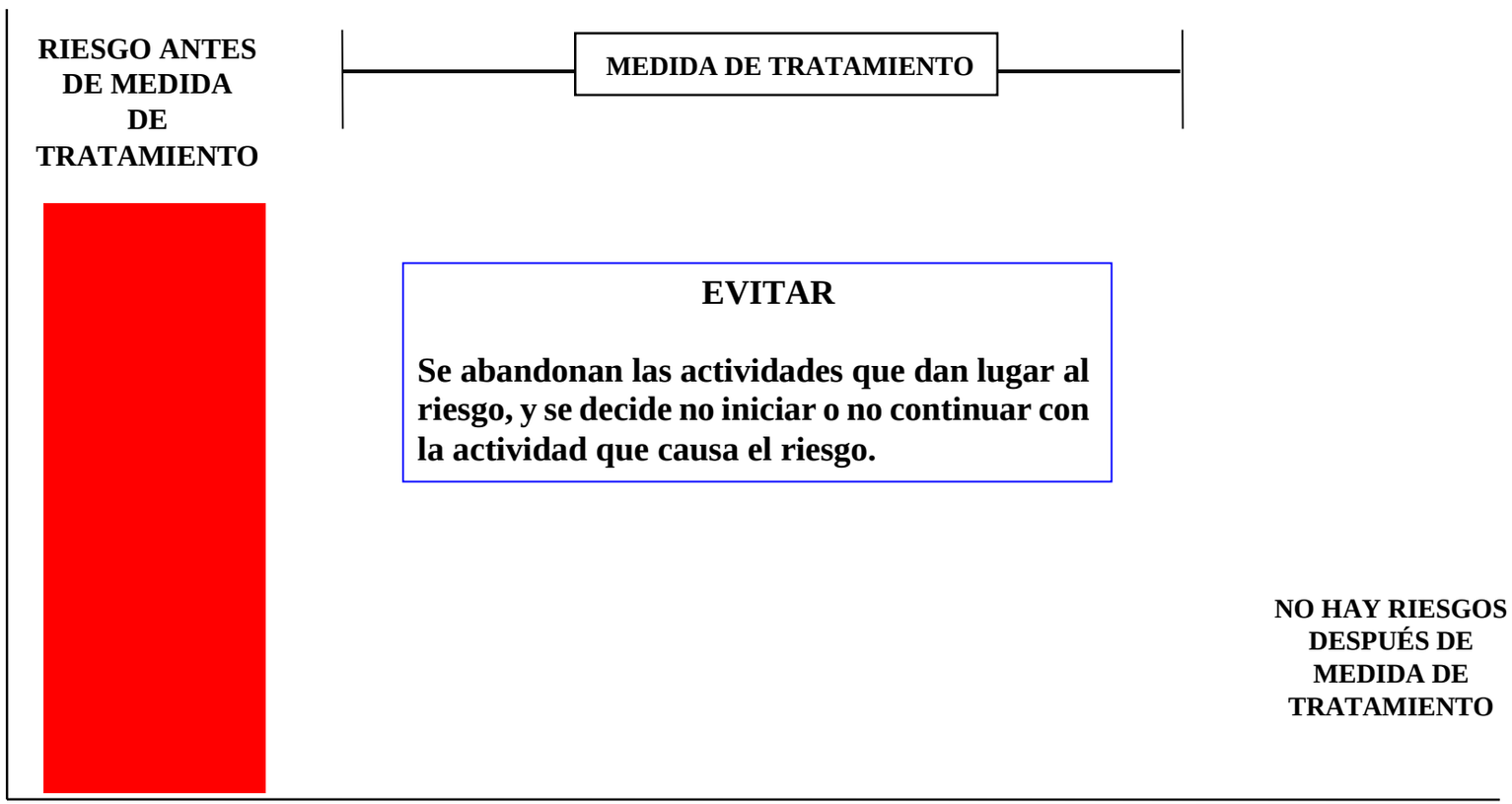
IMPORTANTE
En el caso de riesgos de corrupción, estos no pueden ser aceptados.



La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

Evitar el riesgo

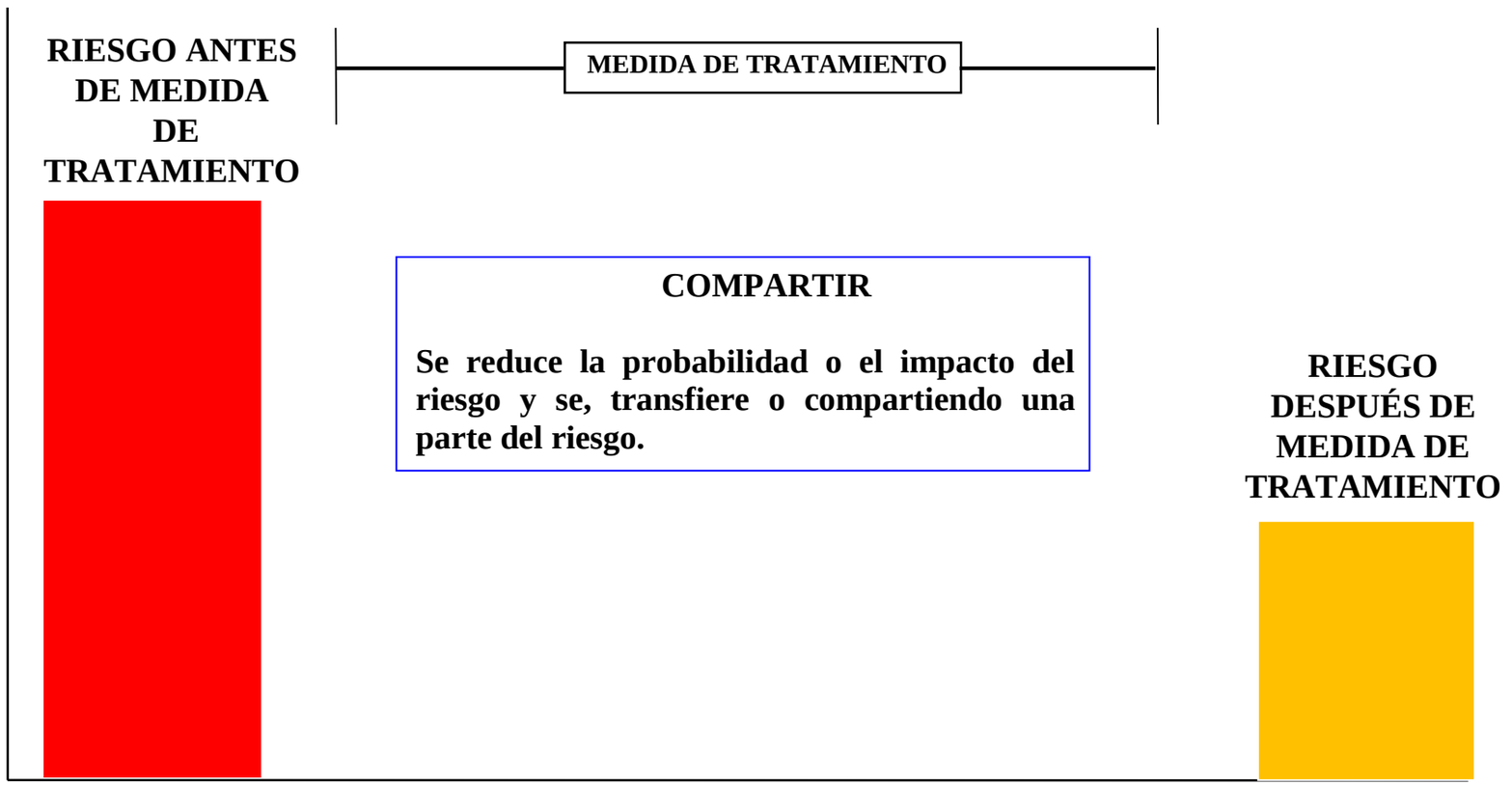
Cuando los escenarios de riesgo identificado se consideran demasiado extremos, se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o conjunto de actividades.



