GOBIERNO DE COLOMBIA · VICEPRESIDENCIA · FUNCIÓN PÚBLICA · MINTIC · GOBIERNO DIGITAL

Guía para la administración del riesgo y el diseño de controles en entidades públicas

RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL

VERSIÓN 4

DIRECCIÓN DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL

FUNCIÓN PÚBLICA

OCTUBRE 2018

Con los servidores 60 años por los ciudadanos

DEPARTAMENTO
ADMINISTRATIVO
DE LA FUNCIÓN
PÚBLICA

BOGOTÁ, COLOMBIA
OCTUBRE 2018

Presidencia de la República
Iván Duque Márquez
Presidente de la República

Martha Lucía Ramírez de Rincón
Vicepresidente de la República

Andrés José Rugeles Pineda
Secretario de Transparencia

Ministerio de las Tecnologías de la Información y las Comunicaciones
Sylvia Cristina Constaín Rengifo
Ministra TIC

Carlos Eduardo Rozo Bolaños
Director de Gobierno Digital

Departamento Administrativo de la Función Pública
Fernando Antonio Grillo Rubiano
Director

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
Juan Carlos Valenzuela Buitrago
Senen Niño Gil
Ángela Janeth Cortés Hernández
Albert Cuesta Gómez

Departamento Administrativo de la Función Pública – Dirección de Gestión y Desempeño 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

Edición
Carolina Mogollón Delgado
Dirección de Gestión del Conocimiento

Diseño y diagramación
Susana Bonilla Guzmán
Oficina Asesora de Comunicaciones

Departamento Administrativo de la Función Pública
Carrera 6 No 12-62, Bogotá, D.C., Colombia
Conmutador: 739 5656 / 86 - Fax: 739 5657
Web: www.funcionpublica.gov.co
eva@funcionpublica.gov.co
Línea gratuita de atención al usuario: 018000 917770

Bogotá, D.C., Colombia.

Contenido

Índice de tablas

Índice de esquemas

Presentación

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.

Con 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; se crea un único sistema de gestión articulado 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. Lo anterior, con el fin de entregar a los ciudadanos lo mejor de la gestión y, en consecuencia, 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 y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital”, incluidos sus anexos, como una herramienta con enfoque preventivo, vanguardista y proactivo que permitirá el manejo del riesgo, 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 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.

* 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.

Probabilidad:
se entiende como la posibilidad de ocurrencia del riesgo. Esta 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.

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.

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

Riesgo inherente:
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 sus correspondientes medidas de tratamiento.

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.

Causa:
todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Mapa de riesgos:
documento con la información resultante de la gestión del 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.

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

Vulnerabilidad:
es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

Integridad:
propiedad de exactitud y completitud.

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.

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.

Control:
medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

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

Disponibilidad:
propiedad de ser accesible y utilizable a demanda por una entidad.

Apetito al riesgo:
magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

Fuente: ICONTEC INTERNACIONAL. (2016). NORMA 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 señalen 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, lo anterior para conocer y entender la entidad y su entorno, lo que determinará el análisis de riesgos y la aplicación de la metodología en general.

Esquema 1. Conocimiento y análisis de la entidad

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

PLANEACIÓN INSTITUCIONAL
Las estrategias de la entidad generalmente se definen por parte de la alta dirección y obedecen a la razón de ser que desarrolla la misma, a los planes sectoriales, las 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 evaluación para materializarla o ejecutarla, por lo tanto la administración del riesgo no puede verse de forma aislada.

ASPECTOS

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

MAPA O RED DE PROCESOS
Es la representación gráfica de los procesos estratégicos, misionales, de apoyo, de evaluación y sus interacciones.

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

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

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.

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

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

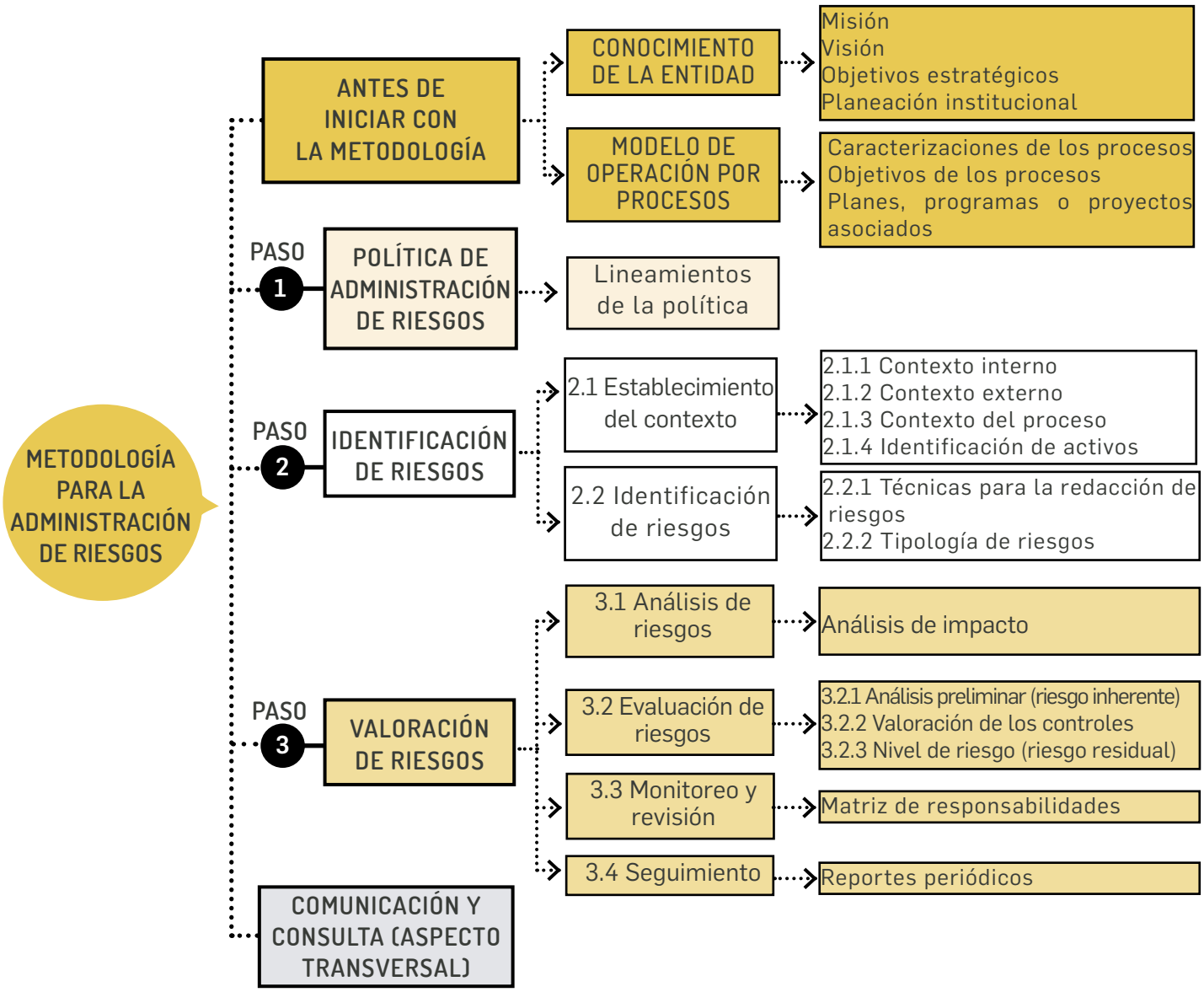
Son los resultados que se espera lograr para cumplir la misión y visión. Determina el cómo logro la política trazada y el aporte que se hace a los objetivos institucionales. Un objetivo es un enunciado que expresa una acción, por lo tanto debe iniciarse con un verbo fuerte como: establecer, identificar,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

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

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 de Riesgos

Esquema 3. Estructuración de la Política de Administración de Riesgos

¿QUÉ ES?

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

¿QUIÉN LA ESTABLECE?

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

POLÍTICA DE ADMINISTRACIÓN DE 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 riesgos en todos los niveles de la entidad

¿QUÉ DEBE CONTENER?

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

IMPORTANTE

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

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

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

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

Aquellos relacionados con la administración del riesgo y con los temas que el manual o guía desarrollen y 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 aceptados 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, p. 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 deben conducir a un tratamiento.

En todos los procesos se pueden presentar riegos 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.

A continuación encontrará un ejemplo de análisis en el proceso de contratación:

La entidad debe adquirir con oportunidad y calidad técnica, en no menos del 90%, los bienes y servicios requeridos para su continua operación.

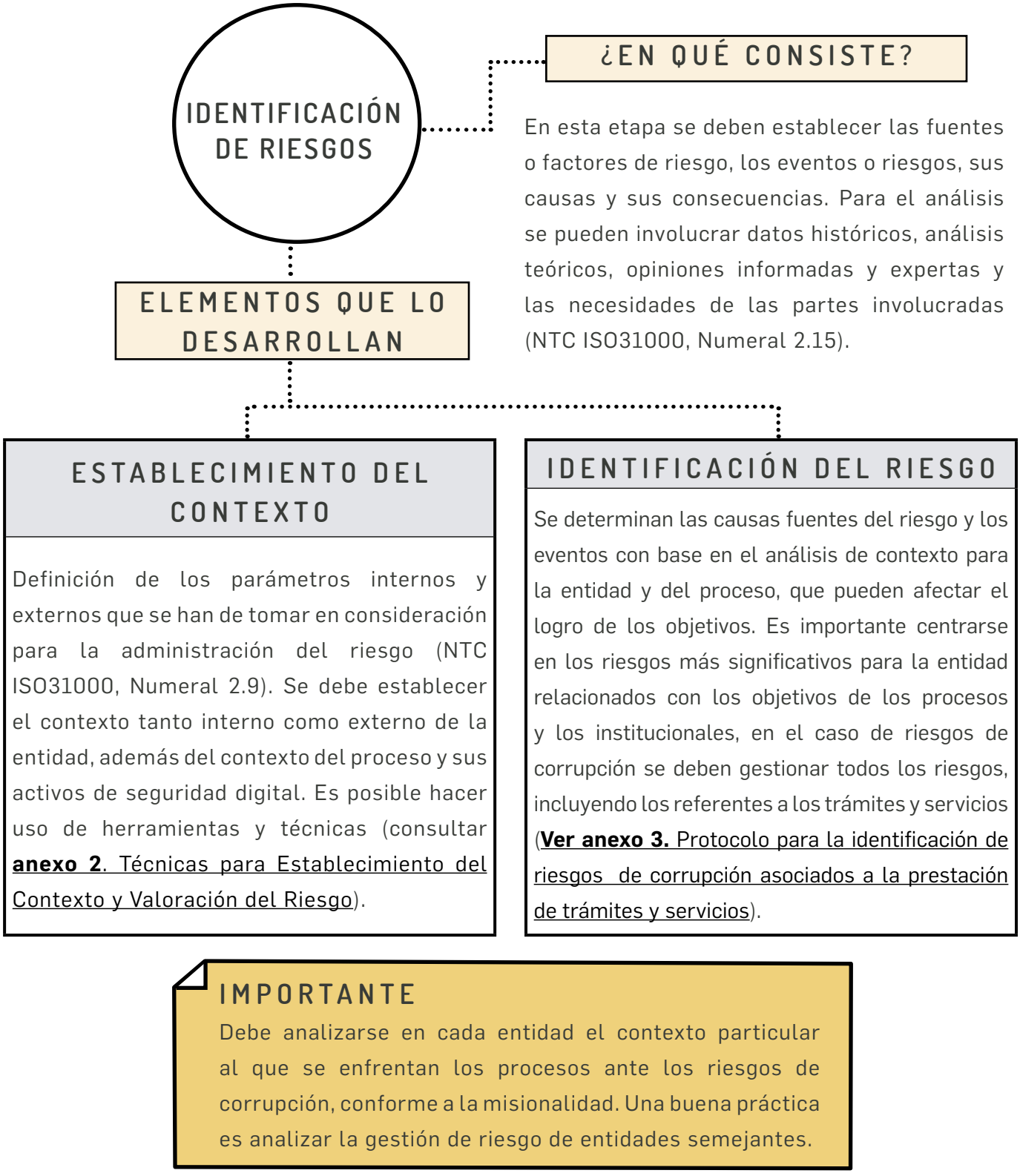
Fuente: Comitte of Sponsoring Orgizations of the Treadway Commission COSO Marco Integrado, Componente Evaluación de Riesgos, Principio. p. 73. 2013.

IMPORTANTE

Los objetivos deben incluir el “qué”, “cómo”, “para qué”, “cuándo”, “cuánto”.
Si no están bien definidos los objetivos, no se puede continuar con la metodología de gestión del riesgo.

Paso 2: identificación de riesgos

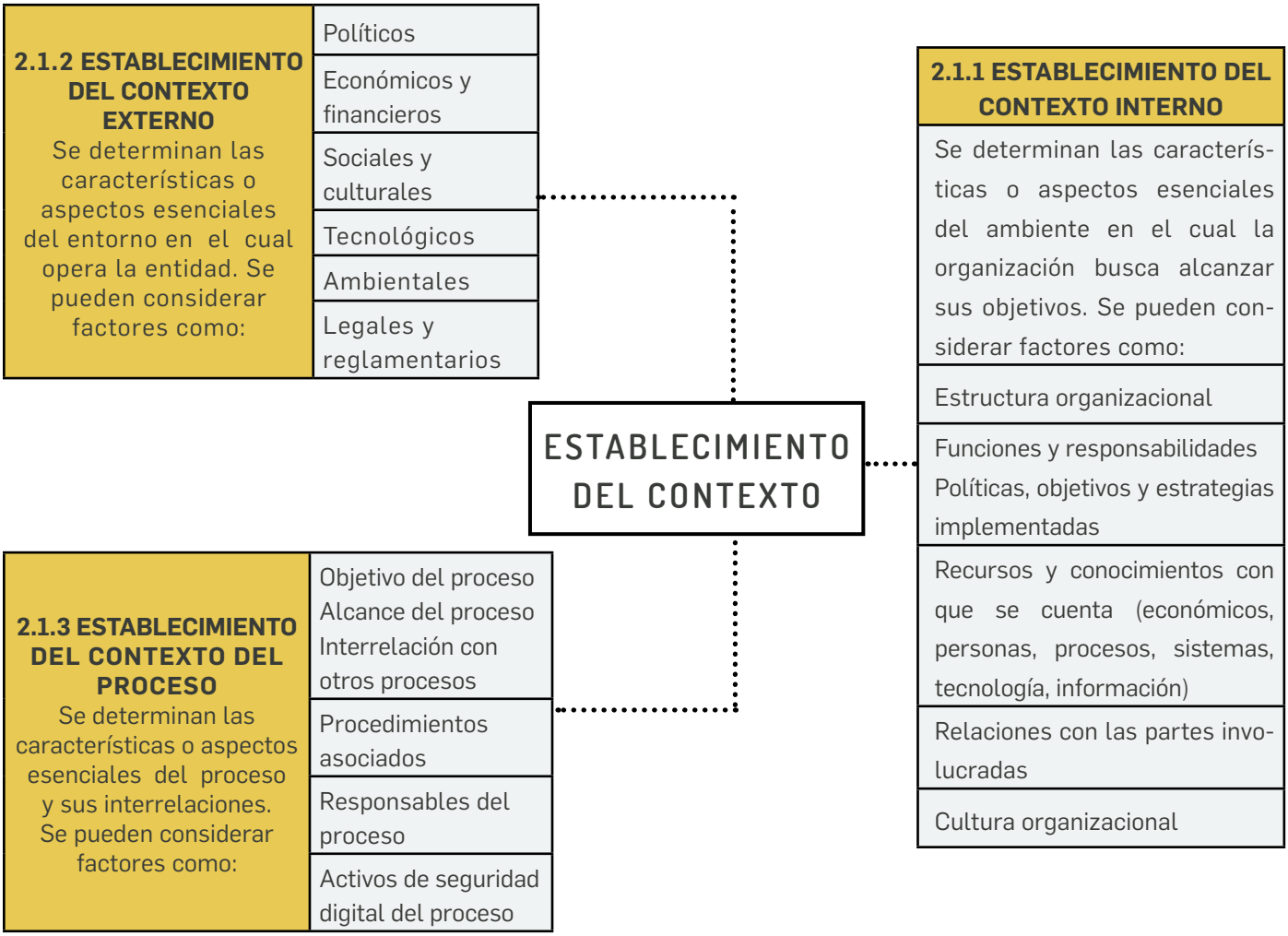
Esquema 4. Aspectos a desarrollar en la identificación del riesgo



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.

Esquema 5. Análisis del contexto externo, interno y 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.

Tabla 1. Factores para cada categoría del contexto

CONTEXTO EXTERNO	POLÍTICOS: cambios de gobierno, legislación, políticas públicas, regulación.
	ECONÓMICOS Y FINANCIEROS: disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	SOCIALES Y CULTURALES: demografía, responsabilidad social, orden público.
	TECNOLÓGICOS: avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
	AMBIENTALES: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	LEGALES Y REGLAMENTARIOS: Normatividad externa (leyes, decretos, ordenanzas y acuerdos).
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 8 y 9.

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 identificar los activos en cada proceso.

IMPORTANTE

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

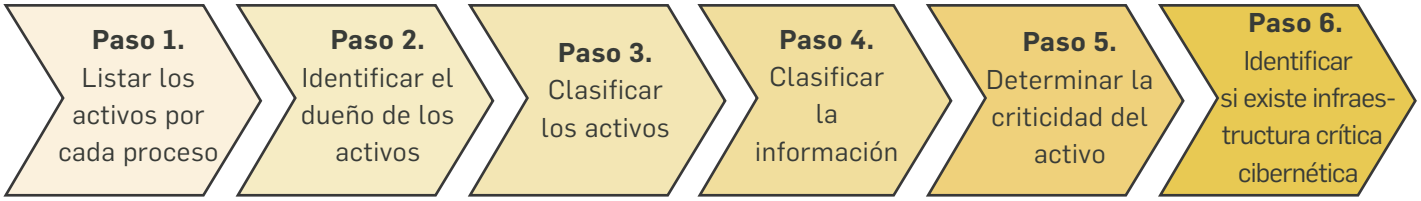
Análisis de los objetivos estratégicos

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO.

Análisis de los objetivos de proceso

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 interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

¿CÓMO IDENTIFICAR LOS ACTIVOS?:



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 lleva a cabo 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 los 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 con el 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.

2.2 Identificación de riesgos - técnicas para la identificación de riesgos

RIESGO DE CORRUPCIÓN

Definición de riesgo de corrupción:

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

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

Es necesario que en la descripción del riesgo 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.

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

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

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

Generalidades acerca de los riesgos de corrupción

- Entidades encargadas de gestionar el riesgo: lo deben adelantar las entidades del orden nacional, departamental y municipal.
- Se elabora anualmente por cada responsable de los procesos al interior de las entidades junto con su equipo.

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

- Publicación del mapa de riesgos de corrupción: se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.

La publicación será parcial y fundamentada en la elaboración del índice deinformación clasificada y reservada. En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014.

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

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

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

Así mismo, dicha oficina adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de

riesgos de corrupción. Deberá dejarse la evidencia del proceso de socialización y publicarse sus resultados.

- **Ajustes y modificaciones:** se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.
- **Monitoreo:** en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.
- **Seguimiento:** el jefe de control interno o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

EJEMPLO

Información anonimizada

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

Información anonimizada

IMPORTANTE

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

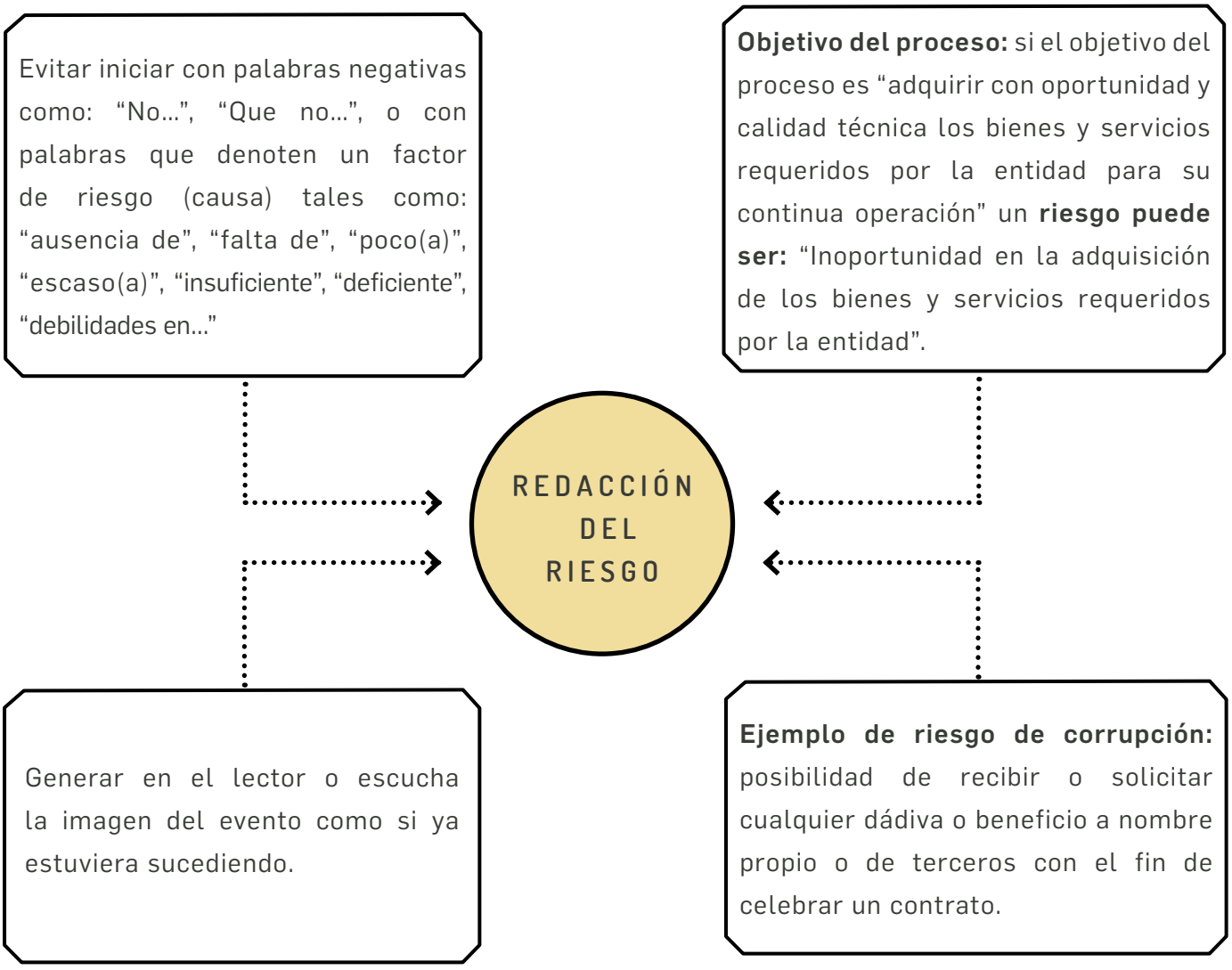
Una resolución no puede calificar la información como clasificada o reservada.