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

Compartir el riesgo

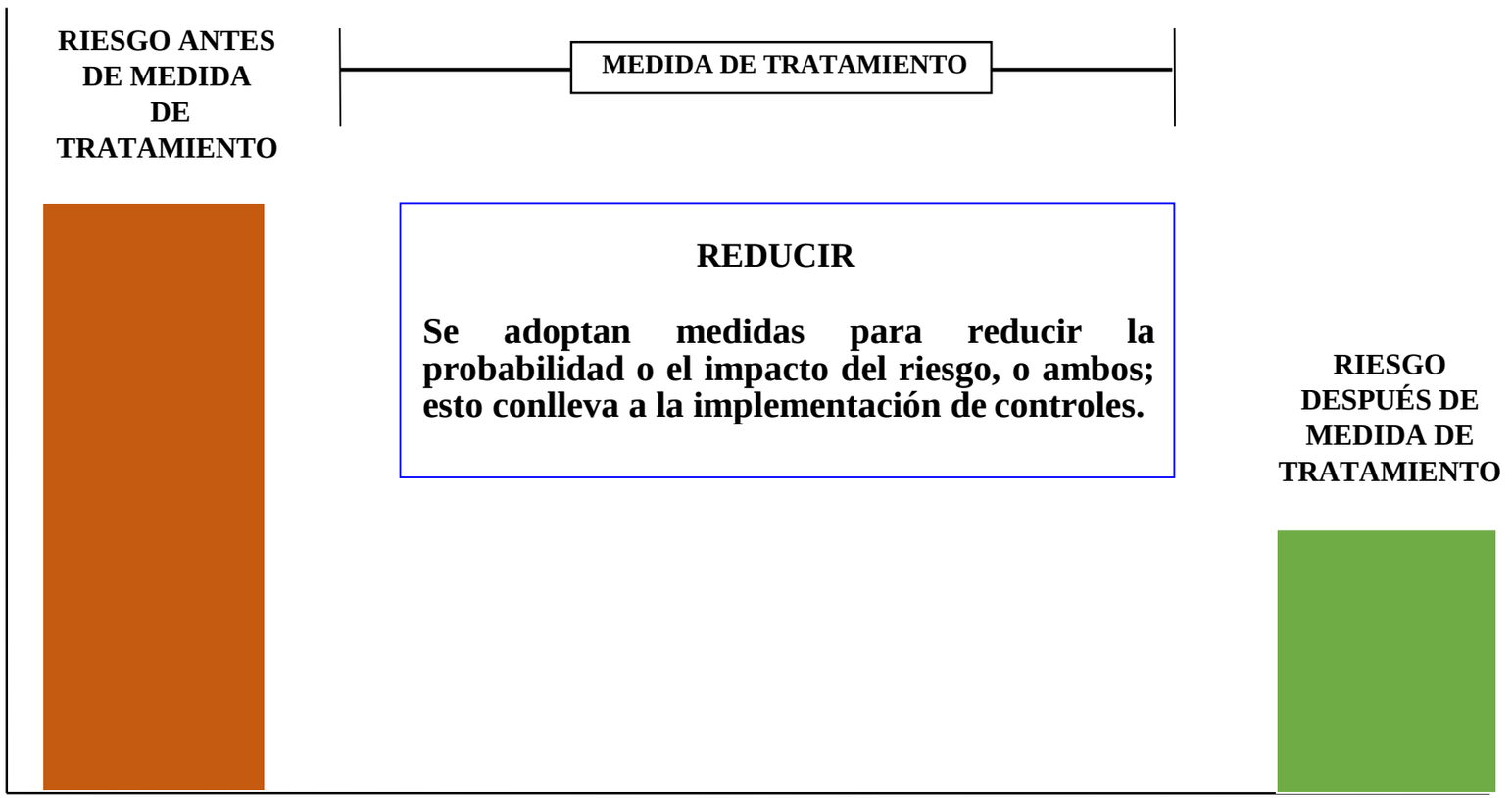
Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable, o se carece de conocimientos necesarios para gestionarlo, el riesgo puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad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



Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización. Estos mecanismos de transferencia de riesgos deberían estar formalizados a través de un acuerdo contractual.

Reducir el riesgo

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



Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado, logre la reducción prevista sobre el riesgo.
Para mitigar/tratar los riesgos de seguridad digital, se deben emplear como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, los cuales igualmente se encuentran en el Anexo 4. “Lineamientos para la gestión del riesgo de seguridad digital de la presente guía”

Tratamiento del riesgo – Rol de la primera línea de defensa

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

¿Qué son actividades de control?

Son las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

ACTIVIDADES DE CONTROL DOCUMENTADAS EN

POLÍTICAS

Las políticas establecen las líneas generales del control interno [1]

PROCEDIMIENTOS

Los procedimientos son los que llevan dichas políticas a la práctica

IMPORTANTE

- Una política por si sola no es un control.
- Los controles se despliegan a través de los procedimientos documentados.
- La actividad de control debe por si sola mitigar o tratar la causa del riesgo y ejecutarse como parte del día a día de las operaciones.
- Para mitigar/tratar los riesgos de seguridad digital, se deben emplear como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, los cuales igualmente se encuentran en el Anexo 3. "Lineamientos para la gestión del riesgo de seguridad digital" de la presente guía

1. Control Interno Marco Integrado – COSO 2013 - actividades de control.

EJEMPLO

La política establece que para los contratos de bienes y servicios se debe tener tres cotizaciones. El procedimiento será la revisión que valide que la política se está cumpliendo, dejando claras las actividades y responsabilidades que asume el personal que lleva a cabo la actividad de control y asegura que existan las tres cotizaciones.

Tanto la política como el procedimiento deben estar documentados. Esto contribuye a que las actividades de control, sean parte del día a día de las operaciones de la entidad.

Las actividades de control, independiente de la tipología de riesgo a tratar, deben tener una adecuada combinación para prevenir que la situación de riesgo se origine, o en caso de que la situación de riesgos se presente, esta sea detectada de manera oportuna.

CLASIFICACIÓN DE LAS ACTIVIDADES DE CONTROL

CONTROLES PREVENTIVOS

Controles que están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos.

CONTROLES DETECTIVOS

Controles que están diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.

Revisión al cumplimiento de los requisitos contractuales, en el proceso de selección del contratista o proveedor.

EJEMPLO

Realizar una conciliación bancaria, para verificar que los saldos en libros corresponden con los saldos en Bancos.

IMPORTANTE
Se deben seleccionar actividades de control preventivas y detectivas que por sí solas ayuden a la mitigación de las causas que originan los riesgos.

3.2.1. Análisis preliminar (riesgo inherente)

Al momento de definir las actividades de control por parte de la Primera Línea de Defensa, es importante considerar que los controles estén bien diseñados, es decir, que estos mitigan las causas que hacen que el riesgo se materialice.

RIESGO ANTES DE CONTROLES

Se identifican los riesgos inherentes o subyacentes que pueden afectar el cumplimiento de los objetivos estratégicos y de proceso.

CAUSAS O FALLAS

Se identifican las causas o fallas que pueden dar origen a la materialización del riesgo

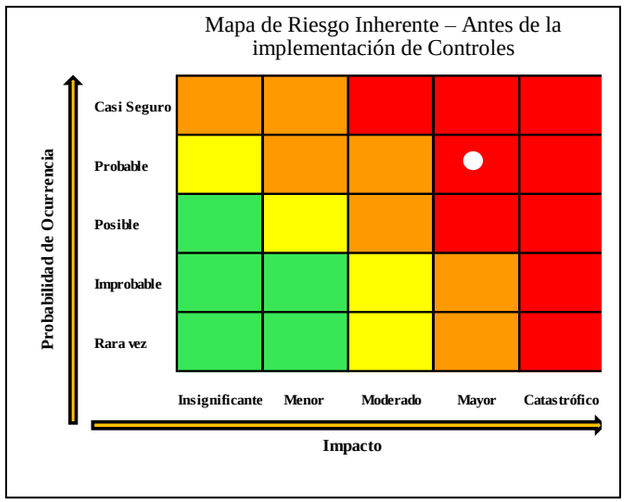
CONTROLES

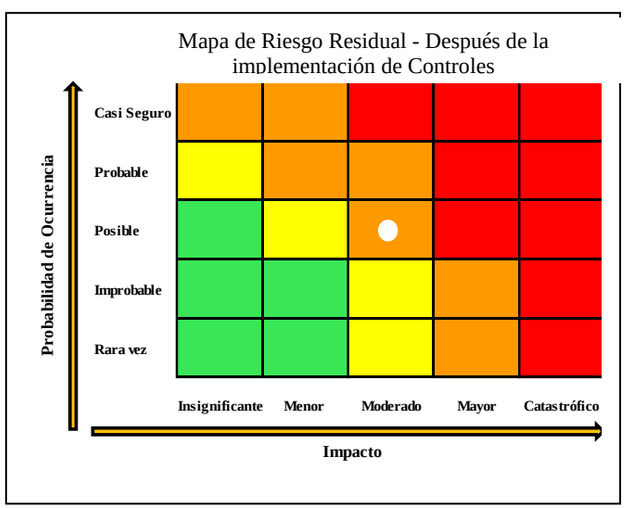
Para cada causa se identifica el control o controles.

RIESGO DESPUÉS DE CONTROLES

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

ESQUEMA 9 Riesgo antes y después de controles





IMPORTANTE

- Para cada causa debe existir un control.
- Las causas se deben trabajar de manera separada (no se deben combinar en una misma columna o renglón).
- Un control puede ser tan eficiente que me ayude a mitigar varias causas, en estos casos se repite el control, asociado de manera independiente a la causa especifica.

3.2.2 Valoración de los controles – diseño de controles

Antes de valorar los controles, es necesario conocer cómo se diseña un control, para lo cual daremos respuesta a las siguientes interrogantes:

¿Cómo defino o establezco un control para que en su diseño, mitigue de manera adecuada el riesgo?

Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo, se debe considerar desde la redacción del mismo, las siguientes variables

VARIABLES A EVALUAR PARA EL ADECUADO DISEÑO DE CONTROLES

PASO 1 — **Debe tener definido el responsable de realizar la actividad de control.**

PASO 2 — **Debe tener una periodicidad definida para su ejecución.**

PASO 3 — **Debe indicar cuál es el propósito del control.**

PASO 4 — **Debe establecer el cómo se realiza la actividad de control.**

PASO 5 — **Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.**

PASO 6 — **Debe dejar evidencia de la ejecución del control.**

IMPORTANTE
Las acciones de tratamiento se agrupan en:
Disminuir la probabilidad: acciones encaminadas a gestionar las causas del riesgo
Disminuir el impacto: acciones encaminadas a disminuir las consecuencias del riesgo

ESQUEMA 10 Pasos para diseñar un control

¿Cómo defino o establezco un control que mitigue el riesgo?

Al momento de definir si un control o controles mitigan de manera adecuada el riesgo, se debe considerar desde la redacción del mismo, las siguientes variables

VARIABLES A EVALUAR PARA EL ADECUADO DISEÑO DE CONTROLES

PASO 1	**Debe tener definido el responsable de la actividad de control.**

Responsable

Persona asignada de ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas. Si ese responsable quisiera hacer algo indebido, por sí solo, no lo podría hacer. Si la respuesta es que cumple con esto, quiere decir que el control está bien diseñado, si la respuesta es que no cumple, tenemos que identificar la situación y mejorar el diseño del control con relación a la persona responsable de su ejecución.

EJEMPLO

Cuando un control se hace de manera manual (ejecutado por personas) es importante establecer el cargo responsable de su realización.

Cuando el control lo hace un sistema o una aplicación de manera automática a través de un sistema programado, es importante establecer como responsable de ejecutar el control, el sistema o aplicación.

PASO 1 **Debe tener definido el responsable de la actividad de control.**

- **El profesional de contratación.**
- **El auxiliar de cartera.**
- **El coordinador de operaciones.**
- **La coordinadora de nómina.**

- **El sistema SAP.**
- **El aplicativo de nómina.**
- **El aplicativo de contratación.**
- **El aplicativo de activos fijos.**

IMPORTANTE

- El control debe iniciar con un cargo responsable o un sistema o aplicación.
- Evitar colocar áreas de manera general o nombres de personas.
- El control debe estar asignado a un cargo específico.

¿Cómo defino o establezco un control que mitigue el riesgo?

Al momento de definir si un control o controles mitigan de manera adecuada el riesgo, se debe considerar desde la redacción del mismo, las siguientes variables

VARIABLES A EVALUAR PARA EL ADECUADO DISEÑO DE CONTROLES

PASO 2 **Debe tener una periodicidad definida para su ejecución.**

Periodicidad

El control debe tener una periodicidad específica para su realización, (diario, mensual, trimestral, anual) etc. y su ejecución debe ser consistente y oportuna para la mitigación del riesgo. Por lo que en la periodicidad se debe evaluar si este previene o detecta de manera oportuna el riesgo. Una vez definido el paso 1 - Responsable del control, debe establecerse la periodicidad de su ejecución.

Cada vez que se releva un control, debemos preguntarnos si la periodicidad en que se ejecuta el control ayuda a prevenir o detectar el riesgo de manera oportuna. Si la respuesta es SÍ, entonces la periodicidad del control está bien diseñada.

EJEMPLO

Hay controles que no tienen una periodicidad especifica, como por ejemplo, los controles que se ejecutan en el proceso de contratación de proveedores. Solo se ejecutan cuando se contratan proveedores. La periodicidad debe quedar redactada de tal forma que indique que cada vez que se desarrolla la actividad, se ejecuta el control.

PASO 2	Debe tener una periodicidad definida para su ejecución

- **El profesional de contratación <u>cada vez que se va a realizar un contrato</u> con un proveedor de servicios.**
- **El auxiliar de cartera <u>mensualmente</u>.**
- **El coordinador de operaciones <u>diariamente.</u>**
- **La coordinadora de nómina <u>quincenalmente.</u>**

- **El sistema SAP <u>cada vez que se va a realizar un pago.</u>**

De igual forma hay controles automáticos que son programados para que se ejecuten en un tiempo específico, estos controles también tienen una periodicidad.

IMPORTANTE
Todos los controles deben tener una periodicidad específica. Si queda a criterio la periodicidad de la realización del control, tendríamos un problema en el diseño del control.

¿Cómo defino o establezco un control que mitigue el riesgo?