2.2 Identificación de riesgos

EJEMPLO

2.2.1 Técnicas para la redacción de riesgos

Esquema 6. Redacción del riesgo



Fuente: Departamento Administrativo de la Función Pública

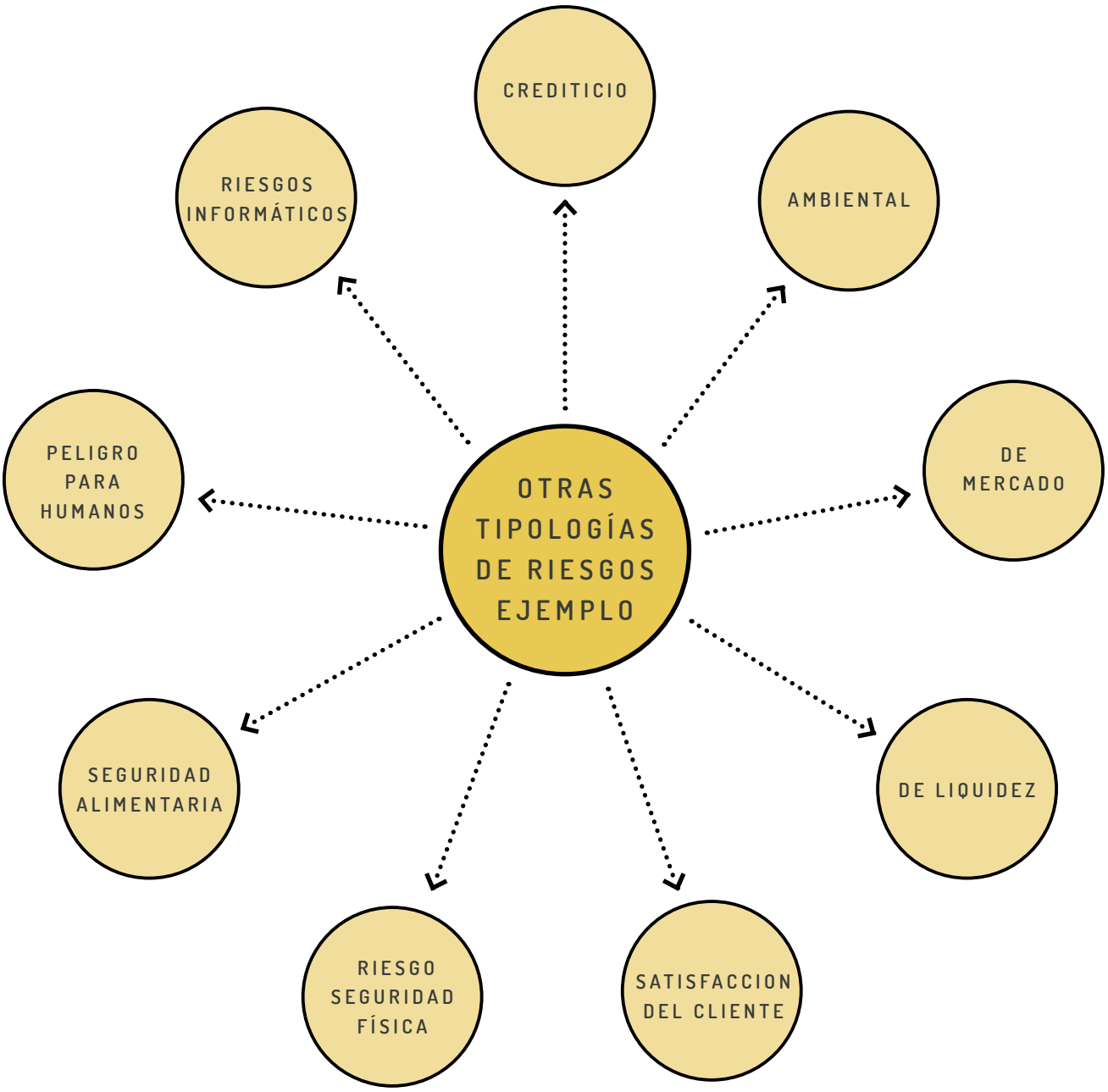
IMPORTANTE

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.

2.2.2 Tipología de riesgos

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 de 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.



Fuente: Departamento Administrativo de la Función Pública.

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.

Ejemplos de 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 y, en consecuencia, afectar 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

Fuente: Departamento Administrativo de la Función Pública.

IMPORTANTE

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

Formato de descripción del riesgo de corrupción

RIESGO	DESCRIPCIÓN	TIPO	CAUSAS	CONSECUENCIAS
Posibilidad de recibir o solicitar cualquier dádiva 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

Procesos, procedimientos o actividades susceptibles de riesgos de corrupción.

A manera de ilustración se señalan algunas actividades susceptibles de riesgos de corrupción. a partir de los cuales la entidad podrá incluir otros que considere pertinentes:

Direccionamiento estratégico (alta dirección).

* Concentración de autoridad o exceso de poder.
* Extralimitación de funciones.
* Ausencia de canales de comunicación.
* Amiguismo y clientelismo.

Financiero (está relacionado con áreas de planeación y presupuesto)

* Inclusión de gastos no autorizados.
* Inversiones de dineros públicos en entidades de dudosa solidez financiera, a cambio de beneficios indebidos para servidores públicos encargados de su administración.
* Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión.
* Inexistencia de archivos contables.
* Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.

De contratación (como proceso o bien los procedimientos ligados a este).

* Estudios previos o de factibilidad deficientes.
* Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular).
* Disposiciones establecidas en los pliegos de condiciones que dirigen los procesos hacia un grupo en particular. (Ej. media geométrica).
* Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación.
* Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados.

* Urgencia manifiesta inexistente.
* Otorgar labores de supervisión a personal sin conocimiento para ello.
* Concentrar las labores de supervisión en poco personal.
* Contratar con compañías de papel que no cuentan con experiencia.

De información y documentación

* Ausencia o debilidad de medidas y/o políticas de conflictos de interés.
* Concentración de información de determinadas actividades o procesos en una persona.
* Ausencia de sistemas de información.
* Ocultar la información considerada pública para los usuarios.
* Ausencia o debilidad de canales de comunicación
* Incumplimiento de la Ley 1712 de 2014.

De investigación y sanción

* Ausencia o debilidad de canales de comunicación.
* Dilatar el proceso para lograr el vencimiento de términos o la prescripción del mismo.
* Desconocimiento de la ley, mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación.
* Exceder las facultades legales en los fallos.

De trámites y/o servicios internos y externos

* Cobros asociados al trámite.
* Influencia de tramitadores
* Tráfico de influencias: (amiguismo, persona influyente).
* Demorar su realización.

De reconocimiento de un derecho (expedición de licencias y/o permisos)

* Falta de procedimientos claros para el trámite.
* Imposibilitar el otorgamiento de una licencia o permiso.
* Ofrecer beneficios económicos para aligerar la expedición o para amañar la misma.
* Tráfico de influencias: (amiguismo, persona influyente).

Formato de descripción del riesgo de seguridad digital

Los riesgos de seguridad digital se basan en la afectación de tres 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

RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/ VULNERA-BILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políti-cas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina.	Modificación no autorizada	Seguridad digital	Falta de políticas de seguridad digital	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.

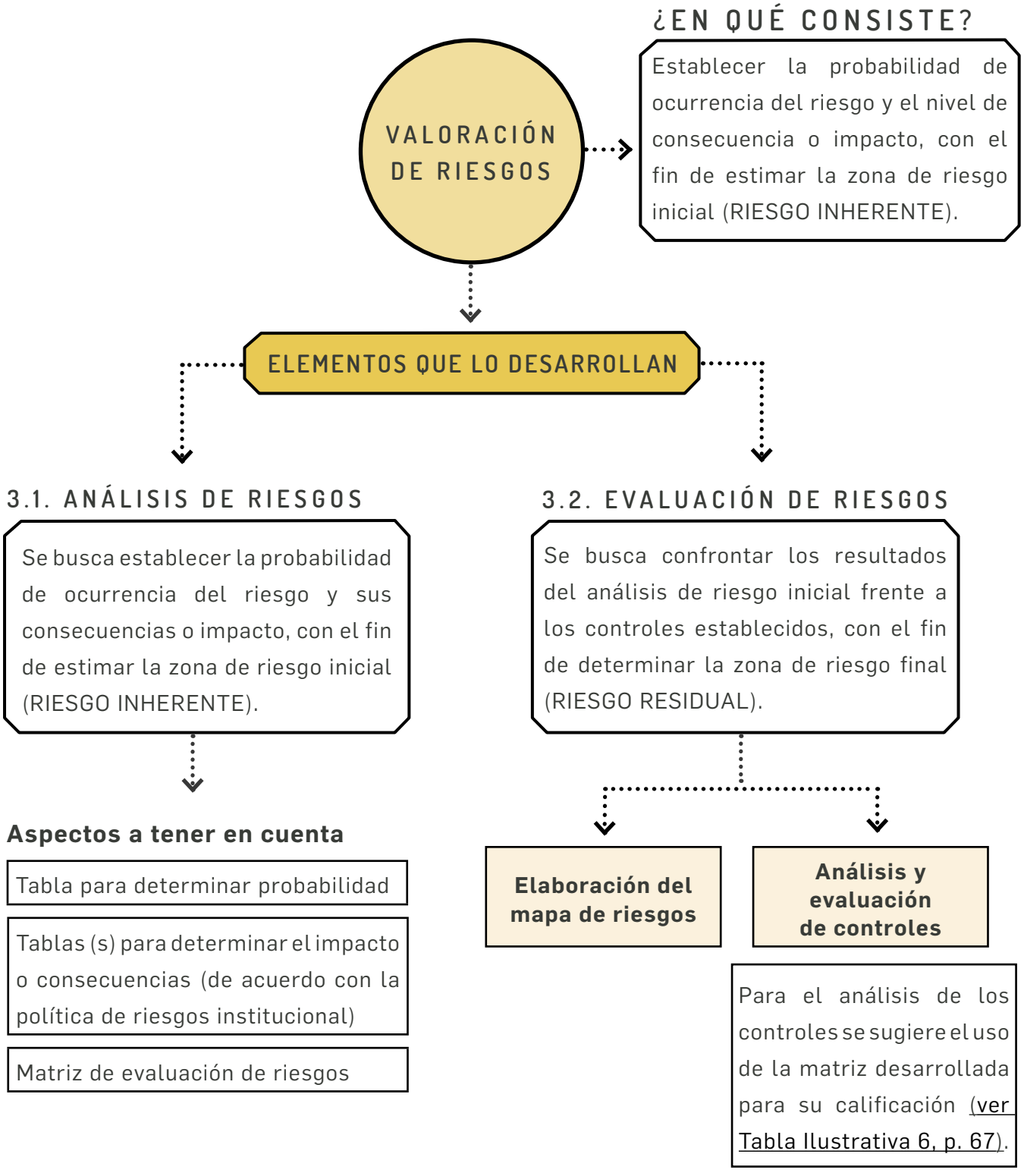
* **NOTA 1:** tener en cuenta que la agrupación de activos debe ser del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.

* **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 los que manejan actualmente.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

Paso 3. valoración de riesgos

Esquema 7. Valoración del riesgo



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).