Al momento de definir si un control o controles mitigan de manera adecuada el riesgo, se debe considerar desde la redacción del mismo, las siguientes variables

VARIABLES A EVALUAR PARA EL ADECUADO DISEÑO DE CONTROLES

PASO 3 **Debe indicar cuál es el propósito del control.**

Propósito

El control debe tener un propósito que indique para qué se realiza el control, y que ese propósito conlleve a prevenir las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar), o detectar la materialización del riesgo, y conlleve a que se realicen los ajustes y correctivos en el diseño del control o en su ejecución. El solo hecho de establecer un procedimiento o contar con una política por sí sola, no va a prevenir o detectar la materialización del riesgo o una de sus causas. Siguiendo las variables a considerar en la evaluación del diseño de control revisadas, veamos algunos ejemplos de cómo se deben redactar los controles, incluyendo el propósito de lo que busca el control.

EJEMPLO

Al momento de identificar los controles para mitigar el riesgo, debemos preguntarnos, si es una actividad o un control y para diferenciarlo es importante que el control (verifica, valida, concilia, coteja, compara, etc.) ayuda a la mitigación del riesgo, por eso es importante que pensemos primero en tener controles preventivos antes que detectivos.

PASO 3	Debe indicar cuál es el propósito del control.

- **El profesional de Contratación cada vez que se va a realizar un contrato verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación.**
- **El Auxiliar de Cartera mensualmente verifica que los valores recaudados en Banco correspondan con los saldos adeudados por los clientes.**

Esto también aplica para controles que son realizados de manera automática a través de un sistema programado.

- **El sistema SAP cada vez que se va a realizar un pago valida que el proveedor al cual se le va a girar el pago no este reportado en listas restrictivas o de lavado de activos y financiación del terrorismo.**

IMPORTANTE
El control debe tener un propósito (verificar, validar, cotejar, comparar, revisar, etc.) para mitigar la causa de la materialización del riesgo

¿Cómo defino o establezco un control que mitigue el riesgo?

Al momento de definir si un control o controles mitigan de manera adecuada el riesgo, se debe considerar desde la redacción del mismo, las siguientes variables

VARIABLES A EVALUAR PARA EL ADECUADO DISEÑO DE CONTROLES

PASO 4 **Debe establecer el cómo se realiza la actividad de control.**

Cómo se realiza

El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control, es confiable para la mitigación del riesgo.

Cuando estemos evaluando el control, debemos preguntarnos, si la fuente de información utilizada ¿es información confiable?, imaginémonos, que la validación de que si el proveedor cumple con los requisitos de contratación, no la estemos realizando con una lista de chequeo, si no de memoria, porque los requisitos no los sabemos de memoria, o que la conciliación la realicemos con un extracto de Bancos que fue suministrado por la misma área de cartera o a través de un archivo en Excel.

EJEMPLO

PASO 4	Debe establecer el cómo se realiza la actividad de control.

- **El profesional de contratación cada vez que se va a realizar un contrato verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor.**

- **El auxiliar de cartera mensualmente verifica que los valores recaudados en Banco correspondan con los saldos adeudados por los clientes, extractando la información directamente del portal Bancario del extracto y generando el auxiliar contable de cuentas por cobrar del aplicativo, identificando las cuentas x cobrar pendientes de pago que fueron canceladas según extracto bancarios.**

- **El sistema SAP cada vez que se va a realizar un pago valida que el proveedor al cual se le va a girar el pago no este reportado en listas restrictivas comparando el Número de Identificación Tributaria (NIT) o Cédula con la información cargada en el aplicativo de las listas de clientes reportados en temas de lavado de activos y financiación del terrorismo.**

Al momento de definir si un control o controles mitigan de manera adecuada el riesgo, se debe considerar desde la redacción del mismo, las siguientes variables

VARIABLES A EVALUAR PARA EL ADECUADO DISEÑO DE CONTROLES

PASO 5	**Debe indicar que pasa con las observaciones o desviaciones resultantes de ejecutar el control.**

Qué pasa con las observaciones o desviaciones

El control debe indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control. Al momento de evaluar si un control está bien diseñado para mitigar el riesgos, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumple, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, debería gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones. Sigamos con nuestros ejemplos prácticos de ayuda, para la interiorización de estos conceptos.

EJEMPLO

PASO 5	Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.

- **El profesional de contratación cada vez que se va a realizar un contrato, verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación, a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor. <u>En caso de encontrar información faltante, requiere al proveedor a través de correo para el suministro de la información y poder continuar con el proceso de contratación.</u>**

- **El auxiliar de cartera mensualmente verifica que los valores recaudados en Banco correspondan con los saldos adeudados por los clientes, extractando la información directamente del portal Bancario del extracto y generando el auxiliar contable de cuentas por cobrar del aplicativo, identificando las cuentas x cobrar pendientes de pago que fueron canceladas según extracto bancarios. <u>En caso de observar cuentas de cobro que a la fecha no se ha recibido el pago, lista las cuentas pendientes de pago y realiza llamadas a los clientes y solicita que le indiquen la fecha para el pago oportuno de las mismas.</u>**

EJEMPLO

PASO 5	Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.

- **El sistema SAP cada vez que se va a realizar un pago valida que el proveedor al cual se le va a girar el pago no esté reportado en listas restrictivas comparando el Número de Identificación Tributaria (NIT) o cédula con la información cargada en el aplicativo de las listas de clientes reportados en temas de lavado de activos y financiación del terrorismo.**

  <u>En caso de encontrar coincidencias el sistema no permite realizar el pago.</u>

IMPORTANTE
Si el responsable de ejecutar el control no realiza ninguna actividad de seguimiento a las observaciones o desviaciones, o la actividad continúa a pesar de indicar esas observaciones o desviaciones, el control tendría problemas en su diseño.

Al momento de definir si un control o controles mitigan de manera adecuada el riesgo, se debe considerar desde la redacción del mismo, las siguientes variables

VARIABLES A EVALUAR PARA EL ADECUADO DISEÑO DE CONTROLES

PASO 6 **Debe dejar evidencia de la ejecución del control.**

Evidencia

El control debe dejar evidencia de su ejecución. Esta evidencia ayuda a que se pueda revisar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control, y se pueda evaluar que el control realmente fue ejecutado de acuerdo a los parámetros establecidos y descriptos anteriormente:

1. Fue realizado por el responsable que se definió.
2. Se realizó de acuerdo a la periodicidad definida.
3. Se cumplió con el propósito del control.
4. Se dejó la fuente de información que sirvió de base para su ejecución.
5. Hay explicación a las observaciones o desviaciones resultantes de ejecutar el control.

EJEMPLO

PASO 6	Debe dejar evidencia de la ejecución del control.

El profesional de contratación cada vez que se va a realizar un contrato, verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación, a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor. En caso de encontrar información faltante, requiere al proveedor a través de correo para el suministro de la información y poder continuar con el proceso de contratación. Como evidencia la respectiva lista de chequeo diligenciada con la información de la carpeta del cliente y correos solicitando la información faltante en los casos que aplique.

EJEMPLO

PASO 6	Debe dejar evidencia de la ejecución del control.

- **El auxiliar de cartera mensualmente verifica que los valores recaudados en Banco correspondan con los saldos adeudados por los clientes, extractando la información directamente del portal Bancario del extracto y generando el auxiliar contable de cuentas por cobrar del aplicativo, identificando las cuentas x cobrar pendientes de pago que fueron canceladas según extracto bancarios. En caso de observar cuentas de cobro que a la fecha no se ha recibido el pago, lista las cuentas pendientes de pago y realiza llamadas a los clientes y solicita que le indiquen la fecha para el pago oportuno de las mismas. <u>Como evidencia queda listado de cuentas por cobrar pendientes de pago en Excel con los compromisos acordados con los clientes y extracto bancario.</u>**

EJEMPLO

PASO 6	Debe dejar evidencia de la ejecución del control.