Esquema 8. Análisis de riesgos

3.1.1. ANÁLISIS DE CAUSAS

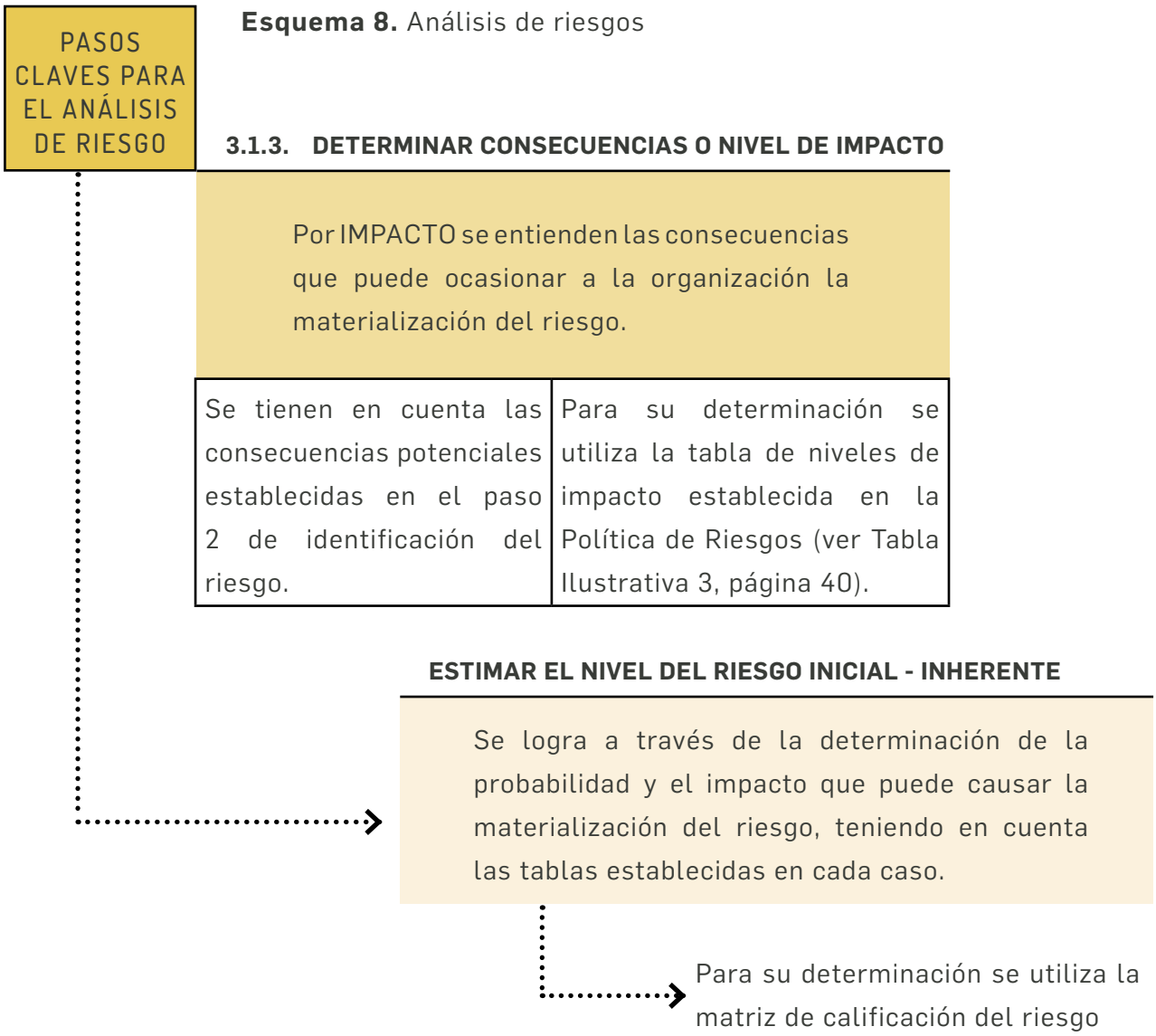
Los objetivos estratégicos y de proceso se desarrollan a través de actividades, pero no todas tienen la misma importancia, por lo tanto se debe establecer cuáles de ellas contribuyen mayormente al logro de los objetivos y estas son las actividades críticas o factores claves de éxito; estos factores se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

PASOS CLAVES PARA EL ANÁLISIS DE RIESGO

3.1.2. DETERMINAR PROBABILIDAD

Por PROBABILIDAD se entiende la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad.

Bajo el criterio de FRECUENCIA se analizan 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.	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 - por Criterios para calificar la probabilidad que se encuentra en la página 39).



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 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 caso de que la entidad no cuente con datos históricos sobre el número de eventos que se hayan materializado en un periodo de tiempo, los integrantes del equipo de trabajo deben calificar en privado el nivel de probabilidad en términos de factibilidad, utilizando la siguiente matriz de priorización de probabilidad.

Matriz de priorización de probabilidad

N.°	RIESGO	P1	P2	P3	P4	P5	P6	TOT	PROM	
1	Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad	Se espera que el evento ocurra en la mayoría de las circunstancias.	**5**	**4**	**3**	**5**	**3**	**4**	**24**	**4** PROBABLE
2	Otros riesgos identificados	Es viable que el evento ocurra en la mayoría de las circunstancias.								
3	Otros riesgos	El evento podrá ocurrir en algún momento.								
Convenciones: **N.°**: 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 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.
MAYOR	- 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.

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
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.
INSIGNIFICANTE	- 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 con su complejidad.

Tabla 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.

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
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 de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. 2017

IMPORTANTE

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

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

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

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

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

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

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

IMPORTANTE

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

3.1.3 Análisis del impacto

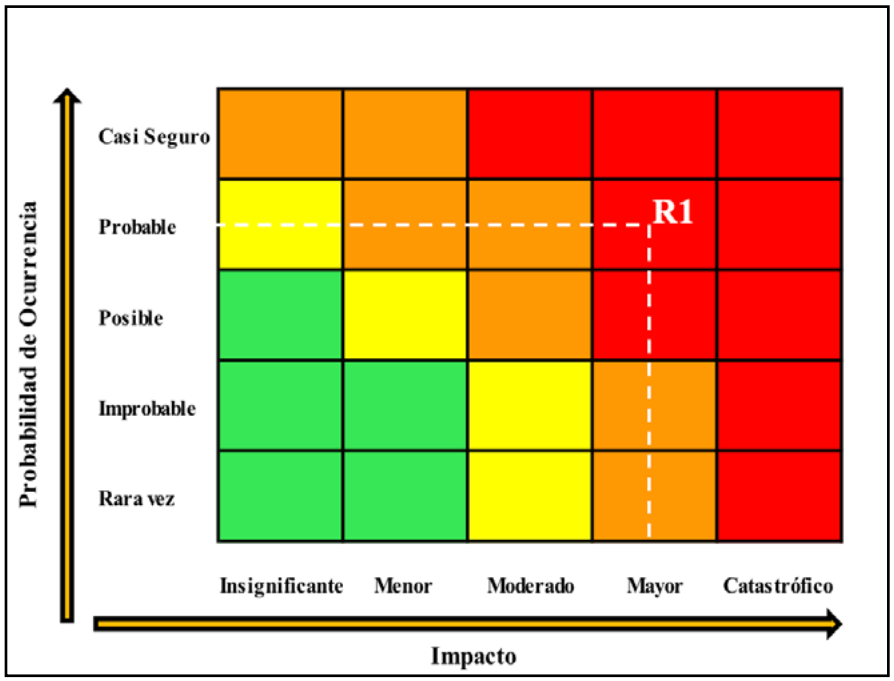
El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo. Para el ejemplo que venimos explicando, el impacto fue identificado como **mayor** por cuanto genera interrupción de las operaciones por más de dos días.

Mapa de calor

Se toma la calificación de probabilidad resultante de la tabla "Matriz de priorización de probabilidad", para este ejemplo se tomará la probalibidad de ocurrencia en **"probable"** y la calificación de

impacto en **“mayor”**, ubique la calificación de probabilidad en la fila y la de impacto en las columnas correspondientes, establezca el punto de intersección de las dos y este punto corresponderá al nivel de riesgo, que para el ejemplo es nivel extremo – color rojo (**R1**), así se podrá determinar el riesgo inherente.

Mapa de calor



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

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.

Tabla 5. Criterios para calificar el impacto - riesgos de corrupción

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

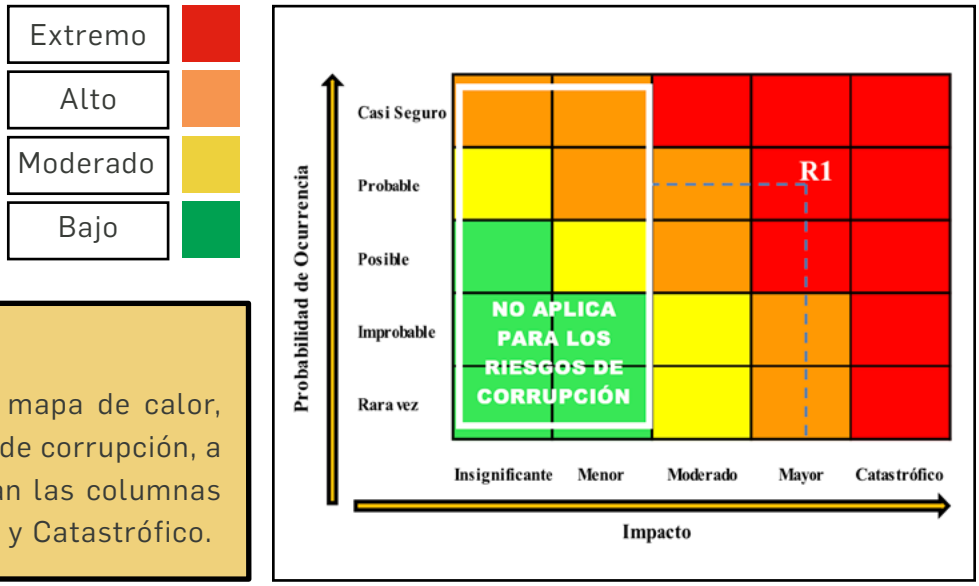
Por cada riesgo de corrupción identificado, se debe diligenciar una tabla de estas.

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 sí aplican para los demás riesgos.

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

Por último ubique en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente, 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 solo les aplican las columnas de impacto Moderado, Mayor y Catastrófico.

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

3.2 Evaluación de riesgos

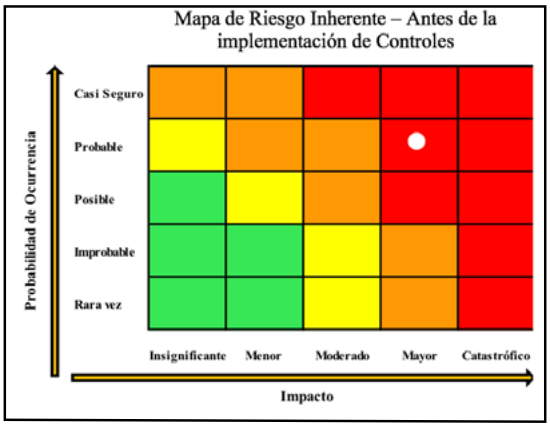
3.2.1. Riesgo antes y después de controles

Esquema 9. Riesgo antes y después de controles

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 efectivamente 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

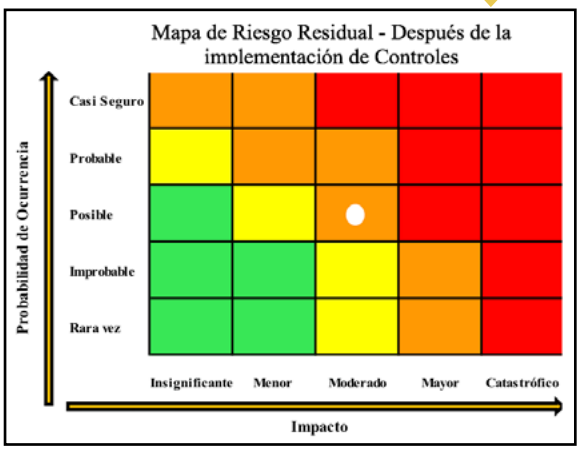
Se identifican las causas o fallas que pueden dar origen a la materialización del riesgo.

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.



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 específica.

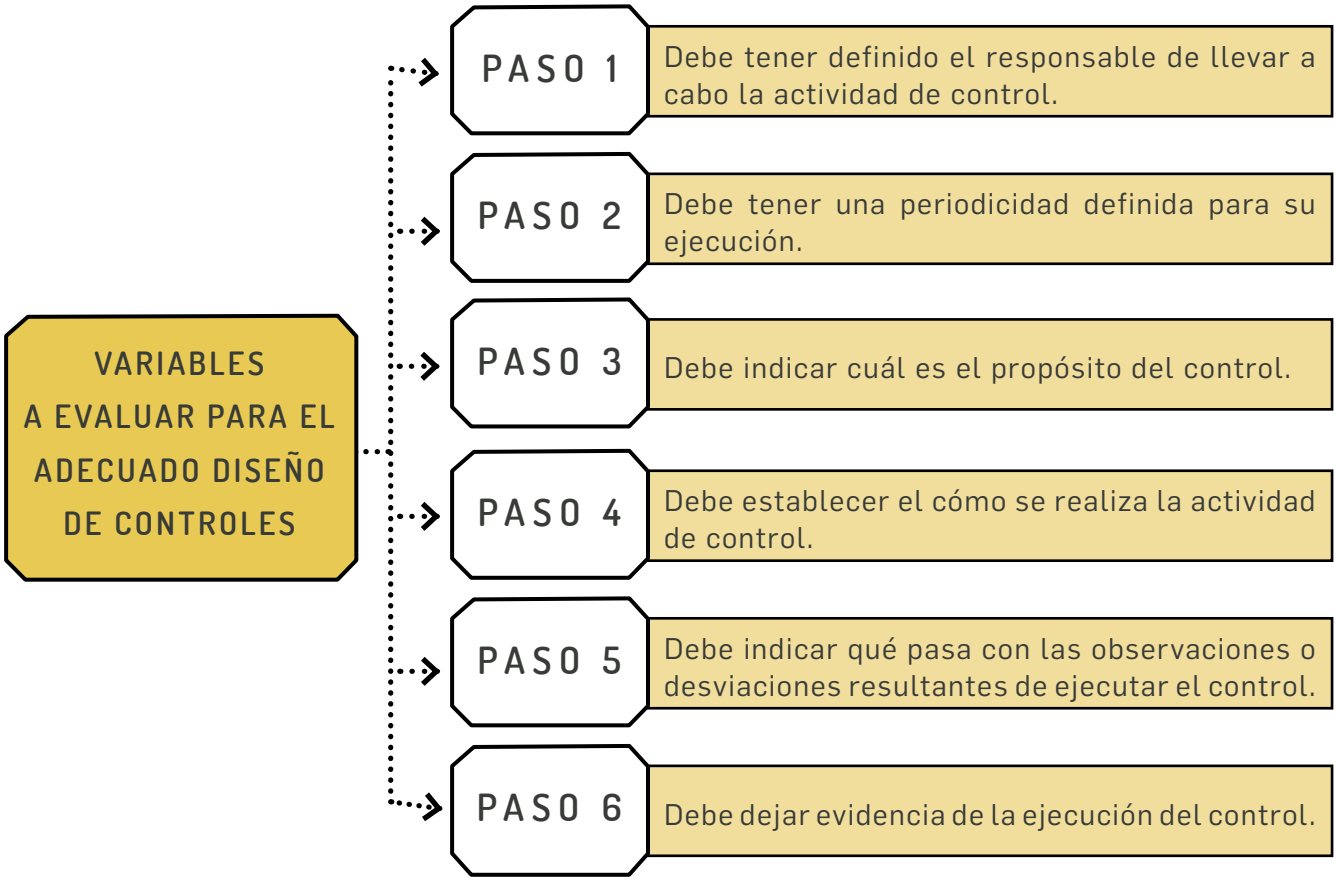
3.2.2 Valoración de los controles – diseño de controles

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 deben considerar, desde la redacción del mismo, las siguientes variables:

Esquema 10. Pasos para diseñar un control



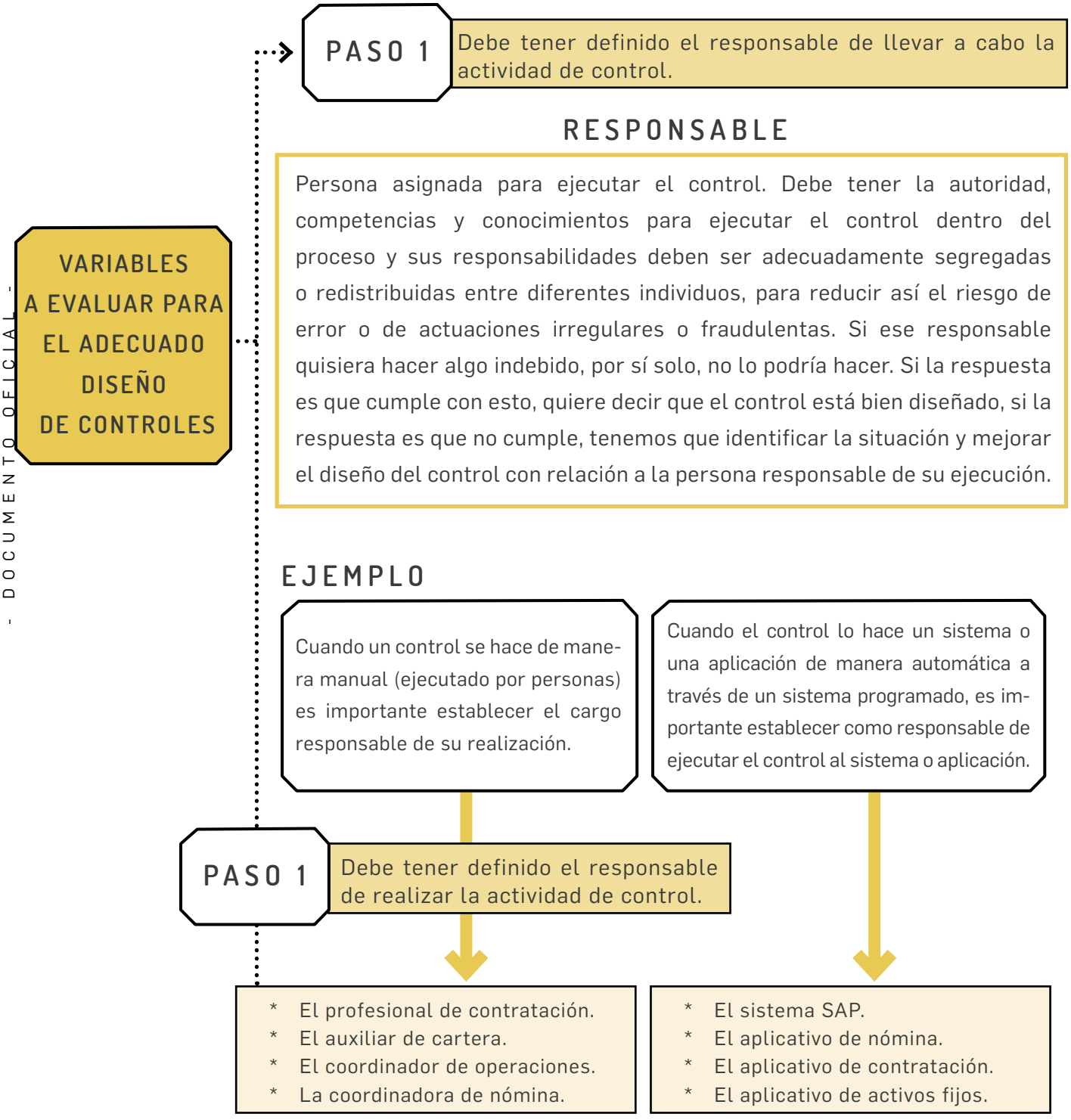
IMPORTANTE

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

¿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 deben considerar, desde la redacción del mismo, las siguientes variables



IMPORTANTE

* El control debe iniciar con un cargo responsable o un sistema o aplicación.
* Evitar asignar 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 deben 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 se 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 este se ejecuta 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 específica 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: **cada vez que se va a realizar** un contrato con un proveedor de servicios.
* El auxiliar de cartera: **mensualmente**.
* El coordinador de operaciones:**diariamente**.
* La coordinadora de nómina: **quincenalmente**.

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

* El sistema SAP cada vez que se va a realizar un pago.

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 deben 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, 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, con el objetivo de llevar acabo 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 del control, es decir, lo que este busca.

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 tener en cuenta 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.

* Cada vez que se va a efectuar un contrato el profesional de contratación **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.

* Cada vez que se va a realizar un pago el sistema SAP **valida que el proveedor al cual se le va a girar el pago no esté 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 deben considerar, desde la redacción del mismo, las siguientes variables:

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

VARIABLES A EVALUAR PARA EL ADECUADO DISEÑO DE CONTROLES

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 confiable.
Ej.: para verificar los requisitos que debe cumplir un proveedor en el momento de ser contratado es mejor utilizar una lista de chequeo que hacerlo de memoria, dado que se nos puede quedar algún requisito por fuera.

EJEMPLO

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

* Cada vez que se va a realizar un contrato el profesional de contratación 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 verifica mensualmente que los valores recaudados en Banco correspondan con los saldos adeudados por los clientes, **este toma dicha información directamente del portal bancario e identifica las cuentas por cobrar, es decir, pendientes de pago y que fueron canceladas según los extractos bancarios revisados.**
* Cada vez que se va a realizar un pago, el sistema SAP 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.**

¿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 deben considerar, desde la redacción del mismo, las siguientes variables:

PASO 5 Debe indicar qué 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 riesgo, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, deberían 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.

VARIABLES A EVALUAR PARA EL ADECUADO DISEÑO DE CONTROLES

EJEMPLO

* Cada vez que se va a realizar un contrato el profesional de contratación, verifica a través de una lista de chequeo que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación. **En caso de encontrar información faltante, requiere al proveedor a través de correo el suministro de la información y poder continuar con el proceso de contratación.**
* El auxiliar de cartera mensualmente verifica que los valores recaudados en 'Banco' correspondan con los saldos adeudados por los clientes, este toma dicha información directamente del portal bancario e identifica las cuentas por cobrar, es decir, pendientes de pago, y que fueron canceladas según los extractos bancarios revisados. **En caso de observar cuentas de cobro que a la fecha no se ha recibido el pago, liste las cuentas pendientes de pago, realice llamadas a los clientes y solicite la fecha para el pago de las mismas.**
* Cada vez que se va a realizar un pago el sistema SAP 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. **En caso de encontrar coincidencias el sistema no permite realizar el pago.**

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.

¿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:

PASO 6 Debe dejar evidencia de la ejecución del control.

VARIABLES A EVALUAR PARA EL ADECUADO DISEÑO DE CONTROLES

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 con los parámetros establecidos y descritos 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

* Cada vez que se va a realizar un contrato, el profesional de contratación verifica a través de una lista de chequeo que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación. En caso de encontrar información faltante, solicita al proveedor por correo la información y poder continuar con el proceso de contratación. **Evidencia: la lista de chequeo diligenciada, la información de la carpeta del cliente y los correos a que hubo lugar en donde solicitó la información faltante (en los casos que aplique).**

EJEMPLO

PASO 6 Debe dejar evidencia de la ejecución del control.

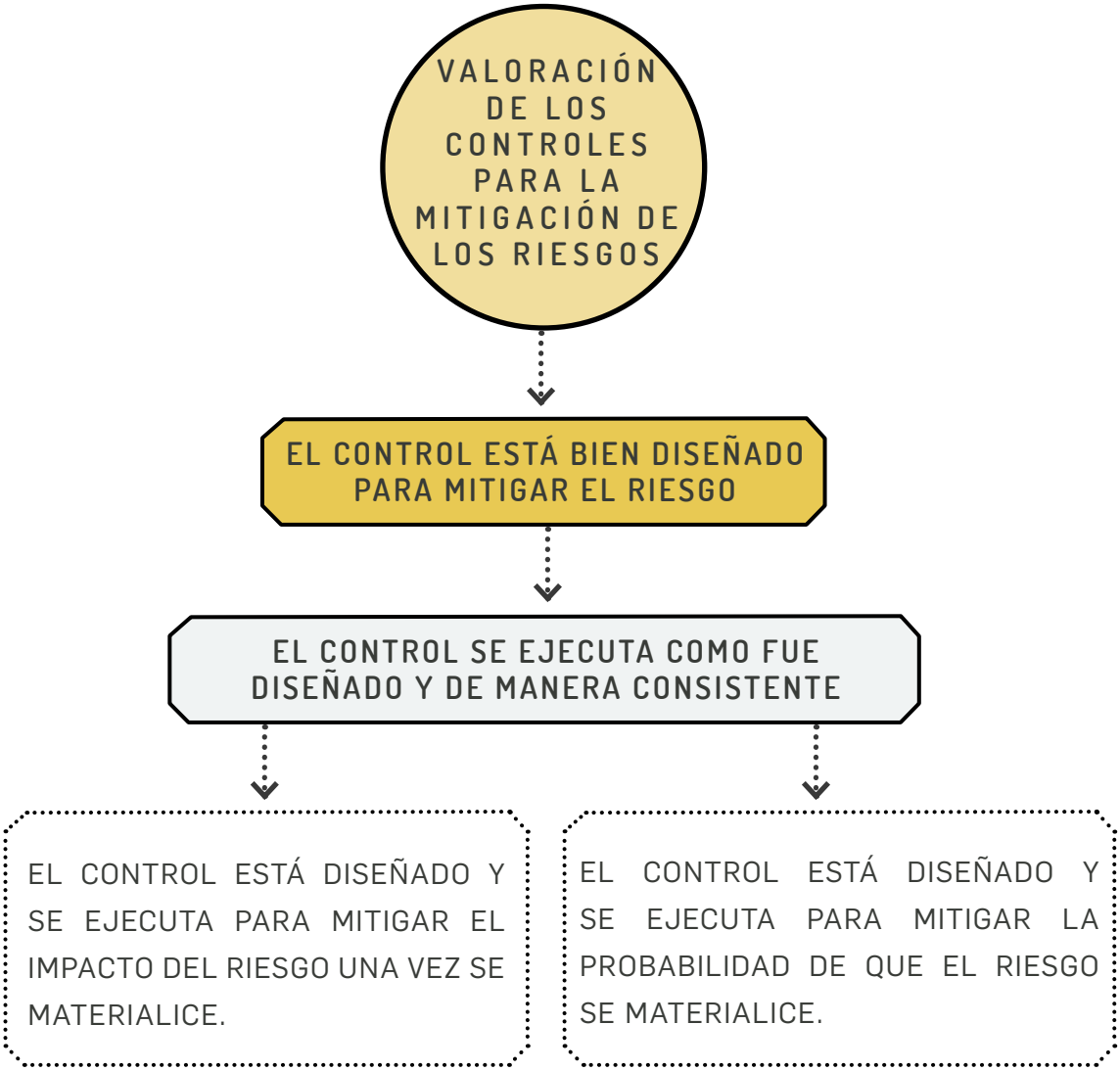
* El auxiliar de cartera verifica mensualmente que los valores recaudados en 'Banco' correspondan con los saldos adeudados por los clientes, este toma dicha información directamente del portal bancario e identifica las cuentas por cobrar, es decir, pendientes de pago y que fueron canceladas según los extractos bancarios revisados. En caso de observar cuentas de cobro que a la fecha no se ha recibido el pago: liste las cuentas pendientes de pago, realice llamadas a los clientes y solicite la fecha para el pago de las mismas. **Evidencia: el listado de cuentas por cobrar pendientes de pago con los compromisos acordados con los clientes y el extracto bancario.**