Hay controles que su evidencia queda en un flujo a través de una aplicación como un aprobado o revisado o que la evidencia cuando es un control automático es la configuración y programación de la aplicación.

- **El sistema SAP cada vez que se va a realizar un pago valida que el proveedor al cual se le va a girar el pago no este reportado en listas restrictivas, comparando el Número de Identificación Tributaria (NIT) o cédula con la información cargada en el aplicativo de las listas de clientes reportados en temas de lavado de activos y financiación del terrorismo. En caso de encontrar coincidencias el sistema no permite realizar el pago. <u>Como evidencia queda programación interna del aplicativo y reporte de coincidencia con listas restrictivas.</u>**

3.2.2 Valoración de los controles

Valoración de los controles para la mitigación de los riesgos

EL CONTROL ESTÁ BIEN DISEÑADO PARA MITIGAR EL RIESGO

EL CONTROL SE EJECUTA COMO FUE DISEÑADO Y DE MANERA CONSISTENTE

EL CONTROL ESTA DISEÑADO Y SE EJECUTA PARA MITIGAR EL IMPACTO DEL RIESGO UNA VEZ SE MATERIALICE

EL CONTROL ESTA DISEÑADO Y SE EJECUTA PARA MITIGAR LA PROBABILIDAD DE QUE EL RIESGO SE MATERIALICE.

IMPORTANTE
Para la adecuada mitigación de los riesgos, no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó.
Porque un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo.

ESQUEMA 11

Valoración de los controles para la mitigación de los riesgos

Tabla ilustrativa 6. Análisis y evaluación de los controles para la mitigación de los riesgos.

Análisis y evaluación del diseño del control de acuerdo con las seis (6) variables establecidas:

Criterio de evaluación	Aspecto a Evaluar en el Diseño del Control	Opciones de respuesta	
1. Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	No asignado
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	Inadecuado
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	Inoportuna
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 o detectar	No es un control
4. Cómo 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	No confiable
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	No se investigan y resuelven oportunamente.
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	Completa	Incompleta / no existe

Tabla ilustrativa 7. Peso o participación de cada variable en el diseño del control para la mitigación del riesgo

Criterio de evaluación.	Opción de respuesta al criterio de evaluación	Peso en la evaluación del diseño del control
1.1 Asignación del 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

.

Resultados de la evaluación del diseño del control

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

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

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

Resultados de la 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 primer línea de defensa que el control se ejecute. Al momento de determinar si el control se ejecuta, inicialmente, el responsable del proceso debe llevar a cabo una confirmación, posteriormente se confirma con las actividades de evaluación realizadas por auditoría interna
o control interno

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.

Análisis y evaluación de los controles para la mitigación de los riesgos

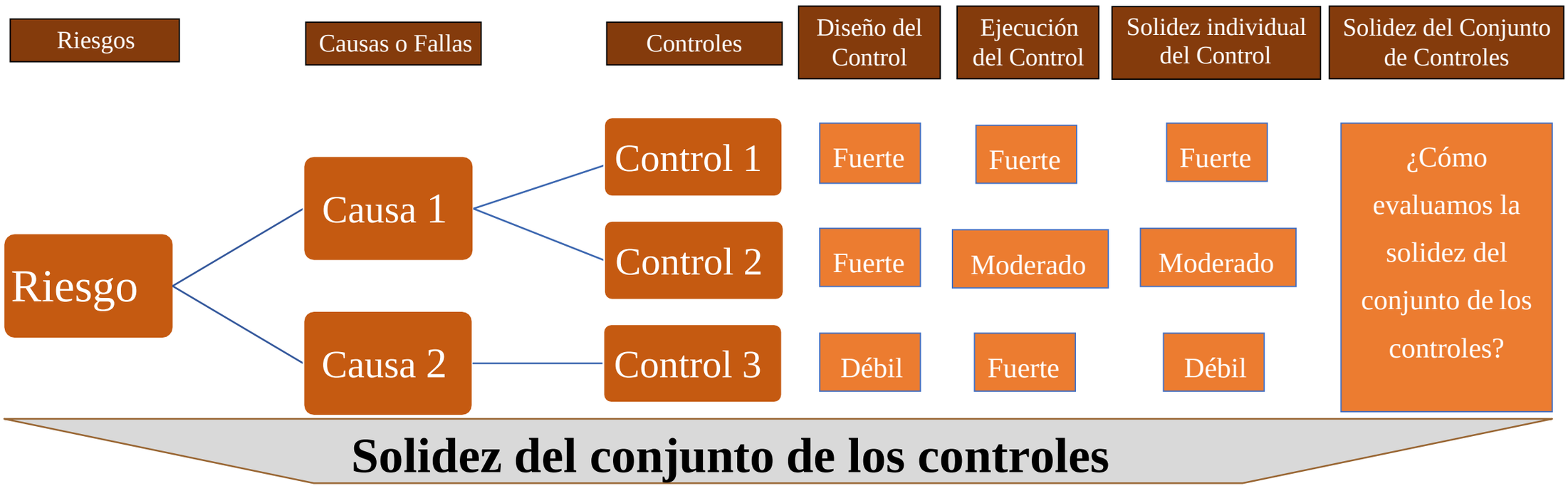
Dado que la calificación de riesgos inherentes y residuales se realiza al riesgo y no a cada causa, hay que consolidar el conjunto de los controles asociados a las causas, para evaluar si estos de manera individual y en conjunto si ayudan al tratamiento de los riesgos, considerando tanto el diseño y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

Peso individual del diseño (DISEÑO)	**El control se ejecuta de manera consistente por los responsables. (EJECUCIÓN)**	**Solidez individual de cada control fuerte:100 moderado:50 debil:0**	**Aplica plan de acción para fortalecer el control Sí / NO**
fuerte calificación entre 96 y 100	**fuerte** (siempre se ejecuta)	**fuerte + fuerte = fuerte**	**No**
	moderado (algunas veces)	**fuerte + moderado = moderado**	**Sí**
	débil (no se ejecuta)	**fuerte + débil = débil**	**Sí**
moderado calificación entre 86 y 95	**fuerte** (siempre se ejecuta)	**moderado + fuerte = moderado**	**Sí**
	moderado (algunas veces)	**moderado + moderado = moderado**	**Sí**
	débil (no se ejecuta)	**moderado + débil = débil**	**Sí**
débil entre 0 y 85	**fuerte** (siempre se ejecuta)	**débil + fuerte = débil**	**Sí**
	moderado (algunas veces)	**débil + moderado = débil**	**Sí**
	débil (no se ejecuta)	**débil + débil = débil**	**Sií**

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.



Solidez del conjunto de los 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.

IMPORTANTE.
La solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de los controles por cada riesgo.

ESQUEMA 12

Solidez del conjunto de controles

Solidez del conjunto de controles para la adecuada mitigación del riesgo

Disminución de probabilidad e impacto:

La mayoría de los controles que se diseñan son para disminuir la probabilidad de que ocurra una causa o evento que pueda llevar a la materialización del riesgo y muy pocos son dirigidos al impacto:

EJEMPLO

Para poder asignar un contrato, se debe verificar que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación.

Para mitigar el impacto económico en caso de que el contratista incumpla, se deben verificar las pólizas de seguros solicitados al contratista seleccionado.