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

* Cada vez que se va a realizar un pago, el sistema SAP 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. En caso de encontrar coincidencias el sistema no permite realizar el pago. **Como evidencia queda la programación interna del aplicativo y el reporte de coincidencia con listas restrictivas.**

3.2.2 Valoración de los controles

Esquema 11. Valoración de los controles para la mitigación de los riesgos



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.

Tabla 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, Ej.: 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 misma conclusión?	Completa	Incompleta / no existe

Tabla 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 todas las variables para que un control se evalúe 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

Si 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 esté 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 asegurarse por parte de la primera 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 efectúa 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 sí ayudan al tratamiento de los riesgos, considerando tanto el diseño, ejecución individual y promedio de los controles.

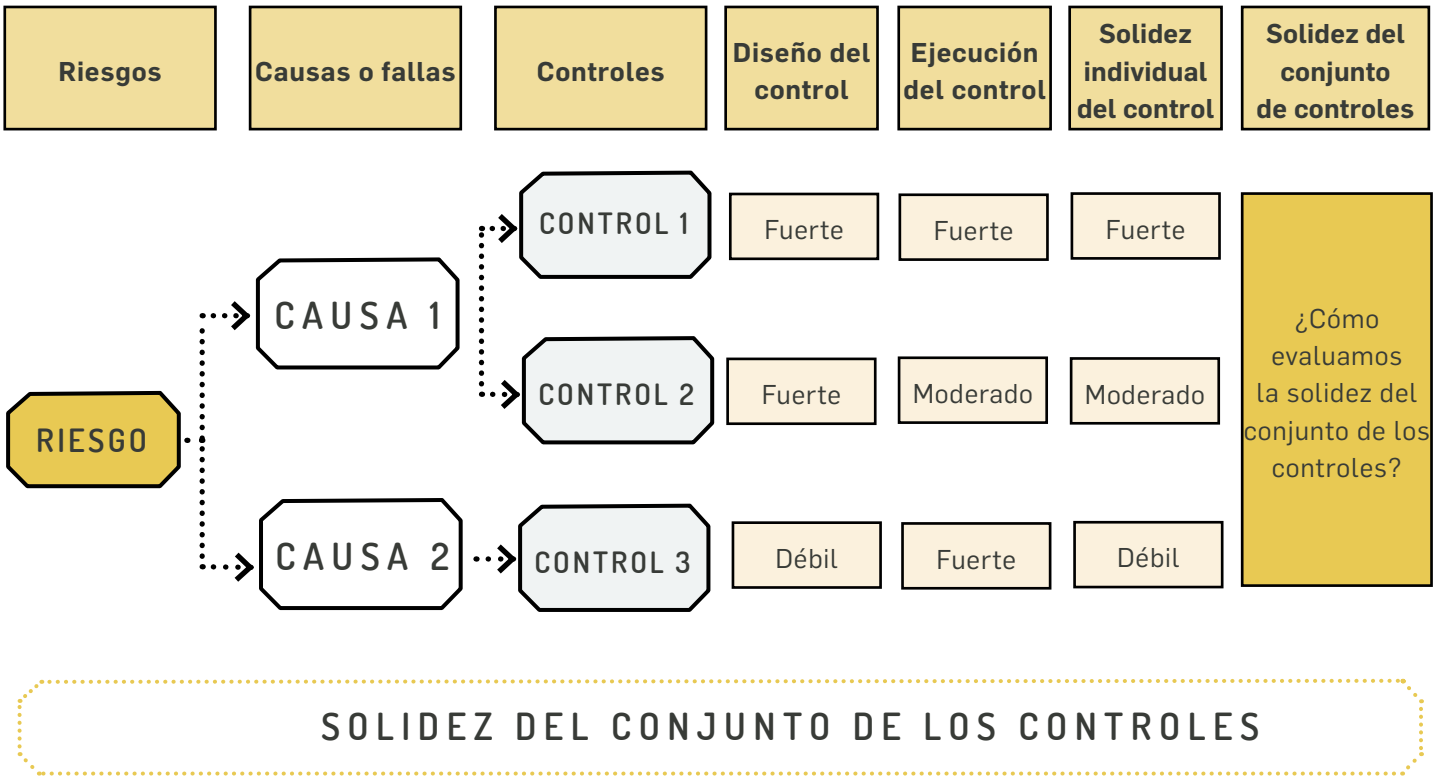
En la evaluación del diseño y ejecución de los controles las dos variables son importantes y significativas en el tratamiento de los riesgos y sus causas, por lo que siempre la calificación de la solidez de cada control asumirá la calificación del diseño o ejecución con menor calificación entre fuerte,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

PESO DEL **DISEÑO** DE CADA CONTROL	PESO DE LA **EJECUCIÓN** DE CADA CONTROL	SOLIDEZ INDIVIDUAL DE CADA CONTROL **FUERTE:100 MODERADO:50 DÉBIL:0**	DEBE ESTABLECER ACCIONES 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: calificación 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	Sí

Solidez del conjunto de controles para la adecuada mitigación del riesgo

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

Esquema 12. Solidez del conjunto de controles



IMPORTANTE

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

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 está entre 50 y 99.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

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 solicitadas 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 sería 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 sería mayor, por tal razón, y para efectos de la elaboración de la matriz 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 con la siguiente tabla:

Tabla 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.

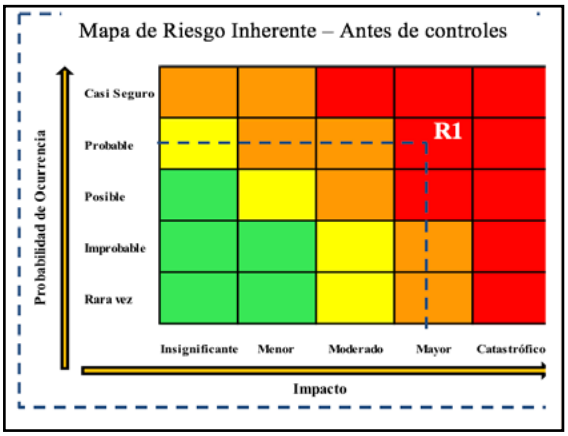
Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, procedemos a la elaboración del mapa de riesgo residual (después de los controles).

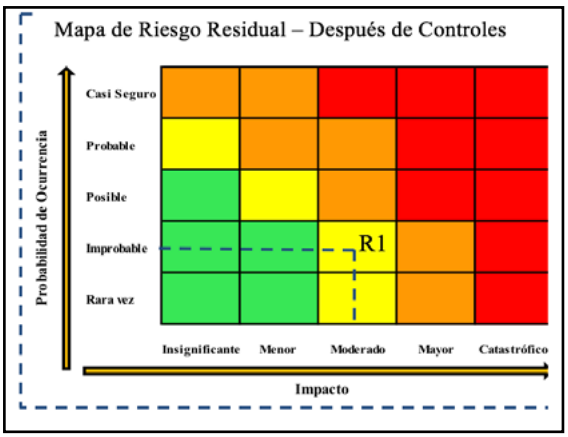
Extremo	
Alto	
Moderado	
Bajo	

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, en caso de materializarse, tiene un impacto mayor para la entidad. Ahora, supongamos que existen controles bien diseñados, 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.

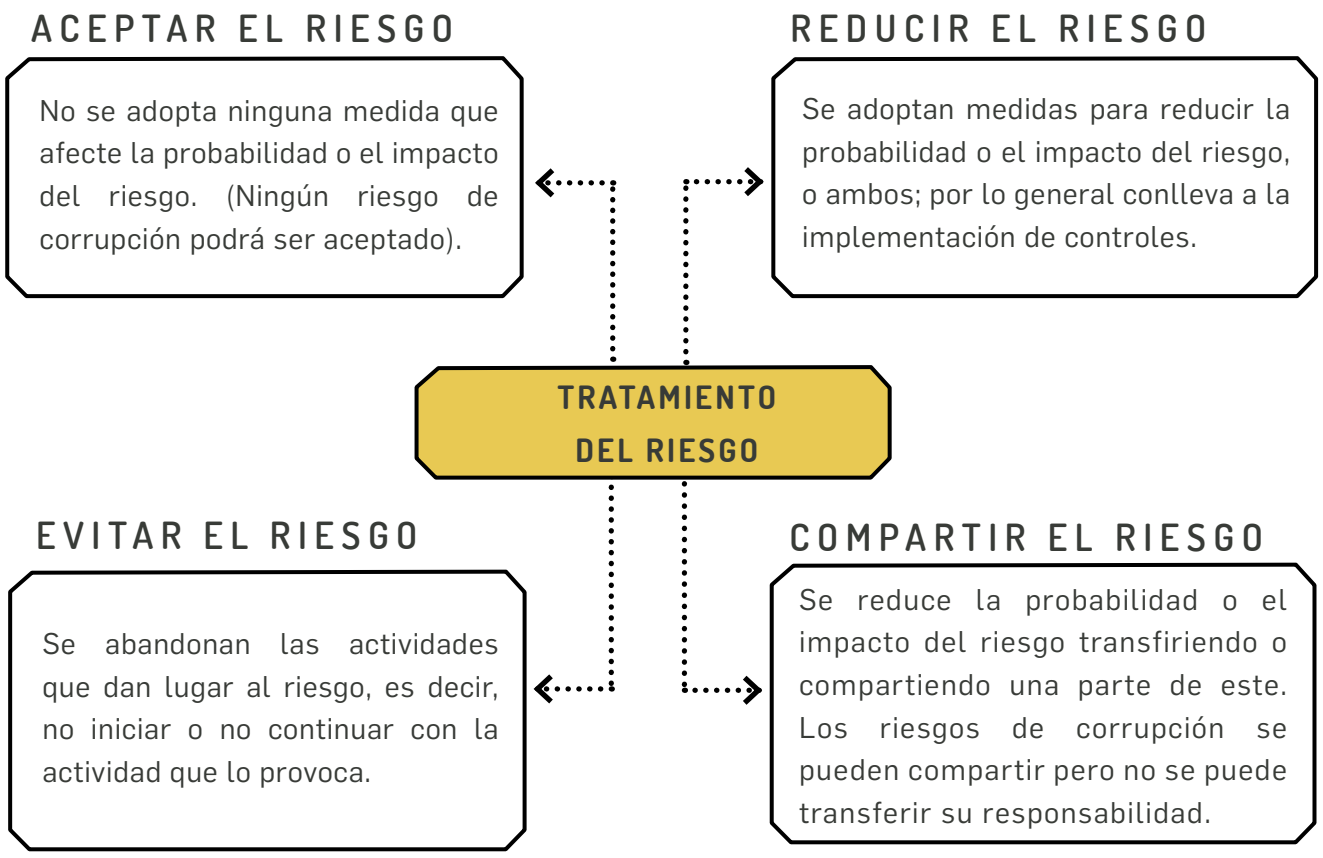




Tratamiento del riesgo

¿Qué es tratamiento del riesgo?