Generalmente se encuentran más controles que disminuyen directamente la probabilidad que el impacto, si no existieran controles para disminuir la probabilidad del riesgo, el impacto de un riesgo por el número de eventos que se llegarían a materializar seria mayor, en nuestro ejemplo, si no existiera el control "verificar que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación para poder asignar un contrato", el número de contratos que se incumplirían, seria mayor, por tal razón y para efectos de la elaboración de la matriz y al momento de evaluar si los controles ayudan a disminuir el impacto o la probabilidad, estos controles se calificarán teniendo en cuenta que de manera indirecta disminuyen también el impacto.

3.2.3 Nivel de riesgo (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 ilustrativa 8. 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

IMPORTANTE
Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo.

IMPORTANTE
Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento.

Resultados del mapa de riesgo residual.

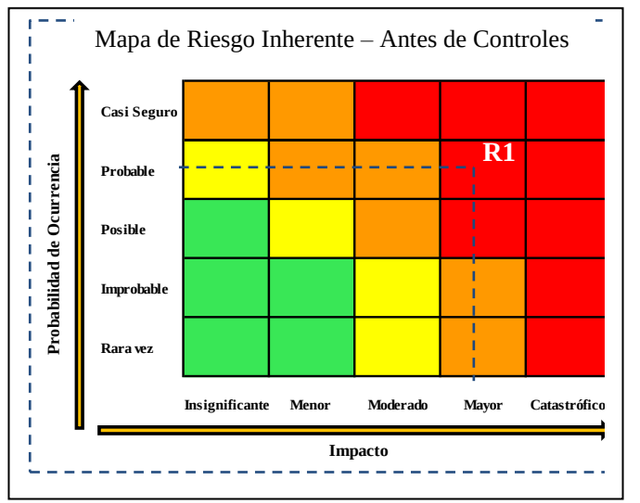
Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, procedemos a la elaboración del mapa de riesgo residual (después de los controles).

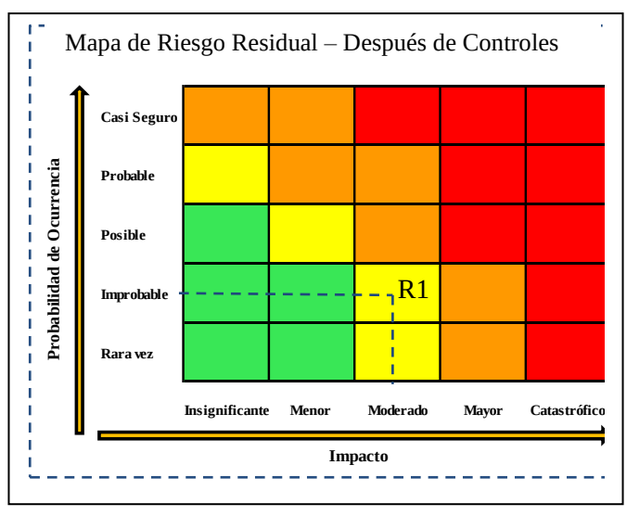
EJEMPLO

Tenemos el Riesgo 1 - Con una calificación de riesgo inherente de probabilidad e impacto como se muestra en la siguiente gráfica:

Como podemos observar es probable que el riesgo suceda y tiene un impacto en caso de materializarse mayor para la entidad, ahora supongamos que existen controles bien diseñados y que siempre se ejecutan, y que estos controles disminuyen de manera directa la probabilidad.

En nuestro ejemplo disminuiría dos cuadrantes de probabilidad, pasa de probable a improbable y un cuadrante de impacto, pasa de mayor a moderado.





3.3 Monitoreo y revisión

¿Por qué debo monitorear y revisar la gestión de riesgos?

Porque la entidad debe asegurar el logro de sus objetivos, anticipándose a los eventos negativos relacionados con la gestión de la entidad. El Modelo Integrado de Plantación y Gestión- (MIPG) en la dimensión 7 “Control Interno” desarrolla a través de las Líneas de Defensa la responsabilidad de la gestión del riesgo y control.

¿Cómo se define el modelo de las líneas de defensa?

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

¿Quiénes son los asignados para monitorear y revisar la gestión de riesgos y cuáles son sus roles?

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

LÍNEA ESTRATÉGICA

Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.

1ª. Línea de defensa	2ª. Línea de defensa	3ª. Línea de defensa
Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.	Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende	Proporciona información sobre la efectividad del S.C.I., a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa
A cargo de los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad. Rol principal: diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad. Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro.	A cargo de los servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: Jefes de planeación, supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión de la entidad, comités de riesgos (donde existan), comités de contratación, entre otros. Rol principal: monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.	A cargo de la oficina de control interno, auditoría interna o quien haga sus veces. El rol principal: proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del S.C.I. El alcance de este aseguramiento, a través de la auditoría interna cubre todos los componentes del S.C.I.

Rol de la línea estratégica en el monitoreo y revisión de los riesgos y actividades de control

LÍNEA ESTRATÉGICA	
Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.	
Actividades de Monitoreo y Revisión a Realizar	La alta dirección y el equipo directivo, a través de sus comités deben monitorear y revisar el cumplimiento a los objetivos a través de una adecuada gestión de riesgos con relación a lo siguiente: ✓ Revisar los cambios en el "Direccionamiento estratégico" y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados. ✓ Revisión del adecuado desdoblamiento de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos. ✓ Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna. ✓ Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. ✓ Hacer seguimiento y pronunciarse por lo menos cada trimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo a las políticas de tolerancia establecidas y aprobadas. ✓ Revisar los informes presentados por lo menos cada trimestre de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos. ✓ Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.

Rol de la primera línea de defensa en el monitoreo y revisión de los riesgos y actividades de control

1ª. LÍNEA DE DEFENSA
Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. Está conformada por los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad.

Actividades de Monitoreo y Revisión a Realizar

Los gerentes públicos y los líderes de proceso deben monitorear y revisar el cumplimiento de los objetivos instituciones y de sus procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente:

- ✓ Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso.
- ✓ Revisión como parte de sus procedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos.
- ✓ Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.
- ✓ Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
- ✓ Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.
- ✓ Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos.
- ✓ Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.

Rol de la segunda línea de defensa en el monitoreo y revisión de los riesgos y actividades de control

2ª. LÍNEA DE DEFENSA

Asiste y guía la línea estrategia y la primera línea de defensa en la gestión adecuada de los Riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y realiza un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos. Está conformada por los responsables de monitoreo y evaluación de controles y gestión del riesgo (jefes de planeación, supervisores e interventores de contratos o proyectos, responsables de sistemas de gestión, etc.)

Actividades de monitoreo y revisión a realizar

Los jefes de planeación, supervisores e interventores de contratos o proyectos o responsables de sistemas de gestión deben monitorear y revisar el cumplimiento de los objetivos institucionales y de procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción, con relación a lo siguiente:

- ✓ Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos.
- ✓ Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
- ✓ Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.
- ✓ Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad.
- ✓ Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos.
- ✓ Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.

Rol de la tercera línea de defensa en el monitoreo y revisión de los riesgos y actividades de control.

3ª. LÍNEA DE DEFENSA
Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primer línea y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. Está conformada por la Oficina de Control Interno o Auditoría Interna.

Actividades de monitoreo y revisión a realizar

La oficina de control interno o auditoría interna monitorea y revisa de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, a través de la adecuada gestión de riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente:

- ✓ Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.
- ✓ Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
- ✓ Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, incluyendo los riesgos de corrupción.
- ✓ Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la Primer Línea de Defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.
- ✓ Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.
- ✓ Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de acción establecidos como resultados de las auditorías realizadas, se realicen de manera oportuna, cerrando las causas raíz del problema, evitando en lo posible la repetición de hallazgos o materialización de riesgos.