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

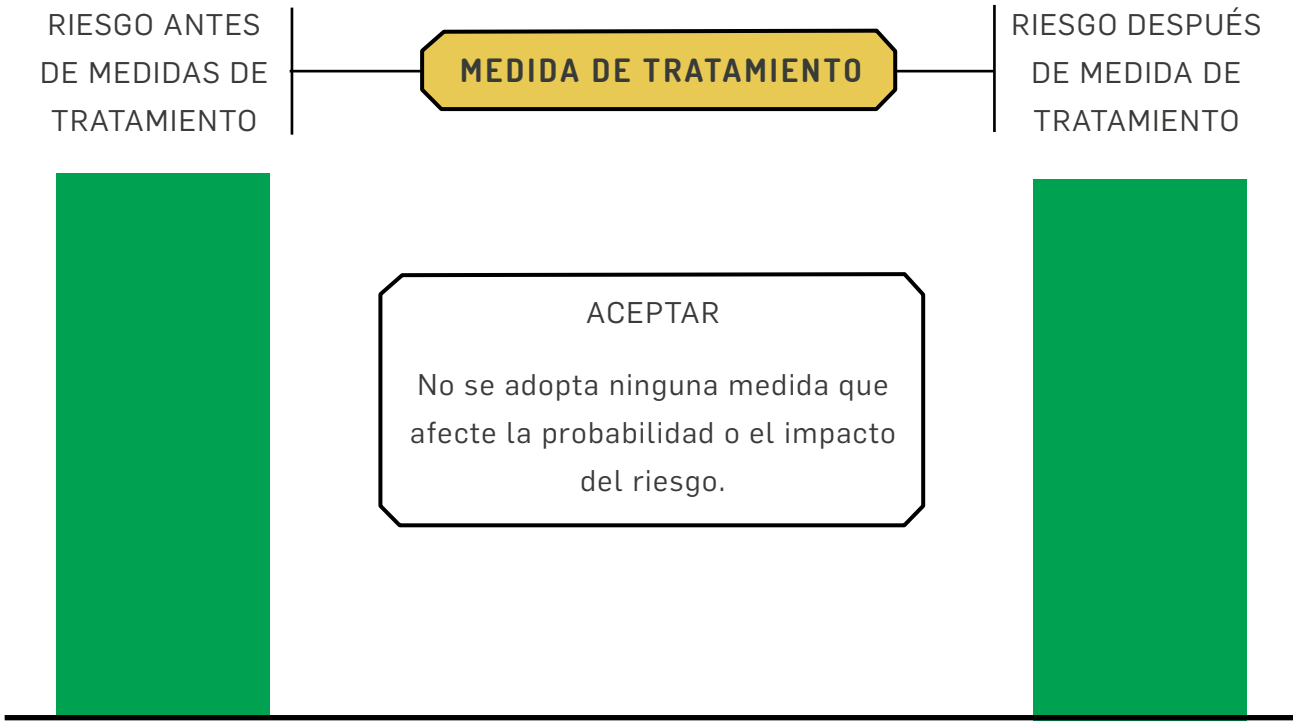


ACEPTAR EL RIESGO

Si el nivel de riesgo cumple con los criterios de aceptación de riesgo no es necesario poner controles y este puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo.

IMPORTANTE

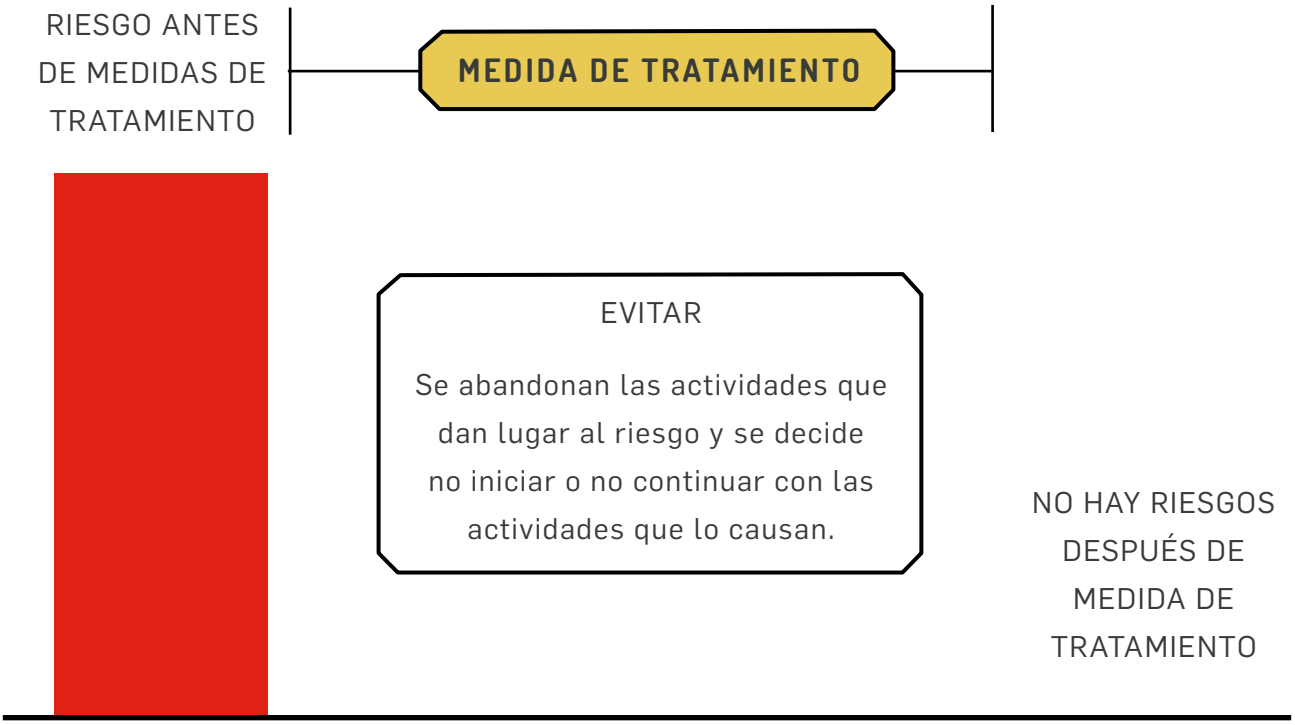
En el caso de riesgos de corrupción, estos no pueden ser aceptados.



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

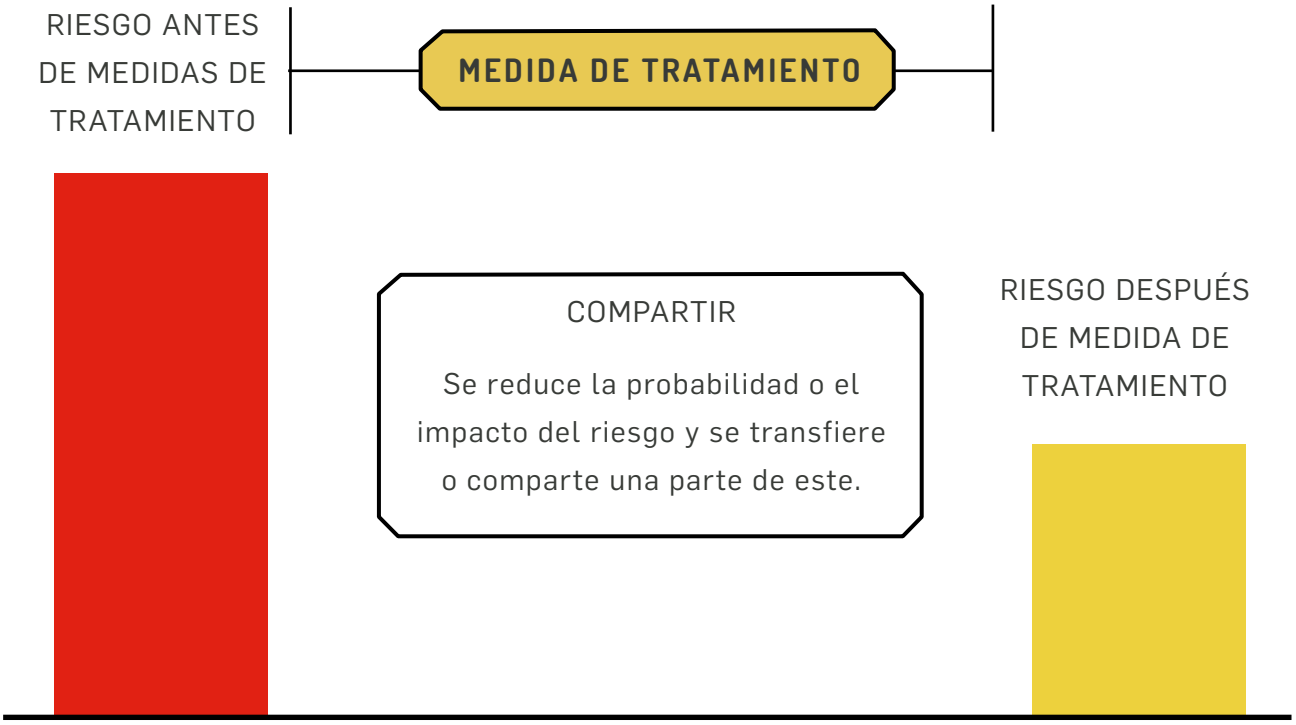
Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades.



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

COMPARTIR EL RIESGO

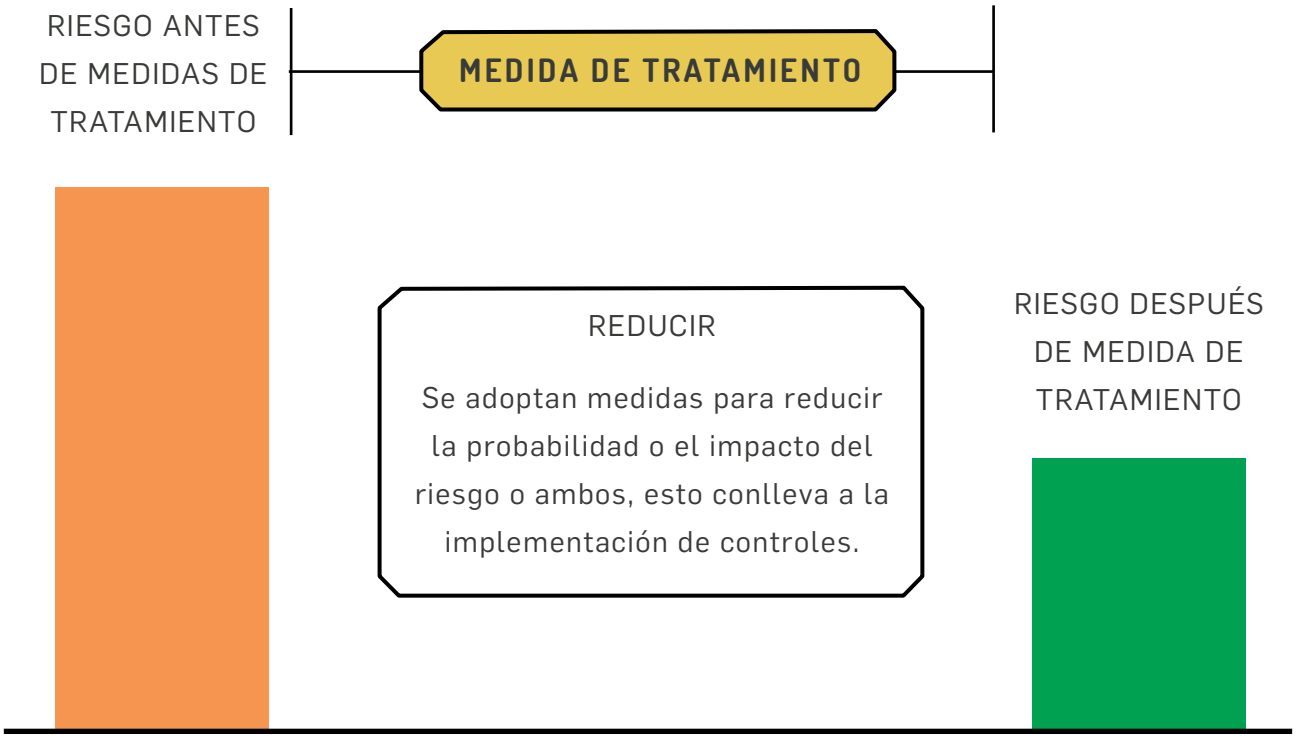
Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del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



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.

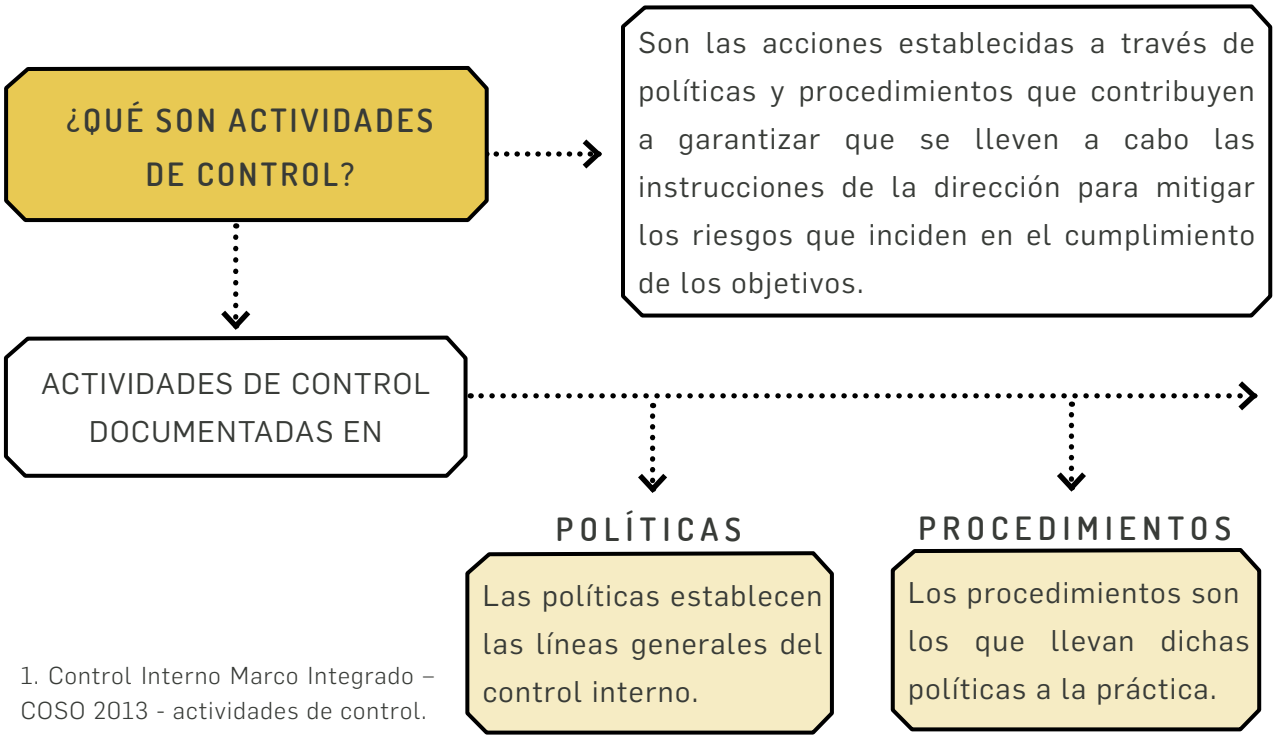


Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

Para mitigar/tratar los riesgos de seguridad digital se deben emplear como mínimo los controles del anexo A de la ISO/IEC 27001:2013, estos también 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.



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

IMPORTANTE

* Una política por sí sola no es un control.
* Los controles se despliegan a través de los procedimientos documentados.
* La actividad de control debe por sí 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, estos también se encuentran en el anexo 3. "Lineamientos para la gestión del riesgo de seguridad digital" de la presente guía.

EJEMPLO

La política establece que para los contratos de bienes y servicios se deben 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, independientemente de la tipología de riesgo a tratar, deben tener una adecuada combinación para prevenir que la situación de riesgo se origine. Ahora, en caso de que la situación de riesgos se presente, esta debe ser 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.

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

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.

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.

3.3. 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, además de 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 institucionales 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 primera línea de defensa en el monitoreo y revisión de los riesgos y actividades de control

2ª. LÍNEA DE DEFENSA	
Soporta 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 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 lleva a cabo 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 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, además de incluir los riesgos de corrupción con relación a lo siguiente: ■ Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo 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 determinar 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 primera 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 primera 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. La tercera línea de defensa 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, además de incluir los riesgos de corrupción con relación a lo siguiente: ■ Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo 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, además de incluir 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 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 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. ■ para mitigar los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.

Monitoreo de riesgos de corrupción

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

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

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

Reporte del Plan de Tratamiento de Riesgos

Consolidar información para la gestión del riesgo

Esquema 13. Consolidación Plan de Tratamiento de Riesgos

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.

continuación esquema 13

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 incluirlas 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 inglés) 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).

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

N.	RIESGO	CLASIFICACIÓN	CAUSAS	PROBABILIDAD	IMPACTO	RIESGO RESIDUA	OPCIÓN MANEJO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	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				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 manera que se comunique toda la información necesaria para su comprensión y tratamiento adecuado.

Formato mapa y plan de tratamiento de riesgos

N.	RIESGO	CLASIFICACIÓN	CAUSAS	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN MANEJO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
2	**Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros para celebrar un contrato**	Corrupción	Debilidades en la etapa de planeación	**Probable**	**Catastrófico**	**Extremo**	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 administrativo conformando comité	Jefe de contratos	Trimestralmente	
			Carencia de 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 Contingencia	Iniciar la investigación disciplinaria, fiscal o remitir a las instancias correspondientes para el proceso penal.	Comunicación iniciando o remitiendo investigación	Jefe control disciplinario interno	1 semana una vez el riesgo de iliquidez se materialice	

Reporte de la gestión del riesgo de seguridad digital

Así mismo, 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

N.	RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
2	**Pérdida de la integridad**	Base de datos de nómina	Seguridad digital	Modificación no autorizada	Ausencia de políticas de control de acceso	**Probable**	**Menor**	**Moderado**	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **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	Tercer trimestre de 2018	
					"Ausencia de bloqueo				Reducir	A.11.2.8 Equipos de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Tercer trimestre de 2018	

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

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 cuanto a 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 que la gestión y seguimiento se conviertan en algo muy 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 en el periodo actual - # de incidentes de confidencialidad en el periodo previo) / Incidentes de confidencialidad en el 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 de riesgos de corrupción

GESTION RIESGOS DE CORRUPCIÓN

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

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

En especial deberá adelantar las siguientes actividades:

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

Acciones a seguir en caso de materialización de riesgos de corrupción

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

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

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

Las acciones adelantadas se refieren a:

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

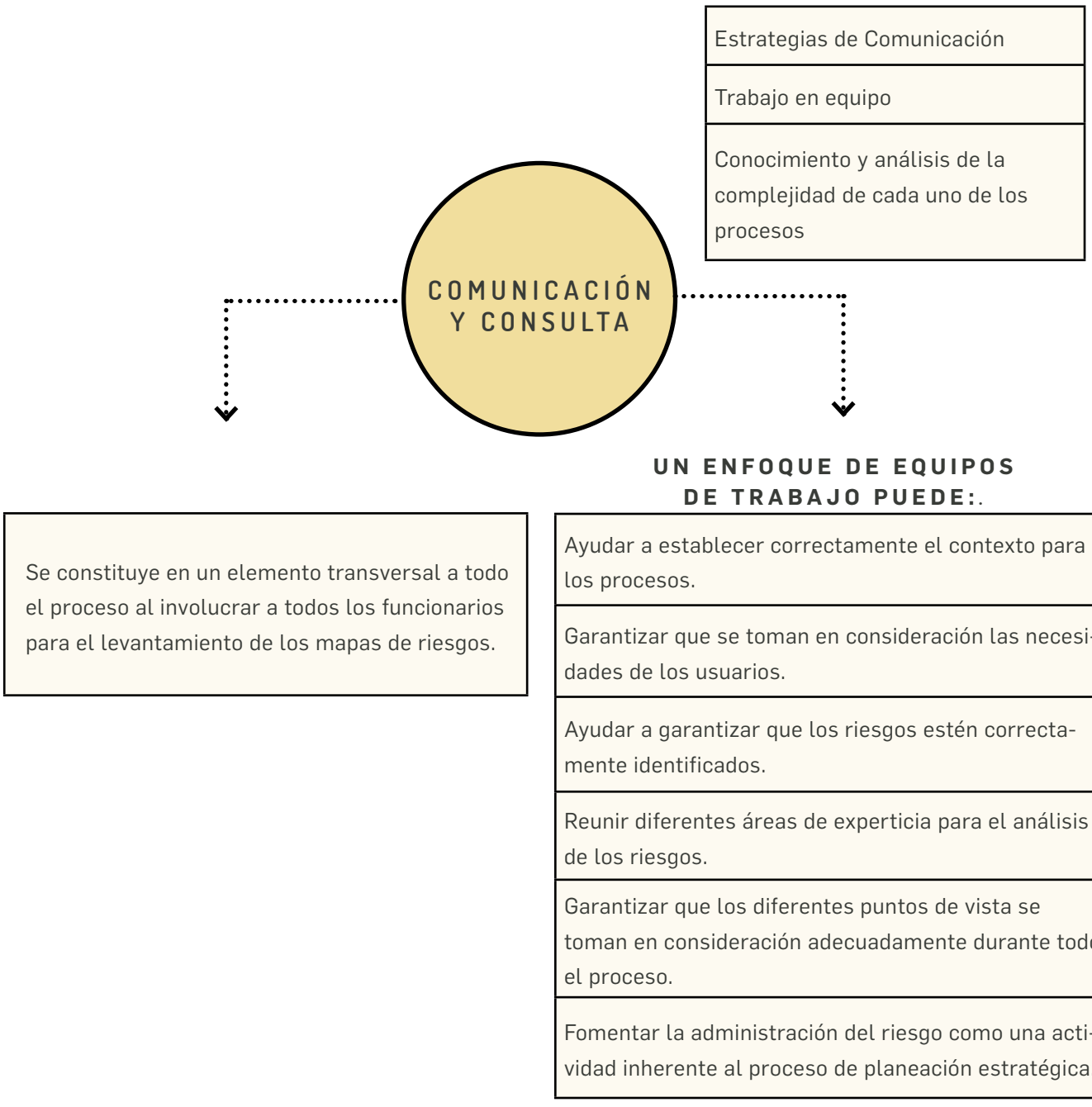
Comunicación y consulta

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].

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

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.

Esquema 14. Comunicación y consulta – Aspecto transversal



Información, comunicación y reporte

Esquema 15. Responsabilidades por línea de defensa para la Información, comunicación y reporte.

LÍNEA ESTRATÉGICA

Corresponde al Comité de Auditoría 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 lo 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.

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

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

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 de seguimiento riesgos de corrupción

FUNCIÓN PÚBLICA

OCTUBRE 2018

Guía para la administración del riesgo y el diseño de controles en entidades públicas

RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL

VERSIÓN 4

DIRECCIÓN DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL

Departamento Administrativo de la Función Pública
Carrera 6 No 12-62, Bogotá, D.C., Colombia
Conmutador: 7395656 Fax: 7395657
Web: www.funcionpublica.gov.co
eva@funcionpublica.gov.co
Línea gratuita de atención al usuario: 018000 917770

Bogotá, D.C., Colombia.

VISÍTANOS O ESCRÍBENOS:

GOBIERNO DE COLOMBIA · VICEPRESIDENCIA · FUNCIÓN PÚBLICA · MINTIC · GOBIERNO DIGITAL