Monitoreo riesgos de corrupción

Los líderes de los procesos en conjunto con sus equipos deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es del caso ajustarlo, (primera línea de defensa). Le corresponde, igualmente a la oficina de planeación adelantar el monitoreo, (segunda línea de defensa) para este propósito se sugiere elaborar una matriz para el monitoreo periódico. Este monitoreo será en los tiempos que determine la entidad.

Su importancia radica en la necesidad de monitorear permanentemente la gestión del riesgo y la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es - por sus propias características una actividad difícil de detectar.

Para el efecto deben atender las actividades descritas en la primera y segunda línea de defensa de este documento.

Reporte Plan de Tratamiento de Riesgos

Consolidar información para la gestión del riesgo

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 Mapa y Plan de Tratamiento de Riesgos, se inicia con el registro del riesgo identificado, luego se especifica la clase de riesgo, se transcriben las causas raíz o causas priorizadas, 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 de supervivencia 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 la acción de contingencia a implementar una vez el riesgo se materialice, para ello se deben analizar las estrategias DA o estrategias de fuga provenientes de la Matriz DOFA, seleccionando la(s) más apropiada(s) para el riesgo identificado.

No olvidar colocar el soporte, responsable y tiempo de ejecución, teniendo en cuenta que este tipo de acciones son de aplicación inmediata y a corto plazo para restablecer cuanto antes, la normalidad de las actividades para el logro de los objetivos del proceso o la estrategia.

Por último, se formulan los indicadores clave de riesgo (KRI por sus siglas en ingles) que permitan monitorear el cumplimiento (eficacia) e impacto (efectividad) de las actividades de control, siempre y cuando conduzcan a la toma de decisiones (Por riesgo identificado en los procesos)

ESQUEMA 13 Consolidación Plan de Tratamiento de Riesgos

Reporte de la gestión del riesgo

La primera línea de defensa reporta a la segunda línea de defensa, el estado de avance del tratamiento del riesgo en la operación, y la consolidación de los riesgos en todos los niveles será reportada por la segunda línea de defensa (encargado de la gestión del riesgo) hacia la alta dirección.

Formato mapa y plan de tratamiento de riesgos

Nro	Riesgo	Clasifica - ción	Causas	Proba-bilidad	Impacto	Riesgo Residua	Opción Manejo	Actividad de Control	Soporte	Respon-sable	Tiempo	Indicador
1	Desabastecimiento de bienes y servicios requeridos por la entidad	Financiero	Desactualización de la base de datos	Improbable	Mayor	Moderado	Reducir	D2O1: Adquirir software para mantener actualizada la base de datos de proveedores y el registro de contrataciones.	Contrato y factura software	Director de T.I. y Jefe Contratos	Primer trimestre de 2018	**EFICACIA:** **Índice de cumplimiento actividades=** (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** **Efectividad del plan de manejo de riesgos=** ((# de casos de desabastecimiento presentados periodo actual - # de casos de desabastecimiento presentados periodo anterior) / # de casos de desabastecimiento presentados periodo anterior) x 100
			Insuficiente capacitación del personal de contratos				Reducir	D1O2: Realizar convenios con entidades educativas para capacitar al personal de contratos.	Convenios firmados	Director Financiero	Trimestralmente Del 01012018 al 31122018	
			Cambios en la regulación contable y presupuestal				Reducir	F2A1: Establecer mayor frecuencia de reinducción para actualizar al personal ante los cambios normativos contables.	Circular interna	Director Talento Humano	Del 01012018 al 31012018	
							Reducir	F2A1: Realizar reinducciones para actualizar al personal ante los cambios normativos contables.	Actas reinducción	Jefe Cartera	Trimestralmente Del 01012018 al 31122018	
			Hackeo				Reducir	F1A2: Fortalecer los Firewall en la red de la organización para detectar posibles incursiones	Reporte cumplimiento Firewall fortalecido	Director de T.I.	Del 01022018 al 28022018	
							Acción de Contingencia	D1,2A1,2: D1,2A1,2: Convocar en forma extraordinaria un comité Institucional de coordinación de Control Interno para analizar y aplicar medidas inmediatas que, dentro de la legalidad, permitan el reabastecimiento inmediato de bienes y servicios.	Acta de comité de coordinación institucional de control interno firmada	Director Financiero	1 semana una vez el riesgo se materialice	

Reporte de la gestión del riesgo de corrupción

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

Formato mapa y plan de tratamiento de riesgos

Nro	Riesgo	Clasificación	Causas	Probabilidad	Impacto	Riesgo Residual	Opción Manejo	Actividad de Control	Soporte	Responsable	Tiempo	Indicador
2	Posibilidad de recibir o solicitar cualquier dadiva o beneficio a nombre propio o de terceros para celebrar un contrato	Corrupción	Debilidades en la etapa de planeación	Probable	Catastrófico	Catastrófico	Reducir	Manual de contratación Implementado con parámetros técnicos y financieros para cada tipo de contratación, formalizado en procedimiento.	Manual de contratación	Jefe de Contratos	Primer trimestre de…	**EFICACIA:** **Índice de cumplimiento actividades=** (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** **Efectividad del plan de manejo de riesgos=** ((# de casos de favorecimiento a proponentes presentados periodo actual - # de casos de favorecimiento a proponentes presentados periodo anterior) / # de casos de favorecimiento a proponentes presentados periodo anterior) x 100
			Presiones indebidas				Reducir	Comité de Contratación	Acto administrati-vo conformando comité	Jefe de Contratos	Trimestral mente	
			Carencia d e controles en el procedimiento de contratación				Reducir	Difusión y capacitación a todos los funcionarios del proceso.	Actas de capacitación	Director Talento Humano	Del (día /mes/año) al (día /mes/año)	
			Excesiva discrecionalidad				Acción de Contingen-cia	Iniciar la investigación disciplinaria, fiscal o remitir a las instancias correspondientes para el proceso penal.	Comunica-ción iniciando o remitiendo investigación	Jefe Control Disciplina-rio Interno	1 semana una vez el riesgo de iliquidez se materialice	

Reporte de la gestión del riesgo de seguridad digital

Igualmente en el caso de los riesgos de seguridad digital, se debe reportar en el mapa y planes de tratamiento. **El responsable de seguridad digital apoyará y acompañará** a las diferentes líneas de defensa tanto para el reporte, como para la gestión y el tratamiento de estos riesgos.

Formato mapa y plan de tratamiento de riesgos de seguridad digital

Nro	Riesgo	Activo	Tipo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo residual	Opción tratamiento	Actividad de Control	Soporte	Responsable	Tiempo	Indicador
1	Pérdida de la integridad	Base de Datos de Nómina	Seguridad Digital	Modificación no autorizada	Ausencia de políticas de control de acceso.	Probable	Menor	Moderado	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	**EFICACIA: Índice de cumplimiento actividades=** (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD: Efectividad del plan de manejo de riesgos=** (# de modificaciones no autorizadas)
					Contraseñas sin protección				Reducir	A.9.4.3 Sistema de gestión de contraseñas	Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018	
					Ausencia de mecanismos de identificación y autenticación de usuarios				Reducir	A 9.4.2 Procedimiento de ingreso seguro	Procedimiento para ingreso seguro	Oficina TI	Cuarto trimestre de 2018	
					Ausencia de bloqueo de sesión				Reducir	A.11.2.8 Equipos de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Cuarto Trimestre de 2018	

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

Indicadores - gestión del riesgo de seguridad digital

Igualmente, en el caso de los riesgos de seguridad digital, se deben generar indicadores, para medir la gestión realizada, en esencia la eficacia y la efectividad de los planes de tratamiento implementados.

La entidad debería definir como mínimo 2 indicadores POR PROCESO de la siguiente manera:

- ✓ 1 indicador de eficacia, que indique el cumplimiento de las actividades para la gestión del riesgo de seguridad digital en cada PROCESO de la entidad.
- ✓ 1 indicador de efectividad, para cada riesgo o la suma de todos los riesgos de seguridad digital (pérdida de confidencialidad, de integridad, de disponibilidad).

IMPORTANTE
No se definirán indicadores por activo, teniendo en cuenta que pueden generarse un sinnúmero de indicadores lo que haría la gestión y seguimiento demasiado complejo para la entidad.

Ejemplos:

EFICACIA:

Porcentaje de controles implementados = (#controles implementados / #controles definidos) x 100

EFECTIVIDAD:

 # Riesgos materializados de confidencialidad = (# de incidentes que afectaron la confidencialidad de algún activo del proceso)

Variación de incidentes de confidencialidad (para entidades con mediciones anteriores) =
((# de Incidentes de Confidencialidad Periodo Actual - # de Incidentes de Confidencialidad Periodo Previo) / Incidentes de Confidencialidad Periodo Previo) * 100%

Fuentes adicionales para formular indicadores de seguridad digital: http://kpilibrary.com/categories/informationsecurity?page=1 http://kpilibrary.com/categories/risk-it-information-technology

3.4. Seguimiento riesgos de corrupción

GESTION RIESGOS DE CORRUPCIÓN

- **Seguimiento:** El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.
- ***Primer seguimiento:*** Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
- ***Segundo seguimiento:*** Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- ***Tercer seguimiento:*** Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la Entidad o en lugar de fácil acceso al ciudadano.

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

Acciones a seguir en caso de materialización de riesgos de corrupción

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

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

Teniendo en cuenta que la Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riego y están funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

- Acciones encaminadas a determinar la efectividad de los controles.
- Acciones encaminadas a mejorar la valoración de los riesgos.
- Acciones encaminadas a mejorar los controles.
- Analizar el diseño e idoneidad de los controles, si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo .
- Revisar las acciones del monitoreo.

Comunicación y consulta

La comunicación y consulta con las partes involucradas tanto internas como externas debería tener lugar durante todas las etapas del proceso para la gestión del riesgo[12]

Este análisis 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.

Estrategias de Comunicación

Trabajo en Equipo

Conocimiento y análisis de la complejidad de cada uno de los procesos

COMUNICACIÓN Y CONSULTA

Se constituye en un elemento transversal a todo el proceso al involucrar a todos los funcionarios para el levantamiento de los mapas de riesgos.

UN ENFOQUE DE EQUIPOS DE TRABAJO PUEDE:

- Ayudar a establecer correctamente el contexto para los procesos
- Garantizar que se toman en consideración las necesidades de los usuarios
- Ayudar a garantizar que los riesgos estén correctamente identificados
- Reunir diferentes áreas de experticia para el análisis de los riesgos
- Garantizar que los diferentes puntos de vista se toman en consideración adecuadamente durante todo el proceso
- Fomentar la administración del riesgo como una actividad inherente al proceso de planeación estratégica

12. Instituto Colombiano de Normas Técnicas y Certificación - ICONTEC. Norma Técnica Colombiana NTC-ISO31000. 2011. p. 132

ESQUEMA 14 Comunicación y consulta – Aspecto transversal

Información, comunicación y reporte

Línea estratégica

Corresponde al Comité de Auditoráa de las Empresas Industriales y Comerciales del Estado y/o a los Comités Institucionales de Coordinación de Control Interno, establecer la Política de Gestión de Riesgos y asegurarse de su permeabilización en todos los niveles de la organización pública, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo.

Primera línea de defensa

Corresponde a los jefes de área y/o grupo (primera línea de defensa) asegurarse de implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades

Segunda línea de defensa

Corresponde al área encargada de la gestión del riesgo (segunda línea de defensa) la difusión y asesoría de la presente metodología, así como de los planes de tratamiento de riesgo identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación.

Tercera línea de defensa

Le corresponde a las Unidades de Control Interno, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la entidad, catalogándola como una unidad auditable más dentro de su universo de auditoría, y por tanto debe dar a conocer a toda la entidad el Plan Anual de Auditorias basado en riesgos, y los resultados de la evaluación de la gestión del riesgo.

ESQUEMA 15 Responsabilidades por línea de defensa para la 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.
Adicionalmente, los riesgos de seguridad digital deberán ser reportados a las autoridades o instancias respectivas que el gobierno disponga.

Referencias bibliográficas

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

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

COSO Committee of Sponsoring Organizations of the Treadway Commission. PwC. Instituto de Auditores Internos de España. (2013). *Control Interno - Marco Integrado. Marco y Apéndices.* Instituto de Auditores Internos de España.

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

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

ICONTEC Internacional. (2013). *NORMA TÉCNICA COLOMBIANA NTC-IEC/ISO 31010. GESTION DE RIESGOS. TÉCNICAS DE VALORACIÓN DEL RIESGO.* Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

Instituto de Auditores Internos de Colombia. (2017). *MARCO INTERNACIONAL PARA LA PRÁCTICA PROFESIONAL DE LA AUDITORÍA INTERNA.* Bogotá D.C.

Núñez, A. C. (9 de 11 de 2016). *Inboundlead Blog.* Obtenido de Los 7 Mejores Ejemplos de Objetivos SMART: https://blog.inboundlead.com/los-7-mejores-ejemplos-de-objetivos-smart-o-inteligentes-para-empresas

INDICE DE TABLAS ILUSTRATIVAS

PÁGINA

1. Factores para cada categoría del Contexto 17
2. Criterios para calificar la probabilidad 30
3. Criterios para calificar el Impacto – Riesgos de Gestión 31
4. Criterios para calificar el Impacto – Riesgos de Seguridad Digital 32
5. Criterios para calificar el Impacto - Riesgos de Corrupción 35
6. Análisis y Evaluación de los Controles para la Mitigación de los Riesgos. 63
7. Peso o participación de cada variable en el diseño del control para la mitigación del riesgo 64
8. Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos. 69

ÍNDICE DE ESQUEMAS PÁGINA

1. Conocimiento y análisis de la entidad 10
2. Metodología para la Administración del Riesgo 11
3. Estructuración de la Política de Administración de Riesgos 12
4. Aspectos a desarrollar en la Identificación del Riesgo 15
5. Análisis del Contexto Externo, Interno y del Proceso 16
6. Redacción del Riesgo 23
7. Valoración de Riesgos 28
8. Análisis de Riesgos 29
9. Riesgo antes y después de controles 45
10. Pasos para diseñar un control 46
11. Valoración de los controles para la mitigación de los riesgos 62
12. Solidez del conjunto de controles 67
13. Consolidación Plan de Tratamiento de Riesgos 78
14. Comunicación y consulta – Aspecto transversal 85
15. Responsabilidades por línea de defensa para la Información, comunicación y reporte 86

LISTADO ANEXOS

1. Formato de caracterización de procesos
2. Técnicas para Establecimiento del Contexto y Valoración del riesgo
3. Protocolo para la identificación de riesgos de corrupción asociados a la prestación de trámites y servicios
4. Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas
5. Análisis y priorización de causas
6. Matriz seguimiento riesgos de corrupción